НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”

Катедра “Информационна сигурност”

Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я 2 0 1 1

ПРОБЛЕМИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ XXI ВЕК

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2011

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Проблеми на информационната сигурност през XXI век", проведена във Факултет "Артилерия, ПВО и КИС" към Национален военен университет "Васил Левски" - гр. Шумен, на 16 и 17 юни 2011 г.

Докладите са представени за издаване от авторите без допълнително редактиране от издателите. Отговорността за фактологическите, технически, езикови грешки и произтичащите от това последствия носят изцяло авторите на публикуваните трудове.

От редакционната колегия

©НВУ "В. Левски" – факултет "Артилерия, ПВО и КИС"
Шумен, 2011.
c/o Jusautor, Shumen
ISBN 978-954-9681-49-9

Съдържание

ПРИВЕТСТВИЕ КЪМ УЧАСТНИЦИТЕ В КОНФЕРЕНЦИЯТА

от декана на факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи" – Шумен полковник доцент доктор Нелко Ненов

Уважаеми колеги,
скъпи гости,
госпожи, госпожици и господа,

От името на ръководството и академичната общност на факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Национален военен университет „В. Левски" бих искал да Ви приветствам с добре дошли на научната конференция, провеждаща се тази година под надслов „Проблеми пред информационната сигурност през XXI век".

В продължение на два дни всички Вие ще имате възможност да представите своите постижения, да споделите идеи си, да осъществите важни и полезни контакти, да разширите своя кръгозор.

Целта, която си поставяме, е обмен на знания и опит в областта на информационната сигурност във всичките й аспекти.

Над 50 са участниците в тазгодишната конференция. Те представят повече от 15 учебни, научни, държавни и частни институции.

С гордост ще отбележа участието на директора на Дирекция „Сигурност на информацията" в Министерството на отбраната полк. Иван Иванов, директора на Дирекция „Вътрешна сигурност" в Държавната комисия по сигурността на информацията г-н Димитър Гуцалски, г-жа Камелия Василева - началник на отдел „Техническо осигуряване на АИС и мрежи" в Държавната комисия по сигурността на информацията, директора на Дирекция „Комуникационни и информационни системи" в Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" към Министерството на транспорта, информационните технологии и съобщенията г-н Васил Грънчаров и редица други експерти.

Очакваме много научни доклади, съобщения и презентации, които да обогатят и спомогнат за развитието на теорията и практиката. В една неформална атмосфера на споделяне на опит и създаване на контакти между колеги и съмишленици ще се постараем да Ви подпомогнем във Вашите професионални интереси и търсения.

Като основно учебно и научно звено на Военния университет нашият факултет се стреми да допринесе за развитието на процеса на предлагане на ефективни решения за информационна сигурност в публичния и частния сектор.

За нас е основен приоритет да развиваме едно ефективно обучение и научни изследвания в сектора за сигурност и по-конкретно в направление на информационната сигурност.

Ето защо и тази година подходихме с много отговорност и внимание към подготовката и организацията на конференцията по проблемите на информационната сигурност, която се превръща в традиционна научна изява на факултета.

Постарахме се да създадем нужната организация и към деня на отриването й да съберем, редактираме и отпечатаме сборника с научни трудове на всички участници. Днес имам възможността на всички Вас да поднеса готовия сборник, за да

можете да се запознаете в дълбочина с представените от колегите анализи и изследвания. Надявам се с това да Ви бъдем по-полезни и да Ви дадем възможност да се запознаете подробно с постиженията в тази сфера.

В продължение на шест години работихме в тясно сътрудничество с Държавната комисия за сигурност на информацията и Дирекция „Сигурност на информацията" към Министерството на отбраната, за което изказвам своята искрена благодарност лично на г-жа Цвета Маркова и полк. Иван Иванов и на всички останали колеги.

Днес и утре ще имате възможност да видите и чуете най-новите изследвания, проучвания и постижения в областта на кибертероризма, киберотбраната, сигурността на автоматизираните информационни системи и мрежи, както и изискванията на НАТО и Европейския съюз в тази област.

Не се съмнявам, че дискусиите ще бъдат интересни, оживени не само защото всички гости са високо компетентни професионалисти, но и защото представляват широк спектър от университети, научни организации и институции, които притежават различни функции и имат различни отговорности.

Изключително съм удовлетворен, че в работа на конференцията се включиха много млади хора – курсанти, студенти и докторанти. Силно се надявам, че тази тенденция ще се запази и задълбочи.

Благодаря на организаторите на конференцията – колегите от катедра „Информационна сигурност".

Благодаря на нашите спомоществователи „Сектрон" - ООД и национална агенция за сигурност „Телепол".

Очаквам с нетърпение два интересни дни тук в Шумен.

Желая на всички приятно, спорно и ползотворно пребиваване при нас и успех по време на конференцията.

Откривам Научната конференция и Ви желая на добър час.

ПЛЕНАРНИ ДОКЛАДИ

СЪСТОЯНИЕ НА СТАНДАРТИЗАЦИОННАТА БАЗА ЗА ИЗГРАЖДАНЕ НА СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ И ПРОБЛЕМИ ПРЕД ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ XXI ВЕК

Проф. д.н. Манол П. Млеченков

***ABSTRACT**: In the lecture the author gives a short overview of the International Standards and the problems policy on the information security systems in the beginning of the 21ST century.*

***KEY WORDS:** International Standards, Guidelines for the Accreditation of Bodies Operating Certification of Information Security Management Systems.*

Последните две десетилетия на XX в. и първото десетилетие на XXI в. се характеризират с ускоряване на процеса на глобализация на цивилизования свят. Разширява се периметъра на бизнеса, културния и информационния обмен между фирмите, организациите и отделните лица. Обменът на информация излиза извън пределите на националните граници. Утвърждават се нови модели на общуване, все по-широко приложение намират средствата за масова комуникация.

Глобализацията на света налага нови приоритети и изисква своевременни и адекватни мерки за управление на тези процеси от страна на държавата, местните органи за управление и организациите. Този нов тип отношения, основаващи се на споделянето на информация доведе до въвеждане на понятието – *информационно общество*. Съществен принос за развитието и утвърждаването на този процес имат глобализацията на мобилните комуникационни, усъвършенстването на информационните технологии и възможностите на глобалната мрежа Интернет. Наред с положителните страни на процеса се появиха и много непознати и недостатъчно изследвани до този момент рискове и заплахи, породени от уязвимостите на организациите, които изискват гарантирана защита на техните информационни активи.

Постепенно се повишават изискванията към информационната сигурност като съществено условие за успешното функциониране на държавните и корпоративните структури. Развива се и националното законодателство в направление защита на интересите на личността, организациите и обществото в информационното пространство и защитеността на информационната инфраструктура и активи на индивидуално, групово, държавно и международно ниво. Натрупаният опит показва, че такава сигурност може да се реализира само чрез адекватно разработена и функционираща система за управление на информационната сигурност (СУИС).

Развитието на информационното общество в България, от една страна, и стратегиите за информационни войни и информационни престъпления, от друга, извеждат въпроса за информационната сигурност като един от възловите въпроси за

осигуряване на националния суверенитет на страната през XXI век. Информационната сигурност на комуникационно-информационните системи е и едно от условията за интегрирането на страната в НАТО и евро-атлантическите структури и важно предизвикателство пред ИТ сектора. Тя не бива да се възприема като проблем само на държавните структури от сектора за сигурност, а да се приеме за жизнено необходима и за корпоративната сфера. Сега, в началото на XXI в. предизвикателствата на времето налагат на всяка организация да осигури защитата на своите информационни активи от широкия спектър от възможни заплахи и атаки. Могат да се дефинират десетки проблеми и предизвикателства при изграждането СУИС, но в настоящият доклад се разгледат три основни момента и са изведени няколко проблема, които могат да се определят като основни за настоящия етап.

Първият момент, който ще разгледаме е свързан със състоянието на стандартизационната база към момента и как са се развивали схващанията за изграждането на системите за информационна сигурност.

Вече повече от век Британският институт за стандартизация ***(British Standards Institute – BSI)*** и Международната организация по стандартизация ***(ISO)*** определят критериите за утвърждаване на технологични и производствени стандарти. В началото на 90-те години на миналия век браншовите бизнес организации от банковият сектор и промишлеността в Англия разработват съвкупност от практики и правила за управление на сигурността, които в последствие са одобрени от Британският департамент на търговията и промишлеността (***BDTI***). Първата стъпка е направена през 1995 г., когато BTDI издава официален документ с името „Сборник на добри практики за управление на информационната сигурност" **(*Code of practice for information security management)*** - признат и възприет от BSI като стандарт с номенклатурен номер BS 7799.

Следващата стъпка е продиктувана от необходимостта от регламентиране нормите за сигурност при реализиране на работните процеси в Интернет. Тя се реализира с публикуването на този сборник като стандарт на Британския институт по стандартизация през 1995 г. под номер BS 7799:1995, който първоначално не е задължителен за приложение. Вземайки предвид това, през 1998 г. BSI публикува нов стандарт BS 7799-2, дефиниращ изискванията към системата за управление на сигурността на информацията ***(Information System Management System - ISMSs).*** През април 1999 г. двата стандарта са съгласувани и публикувани отново като BS 7799-1:1999 и BS 7799-2:1999, които са широко разпространени с активното съдействие и спонсорство на правителството.

Със сътрудничеството на редица световно известни компании стандартът е доразвит и през 2000 г. и BS 7799-1 с малки изменения става международен стандарт публикуван като ISO/IEC 17799:2000 - „*Information technology – Code of practice for information security management"* (Информационни технологии - Кодекс за добра практика за управление сигурността на информацията). Този стандарт се утвърждава като начална база за разработване на специфични за конкретните организационни структури ръководства, наредби, практики, процедури и пр. Във връзка с направените забележки по втората част, касаещи процедурите по сертифициране на системите за управление на сигурността, BSI я ревизира и през 2002 г. и публикува като BS 7799-2:2002. В рамките на редовния преглед и ревизия на стандартите Международната организация по стандартизация ***(ISO)*** и Международната електротехническа комисия (***IEC***) приемат следващата версия - ISO/IEC 17799:2005.

която носи наименованието „Системи за управление на информационната сигурност – спецификация и насоки за приложение".

Бързото развитие на информационните технологии в края на XX в. поставят нова задача – разработване на стандартизационна база за защита на информацията при използването на новите информационни технологии. Разработени и публикувани са нови пет стандарта от серията ISO/IEC TR 13335-(1–5):2002 (Информационни технологии. Ръководство за управление сигурността на информационните технологии (ИТ)).

В началото на XXI в. еволюира и схващането за развитието на обществото. Възприема се разбирането, че светът постепенно излиза от ***индустриалния*** си етап на развитие навлиза в ***информационния***. Очертават се контурите и на следващият етап – ***мрежовия***. Информационната сигурност като основен елемент на мрежовата (комуникационната) сигурност, придобива все по-важно значение. Необходимостта от полагане на грижи за сигурността на електронните мрежи и информационни системи става все по-мащабна с тяхната глобализация, бързото нарастване на броя на мрежовите потребители и на ценността на техните транзакции. Днес полагането на грижи за сигурността на електронните мрежи и информационни системи е вече обект на политика не само на корпоративно, но и на държавно и на международно ниво.

Постановъчен документ в това направление се явява „Резолюция на Европейския съвет за общ подход и специфични дейности в областта на мрежовата и информационна сигурност" от 28 януари 2002 г. (***COUNCIL RESOLUTION of 28 January 2002 on a common approach and specific actions in the area of network and information security)***. В него са цитирани действащите към момента на издаването му базови международни стандарти: ISO/IEC 15408-1:1999 „*Information technology – Security techniques – Evaluation for IT security – Part-1: Introduction and general model"* (Информационни технологии – Техники на сигурност – Критерии за оценка на сигурността на ИТ – Част 1: Въведение и общ модел), като базис за дефиниране на изисквания към сигурността на компютърните и мрежови продукти и ISO/IEC 17799:2000 (BS 7799-1) като базис за изграждане на политики за управление на сигурността в частни и обществени организации и на държавно ниво. Особеност на цитираните стандарти е, че взаимно се допълват и прилагането на стандарта ISO/IEC 17799 предполага използване на резултати от прилагането на стандарта ISO/IEC 15408.

През 2005 г. излиза и съгласуваната версия на Сборника от добри практики като ISO 17799:2005, който през 2007 г. е коригиран от Международната организация по стандартизация (ISO 17799:2005 /Cor.1:2007). Особено важно значение има ***Приложение А*** на стандарта – Цели по контрола и механизми на контрол. Формулираните в него цели са определени като задължителни за прилагане от организациите при формирането и управлението на процесите в Системите за управление на информационна сигурност (СУИС).

През 2006 г. българският Институт по стандартизация в изпълнение на своята програма официално приема стандарта с означение БДС ISO/IEC 17799:2006, като национален.

От 2005 г. е поставено началото на издаване на ***нови стандарти от серията 27 К.*** Публикуван е ISO 27001:2005 "*Information technology – Security techniques – Information security management systems – Requirements" (ISMSs),* (Информационни

технологии – Техники за сигурност – Системи за управление на информационната сигурност – Изисквания).

След като през 2007 г. ISO приема коригирана версия на ISO/IEC 17799:2005/Cor.1:2007, променя и номера за позоваване на стандарта от 17799 на 27002, което е първото издание на стандарта ISO/IEC 27002:2005 – „*Information technology - Security techniques - Code of practice for information security management"* (Информационни технологии - Методи за сигурност - Кодекс за добра практика за управление на сигурността на информацията). Стандартът обхваща структурата и съдържанието на ISO/IEC 17799:2005 и коригираната му версия от 2007 г. Година по-късно двата стандарта са приети за национални като БДС ISO/IEC 27002:2006, а Приложение А на ISO/IEC 17799:2005 е включено в стандарта БДС ISO/IEC 27001:2006. По този начин е реализирана приемственост между разработваните до този момент стандарти и е обобщен положителния опит по изграждането и функционирането на системите за управление на информационната сигурност (СУИС).

Основната цел при въвеждане в практиката на стандартите от серията БДС ISO/IEC 27000:2009 е да се представят базови препоръки за управление на сигурността на информацията във всяка организация. Стандартите са замислени и реализирани така, че да дадат основните постановки за разработване на правилата за сигурност в организацията, да осигурят ефективно управление на сигурността на информацията и да предоставят основните насоки за защита и конфиденциалност на информацията при междуорганизационни комуникации, обмен на данни и/или сделки.

Стандартът БДС ISO/IEC 27000:2009 - предоставя общ поглед върху системите за управление на сигурността на информацията и дефинира терминологията, които са основа на цялата фамилия стандарти за СУСИ. В резултат на внедряване на ISO/IEC 27000:2009 се очаква всички типове организации (държавни агенции, търговски дружества, юридически лица и неправителствени организации) да генерират доверие у своите партньори и клиенти, да работят със защитени системи и да сведат до минимум риска, а оттам и разходите за възстановяване на работоспособността на системите и/или интегритета на данните. Целите на стандарта са да предложи на публичния сектор и бизнеса термини и дефиниции и да послужи като въведение в серията стандарти, които:

- дефинират изискванията за СУСИ и онези, които сертифицират тези системи;
- предлагат директна помощ, детайлни указания и интерпретиране на изискванията и цялостния *Plan-Do-Check-Act* (PDCA) процес;
- определят специфични за отделните сектори указания за СУСИ;
- определят изискванията за оценка за съответствие - акредитиране на сертифициращите органи и сертификация на внедрени СУСИ.

Международният стандарт ISO/IEC 27001:2005 е създаден, за да осигури модел за разработване, внедряване, действие, наблюдение, преглед, поддръжка и подобрение на СУИС. Внедряването на СУИС е стратегическо решение на организацията и зависи от нейните бизнес нужди и цели, от изискванията по отношение на сигурността, от включените процеси и от размера и структурата на самата организация. Той дефинира изчерпателно изискванията за ISMSs, които да обхващат всички технически и човешки аспекти на информационната сигурност във всички оперативни процеси на организацията. Той изисква организациите да бъдат одити-

рани от сертифициращи органи и получавайки сертификат да гарантират на своите клиенти, доставчици, партньори и регулаторни органи, че техните процеси осигуряват сигурност по отношение на обработката на информация. Основната цел на ISO 27001 е да осигури обща база за развитие на стандартите за информационна сигурност в организацията и ефективните практики за управление на сигурността, както и да осигури сигурност в междуфирмените операции.

Стандартът трябва да се използва от вътрешни и външни заинтересовани страни с цел да се оцени до колко организацията е в състояние да удовлетвори собствените си изисквания, изискванията на клиентите и на нормативната база. Той насърчава използването на „процесния подход" при изграждането, внедряването, действието, наблюдението, прегледа, поддръжката и подобрението на СУИС на организацията.

„Процесният подход" е определен като прилагане на система от процеси в организацията, заедно с идентифицирането и взаимодействието на тези процеси и тяхното управление. Такъв подход позволява да се разберат изискванията за сигурност на организацията и на необходимостта от създаването на политика и цели за информационна сигурност; внедряването и прилагането на различни начини на контрол в контекста на управлението на общия бизнес риск на организацията; наблюдението и прегледа на действието и ефективността на СУИС и непрекъснато подобрение, основано на обективни измервания.

Стандартът приема модела *„Plan-Do-Check-Act"* (PDCA), който се прилага за всички процеси в рамките на СУИС. Възприемането на този модел отразява също така и принципите, посочени в указанията на Организацията за икономическо сътрудничество и развитие (***OECD:2002***)[1], управляващи сигурността на информационните системи и мрежи. Този международен стандарт осигурява стабилен модел за прилагане принципите на тези указания при оценка на риска, проектиране и прилагане на сигурността, нейното управление и повторна оценка. **ISO 27001:2005** изисква стриктно спазване на съответните законови, подзаконови и договорни задължения по отношение на сигурността на информацията, оптимизирано използване на наличните ресурси, както и периодични вътрешни проверки на системата с цел непрекъснатото и усъвършенстване.

Стандартът БДС ISO/IEC 27002:2008 установява указания и общи принципи за управление на сигурността на информацията в една организация. Стандартът съдържа най-добрите практики за контроли в следните области на СУИС:

- политика за сигурност;
- организиране на сигурността;
- оценка на активите;
- сигурност, свързана с персонала;
- сигурност на физическата и окръжаващата среда;
- управление на комуникациите и експлоатацията;
- контрол на достъпа;
- придобиване на информационни системи, разработка и експлоатация;
- управление на инциденти със сигурността на информацията;
-управление на непрекъснатостта на бизнеса;

[1] Организация за икономическо сътрудничество и развитие. „*Указания за сигурността на информационни системи и мрежи – Към култура на сигурността"*. Париж: OECD, Юли 2002. www.oecd.org

- съответствие с регулаторната рамка.

Стандартът не предоставя дефинитивна или строго специфична информация по всеки въпрос, свързан със сигурността на информацията за разлика от другите технологично ориентирани международни стандарти. Той е замислен като обща база и практическо ръководство за разработване на контроли, процедури и ефикасни практики за управление на сигурността, както и да подпомогне изграждането на доверие в партньорските взаимоотношения с доставчици, контрагенти и клиенти на организацията.

Към момента са публикувани и действат четири стандарта от серията 27 К. Останалите са в процес на разработване и предстои тяхното внедряване. По-подробна информация за отменените и действащите към момента стандарти е представена в приложение 1.

Характерна черта на политиката на ISO е приемствеността между отделните публикации и съвместимостта между стандартите, регламентиращи управлението на системи от различни сфери на бизнеса. В тази връзка ISO 27001:2005 е съобразен с ISO 9001:2008 (Системи за управление на качеството – Изисквания) и ISO 14001:2004 (Системи за управление на околната среда – Изисквания с указания за прилагане), с цел да се поддържа съвместимо и интегрирано внедряване и действие със съответните стандарти за управление. Една подходящо проектирана интегрирана система за управление може да отговори на изискванията на всички тези стандарти. Това осигурява възможност на организациите да синхронизират или интегрират своите СУИС със съответните изисквания към системата за управление.

Унифицират се и термините и определянията от ISO/IEC 27001:2005 с тези от ISO/IEC 17799:2005, ISO/IEC 13335-1:2004 (Информационни технологии – Техники за сигурност – Управление сигурността на информационни и комуникационни технологии – Част 1: Концепции и модели за управление на сигурността на информационните и комуникационните технологии), ISO/IEC TR 18044:2004 (Информационни технологии – Техники за сигурност –Управление на инциденти по сигурността на информацията) и ISO/IEC Guide 73:2002 преиздаден в ISO/IEC Guide 73:2009 (Управление на риска - Речник – Указания за прилагане в стандартите).

След създаването на обединения технически комитет от ISO и IEC (ISO/IEC JTC 1) продължава процесът по разработването на международните стандарти в областта на информационните технологии. Ускореното развитие на информационните технологии и разширяване сферата на предоставяните ИТ услуги наложи по ускорена процедура, паралелно с процеса на одобрение от националните органи на страните членки на ISO и IEC, през 2005 г. да се разработи и публикува стандарта ISO/IEC 20000, който се състои от две части под общото заглавие Информационни технологии – Управление на услуги: **БДС ISO/IEC 20000-1:2005 –** *Спецификация* и БДС ISO/IEC 20000-2:2005 - *Кодекс за добра практика при управление на услуги.* Тъй като двете части на стандарта взаимно се допълват, следва да се разглеждат и прилагат съвместно.

За да реализират своите бизнес нужди потребителите изискват от доставчиците и разработчиците по-съвършени средства и услуги при минимални разходи. Засилва се важността на предоставяните ИТ услуги и значението им за нормалното функциониране на организациите и за генериране на приходи при ниски разходи. Серията стандарти ISO/IEC 20000 позволява на доставчиците на услуги да разберат

как да повишат качеството на услугата, която те предоставят на своите клиенти, както вътрешни, така и външни. За целта те трябва да поддържат високо ниво на качеството на услугите чрез прилагането на достъпни технологии и добри практики, кратки срокове за внедряване чрез оперативно планиране, обучение на персонала, мониторинг и изследване работата с клиентите.

ISO/IEC 20000-2 представя постигнатото от ИТ отрасъла съгласие относно стандартите за качество на процесите за управление на ИТ услугите, които осигуряват възможно най-добрата услуга, която да отговори на бизнес потребностите на клиента в рамките на съгласувани нива на ресурсите, т.е професионална услуга на изгодна цена и ниски нива на рискове, които са установени и управлявани.

Като процесно ориентиран стандарт тези практики за управление не са предназначени за оценяване на качеството на продукта. Независимо от това, организации, чиято дейност е свързана с развитие на инструменти, продукти и системи за управление на услуги, биха могли да използват както спецификацията, така и практиките за управление в помощ при разработване на инструменти, продукти и системи, които поддържат най-добри практики за управление на услуги. ISO/IEC 20000-2 осигурява указания за одиторите и предлага помощ на доставчиците на услуги да планират подобрения в услугата или одитиране за съответствие при прилагане на ISO/IEC 20000-1. При реализирането на системата за управление качеството на ИТ услугите се препоръчва прилагането на препоръките на стандарта ISO/IEC 27001:2005.

През последните 10 години на миналия век и първите години на XXI в. по въпросите за риск-мениджмънта активно работят и националните стандартизационни органи в страните от Азиатско-Тихоокеанския регион - Австралия и Нова Зеландия (AS/NZS 4360, приет през 1995 г., доработен през 1999 г. и 2004 г.)[2], Канада (CAN/CSA-Q850 – 97, приет през 1997 г.); Япония (JIS Q 2001, приет през 2001 г.), Великобритания - в сферата на управление на рисковете при проектиране (BS-6079-3:2000, приет през 2000 г.). Отделни разработки в тази област се извършват и в други страни (например в Норвегия, където действа стандарт Z-013 „Анализ на готовността за риск и възникване на аварийна ситуация", разработен за нефтената и газова промишленост).

Един от най-пълните национални стандарти в областта на управлението на риска експертите признават стандарта по риск-мениджмънт на Австралия и Нова Зеландия. Стандартът AS/NZS 4360 има общ (всеотраслов) характер и неговите основни положения са адаптирани за изграждане на системи за управление на рисковете в редица транснационални компании. От 2004 г. версия на този стандарт е приета от много организации извън Австралия и Нова Зеландия като основа за техните подходи за управление на риска.

Стандартът препоръчва организацията още в началото на разработване на своята стратегия за информационна сигурност и управление на риска да вземе решение по стратегията си за комуникация и консултиране. Това е необходимо за обменяне на информация между нея, като заинтересованата страна и експерти по информационната сигурност, за да се дефинират възгледите и препоръките по отношение на същността, природата, формата, тежестта на последствията и приемливостта на рисковете за организацията. Консултантите ще подпомогнат организацията при

[2] В допълнение към стандарта AS/NZS 4360 е издадено подробно ръководство за неговото използване (Australian Handbook, HB 254-2003).

разработването и реализирането на СУИС като проведат обучение на служителите по реализирането на отделните процедури на системата.

Реализирането на всеки един от етапите на процеса по управление на риска е необходимо да се интегрира с процеса за мониторинг и анализ на риска. По този начин ще се откриват измененията в характеристиките на рисковете под влияние на измененията на средата и потвърждаване адекватността на прилаганите процедури по риск-мениджмънта при изменените условия. През 2005 г. Международната организация по стандартизация пристъпва към създаването на международен стандарт, основан на AS/NZS 4360:2004.

На негова основа е разработен ISO 31000:2009 *„Risk management - Principles and guidelines"* (Управление на риска - принципи и указания) като нов стандарт за управление на риска. Той предоставя обща рамка за определяне на риска, неговият анализ, оценка, лечение и наблюдение. Той е първият от серията стандарти за управление на риска и има връзка с*:* ISO Guide 73:2009, който дефинира общите понятия и въвежда единна терминология, свързани с управлението на риска и има за цел да уеднаквява разбирането и подхода при описанието на дейностите свързани с управлението на риска и със стандарта ISO/IEC 31010 *„Risk management - Risk assessment techniques"* (Управление на риска – техники за оценка), който се явява поддържащ за ISO 31000 и който предлага набор от насоки за избор и прилагане на систематичен метод за оценка на риска.

В същото време, Международната организация ISO чрез публикуването на ISO Guide 73:2009 допълва ISO 31000 посредством събирането на термини и определения, свързани с управлението на риска. В ISO 31000 е въведена нова дефиниция за риск. Докато в ISO/IEC 17799:2005 рискът е дефиниран като – *комбинация от вероятността за настъпване на нежелано събитие и неговите последици (възможни щети или нанесен ущърб, загуби)*, то в ISO 31000:2009 рискът е определен като *„ефект на несигурност относно целите на организацията"*.

За стандарта ISO 31000:2009 Кевин Кон, председател на работната група от ISO, която го разработи дава следното обяснение: „Всички организации, без значение колко големи или малки, са изправени пред вътрешни и външни фактори, които създават несигурност за това дали ще могат да постигнат целите си. Ефектът на тази несигурност е „риск" и е присъщ на всички дейности. Всъщност може да се твърди, че световната финансова криза е резултат от неуспеха на схващането (разбирането), оперативното и ефективно управление на риска. ISO 31000 се очаква да помогне на индустрията и търговията, обществените и частни организации, за уверено излизане от кризата."

ISO 31000:2009 не е непосредствено предназначен за целите на сертифициране, но се предвижда да се използва за хармонизиране на процесите на управление на риска в съществуващите и бъдещите стандарти. Този стандарт осигурява общ подход при прилагането на стандартите за управление на специални рискове и/или сектори, и не замества тези стандарти.

Стандартът препоръчва организациите да развиват, прилагат и непрекъснато подобряват рамката за управление на риска като неразделна част от тяхната система за управление. Тази рамка трябва да интегрира процеса на управление на риска през целия жизнен цикъл на организацията при разработване на стратегията, планирането, управлението, дефинирането и управлението на активите, отчитане на процесите, избора на политики и практики. Този процес може да се прилага както

за цялата организация, така и за отделни нейни елементи или за конкретни проекти или дейности.

Рисковете, които засягат организациите, могат да имат последствия от гледна точка на обществото, околната среда, технологиите, безопасността и сигурността, търговски, финансови и икономически измерения, както и въздействие е върху социалната, културната и политическата репутация. Когато възникнат рискове, организациите винаги трябва да си зададат въпроса: „Дали нивото на риска е допустимо и приемливо, и дали изисква по-нататъшно лечение?" Това прави оценката на риска е неразделна част от управлението на риска, която предоставя структуриран процес на организациите да установят как поставените цели могат да бъдат засегнати. Той се използва за анализ на риска по отношение на последиците и вероятностите, преди организацията да реши да предприеме по-нататъшно лечение, ако е необходимо.

Оценката на риска предоставя на органите и структурите вземащи решения и отговорните страни по-добро разбиране на рисковете, които могат да засегнат достигането на целите, както и на адекватността и ефективността на контрола вече налице. Стандартът представлява основа за избор на най-подходящ подход за лечение на определените рискове. Структурата на процеса е представен на фигура 1.

За ефективното реализиране на процеса за управление на риска е целесъобразно от всички управленски нива да се прилагат следните основни принципи:

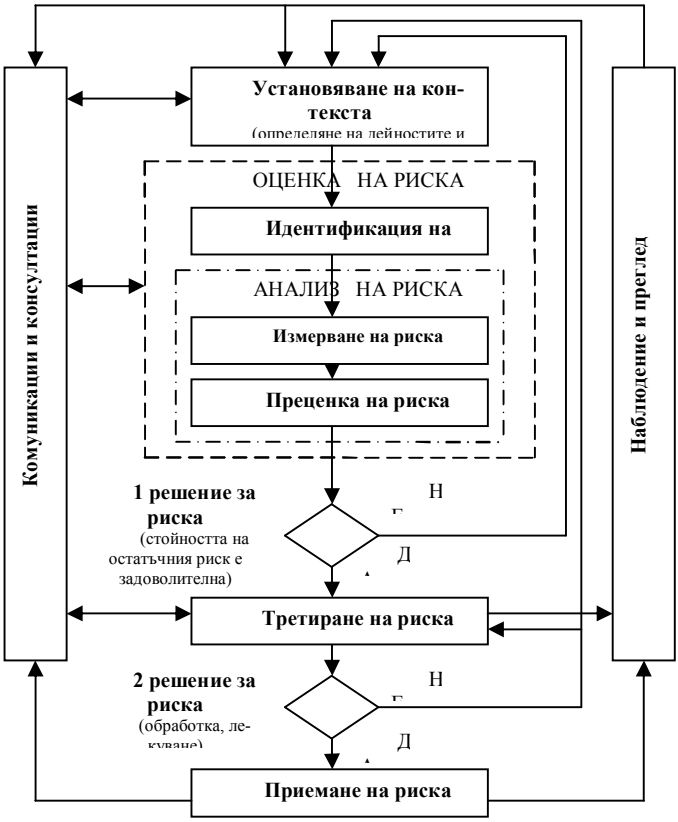
- управлението на риска създава и защитава стойност;
- управлението на риска е неразделна част от всички организационни процеси;
- управлението на риска е част от процеса на вземане на решения;
- управление на риска е насочено срещу несигурността;
- управлението на риска е систематично, структурирано и навременно;
- управлението на риска се основава на най-пълната налична информация;
- управлението на риска е приспособено към организацията;
- управлението на риска отчита човешките и културните фактори;
- управлението на риска е прозрачно и всеобхватно;
- управлението на риска е динамично, повтарящо се и отговарящо на промените;
- управлението на риска улеснява постоянното усъвършенстване – просперитета на организацията.

Процесът на оценяване на рисковете е развит обстойно в стандарт **ISO/IEC 31010:2009 (Управление на риска – техники за оценка на риска).**

Оценяването на риска е неразделна част от управлението на риска и представлява структуриран процес, който позволява на организациите да установят как рисковете могат да повлияят или засегнат целите на организацията. Той се използва за анализ на риска по отношение на вероятностите от възникването му и последиците от него, преди организация да реши как по-нататък ще управлява оценения вече риск и какви възможности за неговото третиране съществуват.

Управлението (третирането) на риска включва избирането на една или повече възможности за неговата промяна. Прилагането на широкия спектър от техники се въвежда със специфични препратки към други международни стандарти, когато концепцията и прилагането на методи са описани по-подробно.

Оценката на риска не е самостоятелна дейност и трябва да бъде изцяло интегрирана с другите компоненти по управление на риска.



Край на първата итерация и преминаване към след-

Фиг. 1. Структура на процеса за управление на риска

Цялостна програма за управление на риска може да осигури ефективен начин за установяване, анализиране и намаляване на риска, осигуряване на непрекъсваемост на работата, спестяване на пари и репутацията на компанията и осигуряването на безопасността на продуктите и производствените процеси. ISO 31000 гарантира, че е налице:

- обща видимост на риска и възможност да бъде отчетен;
- хармонизиране на всички рискове и възможност те да бъдат достъпни помежду си;
- определяне на приоритети на риска, така че най-важните рискове, да се намаляват на първо място;
- план за действие, разработен за намаляване и наблюдение на рисковете в организацията.

ISO/IEC 31010 предвижда конкретни насоки за избора на правилните техники

за оценка на риска в зависимост от нуждите на бизнеса, в това число със съответните приоритети, избор на методика, правилното идентифициране на рисковете и как да отговарят на определените нормативни изисквания.

Ако направим преглед на събитията в световен план, довели до огромни финансови загуби, много човешки жертви, разрушения и екологични катастрофи през последните 3 години можем да видим до какво води подценяването на процеса на анализа на риска. На първо място следва да поставим световната финансова криза, довела до значителни финансови загуби, спад в икономиката, свиване на потреблението и значително забавяне темповете за развитие на почти всички страни в света. През това време сме свидетели на осъществени заплахи от естествен произход довели до значителни последици: земетресения в Китай - през май 2008 г., с над 8600 души жертви, през април 2010 г. с над 400 души жертви, много ранени и разрушения; земетресения в Чили – през февруари и май 2010 г.; земетресение в Хаити – януари 2010 г. – с 230 000 жертви, много ранени и разрушения; земетресение в Нова Зеландия – февруари 2011 г. с няколко стотин жертви; изригване на вулкана в Исландия (който 190 г. не е проявявал признаци на активност) – март 2010 г. – евакуирани над 700 души, прекъсване на въздушния транспорт в Европа и основните световни дестинации, довело до значителни финансови загуби; опустошително земетресение в Япония на 11 март 2011 г. довело до силно цунами и ядрената катастрофа в ядрените реактори на АЕЦ Фукушима 1 – до сега 13 000 жертви и 11 000 безследно изчезнали.

Ако се прибавят и терористичните актове в Лондон, метрото в Москва и Минск, картината става още по-мрачна.

Всички тези финансови загуби, екологични катастрофи и терористични актове са красноречиво доказателство за това до какво може да доведе подценяването или недооценката на рисковите фактори, укриването на данни за реалното положение и подценяване подготовката на обслужващия персонал на организациите. Тяхното предотвратяване или свеждането до минимум на последствията изискват зрялост при управлението на риска чрез изграждане на култура на управление на всички йерархични нива на организацията.

От изложеното до тук може да се направи извода, че наличната и разработваната международна стандардатизационна база е актуална и способства за разработването и функционирането на ефективни СУИС.

Вторият момент, който ще разгледаме е свързан с въпроса как се прилага стандартизационна и нормативната база при изграждането на СУИС от организациите.

На първо място следва да се изясни въпроса за съответствие на националното законодателство на европейското и каква е връзката му с действащите международни стандарти.

Аналитичният преглед на националното законодателството за съответствие на европейското започва от април 1998 г., а от март 2000 г. започват преговори по глави за присъединяване на страната към Европейския съюз (ЕС), който завършва с подписването на Договора за присъединяване от 1 януари 2007 г. През периода на преговорите протича и процес на хармонизация на националното законодателство с това на съюза.

Съгласно правовите норми в Европейската общност, Европейския съвет и Съда на Европейската общност, съществува първично и вторично право.

Първичното право обхваща Учредителните договори на трите общности, както и договорите и актовете за тяхното изменение и допълнение (в това число и договорите за присъединяване на нови държави-членки). Те съставят „конституционна харта" на Общностите.

Вторичното право обхваща приетите: *регламенти* (прилагат се пряко и не е необходимо да се транспонират в националното законодателство); *директиви* (не са актове с пряко приложение и трябва да се транспонира в националното законодателство); *решения* (задължителни и имат директен и непосредствен ефект); *препоръки* и *становища* (формално са без правна сила и нямат обвързващ адресатите си ефект).

Националното законодателство (закони, правилници, наредби, постановления) се развива и хармонизира в съответствие с него.

Стандартите са документи, обединяващи резултатите от науката, технологиите и производствения опит, и предоставят на бизнеса и обществото модел и правила за поведение. Те съдържат общопризнати правила и норми и в редица случаи определят характеристики и изисквания към продуктите, процедури за производство, методи за изпитване и оценяване на съответствието. Те отразяват световен опит, добрите практики и съдържат общите изисквания да се прилагат от националното законодателство, като основа (минимум от изисквания), за да се стигне до сертификация на организацията. Стандартите съдържат изисквания и/или препоръки за правилна и ефективна работа. Тези изисквания или препоръки са съставени на база изследване на *"know-how"* на най-успешните световни компании. Това не ги прави обаче задължителни, а доброволни и препоръчителни.

Приетите за национални стандарти от Националния институт по стандартизация съдържат препратки към законодателството на страната и изискват сертификат за съответствие на качество, сигурност на информацията и др. При прилагането на стандартите се постига по-добра ефективност при производството на продукти или предоставянето на услуги. Част от стандартите са насочени към удовлетворяване в по-голяма степен на очакванията на потребителите и клиентите. Стандартите се развиват постоянно в зависимост от новостите в развитието на науката и технологиите. Те са свързани пряко както с начина ни на живот, така и с условията на работа и правят живота на хората по-безопасен, по-здравословен и по-лесен. Те предлагат модели на поведение на предприятията и организациите и реалното и правилно прилагане на такива международни стандарти води до висока степен на удовлетвореност на заинтересованите страни – организациите и потребителите.

Законодателната и стандартизационната база определят основните законови рамки за разработване и оценяване на съответствието на Системи за управление на качеството и на СУИС на организациите. Разработването на системите, които са декларация за съответствие на предлаганите продукти и услуги, следва да се извърши от организацията, а оценката и доказването на съответствието се извършва от трета независима страна – орган за сертификация.

Европейският орган оторизиран да извършва *акредитация* на органите в областта на информационните и комуникационните технологии на национално ниво е Европейската организация за акредитация – *European co-operation for Accreditation (EA).*[3] Основният и документ е Публикация EA-7/03 от февруари 2000

[3] http://www.europesn-accreditation.org

г. – *EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems* – Насоки за акредитация на органите които извършват сертификация/Регистрация на СУИС. Списъкът на всички публикации на секретариата на ЕА – *List of EA Publications* е издаден на 28 февруари 2011 г.

На национално ниво акредитационния орган е Изпълнителна агенция *„Българска служба за акредитация"* към Министерството на икономиката, енергетиката и туризма. Неговата дейност е регламентирана със Закон за националната акредитация на органи за оценяване на съответствието, в сила от 1 юни 2010 г. и при спазване на положенията на Регламент (ЕО) 765/2008 на ЕА.

Сертификацията е процедура, чрез която трета страна (орган по сертификация) дава писмена гаранция, че даден продукт, процес или услуга отговаря на съществените изисквания.

Сертификацията (за съответствие) има за цел да докаже чрез сертификат, знак или етикет придържането (към съответствието) на дадена референтна система. Прилага се към продукти, услуги, организации и хора. Съответствието се оценява спрямо различни типове референтни системи: стандарти, спецификации или технически правила, таблица на условията норми, степен на компетентност. Използват се различни техники според референтните системи: тестове, одити, инспекции, изпити).

Сертификацията може да бъде законово наложена (регулаторна сертификация), или може да бъде избор на самите производители, главно по търговски причини (доброволна сертификация). За България е възприет принципа на доброволна сертификация.

Продуктите с маркировка CE (CO) се придружават от *Декларация за съответствие*. В тази декларация производителят удостоверява, че те съответстват на хармонизираните стандарти и удовлетворяват съществените изисквания за безопасност на директивите. С тази декларация производителят поема отговорността, че продуктите са безопасни. С цел да се постигне свободно движение на стоките в Европейския Съюз е въведено взаимно признаване на изпитванията и сертификатите. Така се стига до концепцията за „Нов подход" за техническо регламентиране и стандартизация (чрез директиви) и „Глобален подход" за оценяване на съответствието, предпоставка за безпрепятствен стокообмен на Единния пазар.

Всяка организация следва да подходи конкретно при определяне на показателите за избор на сертифициращ орган (авторитет, цени, начин на плащане, удобство и срокове на процедурите и др.). Препоръчително е да надделеят маркетинговите и търговски съображения за доверието на ключовите клиенти на фирмата в компетентността на сертифициращия орган. Точно ключовите клиенти ще подскажат на кого биха се доверили.

Сертифицирането не бива да се извърши само за да се сдобие фирмата с документа „сертификат". Той трябва да донесе и търговски дивиденти, за това е отговорна маркетингова задача свързана с целеви пазари, дългосрочна търговска политика, отчитаща зависимостта от определени партньори.

Националното законодателство, което урежда положенията по защитата на информацията и регламентира въвеждането на Системи за управление на сигурността към момента е следното:

- Закон за защита на класифицираната информация (в сила от 30.04.2002 г.) и

Правилника за неговото прилагане (в сила от 10.12.2002 г.);

- Закон за защита на личните данни (в сила от 01.01.2002 г.);
- Закон за електронния документ и електронния подпис (в сила от06.10.2001 г.);
- Закон за електронните съобщения (в сила от 10.05.2007 г.);
- Закон за електронното управление (в сила от 13.06.2008 г.);
- Закон за МВР и Правилник за неговото прилагане (в сила от 05.07.1999 г.);
- Закон за частната охранителна дейност (в сила от 24.02.2004 г.);
- Наредба за задължителните общи условия за сигурност на АИС и мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация (в сила от 10.05.2003 г.);
- Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (в сила от 25.11.2008 г.).

Сертификацията на СУИС се извършва в съответствие със стандарта БДС ISO/IEC 27006:2009, а на системите по качеството по стандарт БДС EN ISO 19011:2004. Особено внимание е отделено на механизмите и лицата, които ще сертифицират системите за управление на сигурността.

На второ място следва да се даде отговор на няколко основни въпроса, имащи отношение към въвеждането и сертификацията на СУИС.

Първият въпрос е: Какво представлява системата за управление?

Системата за сигурност е набор от писани задължителни правила за изпълнение и управление на дейностите във фирмата (организацията). В повечето случаи документацията на системата се състои от Наръчник, процедури, инструкции и работни формуляри (и планове и програми при някои системи).

В процедурите се описва „кой какво прави и какви са отговорностите му" (например, процедура за търговската дейност). *В инструкциите* се формулира „кое как се прави" и/или „кое как не се прави" (например, инструкция за посрещане на клиенти). *В работните формуляри* се записва, че това, което е изисквано от системата, е направено, както и какъв е резултатът. Попълнените формуляри се наричат *„записи"*.

Одиторите проверяват дали документите покриват изискванията на съответния стандарт, дали се водят записи и дали ръководството и служителите разбират и спазват писаните правила.

Вторият въпрос е: Какво означава да бъде въведена една система?

Това е процес на създаване на документирани правила за изпълнение и управление на дейностите във фирмата (организацията), с което се гарантира правилното им изпълнение и ефективност на управлението им. По този начин се постига съответствие с изискванията на приложимия стандарт за Система за управление (например, за ISO 9001 - Система за управление на качеството и за ISO/IEC 27001:2005 – Система за управление на информационната сигурност). Въвеждане на системата и изграждане на системата е едно и също нещо. Подготовката за сертификация е финален етап на изграждането на системата, на който й се придава готовност да бъде демонстрирана пред орган за сертификация. Времето за въвеждане на системата е между 3 и 12 месеца и зависи от много фактори.

Третият въпрос е: Какво представлява ISO сертификатът?

Сертификатът е официален документ, издаден от Орган за сертификация и е доказателство, че фирмата (организацията) е въвела и има реално работеща Стандартизирана система за управление. Сертификацията е действие, което се изпълня-

ва след като системата е вече **въведена**. Консултациите по въвеждането на системата, ако са необходими такива, се извършват от консултантска фирма, която е различна и независима от органа за сертификация. Смисълът на това изискване е да се постигне безпристрастност на сертификацията.

Организацията подава заявка за сертификация до избрания орган за сертификация, който изпраща одиторски екип да провери и оцени дали стандартизирана система за управление съответства на изискванията на стандарта. След положителен доклад от одита, органът за сертификация взема решение по сертификацията, издава сертификат, регистрира го и го публикува.

Процедурата по първоначална сертификация трае между 1 и 3 месеца, считано от датата на подаване на заявка към органа за сертификация. Това важи, ако системата съответства напълно или в голяма степен на изискванията на съответния стандарт.

Сертификатът е валиден 3 години, който се наричат „надзорен период". През надзорния период се извършват надзорни одити, с които се проверява и оценява дали системата продължава да съответства на изискванията на стандарта, т.е. дали е „поддържана". Повечето органи за сертификация правят надзорни одити веднъж годишно. Сертификацията се подновява на всеки 3 години.

Нормално е да се зададе и *четвъртия въпрос: Каква е ползата за организацията от сертифицирането?* Основните от тях са следните:

- повишаване на доверието към фирмата (организацията);
- чувствително подобряване на вътрешния ред и ефективността;
- значително намаляване на разходите;
- намаляване на риска;
- управление жизнения цикъл на продукта;
- развитие на нови пазари;
- бърза реакция на развитието на технологиите;
- при участие в търгове и процедури, особено по Закона за обществените поръчки, често се изисква кандидатите да имат действащи сертифицирани системи.

Други конкретни ползи произтичат и от същността на конкретните системи.

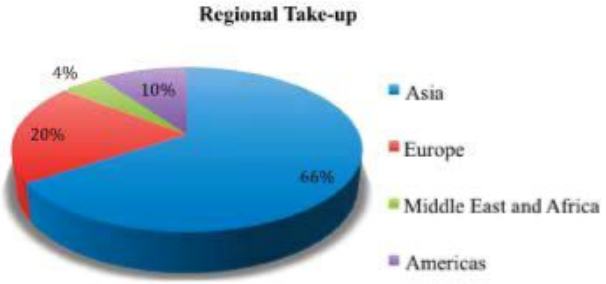
На трето място за да изведем проблемите при внедряване на СУИС, следва да направим анализ на световната и националната практика по внедряване на стандарта ISO/IEC 27001:2005.

На фигури 2 и 3[4] са показани данните от сертификацията по региони и по сектори на приложение.

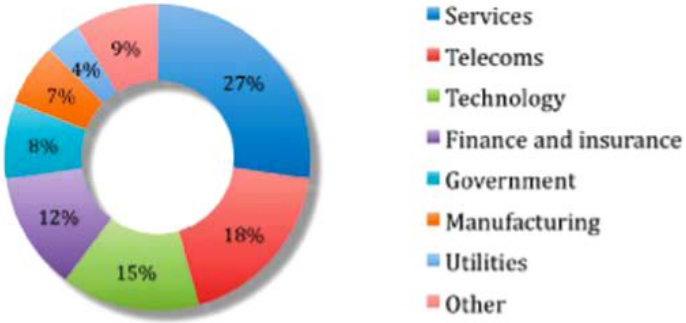
От представените на фигура 2 данни се вижда, че най-голям е процентът на сертифицираните фирми по стандарта ISO/IEC 27001:2005 в Азия - 66 %, докато в Европа те са само 20 %.

По сектори (фигура 2) сертификациите се разпределят по следния начин: в сферата на услугите – 27 %; в телекомуникациите – 18 %; в сферата на технологиите – 15 %; във финансите и застраховането – 12 %; в правителствения сектор – 8 %; в промишления сектор – 7 %; в сферата на комуналните услуги – 4 %; в други сектори – 9 %.

[4] CIO, бр. 4, С., 2009.



Фиг. 2. Количество сертификации по региони по ISO/IEC 27001, към март 2009.



Фиг. 3. Количество сертификации по отрасли по ISO/IEC 27001, към март 2009.

В България към 1 май 2011[5] г. са сертифицирани общо 43 фирми по ISO/IEC 27001:2005 от всички отрасли - таблица 1. Най-много - 21 фирми разработили и внедрили СУИС са от ИТ сектора. На второ място - 11 са организациите от сферата на публичната администрация.

Във фирмите от ИТ сектора към този период са внедрени 78 сертифицирани системи по действащите към момента стандарти – таблица 2. Данните показват,че най-много 54 са внедрените системи по управление на качеството по стандарт ISO 9001:2008 и по-малко от два пъти – 21 са внедрените сертифицирани системи за управление на информационната сигурност по ISO/IEC 27001:2005 и нито една система за управление на услугите по ISO/IEC 20000.

[5] Българският сертификационен портал. http://bgcert.com/bg/stats.php?g_id=1

Таблица 1

Количество на сертифицираните фирми по ISO/IEC 27001:2005 по отрасли към 01.05.2011 г. по кодовете за сертификация на Европейската организация за сертификация (EA)

№ по ред	Отрасли на дейност	Брой сертифицирани фирми
1.	Информационни технологии (EA Code 33)	21
2.	Публична администрация (EA Code 36)	11
3.	Други услуги (EA Code 35)	5
4.	Финансово посредничество; недвижими имоти; наеми (EA Code 32)	2
5.	Печатници (EA Code 9)	1
6.	Електрическо и оптическо оборудване (EA Code 19)	1
7.	Транспорт, съхранение и комуникации (EA Code 31)	1
8.	Образование (EA Code 37)	1
	ВСИЧКО:	43

От тези данни може да се определи тенденцията и формулират следните два проблема:

*Първия*т - фирмите от ИТ сектора се задоволяват с внедряване на системи за управление на качеството и подценяват разработването и внедряването на СУИС. Това се дължи на ограничаването само в единият от елементите на системата, компютърната сигурност, и се предоверяват на заложените защити в хардуера и софтуера.

Таблица 2

Количество сертифицирани системи във фирми от ИТ сектора към 01.05.2011 г.

№ по ред	Стандарти	Брой сертифицирани фирми
1.	ISO 9001:2008 - Система за управление на качеството	54
2.	ISO/IEC 27001:2005 - Системи за управление на информационната сигурност	21
3.	ISO 14001:2004 - Система за управление на околната среда	2
4	ISO 13485:2003 - Системи за управление на качеството на медицинските устройства	1
	ВСИЧКО:	78

Вторият е, че в резултат от доброволния режим на сертификация на фирмите (организациите), държавните регулаторни органи при издаването на лицензии не изискват сертификации по стандартите за защита на информацията и осигуряване качеството на предоставяните комуникационни и информационни услуги. Практиката показва, че възползвайки се от този режим, такива клаузи липсват и в сключ-

ваните договори с клиентите, те са ощетената страна и са лишени от възможността да изискват качествени услуги или да предявяват искове.

Потвърждение на дефинираният проблем е факта, че на 15 март 2011 г. в Raiffeisen Bank Kosovo JSC се реализира първата сертификация на банка в Югоизточна Европа, по стандарта ISO/IEC 20000 от престижния одитор Lloyd's Register - България. Банката е консултирана от българки консултанти сертифицирани от ITCE (Infrastructure, Security, Reporting) и български одитор – ITCE, т.е. имаме квалифицирани консултантски и сертификационни фирми, но нямаме желаещи да въведат и сертифицират съответните системи за управление.

През последните години усилията на банките, които оперират на българския пазар са насочени основно в следните направления:

- подобряване на информационната среда и внедряване на нови продукти за удобство на клиентите;
- подобряване на технологичната среда и миграция към нови версии на основните банкови системи;
- намаляване на риска за банковите услуги чрез подобрения в електронния обмен на данни;
- подобряване на средствата за мониторинг на информационната система и оценка нивото на сигурност и риск чрез тестове за проникване (Penetration tests);
- централизация на банково-информационната система и използване на единна информационна инфраструктура;
- внедряване на интегриран бизнес и информационен модел с възможност за динамично оценяване на клиентите и управление на риска и др.

До тук добре, но само на оценка и защита подлежат активите на банката. А кой може да покаже и да докаже на какво ниво е сигурността на информационните им масиви и с какви средства и практики се съхраняват личните данни на клиентите?

Това определя и *третият проблем:* Има действаща законова и стандартизационна база, но тя не се спазва и не се налагат ефективни мерки за нейното налагане.

Ръководейки се само от правилото: „Бизнесът определя целите и ИТ отделът трябва да се впише в тази картина", не винаги е в полза на интересите на клиентите. Това изисква от ИТ отдела и Отдела по управление на информационния риск да разработят и приложат интегрирана система по прилагане на стандартите ISO 9001:2008, ISO/IEC 27001:2005, ISO/IEC 20000:2005 и ISO/1401:2004. Това ще доведе до: значително повишаване на ефективността в дейността на организациите; понижаване на риска; посрещане на договорните и пазарните изисквания към нея; демонстриране на качество на услугите и доставката им на най-добра цена. Организациите ще имат възможност да усъвършенстват своята способност за доставка на услуги, да разделят приоритетно нивата на услугите си и да измерват качеството на своята дейност.

Това изискване е валидно днес, в началото на XXI в., когато организациите от ИТ сектора са подложени на постоянен натиск във връзка с доставката на високо качествени услуги на минимална цена. Фирмите потребители на тези услуги повишават изискванията си, докато предлаганите услуги от вътрешен ИТ отдел или от външна организация не винаги са напълно наясно с изискванията на бизнеса, неговите клиенти и публикациите на международните стандарти. Това налага организациите да потърсят услугите на квалифицирани консултанти и сертифициращи фирми.

В тази връзка актуално звучи следната констатация на Радослав Радев – мениджър по управление на риска в ING Животозастраховане и ING Пенсионно осигуряване: „Практиката показва, че вътрешната експертиза, която дава ИТ отделът, понякога е повлияна от нагласите на служителите, които са работили по този проект. Те приемат някои от фактите за даденост. За това се нуждаем от външен консултант, който да притежава необходимите компетенции. Той трябва да подходи обективно, като подложи на критичен анализ всеки компонент."[6]

Такъв одит е нужен когато системата е навлязла в етап редовно внедряване и функционира. Тогава висшето ръководство на организацията може да помисли за сертифициращ орган. При самото проектиране на системата следва да се избягва всякаква нагласа към спецификата или предварително разузнати изисквания на сертифициращата организация, като по този начин се заобиколят изискванията на клиентите и реалните вътрешни нужди от подобрения.

Третият момент, който е пряко свързан с изграждането на СУИС, е състоянието на кадрите от ИТ сектора, нивото на тяхната подготовка и подбор.

Повишеното внимание към защитата на информационните ресурси и среда доведе до значително нарастване на търсенето на професионалисти по ИТ сигурност. Мениджърите по управление на информационната сигурност *(Security Management – SM)*, които се занимават с въпроса за подбора на опитни специалисти в тази сфера, често стигат до извода, че те не са толкова много, колкото биха искали. Нека накратко се спрем на въпроса: *Какво е състоянието с подготовката на ИТ кадри и какви са тенденциите в началото на XXI век?*

За изясняването на този важен въпрос можем да се опрем на резултатите от проведеното изследване от списание CIO „Въпроси за ИТ кадрите & ИТ образованието", проведено през октомври 2010 г. за четвърти пореден път.[7]

Резултатите показват, че българските организации повече от четири години са срещали затруднения в тази област, в резултат от липсата на специалисти, по години те са както следва: през 2007 г. – 55 %; през 2008 г. – 62 %; през 2009 г. – 65 %; през 2010 г. – 61 %. По степени на осигуреност за последните три години положението е следното (таблица 3):

Таблица 3

Степен на осигуреност, в %	Срок на изследването		
	2008 г.	2009 г.	2010 г.
По-голяма от необходимото	5	3	4
Достатъчна	33	32	35
Недостатъчна, но въпреки това не е изключително съществено	-	24	8
Недостатъчна	62	41	53

Основните причини за недостига на кадри, изведени от изследването се де-

[6] CIO, бр.4. С., 2011.

[7] CIO, бр.10. С., 2010.

финират в диапазона от трудното привличане на младежите към ИТ специалността и адекватна университетска подготовка на студентите, до ограничените възможности на организациите да инвестират в квалификацията на своите ИТ специалисти и в тяхната мотивация.

Динамиката в търсенията на уменията от ИТ специалистите от организациите може да се проследи от данните изведени в таблица 4.

Данните показват, че от 2007 г. до 2010 г., най-търсени са ИТ специалистите притежаващи умения в ИТ сигурността. Най-голям скок има в уменията по мрежово осигуряване – от десето на първо място. Значително са променени търсенията на умения по управлението на бази данни – от осмо на четвърто, на уменията по Web услуги - от тринадесето на пето и на подготовката за управление на системната архитектура – от дванадесето на шесто място. Стабилизация има при уменията за поддръжка на потребители и бизнес анализи. Най-голям спад има специализацията по управление на проекти, която от втора най-търсена през 2009 г., през 2010 г. е на десето място.

Таблица 4

Най-търсени умения от ИТ специалистите	Степен на важност по години	
	2009 г.	2010 г.
ИТ сигурност	1	2
Управление на проекти	2	10
Управление на бизнес процесите	3	8
Поддръжка на потребители	4	3
Бизнес анализи	5	7
Системен анализ	6	11
Разработване на приложения	7	9
Управление на бази данни	8	4
QA/Тестове	9	13
Мрежово осигуряване	10	1
Стратегическо осигуряване / Вътрешно консултиране	11	12
Проектиране на системна архитектура	12	6
Web услуги	13	5
ИТ финанси	14	14

От представените в таблица 4 резултати могат да се направят изводи и за тенденциите за развитие на ИТ кадрите и тези по информационна сигурност за следващите 4-5 години. Може да се определи, че най-съществения фактор за формирането на високо квалифициран ИТ специалист е адекватното висше образование и целенасоченото самообучение. Това се потвърждава и от резултатите представени на фигура 4. Вижда се, че почти половината от знанията и уменията се формират при обучението – 48 % (23 % при редовния учебен процес и 25 % чрез самообучението) на специалиста. На следващо място за успешното професионално развитие може да се постави политиката на организациите за формиране на корпоративна култура чрез включване на млади специалисти в значими проекти по различни програми, изучаване на нови технологии и обучение в специализирани курсове, които формират 62 % от професионалните умения.

В тази връзка можем да се опитаме да дадем отговор на въпроса за формирането на квалифицирани ИТ кадри и да дадем отговор на въпроса: *В каква степен учебните програми в българските ВУЗ в областта на ИТ образованието са съгласувани с потребностите на пазара на труда?*

Фиг. 4. Фактори, формиращи ИТ специализацията

За самите ВУЗ, след като учебните планове и програми осигуряват хорариума на академичния състав, може да изглеждат добри, но какво показват резултатите от изследването в бизнес средите. Според изследването на CIO България на 64 анкетирани ръководители на ИТ подразделения и мениджъри в ИТ компании, средната оценка за степен на съгласуваност на учебните програми с потребностите на реалната работна среда е 3,9 по десетобалната скала. Това определя и главното направление за съсредоточаване на усилията – обновяване на учебните програми, развитието на стажантски програми с фирмите, които са потенциални работодатели на кадрите от сферата на информационната сигурност и сътрудничеството с големи фирми от сектора за сигурност. В това отношение е нужна помощта и готовността на фирмите за такова сътрудничество.

Тези резултати позволяват да се изведе *четвъртия проблем:* Учебните планове и програми за обучение на ИТ специалистите и на тези от сферата на информационната сигурност трябва периодично да се адаптират с потребностите на работната среда.

В това отношение като добър симптом може да бъде оценен факта, че през 2010 г. организациите от ИТ сектора са заделили 9 % от фирмените си бюджети за повишаване на квалификацията на служителите си (независимо от общият спад на бюджетите в условията на кризата), спрямо 4 % през 2009 г., 7,2 % през 2008 г., и 5,4 % през 2007 г.

Друг не по-маловажен фактор, който мениджърите следва да оценяват е свързан със заплащането на специалистите. Факторите с най-силен мотивиращ ефект за ИТ специалистите за последните три години са били: заплащането, възможността за професионално развитие, възможност за обучение и възможност за развитие в служебната йерархия.

Будят притеснение обаче проблемите свързани с развитие на ИТ персонала за последните две години (таблица 5). Данните показват, че вследствие на икономическата криза и свиване на бюджетите на фирмите, работодателите са прибягнали до съкращаване на 14 % от ИТ персонал, който притежава необходимите умения (запазени са 48 % от наличните 62 %) и са намалили с 35 % наемането на нов персонал (от 77 % на 42 %). Запазва се количеството на персонала с ниска мотивация – в границите на 38 % – 41 %, което показва застой във фирмената политика за развитие на кадрите.

Таблица 5

Основни проблеми за ИТ специалистите	Стойност по години, в %	
	2009 г.	2010 г.
Запазване на персонала, който притежава необходимите умения	62	48
Наемане на нов персонал с необходими умения	77	42
Финансиране на ИТ обучение	23	41
Персоналът е с ниска мотивация	38	41
Определяне на оптимално съотношение от ИТ умения за период от 2 до 5 години	15	28
Откриване на кандидати подходящи за ИТ мениджъри	23	28
Изисквания за намаляване на работното натоварване	15	22
Определяне на оптималното съотношение от ИТ умения необходими сега	15	16

Като положителна тенденция може да се отчете увеличаването с 18 % на заделените средства за финансиране на обучението.

В този не лек момент се откроява фигурата на мениджъра по сигурността, (*SM*) който носи цялата отговорност за информационната сигурност. Той трябва да осъществява връзката с мениджърите от останалите процеси. Това налага за такъв да се назначава специалист по сигурността, който е включен в ръководния състав на организацията. Стратегическото ниво на фирмата следва безрезервно да застане зад имплементирането на SM, като го ангажира с дефиниране на целите и следи за реалното въвеждане на решенията по информационната сигурност в рамките на зададените му параметри. Той е длъжностното лице, което ще управлява процесите за управление на инцидентите (*Change and Incident Management*), защото те са от съществено значение за сигурността, особено в условията на засилване на киберпрестъпността и кибертероризма в световен мащаб.

От решаващо значение за успеха на SM е манталитетът, фирмената култура и кадровата политика на организацията. Тези фактори често пъти се явяват решаващи за ефективността на СУИС на организациите.

Към настоящият момент не са редки случаите на назначаване на длъжности в държавните и общинските администрации и в немалко фирми на бивши служители на МВР и МО, като по презумпция се приема че те са подготвени за такава дейност или на лица с протекции на политически сили или на влиятелни личности. Малка

част от тях успяват да се квалифицират и успешно да се впишат в направлението на системите за сигурност. Останалите си живеят безпроблемно и не позволяват на тези длъжности да бъдат назначени млади подготвени специалисти. Това се превръща в немалък проблем за специалистите по административна и информационна сигурност и за инженерите от ИТ специалността, завършили ВУЗ. Показателен в това отношение факта, че 1 от завършилите магистратура и 1-2 от бакалаврите от специалност „Административна и информационна сигурност" са започнали работа по специалността.

В тази връзка може да се формулира и *петия проблем:* Фирмите от ИТ сектора не бива само да очакват готовият продукт на ВУЗ, а активно да се включват при определяне на учебното съдържание, да формират и провеждат адекватна фирмена и кадрова политика за подбор и обучение на своите специалисти по сигурността на информацията и активно да се включват при изграждането на учебната база и предоставят своята за развитие на практическите умения на студентите.

Младите специалисти имат добра теоретична подготовка, гъвкави са и приспособими към изискванията на съвременната динамична среда. Липсва им практически опит, но при една правилна фирмена политика и умело ръководене от добронамерен и амбициозен мениджър могат да се изградят и утвърдят като качествени специалисти в сектора за информационна сигурност.

Заключение

Това са основните моменти по състоянието на сертификационната и законодателната рамка в началото на XXI век. Разрешаването на дефинираните проблеми изискват компетентната намеса на ръководствата на организациите за изучаване на изискванията на международните стандарти и тяхното прилагане за сертифициране на фирмите предоставящи различни стоки и услуги.

Сигурността не трябва да се възприема като нещо абстрактно и статично. Тя е качествено и динамично състояние, пораждащо трайно усещане за стабилност и спокойствие. Сигурността не касае само информационно-технологичната среда, а цялостния живот на гражданите. Постоянното усложняване на системите за защита на информацията и повишаване на значимостта на ИТ и управлението на риска в бизнеса изисква постоянен анализ на факторите, оформящи стратегическата среда за сигурност, адекватен анализ на риска, изграждане и компетентно управление на системите за сигурност. Това може да се осъществи от подготвени кадри, добро финансиране и правилна фирмена и кадрова политика. Компетентните и опитни специалисти, са част от капитала на компанията. Тяхното откриване, привличане, стимулиране, повишаване на квалификацията и задържане в организацията изискват както повишено внимание от страна на ръководството, така и висок професионализъм от страна на мениджърските екипи.

Приложение 1

ТАБЛИЦА
на стандартите по информационна сигурност,
валидни към 01.05.2011 г.

№	*Стандарт*	*Предназначение*	*Заменен от*	*Статут*
1.	БДС ISO/IEC TR 13335-1:2002	Информационни технологии. Ръководство за управление сигурността на ИТ. Част 1. Концепции и модели за управление на сигурността на ИТ.	ISO/IEC 13335-1:2004	Отменен 2002 г.
2.	БДС ISO/IEC TR 13335-4:2002	Информационни технологии. Ръководство за управление сигурността на ИТ. Част 4: Подбор на гаранции.	БДС ISO/IEC 27005:2009	Отменен 2002 г.
3.	БДС ISO/IEC TR 13335-5:2004	Информационни технологии. Ръководство за управление сигурността на ИТ. Част 5: Ръководство за управление на сигурността на мрежата.		Отменен 2004 г.
4.	БДС ISO/IEC TR 13335-2:2002	Информационни технологии. Ръководство за управление сигурността на ИТ. Част 2: Техники за управление на сигурността на ИТ.		Отменен 2002 г.
5.	БДС ISO/IEC TR 13335-3:2002	Информационни технологии. Ръководство за управление сигурността на ИТ. Част 3: Техники за управление на сигурността на ИТ.	БДС ISO/IEC 27005:2009	Отменен 2002 г.
6.	ISO/IEC 13335-1:2004	Информационни технологии – Техники за сигурност – Управление сигурността на информационни и комуникационни технологии – Част1: Концепции и модели за управление на сигурността на информационните и комуникационните технологии		Действащ
7.	БДС ISO/IEC 17799:2005	Информационни технологии. Кодекс за добра практика за управление сигурността на информацията.		Отменен 2007 г.
8.	БДС ISO/IEC 17799:2006	Информационни технологии. Кодекс за добра практика за управление сигурността на информацията.	ISO 17799:2005 /Cor.1:2007 БДС ISO/IEC 27002:2006, а приложение А в БДС ISO/IEC 27001:2006	Отменен 2007 г.
9.	БДС ISO/IEC	Информационни технологии за		Действащ

№	*Стандарт*	*Предназначение*	*Заменен от*	*Статут*
	27000:2009 (E)	сигурност. Техники по сигурността на информацията и системи за управление. Общ преглед и речник.		
10.	БДС ISO/IEC 27001:2006	Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията.		Действащ
11.	БДС ISO/IEC 27002:2008	Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурност-та на информацията.		Действащ
12.	ISO/IEC 27003:2009	Информационни технологии. Техники на сигурност. Практическо ръководство за внедряване на организационните политики, правила, процедури и контроли за сигурност на информацията.		Очаквана дата за публикация 11.09.2009
13.	ISO/IEC 27004:2009	Информационни технологии. Техники на сигурност. Системи за управление на сигурността на информацията. Измерване.		Очаквана дата за публикация 14.11.2009
14.	БДС ISO/IEC 27005:2009	Информационни технологии. Методи за сигурност. Управление на риска за сигурност на информацията.		Действащ
15.	БДС ISO/IEC 27006:2009	Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системите за управление на сигурността на информацията.		Действащ, допълва БДС ISO/IEC 27001 и БДС ISO/IEC 17021
16.	ISO/IEC 27007:2010	Информационни технологии. Техники на сигурност. Практическо ръководство за регламентиране и провеждане на одит на документирана система за управление сигурността на информацията.		Очаквана дата за публикация 19.04.2010
17.	БДС ISO/IEC 27011:2008	Информационни технологии. Техники на сигурност. Общи принципи за иницииране, внедряване, експлоатация и усъвършенстване управлението на сигурността на информацията в телекомуникационния сектор.		Действащ
17.	ISO/IEC 27012	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Указания за управление на		Разработва се

№	*Стандарт*	*Предназначение*	*Заменен от*	*Статут*
		сигурността на услуги на е-правителство.		
18.	ISO/IEC 27032:2010	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Ръководство за управление на киберсигурност.		Очаквана дата за публикация 04.11.2010
19.	ISO/IEC 27033-(1-7)	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Ръководство за сигурност на IT мрежи.		Разработва се
20.	ISO/IEC 27034	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Ръководство за сигурност на приложенията.		Разработва се
21.	ISO/IEC 27035	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Указания за управление на инциденти по информационната сигурност.		Разработва се
22.	ISO/IEC 27045	Информационни технологии. Техники за сигурност. Управление на информационната сигурност. Измерване.		Разработва се
23.	ISO/IEC TR 18044:2004	Информационни технологии. Мениджмънт на инцидентите по информационната сигурност.		Действащ
24.	ISO/IEC 31000:2009	Риск-мениджмънт. Принципи и указания.		Действащ
25.	ISO/IEC 31010:2009	Риск-мениджмънт.Техники за оценка на риска.		Действащ
26.	ISO/IEC Guide 73:2002	Управление на риска. Речник. Насоки за използване на стандартите.	ISO/IEC Guide 73:2009	Отменен 2009
27.	ISO/IEC Guide 73:2009	Управление на риска. Речник. Насоки за използване на стандартите.		Действащ
28.	FERMA	Стандарт по управление на риска.		Действащ
29.	ISO/IEC 15408-1:1999	Информационни технологии – Техники на сигурност – Критерии за оценка на сигурността на ИТ – част 1: Въведение и общ модел.		Действащ
30.	**ISO/IEC 20000-1:2005**	Информационни технологии. Управление на услуги – част 1: Спецификация.		Действащ
31.	ISO/IEC	Информационни технологии.		Действащ

№	*Стандарт*	*Предназначение*	*Заменен от*	*Статут*
	20000-2:2005	Управление на услуги – част 2: Кодекс за добра практика при управление на услуги.		
32.	ISO 9000:2000	Системи за управление на качеството. Основни принципи и речник.		Действащ
33.	БДС EN ISO 9001:2000	Системи за управление на качеството – Изисквания.	БДС EN ISO 9001:2008	Отменен 2008 г.
34.	БДС EN ISO 9001:2008	Системи за управление на качеството – Изисквания.		Действащ
35.	БДС EN ISO 9004:2000	Системи за управление на качеството – Ръководство за подобряване на дейността.		Действащ
36.	БДС EN ISO 9011:2004	Указания за одит на системите за управление на качеството и/или за управление на околната среда (ISO 9011:2002).		Действащ
37.	ISO 14050:2002	Управление на околната среда. Речник.		Действащ
38.	ISO/IEC 15504-1:2004 (E)	Информационни технологии – процес на оценка – част 1: Понятия и речник.		Действащ
39.	ISO/IEC 15504-2:2003 (E)	Софтуерно инженерство – процес на оценка – част 2: Извършване на оценка.		Действащ
40.	ISO/IEC 15504-3:2003 (E)	Информационни технологии – процес на оценка – част 3: Указания за извършване на оценка.		Действащ
41.	ISO/IEC 15504-4:2004 (E)	Информационни технологии – процес на оценка – част 4: Насоки за използване на процес за усъвършенстване на процеса		Действащ
42.	ISO/IEC 15504-5:2006 (E)	Информационни технологии – процес на оценка – част 5: Един модел за оценка		Действащ
43.	ISO/IEC 15504-6:2008 (E)	Информационни технологии – процес на оценка – част 6: Един модел за оценка на процеса на жизнен цикъл		Действащ
44.	ISO/IEC TR 15504-7:2008 (E)	Информационни технологии – процес на оценка – част 7: Оценка на организационната зрялост		Действащ

КИБЕРЗАЩИТАТА – ПРИОРИТЕТ НА АЛИАНСА

Иван Г. Иванов

директор на дирекция „Сигурност на информацията" – Министерство на отбраната

1092 гр. София, ул. „Дякон Игнатий" № 3, Министерство на отбраната

CYBER DEFENCE – NATO PRIORITY

col. Ivan G. Ivanov

chief of Information Security directorate, MoD

I. Въведение

В съвременния, бързо развиващ се свят на комуникационните и информационните технологии, сигурността вече не е пожелание, тя е абсолютно необходима. Имайки предвид, че евентуална информационна война ще се води по всички писани и неписани закони, за сигурността и защитата на военните информационни системи и мрежи може дори да се каже, че е жизнено необходима. Ето защо осигуряването на сигурността и защитата на информационните системи и мрежи е от първостепенно значение за органите от звената по сигурност на информацията.

Бурното развитие на информационните технологии доведе до промяна в средствата и схващанията за воденето на съвременните военни операции. В този смисъл информацията се превръща в мощно оръжие. Способността на силите да притежават навременни, пълни, точни и достоверни данни и едновременно с това да притежават възможността да попречат на противника да притежава такива е сериозна гаранция за успех.

Защитата на класифицираната информация, без компромиси в сигурността, е и основата за постигане на целите на Р България като пълноправен член на НАТО.

В много изследвания се доказва, че извършващите се в света глобални промени придават приоритетно значение на информационния аспект на сигурността. На практика той влияе върху всички останали, заемайки централно място в общата концепция за национална сигурност. Това е причината, довела до дефиниране на понятието ***„информационна сигурност"*** и създаване на съответната система за информационна сигурност.

Разбирането, че информацията е основен стратегически ресурс, налага да се направи информационна интерпретация на същността на сигурността. Реализирането на политиката за национална сигурност и отбрана изисква все по-голямо количество от информационни инфраструктури за създаване, съхранение, обработка и пренасяне на критична информация за нуждите на планирането, ръководството, координацията и контрола на текущите дейности. В тези инфраструктури има множество уязвими места, които могат да бъдат атакувани и разрушени от специфични сили с голяма информационна мощ.

Асиметричните заплахи и глобализацията на конвенционалния тероризъм се

увеличават и се наблюдава:

- засилване на разрушителния ефект на кибернетичните атаки и възможностите на групи от хора (терористи) да влияят върху политиката на отделни правителства или големи маси от населението.
- устойчива тенденция на нарастване на интензивността и сложността на провежданите кибернетични атаки.
- промяна в методите и способите за водене на бойни действия, като на първият етап винаги се отрежда постигането на информационно превъзходство над противника, чрез прилагане на съвременни информационни технологии с използване на специализиран софтуер и специални технически средства.
- нарастване броя на страните по света - над 120, които използват Интернет за политически, военни и икономически шпионаж и въздействия върху информационните ресурси на своите конкуренти и противници.

Регистрирани са множество кибернетични атаки по света, като най-съществените през последните години са:

- 1998 г. – около 3000 хакери атакуват организирано индонезийски правителствени сайтове.
- 1999 г. – кибератаки преди началото и в хода на въздушната кампания на НАТО над бивша Югославия.
- 2007 г. – правителствени естонски Web сайтове са атакувани организирано от руски хакери.
- 2009 г. – организирани кибер атаки са извършени от Русия срещу Грузия по време на войната в Южна Осетия.

Чрез кибератаките се цели:

- пълно или частично "парализиране" на публичните и държавните информационни мрежи и системи.
- пълно или частично блокиране на обществените дейности в държавата.
- пълно или частично "сриване" на комуникационно-информационната инфраструктура с цел блокиране на дейностите на държавните институции и възможност за влияние върху общественото съзнание и психика.

Разбира се може да се каже, че при определени обстоятелства е възможна ситуация, в която за информационните ресурси и инфраструктура няма заплахи (външни или вътрешни) и гарантирането на тяхната сигурност не изисква необходимостта от изграждане на съответна система за защита на информацията. Т.е. сигурността е постигната като състояние без да са предприети мерки за защита.

Гореописаната ситуация има по-скоро хипотетичен характер. Във военното дело процесите по създаване, обработка, съхраняване и обмен на информация са от критично значение за поддържане на бойната готовност и осигуряване на информационната поддръжка при изпълнение на поставените задачи. Това обосновава необходимостта от изградена и надеждно функционираща система за защита на информация, защитаваща информационните ресурси в мирно време и по време на кризи и война.

Защитата на информацията трябва да се осъществява през целия неин жизнен цикъл – от момента на нейното създаване, до момента на прекратяване на нейното съществуване в рамките на разглежданата информационна система.

II. Основни уязвимости в автоматизираните информационни системи и мрежи

"От всички възможни неприятности се случва именно тази, която води до най-големи щети."
Трето следствие от Закона на Мърфи

1. Заплахи и атаки към автоматизираните информационни системи и мрежи

Уязвимото място е слабост в информационната система или мрежа и в мерките за нейната защита, която може да доведе до компрометиране сигурността на системата.

Под уязвимо място се разбира всяка точка на автоматизираните информационни системи и мрежи и на системата за тяхната защита, където те са слабо защитени срещу заплахи и атаки, свързани с тяхната сигурност. Уязвимите места в една система зависят от конкретната й реализация.

Заплаха е човек, обект, събитие, процес или явление, които могат да нанесат вреда на автоматизираните информационни системи и мрежи.

Могат да бъдат дадени следните примери за заплахи:

- използване на известен способ за достъп до системата с цел извършване на забранени действия;
- маскиране като истински потребител;
- използване на служебно положение с цел достъп до информация;
- физическо разрушаване на системата или нейни компоненти;
- изключване на системата за защита или нейни компоненти;
- изключване на подсистемите, обезпечаващи работата на системата (електрозахранване, охлаждаща и вентилационна, комуникационна и други);
- промяна на режима на работа на устройства и програми;
- подкуп и шантаж на персонала или отделни потребители;
- кражба и несанкционирано копиране на информационни носители;
- незаконно използване на пароли, пропуски, магнитни карти и други;
- разкриване на шифри (компрометиране на ключови документи) за криптографска защита на информацията;
- включване към системата на апаратни средства и програми, позволяващи несанкциониран достъп;
- заразяване с вируси;
- незаконно включване към комуникационните линии с цел подмяна на законен потребител и предаване на лъжлива информация от негово име;
- незаконно включване към комуникационните линии с цел прехващане на поверителна информация;
- незаконно включване към комуникационните линии с цел анализ на протоколите за комуникация и последващото им имитиране за достъп до системата;
- използване на подслушвателни устройства и устройства за дистанционно видеонаблюдение;
- прехващане на паразитни електромагнитни излъчвания;
- четене на остатъчна информация от оперативната памет и външни запомнящи устройства;
- незаконно използване на терминали и работни станции, оставени без надзор.

Класификацията на видовете заплахи е необходима за оценка на системите за защита. Тя може да бъде направена по различни критерии.

Според своя източник заплахите могат да бъдат ***външни*** и ***вътрешни***. *Външни заплахи* са дейността на разузнавателни и специални служби, дейността на различни политически, икономически и други структури, насочени срещу интересите на организацията, и престъпни действия на отделни групи и лица. *Вътрешни заплахи* са нарушаване на правилата за събиране, обработка, съхраняване и предаване на информацията, незаконна дейност на групировки и лица за прикриване на закононарушения и нанасяне на вреди на интересите на физически и юридически лица на базата на тази информация.

Основните видове заплахи за сигурността на АИС са:

- Стихийни бедствия и аварии.
- Сривове и откази на техническите средства на информационната система или мрежа.
- Последствия от грешки при проектиране и изработка на системата или мрежата.
- Грешки на персонала при работа със системата или мрежата.
- Преднамерени действия на нарушители и зложелатели

Според произхода си заплахите могат да бъдат ***естествени*** и ***изкуствени***.

Естествени са заплахите от обективни физически процеси или стихийни природни явления, независещи от човека - пожари, наводнения, урагани, земетресения и нарушения в инфраструктурата (аварии в електрозахранването, аварии в системите за комуникация, прекъсване на водоснабдяването и т.н.). Не е възможно те да бъдат предотвратени, но могат де се минимизират, като се използват противопожарни и други технически средства.

Изкуствените заплахи са предизвикани от действията на хора. Те биват непреднамерени (неумишлени, случайни) и умишлени. Според статистиката около 65% от щетите, нанесени на информационните системи и мрежи, са следствие на непреднамерени грешки, а само 13% на стихийни бедствия и аварии.

Според въздействието си върху процеса на обработка на информацията, заплахите са:

- за обектите на информационните системи и мрежи;
- за процесите, процедурите и програмите за обработка;
- за информацията, предавана по комуникационните канали;
- за системата за защита на информацията (СЗИ).

Има 3 основни вида заплахи за сигурността на информацията:

- заплахи от разкриване - информацията да стане известна на този, който не трябва да я знае. Понякога вместо "разкриване" се използват термините "кражба" или "изтичане";
- заплахи за целостта - включват всяка умишлена промяна на данните, съхранявани в автоматизираната информационна система или мрежа или предавани от една система към друга;
- заплахи от отказ на обслужване - възникват всеки път, когато като резултат от нечии действия се блокира достъпът до някакъв ресурс на автоматизираната информационна система или мрежа. Блокирането може да бъде постоянно (тогава желаният ресурс никога не се получава) или да предизвика само временна задръж-

ка на получаването на ресурса, докато той стане ненужен.

Заплахите от разкриване произлизат от различни канали за изтичане на информацията.

Канал за изтичане на информацията е метод, позволяващ на даден нарушител да получи достъп до информацията, обработвана или съхранявана в системата.

Според средството за получаване на информация каналите за изтичане биват:

- канали за изтичане, в които средство за получаване на информация са хората (кражба на носители, четене на информация от екрана от външни лица, четене на информация от оставени без надзор разпечатки);
- канали за изтичане, в които средство за получаване на информация е апаратурата (включване към компютърните устройства на специално разработени апаратни средства за достъп до информацията или използване на специални технически средства за прихващане на електромагнитни излъчвания от хардуера).

Канал за изтичане на информацията може да има и заради паразитните електромагнитни излъчвания (ПЕМИ). Това са паразитни електрически магнитни полета, създавани от основните и спомагателните технически средства и системи, индуктиране на информационни сигнали по всевъзможни линии и кабели, излизащи зад границите на контролираната зона и други.

Атаката е целенасочено действие на преднамерен нарушител, състоящо се в търсене и използване на слаби места (уязвимости) с цел сриване сигурността на автоматизираната информационна система или мрежа.

В резултат на успешна атака се постига:

- изтичане на информация;
- отказ от обслужване (блокиране);
- външна злоупотреба с ресурсите на организацията, кражба на услуги;
- записване и използване на мрежовия трафик на организацията от външни лица;
- разрушаване на информация;
- измама с данни;
- инсталиране на зловреден софтуер;
- индиректна (непряка) злоупотреба (използване на други системи за създаване на зловреден софтуер);
- разбиване на пароли;
- влошено администриране.

Средствата за атака могат да се разделят в следните категории:

- потребителски команди - въвеждани от командната линия или посредством графичен потребителски интерфейс;
- низове (скриптове) или софтуер - стартирани от атакуващия и използващи слабите места на автоматизираните информационни системи или мрежи;
- анонимни агенти - инсталира се софтуер или фрагменти от него, които работят в последствие независимо от потребителя и използват слабите места на системата;
- средства за разработване - софтуерни пакети, съдържащи скриптове, програми или анонимни агенти;
- разпределени средства - средствата за атака се разпределят върху различни компютри (работни станции, терминали);

• извличане на данни - когато се подслушва магнитното излъчване от автоматизираните информационни системи и мрежи чрез устройства, външни за тях.

Формите на организиране на атаките са много разнообразни, но като цяло те се включват в една от следните категории:

• отдалечено проникване в автоматизирана информационна система или мрежа чрез софтуер, който получава неоторизиран достъп до друга работна станция през мрежата;

• отдалечено блокиране на автоматизирана информационна система или мрежа чрез софтуер, който през мрежата блокира работата на отдалечена работна станция или на отделна инсталирана на нея програма;

• локално проникване в работна станция (компютър) чрез софтуер, който получава неоторизиран достъп до работната станция, на която работи;

• локално блокиране на работна станция чрез софтуер, който блокира работата на работната станция, на която работи;

• чрез мрежови скенери - софтуер, който събира информация за мрежата, за да определи кои от работните станции и инсталирания на тях софтуер са потенциално уязвими за атаки;

• чрез скенери за слабите места - софтуер, който проверява големи групи от работни станции в търсене на слаби места към конкретен вид атаки;

• чрез разбивачи на пароли - софтуер, който открива лесно разгадаеми пароли в кодираните файлове с пароли;

• чрез мрежови анализатори (снифери) - софтуер, прослушващ мрежовия трафик и имащ възможност за автоматично отделяне на имена на потребители и пароли от трафика;

• модификация на предаваните данни или подмяна на информацията;

• подмяна на доверения обект с лъжлив обект.

Форма на атака срещу сигурността на системата е и т.нар. "социално инженерство" - получаването на несанкциониран достъп до информация по друг начин, без разбиване на програмното обезпечаване. Целта е да се надхитрят хората, за да се получат паролите за достъп до системата или друга информация, помагаща да се наруши сигурността й.

Голямо е разнообразието на ***атаките срещу компютърните мрежи***, които могат да бъдат разделени на две големи групи:

• пасивно подслушване на мрежата - наблюдение на потока от съобщения, без намеса в него;

• активно подслушване на мрежата - включва някои видове обработка на съобщенията (съобщенията могат да бъдат избирателно променяни, изтривани, забавяни; промяна на реда или дублиране и повтаряне по-късно; повторно изпращане; вмъкване на фалшиво съобщение; IP измами и други).

За получаване на информация, нарушителите могат да използват ***специални методи и технически средства***, които са:

• специално внедрени електронни средства, разрушаващи или изкривяващи информацията;

• средства, предаващи обработваната в автоматизираната информационна система или мрежа информация или речева информация - разговори в помещенията, в които се намират работните станции;

• облъчване на техническите средства на автоматизираната информационна система или мрежа със сондиращи сигнали;

• разрушаване на елементите на хардуера чрез подаване на високо напрежение и други.

Най-ефективните методи за получаване на конфиденциална информация са акустичният контрол и подслушване на разговорите по комуникационните линии.

От изложението до сега могат да се направят следните изводи:

1. Защитата на информацията в АИС или мрежи изисква комплексен подход – изгражданата система за защита на информацията трябва да отговаря на изискванията за цялостност, за да бъдат обхванати дефинираните при анализа на риска възможни заплахи и атаки системите.

2. Изграждането на системата за защита на информацията е планомерен процес, който изисква задълбочен анализ, детайлно планиране, акуратно изпълнение и последващо поддържане на системата за защита в синхрон с настъпилите изменения в конфигурацията на системата или условията на средата за взаимодействие.

3. Системата за защита на информацията в АИС или мрежи изисква устойчиво управление, като за целта в организацията е необходимо наличието на специализирана служба по сигурността на информацията и определени длъжностни лица, отговарящи за сигурността на информацията в АИС или мрежи.

III. Инициативи на НАТО в областта на киберзащитата

За постигане на способности за киберзащитата НАТО предприе множество политически инициативи.

• Prague Summit 21 September 2002 – взето е решение за усилване възможностите на Алианса за противодействие срещу кибератаки.

• Riga Summit 29 November 2006 – взето е решение за подобряване възможностите за защита на информационните системи с критично значение срещу кибератаки.

• Strasbourg-Kehl Summit 4 April 2009 - в съответствие с одобрените Политики за кибер-защита, е създадена NATO Cyber Defence Management Authority, подобриха се съществуващите възможности за отговор на компютърни инциденти и беше активиран Съвместен център за изследване и обучение на НАТО в Естония.

• На последната среща на върха в Лисабон киберзащитата е изведена като приоритет на НАТО и са заявени Амбиции за обединяване на отделните национални проекти за киберзащита с цел съкращаване времето за разработването им и намаляване на разходите.

В резултат на политическите инициативи НАТО предприе и конкретни действия в тази област.

• През 2002 г. НАТО одобри Програма за киберзащита, включваща три етапа:

Първи етап (NCIRC – IOC) инициращ - за постигане на съюзни способности за реагиране на компютърни инциденти.

Втори етап (NCIRC – IDS IOC) за елиминиране на слаби места в киберзащитата и използване на нови технологии за редуциране на риска.

Трети етап (NCIRC – FOC) финален - за достигане на пълни оперативни способности.

• През 2008 г. (януари) на срещата на високо равнище на НАТО в Букурещ беше утвърдена официалната политика на НАТО в областта на киберсигурността.

• През 2008 г. (април) беше одобрена Съвместната концепция за киберзащита.

• През 2008 г. (август) НАТО утвърди Указания за сътрудничество в областта на киберзащитата с партньори и международни организации.

• През 2008 г. НАТО ситуира орган за Управление и Ръководство на киберзащитата NCDMA (NATO Cyber Defence Management Authority) с борд NCDMB (NATO Cyber Defence Management Board).

• През 2008 г. НАТО сертифицира CCD COE в Естония, като научно-приложно звено по проблемите на киберсигурността.

• През 2009 г. (април) НАТО прие Рамка за сътрудничество в областта на киберзащитата със страните партньори.

• През 2009 г. НАТО проведе второто учение по киберзащита NCDEX 09.

• През 2010 г. НАТО създаде нова дирекция в Международния секретариат ESCD (Emerging Security Challeng Division) по проблемите на тероризма, разпространението на ОМП, енергийната сигурност и киберотбраната.

• През 2010 г. (септември) – по време на годишния симпозиум на НАТО по информационна сигурност в Монс, Агенцията NC3A анонсира документ (White Paper) – Multinational Cyber Defence Programme

• През 2010 г. (ноември) в Монс, Белгия НАТО проведе третото учение по киберзащита Cyber Coalition 2010, където експерти на МО взеха участие като Наблюдатели.

• През 2010 г. (ноември) експерти от МО в състава на междуведомствена работна група, след съгласуване с НАТО изготвиха финалния вариант на Меморандум за разбирателство между Р България и НАТО, който на практика ще позволи споделянето на информация и услуги свързани с киберзащитата.

С подписването на Меморандум за разбирателство между Република България и НАТО, създаващ правната рамка за сътрудничество в областта на кибернетичната защита ще бъде постигнато:

• разширяване на националните възможности за кибернетична защита;

• повишаване на оперативната съвместимост между Националния орган за кибернетична защита и НАТО (NCDMA);

• подобряване на възможностите за предсказване, откриване и реагиране срещу кибератаки;

• обмен на информация за кибернетичната защита на реципрочна и балансирана основа.

3.1. Структури на НАТО имащи отношение по киберзащитата

• ESCD (Emerging Security Challeng Division).

• Strategic Commands.

• NCDMA/NCDMB – Орган за Ръководство и Управление на киберзащитата в НАТО.

• NC3A/NC3B – Агенцията на НАТО за консултации, командване и контрол и съответно С3 Борда на НАТО.

• NCSA – Агенцията на НАТО за КИС.

• NIATC–Технически център на НАТО за информационна сигурност.

• CD CSC - NATO Cyber Defence Coordination and Support Centre.

• NCIRC – Център за отговор на компютърни инциденти.

• CCD COE – Център по компетентност за сътрудничество в киберзащитата/киберотбраната.

3.2. Организация на киберзашитата в някои страни членки на Алианса и по света

Структури на стратегическо ниво:

- Киберкомандвания – САЩ, Русия, Китай, Иран и др.
- Център за безопасност на виртуални операции – Великобритания.
- Департамент по информационни и компютърни мрежови операции - Германия.

Правителствени,ведомствени и военни центрове за киберзащита има в почти всички страни членки на НАТО.

В Република България:

- GOV CERT в МТИТС- статус "сертифициран".
- Център за Управление и Реагиране при Компютърни Инциденти (ЦУРКИ) в Министерство на отбраната, който е съвместим с NCIRC на НАТО. Центърът е изграден в съответствие с регламентиращите документи на НАТО и е предназначен за защита на критични за сигурността на информацията данни и сървери в АИС и мрежи на МО и БА. Планира се достигане на пълната функционалност на ЦУРКИ през 2013 г.

IV. Методология за изграждане на CERT (CERT/CC)

CERT или CERT/CC (Computer Emergency Response Team / Coordination Center) е екип от експерти по сигурността в областта на ИТ, чиято основна дейност е да реагира при кризисни ситуации в компютърната сигурност. Той предоставя необходимите услуги за справянето с тях и подпомага потребителите при възстановяване от пробиви. За смекчаване на рисковете и намаляване на броя на необходмите действия, повечето CERT предлагат на своите потребители както превантивни така и образователни услуги. Издават бюлетини за уязвимости в използвания софтуер и хардуер и също така уведомяват потребителите за експлойти и вируси, които се възползват от тези недостатъци. По този начин потребителите могат бързо да поправят и актуализират системите си. Ползването на специализиран екип по ИТ сигурността помага на организацията да смекчи и предотврати кризисни ситуации и помага за защитата на ценни активи.

Други предимства са:

- централизирана координация по въпросите на ИТ сигурността в рамките на организацията (контактно звено);
- централизирано и специализирано действие при/и в отговор на ИТ кризисни ситуации;
- налична експертиза за поддръжка и подпомагане на потребителите за бързо възстановяване от кризисни ситуации в сферата на сигурността;
- справяне с правни въпроси и запазване на доказателствен материал в случай на съдебен процес;
- проследяване на събития в областта на сигурността;
- стимулиране на сътрудничеството в областта на ИТ сигурността в рамките на групата потребители (повишаване на информираността).

При създаването на CERT е много важно бързо да се разработи ясна визия за това кои са потребителите и за какъв тип среда ще бъдат предлагани услугите на CERT. В момента се наблюдават отделни „сектори" където са фокусирани CERT.

В зависимост от това за кой сектор е фокусиран CERT се определят потребите-

лите, както и комплекта предоставяни услуги.

Така например CERT за академичния сектор предлага услуги на академични и учебни заведения като университети или изследователски центрове в интернет средата на района на учебното заведение, като типичните потребители на този тип CERT са университетските служители и студенти.

CERT във военния сектор предоставя услуги на военни организации с отговорности за необходима за отбранителни цели ИТ инфраструктура с потребители служителите на военни институции или тясно свързани органи, например Министерство на отбраната.

Националния CERT се счита за контактно звено по сигурността на информацията за страната. Обикновено този вид CERT няма преки потребители и играе само ролята на посредник (дистрибутор) за цялата страна.

Комплекта услуги, който предоставя съответния CERT на потребителите в зависимост от сектора към който е фокусиран е различен и включва следните типове услуги : (таблица 1)

Реактивни услуги	**Проактивни услуги**	**Справяне с артефакти**
1.Сигнали и предупреждения 2.Справяне с инциденти 3. Анализ на кризисни ситуации 4. Поддръжка при действие при кризисни ситуации 5. Координация на действие при кризисни ситуации 6. Действие на място при кризисни ситуации 7. Справяне с уязвимост 8. Анализ на уязвимост 9. Действие при уязвимост 10. Координация на действие при уязвимост	1. Съобщения 2. Наблюдение на технологиите 3. Одити и оценки на сигурността 4. Конфигурация и поддръжка на сигурността 5. Разработване на инструменти по сигурността 6. Услуги по откриване на пробиви 7. Разпространяване на информация, свързана със сигурността.	1. Анализ на артефакти 2. Действие при артефакти 3. Координация на действия при артефакти
Управление на качеството на сигурността		
1. Анализ на риска 2. Непрекъснатост на бизнес процеса и възстановяване от бедствия 3. Консултации по сигурността 4. Повишаване на информираността 5. Образование/ обучение 6. Оценка или сертификация на продукт		

Централни услуги (отбелязани с по-тъмен шрифт в таблицата): прави се разлика между реактивни и проактивни услуги. Проактивните услуги целят да предотвратят кризисни ситуации чрез повишаване на информираността и обучението, докато реактивните имат за задача да се справят с кризисни ситуации и да смекчат произтичащите от тях вреди.

Справянето с артефакти обхваща анализа на всякакви файлове или предмети, открити в дадена система, които може да са замесени в зловредни действия, като останки от вируси, червеи, скриптове, троянски коне и др. Включва и обработката и разпространението на произтичащата от това информация към дистрибутори и други заинтересовани страни с цел да се предотврати по-нататъшното разпростра-

няване на малуер и да се намалят рисковете.

Услугите по управление на качеството на сигурността са услуги с по-дългосрочни цели и включват консултации и образователни мерки.

От изключително важно значение при изграждането на CERT е извършването на анализ на потребителите и определяне мисията на CERT, като основната цел е да се изберат правилните комуникационни канали, а именно:

- определяне на комуникационния подход към потребителите;
- определяне на мисията на центъра;
- изготвяне на реалистичен план за реализация на проекта;
- определяне на услугите на CERT;
- определяне на организационната структура;
- определяне на политиката по информационна сигурност;
- набиране на подходящи служители;
- използване на офиса на CERT;
- търсене на сътрудничество с други CERT и възможни национални инициативи.

В този смисъл, много важно е да се познават нуждите на потребителите, както и собствената комуникационна стратегия, която включва и комуникационните канали, най-подходящи за предоставяне на информация към тях.

В теория на управлението са известни няколко възможни подхода към този проблем, като всички те се базират на анализ на целевата група на основата на SWOT и PEST анализи.

Обикновено CERT работят с комплект от комуникационни канали, най-използваните от които са:

- обществено достъпен уебсайт;
- затворен сектор за членове в рамките на уебсайта;
- уеб формуляри за докладване за кризисни ситуации;
- мейлинг листи;
- индивидуална електронна поща;
- телефон / факс;
- SMS;
- „старомодни“ писма на хартия;
- месечни или годишни доклади.

Освен електронна поща, уеб формуляри, телефон или факс за улесняване на справянето с кризисни ситуации (за да получават доклади за кризисни ситуации от потребителите, да координират с други центрове или да предоставят обратна връзка и поддръжка на жертвата) много CERT публикуват свои бюлетини по сигурността на уебсайт, достъпен за обществеността и чрез мейлинг листи.

След анализа на нуждите и желанията на потребителите по отношение на услугите на CERT следващата стъпка следва да бъде изготвянето на мисия на центъра. Мисията описва основната функция на организацията в обществото по отношение на продуктите и услугите, които предлага на потребителите си. Това позволява ясното представяне на съществуването и работата на изграждания CERT. Добра практика е текстът на мисията да е компактен, но не прекалено сбит, защото той обикновено остава непроменен в продължение на няколко години.

Тук е представен пример за текст на мисия на CERT: „***CERT осигурява инфор-***

мация и съдействие на своите потребители при прилагането на проактивни мерки за намаляване на рисковете от кризисни ситуации в компютърната сигурност, както и при действие при подобни кризисни ситуации, когато те възникнат.“

Следващата стъпка е да се определи бизнес планът и се предложи финансов модел, а именно какви параметри на предлагане на услугата са както подходящи, така и рентабилни. За целта се използват съответно финансов модел на разходите и финансов модел на приходите. При финансовия модел на разходите двата основни фактора, които влияят върху разходите, са определянето на работното време за обслужване на потребителите и броя (и качеството) на служителите, които следва да бъдат наети. Необходимо ли е да се осигурява действие при кризисни ситуации и техническа поддръжка 24x7, или тези услуги могат да се предлагат в традиционното работно време? Един от възможните сценарии е предоставянето на проактивни услуги и действие в традиционното работно време. Извън работното време ще бъдат предлагани единствено ограничени услуги от дежурен служител на повикване, като например единствено в случай на значителни бедствия и кризисни ситуации.

Друга възможност е да се търси международно сътрудничество с други CERT центрове. Това намалява разходите, защото екипите винаги работят само в традиционно работно време и също така предлагат услуги на „спящата част“ от света.

Особено добра практика е подробно да се анализира необходимостта от услуги 24x7 сред потребителите. Няма голям смисъл в изпращането на сигнали и предупреждения през нощта, когато получателят ще ги прочете едва на сутринта. Съществува тънка граница между „да имаш нужда от услуга“ и „да искаш услуга“, но специално работните часове водят до голяма разлика в броя на служителите и необходимото оборудване и по този начин оказват голямо въздействие върху модела на разходите.

При модела на приходите, когато разходите са известни, следващата добра стъпка е да се обмислят моделите за приходи: как могат да се финансират планираните услуги, като са възможни следните сценарии:

- сценарий с използване на съществуващи ресурси, при който винаги е от полза да се оценят вече наличните ресурси в други части на организацията. Има ли вече наети подходящи служители (например в действащия ИТ отдел) с необходимия опит и експертни познания? Вероятно с ръководството би могло да се уреди този персонал да бъде изпратен в CERT за началната фаза или при необходимост да осигурява поддръжка на CERT.
- сценарий основан на такса за членство, при който продавате Вашите услуги на потребители чрез годишна/ тримесечна такса за членство. Допълнителните услуги могат да се заплащат на база използването им, като например консултантски услуги или одити на сигурността. Друг възможен сценарий: услугите за (вътрешни) потребители се предоставят безплатно, но услугите за външни клиенти трябва да се заплащат. Друга идея е да се публикуват бюлетини по сигурността и информационни бюлетини на обществено достъпните уебсайтове и да има сектор „Само за членове“ със специална, по-подробна или специално изготвена информация. Доказано на практика е, че „абонаментът за услуга на CERT “ има ограничено значение за осигуряването на достатъчно финансиране, особено в началната фаза. Например, има фиксирани основни разходи за екипа и оборудването, които трябва

да се платят предварително. Финансирането на тези разходи чрез продажба на услуги на CERT е трудно и изисква много подробен финансов анализ, за да се открие „критичната точка“.

- сценарий основан на субсидия, при който се кандидатства за субсидия за проект, отпусната от правителството или правителствен орган.
- комбиниран сценарий, когато се съчетават преимуществата на изброените по-горе.

Следващата стъпка при изграждането на CERT е свързана с определянето на организационната структура, която зависи до голяма степен от съществуващата структура на организацията и потребителите, както и от наличието на квалифицирани експерти, които да бъдат наети за постоянно или временно.

Типичният CERT определя следните роли в рамките на екипа:

Обща:

- Генерален мениджър

Служители

- Офис мениджър
- Счетоводител
- Консултант по комуникации
- Юрист

Оперативен технически екип:

- Ръководител на техническия екип
- Технически сътрудници на CERT, които предоставят услугите
- Изследователи

Външни консултанти:

- Наемани при нужда

Възможни са няколко начина на организационно изграждане на CERT, които се основават на различни бизнес модели, а именно:

1. Независим бизнес модел, при който CERT е основан и действа като независима организация със собствено ръководство и служители;

2. Внедрен бизнес модел, който се използва, ако CERT е създаден в рамките на съществуваща организация, като например се използва съществуващ ИТ отдел. CERT се оглавява от ръководител на екипа и той/тя отговаря за дейностите на CERT. Ръководителят на екипа събира необходимите технически сътрудници при справянето с кризисни ситуации или работа по дейностите на CERT. Той или тя може да поиска съдействие за специализирана поддръжка в рамките на съществуваща организация;

3. Доброволен модел, при който група от хора (специалисти), се събират на доброволен принцип, за да предлагат взаимни съвети и подкрепа. Тази общност не е строго организирана и до голяма степен зависи от мотивацията на участниците.

След взимане на решение за услугите и степента на поддръжка, която ще се предлага и избирането на организационния модел, следващата стъпка е да се намерят подходящият брой квалифицирани служители за работата.

Почти невъзможно е да се представят точни цифри за броя на необходимите технически сътрудници от тази гледна точка, но следните ключови стойности са се доказали като добър подход:

- за да се предлагат две централни услуги като разпространяването на бюлетин по сигурността, както и справянето с кризисни ситуации - минимум 4 човека на

пълен работен ден;

• за пълно обслужване на CERT в традиционно работно време и поддръжка на системи - минимум от 6 до 8 човека на пълен работен ден;

• за пълна заетост със смени 24x7 (2 смени извън традиционното работно време) - минимум от около 12 човека на пълен работен ден.

Посочените цифри включват и резерви за случаи на болест, неработни дни и др. Необходимо е и да се направи справка с местните колективни трудови договори. Ако хората работят извън традиционното работно време, това би трябвало да доведе до заплащането на допълнителни суми.

Следва кратък преглед на основните (ключови) компетенции на техническите експерти за един CERT:

Лични умения

• Гъвкав, креативен дух и умение за работа в екип

• Силни аналитични умения

• Способност за обясняване на сложни технически въпроси на прост език

• Добро чувство за поверителност и работа по процедурния ред

• Добри организаторски умения

• Издръжливост при стрес

• Силни комуникативни умения и умения за писане

• Непредубеденост и желание за учене

Технически умения

• Широки познания в областта на интернет технологиите и протоколите

• Познания за системите Linux и Unix (в зависимост от оборудването на конституентите)

• Познания за системите Windows (в зависимост от оборудването на конституентите)

• Познания за оборудването на мрежова инфраструктура (рутер, контролери, DNS, Proxy, пощенски сървър и др.)

• Познания за интернет приложения (SMTP, HTTP(и), протокол за трансфер на файлове (FTP), telnet, SSH и др.)

• Познания за заплахите за сигурността (атака за отказ на услуга, фишинг, Defacing, „подслушване“ и др.)

• Познания за оценка на риска и практическо реализиране

Допълнителни умения

• Желание за работа на смени 24x7 или за дежурства на повикване (в зависимост от модела на обслужване)

• Максимално разстояние за пътуване (в случай на спешен случай в офиса, максимално време за пътуване)

• Степен на образование

• Опит в работата в сферата на ИТ сигурността.

По отношение на оборудването (хардуер и софтуер), както и използването на офис пространството и физическата сигурност, следва да се каже, че това са доста обширни теми, които са извън обхвата на настоящата методология.

Накрая, но не на последно място по важност е въпроса свързан с разработването на политика в областта на информационната сигурност в зависимост от вида CERT.

Политиката освен да описва желаното състояние на оперативните и административни процеси и процедури, трябва да е съгласувана със законодателството и стандартите, по-специално по отношение на материалната отговорност на CERT. Обикновено CERT е обвързан с националните закони и нормативни актове, които често се прилагат в контекста на европейското законодателство (обикновено директиви) и други международни споразумения. Стандартите не винаги са с пряк задължителен характер, но може да се нареждат или препоръчват от закони и нормативни актове. По-долу е представен кратък списък с възможни закони и политики:

Национални:

- Различни закони относно информационните технологии, телекомуникациите и медиите.
- Закони за защита на данните и правото на неприкосновеност на личния живот.
- Закони и нормативни актове за съхранение на данни.
- Законодателство за финанси, счетоводство и корпоративно управление.
- Етични кодекси за корпоративно управление и управление на ИТ.

Европейски:

- Директива относно електронните подписи (1999/93/ЕИО).
- Директивите относно личните данни (1995/46/ЕО) и правото на неприкосновеност на личния живот в сектора на електронните комуникации (2002/58/ЕО).
- Директиви относно електронните съобщителни мрежи и услуги (2002/19/ЕО – 2002/22/ЕО).
- Директиви относно корпоративно право (например 8-ма директива по корпоративно право).

Международни:

- Споразумението Базел II (специално по отношение на управление на операционен риск).
- Конвенция за киберпрестъпленията на Съвета на Европа.
- Конвенция за защита на правата на човека на Съвета на Европа (член 8 относно правото на зачитане на личния живот).
- Международни счетоводни стандарти (МСС, те до известна степен определят контрола в областта на ИТ).

Стандарти:

- Британски стандарт BS 7799 (информационна сигурност).
- Международни стандарти ISO 2700x (системи за управление на информационната сигурност).
- Най-основните въпроси, на които трябва да се даде отговор при Вашата политика за информационна сигурност при боравене с информация са:
- Как се „маркира“ или „класифицира“ входящата информация?

- Как се работи с информацията, и по-специално по отношение на ограничения достъп?

- Какви съображения са приети за разкриването на информация, по-специално ако информация, свързана с кризисна ситуация е предадена на други центрове или звена?

- Има ли правни съображения, които да се вземат предвид по отношение на работата с информация?

- Следвате ли определена политика относно използването на криптография за

защита на ограничения достъп и интегритета в архиви и/или при съобщаването на данни, особено по електронна поща?

- Тази политика включва ли условия за правни граници като криптосистема с ключ в трета страна или налагане на разшифроване в случай на съдебни процеси?

V. Заключение

В заключение могат да се направят следните изводи:

• На срещата на високо равнище на страните членки на Алианса, която се проведе в Лисабон през м. ноември се потвърди, че киберсигурността е един от приоритетите на новата Стратегическа концепция на НАТО.

• Политиката на Алианса в областта на кибернетичната защита цели осигуряване на единен и координиран подход при защитата на ключовите информационни системи на НАТО и отделните страни членки от кибератаки, както и споделяне на най-добрите практики и предоставяне на способности за подпомагане на съюзниците при отправяне на молба за взаимопомощ. Създадените структури и органите функционират и непрекъснато се развиват с ниво на амбиция да достигнат пълната си функционалсност до 2013 г.

• За Р. България е необходимо своевременно, в контекста на Стратегията за национална сигурност, да бъде разработена Национална стратегия за кибернетична сигурност, където ясно да бъдат регламентирани целите, отговорностите и структурите.

• Сериозността на заплахите от кибератаки за националната сигурност налага консолидацията и координирането на усилията на всички заинтересовани структури в държавата (министерства, агенции, бизнеса, академичната общност и др.) в тази област.

• Министерство на отбраната възстановява традициите на научни изследвания в областта на информационната сигурност и съобразявайки се с новите реалности в Европа и света предприема иновационни програми за изследване и изучаване на новите методи и средства за водене на съвременни информационни операции и кибервойни и начините за защита от тях.

ДЪРЖАВНАТА ПОЛИТИКА ПО ЗАЩИТА НА ИНФОРМАЦИЯТА В НАЧАЛОТО НА 21 ВЕК

Васил А. Грънчаров

Директор на дирекция „Информационни и комуникационни системи", Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи"

STATE POLICY ON INFORMATION SECURITY IN THE BEGINNING OF THE 21ST CENTURY

Vasil A. Grancharov

Director of Information and Communication Systems Directorate Executive Agency "Electronic Communication Networks and Information Systems"

***Abstract**: In the lecture the author gives a short overview of state policy on the information security. The main topics covered include national legislation, activities on establishment and development of the Governmental CERT and involvement in European Union, NATO and global initiatives.*

***Keywords**: Information security, Cyber security, CERT.*

Комуникационните мрежи и информационните системи са станали съществен фактор в икономическото и общественото развитие. Тяхната сигурност става все по-голяма грижа на обществото поради възможността за възникване на проблеми в ключови системи, свързани с обществения живот като: аварии, грешки и атаки, които могат да имат последствия за физическите инфраструктури, явяващи се критични за обществения живот и за гражданите.

Значението на мрежовата и информационна сигурност нараства неимоверно в последните години, защото информацията винаги е била и остава най-търсената и скъпа стока, а това особено важи за съвременното информационно общество.

Какво представлява информационната сигурност?

Информационната сигурност е защитата на информацията от широк кръг заплахи, за да се гарантира непрекъсваемостта на работните процеси, да се минимизират загубите при аварии, инциденти и природни бедствия и да се максимизира възвращаемостта на инвестициите.

Според синхронизирано с терминологията на Европейската комисия „мрежовата и информационната сигурност" е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействие или на случайни събития, които могат да нарушат **наличността** (достъпността и автентичността), **интегритета** и **конфиденциалността** на съхраняваните или предаваните данни и на услугите, свързани с тези мрежи и системи.

Под **конфиденциалност** се разбира, че не трябва да се допуска разкриването на информацията от потребител, които не е оторизиран да има достъп до нея, а за **цялостност (интегритет)** – информацията не трябва да бъде компрометирана или да се допускат неоторизирани (преднамерени или случайни) промени в нея.

Наличност означава, че хардуер и софтуер работят ефикасно и системата има възможност да се възстанови бързо и цялостно, ако възникне инцидент.

Информационната сигурност това е комплексно понятие и не бива да се изключва и взаимодействието с човешкия фактор.

Всички информационни системи на административните органи трябва да отговарят на изискванията и политиката за мрежова и информационна сигурност с оглед защитата им срещу неправомерен или случаен достъп, използване, правене достояние на трети лица, промяна или унищожаване, доколкото такива събития или действия могат да нарушат достъпността, автентичността, целостта и конфиденциалността на съхраняваните или предаваните данни, а също така на предоставяните електронни услуги, свързани с тези мрежи и системи.

За постигане на мрежова и информационна сигурност ръководителите на администрациите провеждат собствена политика, съобразена със спецификата на административните процеси в конкретната администрация, като предприемат съответни административни и технологични мерки. Политиките на отделните административни органи и предприеманите мерки трябва да отговарят на общите принципи съгласно приложение № 1 от „Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (НОИОСИС)".

Документи от националното законодателство свързани с информационната сигурност:

А) За некласифицирана информация:

1. Закон за електронните съобщения, обн. ДВ. бр.41 от 22 май 2007 г. и последно изм. ДВ. бр.97 от 10 декември 2010 г.
2. Закон за електронното управление, в сила от 13.06.2008 г., обн. ДВ. бр.46 от 12 юни 2007 г., изм. ДВ. бр.82 от 16 октомври 2009 г.
3. Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, в сила от 25.11.2008 г., приета с ПМС № 279 от 17.11.2008 г., обн. ДВ. Бр.101 от 25 ноември 2008 г., изм. ДВ. Бр.58 от 30 юли 2010 г., изм. ДВ. Бр.102 от 30 декември 2010 г.

Б) За класифицирана информация:

1. Закон за защита на класифицираната информация, обн. ДВ. бр.45 от 30 април 2002 г., последно изм. ДВ. бр.23 от 22 март 2011 г.
2. Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, приета с ПМС № 99 от 10.05.2003 г., обн. ДВ. бр.46 от 20 май 2003г. и последно изм. ДВ. бр.101 от 18 декември 2009 г.
3. Наредба за криптографската сигурност на класифицираната информация, приета с ПМС № 263 от 11.11.2003 г., обн. ДВ. бр.102 от 21 ноември 2003г. и последно. ДВ. бр.5 от 19 Януари 2010 г.

Документи свързани с информационната/киберсигурността и задължения за държавната политика на Република България като член на НАТО, ЕС и Международния съюз по далекосъобщения.

Международни законови, нормативни и регулаторни изисквания и споразумения в областта на информационната/киберсигурността използвани в държавната политика.

I. Документи от националното законодателство свързани с информационната сигурност

Държавната политика в защитата на информацията това са системата от правила и мерки регламентирани в нормативни актове, регулиращи защитата на чувствителна информация, нарушаването на които води до носене на отговорност.

А) Документи по информационната сигурност за некласифицирана информация:

1. Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, в сила от 25.11.2008 г., приета с ПМС № 279 от 17.11.2008 г., обн. ДВ. Бр.101 от 25 ноември 2008 г., изм. ДВ. Бр.58 от 30 юли 2010 г., изм. ДВ. Бр.102 от 30 Декември 2010 г." (НОИОСИС)" е един от основните документи. Тя урежда:

- Общите изисквания за оперативна съвместимост и мрежова и информационна сигурност за нуждите на предоставянето на вътрешни електронни административни услуги и обмена на електронни документи между администрациите;
- Воденето, съхраняването и достъпът до регистъра на стандартите;
- Начинът на акредитация на лицата по чл. 57, ал. 1 от Закона за електронното управление и изискванията към тяхната дейност;
- Методиката за извършване на оценка за съответствие с изискванията за оперативна съвместимост и мрежова и информационна сигурност;
- Изискванията за водене, съхранение и достъп до списъка на акредитираните лица по чл. 57, ал. 1 от Закона за електронното управление и до списъка на сертифицираните информационни системи.

Наредбата не урежда мрежовата и информационната сигурност на информационните системи на административните органи и правилата за информационна сигурност при използване на класифицирана информация.

В НОИОСИС е посочено кой извършва контрол по спазването на изискванията за оперативна съвместимост и мрежова и информационна сигурност – това е министърът на транспорта, информационните технологии и съобщенията в изпълнение на чл. 60 от Закона за електронното управление и в съответствие с утвърдена от него Методика за текущ контрол на оперативна съвместимост и мрежова и информационна сигурност.

НОИОСИС се състои от следните основни раздели:

1.Общи положения.

2.Оперативна съвместимост.

3.Информационна сигурност.

4.Регистър на стандартите.

5.Акредитация на проверяващи лица.

6.Сертификация за оперативна съвместимост и информационна сигурност. Методика за сертификация.

7.Списък на акредитираните лица и списък на сертифицираните системи и продукти.

2.Законът за електронното управление, приет през 2007 г., урежда дейността на административните органи при работа с електронни документи, предоставянето на административни услуги по електронен път и обмена на електронни документи между административните органи.

В глава четвърта на закона „Оперативна съвместимост и информационна си-

гурност", ясно се регламентират изискванията за постигане на мрежова и информационна сигурност в информационни системи на административните органи.

В същата глава Законът посочва държавния орган, отговорен за разработването и провеждането на политиката в областта на мрежовата и информационна сигурност, включително за упражняването на контрол.

Практиката на автономно развитие на информационни системи във всяка отделна администрация и изискването на Закона за еднократно въвеждане на данни от гражданите и фирмите предизвиква необходимост от интензивен информационен обмен между административните системи създава нов тип заплахи като:

– пренос на уязвимост от една система в друга;

– блокиране на електронна административна услуга на една система при нарушена достъпност на друга и пр.

Ето защо постигането на определено приемливо ниво в мрежовата и информационна сигурност на всички системи в държавата става задължително условие за взаимодействието им.

Б) Документи по информационната сигурност за класифицирана информация:

Държавната политика в областта на информационната сигурност по **отношение защита на класифицираната информация** е регламентирана в:

1. Закон за защита на класифицираната информация.
2. Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация.
3. Наредба за криптографската сигурност на класифицираната информация.

Тази политика е във функциите и задълженията на Държавната комисия по сигурността на информацията.

II. Документи, свързани с информационната/киберсигурността и задължения за държавната политика на Република България като член на НАТО, ЕС и Международния съюз по далекосъобщения

Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" координира основните дейности по киберзащитата на публичните мрежи на държавните институции и изпълнява задълженията на Република България като член на НАТО, ЕС и Международния съюз по далекосъобщения (МСД). Тези дейности са в основата на държавната и националната политика в тази област.

Кратко определение за **киберсигурността** – това са мерките, които се предприемат за защита на компютрите или компютърните системи срещу нерегламентиран достъп или атака или защита на данните в компютрите и компютърните системи работещи в мрежи.

Много автори, не посочват разлики между информационна и киберсигурност и смесват двете понятия така, че по общо може да се говори за информационна и киберсигурност като едно понятие, но трябва да се прави разграничение на двете.

Погледнато от друга страна киберсигурността има и своето политическо измерение, намерило отражение блокирайки дейностите на правителствени и обществени учреждения и организации в – Естония през 2007 г. и Грузия-2008 г.

Преглед на киберсигурността направи и президентът на САЩ Барак Обама по повод 60 дни от встъпването си в длъжност, като заключи, че „кибер заплахите са едни от най-сериозните предизвикателства за икономиката и националната сигур-

ност, пред които САЩ се изправя като нация" и че „икономическото благоденствие на Америка през 21-ви век ще зависи от киберсигурността". Тези думи са подплатени и с конкретни действия – извършване на цялостен преглед на политиката в киберпространството (Cyberspace Policy Review), последван от Всеобхватна инициатива за национална киберсигурност (Comprehensive National Cybersecurity Initiative). Предприети са и съответни институционални мерки – назначаване на Координатор по киберсигурност и създаване на Офис по киберсигурност в рамките на Щаба по национална сигурност. Барак Обама подчертава и стратегическата роля на комуникационно-информационната инфраструктура за повишаване на ефективността на икономиката за осигуряване на икономически просперитет, както и произтичащите отговорности на правителството за преодоляването на уязвимостите в киберпространството.

Все още не е разработена **Национална стратегия за киберсигурност**, определяща отговорностите и ресурсите по киберсигурността на държавно ниво. Предвидено е същата да се разработи в рамките на проект изпълняван по Оперативна програма „Административен капацитет", от МТИТС.

Като пълноправен член на НАТО от 2004 г. България се включва активно в дейностите на политическото и военното ръководство на Алианса в областта на киберсигурността.

НАТО през 2005 г. осъзнава важността и започна активна дейност в областта. Започва се подготовка на основополагащи документи по киберсигурността, изготвят се политики и дейности срещу последствията от кибертероризма, както се определя и необходимостта от създаването на Екипи за реагиране срещу компютърни инциденти (CERTs). Поради тази причина в рамките на CCPC (Civil Communication Planning Committee – Комитет по планиране на гражданските комуникации) и NC3B (NATO Consultation, Command and Control Board – Комисия на НАТО за консултации, командване и управление), където участват и представители на България е разработен документ „Последствия върху гражданското аварийно планиране от кибератаки/информационна война върху критичната гражданска комуникационна инфраструктура и услуги, и последствия върху гражданското аварийно планиране, и създаване на граждански екипи за реагиране при компютърни инциденти". Материалът обединява две теми (информационна и киберсигурност), но тежестта пада върху необходимостта, структурата и задачите на **екипите** за реагиране при компютърни инциденти в съвременните комуникационни и информационни мрежи.

Активни действия по отношение на киберсигурността НАТО предприема след атаките срещу информационните системи в Естония през 2007 г., като приема Доктрина и Политика в областта на кибесигурността и създава Орган за управление на киберзащитата към НАТО (NATO CDMA – Cyber Defence Management Authorities). Новите атаки срещу информационните системи в Грузия през 2008 г., показват че успешен отпор срещу такива атаки е възможен само въз основа на широко сътрудничество между правителство, частен сектор и неправителствени организации. В резултат на такова сътрудничество в Естония е създаден Център за компетентност на НАТО (NATO Centre of Excellence) по въпросите на киберсигурността.

Сериозно внимание на киберсигурността е отделено и в „Декларацията за сигурност на Алианса", приета на Срещата на върха в Страсбург/Кел и в „Стратеги-

ческата концепция на НАТО-2010" приета в Лисабон миналата година.

В момента на страните-членки на НАТО е разпратен проект на Меморандум за разбирателство и сътрудничество в киберсигурността между Органа на НАТО за управление на киберзащитата и националните органи по киберсигурност. Този документ ще формализира обмена на информация за киберсигурност, обменът на услуги за киберсигурност и участието в дейности по киберсигурност на държавите-членки на НАТО. Създадена беше междуведомствена работна група с представители на МТИТС, МО, ДАНС и ДКСИ, чиято задача бе да подготви условията за подписване на този меморандум. Очаква се в най-скоро време той да бъде подписан от министъра на транспорта, информационните технологии и съобщенията и председателя на ДАНС за България и съответно от представител на Офиса по сигурността на НАТО (NATO Office of Security – NOS)

Като член на Европейския съюз от 2007 г., България участва активно в дейностите на Европейската комисия в посока за повишаване на информационната сигурност. Тези дейности бяха особено активни през 2009 г. В Съобщение от Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета за регионите за защита на критичната информационна инфраструктура COM(2009) 149 „Защита на Европа от широкомащабни кибератаки и нарушения, повишаване на готовността, сигурността и устойчивостта" визира конкретни действия за повишаване на готовността, сигурността и устойчивостта, свързани със защита на критичната информационна инфраструктура.

Изискванията към мрежовата и информационната сигурност са конкретизирани и в Резолюция на Съвета на ЕС от 18 декември 2009 г., относно Европейски подход на сътрудничество към мрежовата и информационната сигурност. Основните насоки на дейностите са фокусирани към:

– Повишаване на доверието на крайните потребители към информационните и комуникационните технологии чрез дейности за повишаване на информираността;

– Организиране на национални учения и/или участие в редовни европейски учения в областта на мрежовата и информационната сигурност, включващи разширено планиране и привличане на частния сектор;

– Създаване до края на 2011 г. на добре функциониращи Центрове за реагиране при компютърни инциденти (CERTs) и засилване на сътрудничеството между националните центрове на европейско ниво;

– Изпълнение на програми за образование, обучение и изследвания за мрежовата и информационната сигурност, осигуряващи наличието на технически умения и професионализъм в тази област.

През 2008 г. в резултат на задълбочена и продължителна дейност с помощта на „Инструмент за самооценка на националната киберсигурност/критична информационна инфраструктура" на Международния съюз по далекосъобщения (МСД), беше направена оценка на киберсигурността в България. На основа на документа Работна група под ръководството на Държавната агенция за информационни технологии и съобщения – ДАИТС (сега Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи – ИА „ЕСМИС"), включваща представители на ДАИТС, Комисията за регулиране на съобщенията, Комисията за защита на личните данни, Държавната комисия по сигурност на информацията, Министерството на държавната администрация и административната реформа, Държавната

агенция „Национална сигурност", Министерството на вътрешните работи и Министерството на правосъдието, направи оценка на киберсигурността в България.

В резултат от оценката, бяха направени предложения по съответните елементи на националната рамка по киберсигурност - идентифициране на водеща институция за създаване и прилагане на Национална стратегия за киберсигурност, механизми за получаване на информация от индустрията, възпрепятстване на киберпрестъпления, създаване на Национален Център за реагиране при компютърни инциденти (CERT), развиване на Национална култура на киберсигурност.

Разбира се, необходимостта от създаване на национални центрове за реагиране при компютърни инциденти (CERTs) е осъзната открай време, както от НАТО, така и от ЕС. Основен инициатор на създаването на CERTs в държавите-членки е Европейската агенция за мрежова и информационна сигурност (ENISA). Главната мисия на ENISA е да повишава способностите на Общността и държавите-членки и следователно, бизнеса в тези държави, да предотвратяват, разглеждат и реагират на проблеми, свързани със сигурността на мрежите.

Отношенията на България с ENISA датират от края на 2006 г. Оттогава България има свой член в Управителния съвет на ENISA и национален представител за връзка.

В резултат на активното сътрудничество с ENISA и CERT-Hungary и благодарение на изпълнението на „Проект управление на мрежовата и информационната сигурност в структурите на държавната администрация", от есента на 2008 г. в България започна да действа правителствен Център за реагиране при компютърни инциденти (CERT). Към момента наборът на предлаганите услуги не е голям, но намерението е функционалностите му да бъдат постепенно разширени. През 2009 г. CERT България получи акредитация от Trusted Introducer, с което той беше официално приет в европейската CERT общност.

При изпълнение функциите на CERT съдействие оказва и Агенцията на НАТО за консултации, командване и управление (NC3A).

Други по-важни международни дейности, свързани с киберсигурността в които участваха представители на Република България са:

1. Министерската конференция за защита на критичната информационна инфраструктура, състояла се на 27-28 април 2009 г. в Талин, Естония, организирана от ЕК. На нея се подчерта необходимостта от мерки от страна на държавите-членки и заинтересованите страни за подобряване на готовността, сигурността и устойчивостта на критичните информационни инфраструктури като първа линия на защита и като здрава основа за повишаване на ефективността на борбата срещу киберпрестъпленията и кибертероризма.

2. Горните въпроси бяха и във фокуса на заседанието на Съвета по далекосъобщения, транспорт и енергетика, състояло се на 24 юни 2009 г., като основните изводи от него се свеждат до продължаване на диалога за мрежовата и информационната сигурност на европейско ниво, създаване на ясна и кохерентна стратегия, основана на координация и сътрудничество между държавите-членки, частния сектор и всички заинтересовани страни, обмен на информация и добри практики между държавите-членки, редовни учения за реагиране при инциденти в сигурността и възстановяване след бедствия, глобално сътрудничество в сигурността и устойчивостта на Интернет, продължаване на мандата на ENISA и разширяване на нейните ресурси.

3. Естествено продължение на Министерската конференция в Талин, 2009 г., е Конференцията на министрите по далекосъобщения за защита на критичната информационна инфраструктура, организирана от Унгарското председателство на Европейския съюз през април Унгария 2011 г. в Балатонфюред, Унгария. По време на дискусиите стана ясно, че два от въпросите, повдигнати на Талинската конференция, все още не са решени задоволително в европейски мащаб –има страни-членки, в които не са създадени Центрове за реагиране срещу компютърни инциденти (CERTs), редица страни-членки не организират национални учения по киберсигурност и не участват в пан-европейски учения. Наред с тези два въпроса, настоятелно беше посочена необходимостта от създаване на национални стратегии за киберсигурност, които ясно да очертаят отговорностите и ресурсите, нужни за осигуряване на по-високо ниво на киберсигурността и необходимостта от установяване на Публично-частни партньорства, като доказана ефективна форма на сътрудничество между обществения и частния сектор, и важността от разработване на национални аварийни планове за действия при кибер инциденти.

4. В края на миналата година в Организацията на обединените нации беше приета Резолюцията „Създаване на глобална култура на киберсигурност и оценяване на националните усилия за защита на критични информационни инфраструктури". Тук трябва да се подчертае, че Република България стана съвносител на тази резолюция, основавайки се до известна степен и на своя опит в областта на киберсигурността.

5. Като член на Международния съюз по далекосъобщения (МСД) България беше привлечена и в друга инициатива в областта на киберсигурността. Подписан е „Меморандум за разбирателство", с което България се присъедини към проекта „Международно многостранно партньорство срещу киберзаплахите (IMPACT)", създаден от МСД като част от инициативата „Дневен ред на глобалната киберсигурност (Global Cybersecurity Agenda)".

От ноември 2009 г. Изпълнителната агенция „Електронни съобщителни мрежи и информационни системи" поддържа постоянна връзка с Глобалния център за реагиране (GRC) на проекта IMPACT. Този център предоставя в реално време „Мрежова система за ранно предупреждение (NEWS - Network Early Warning System)", която помага за определяне на киберзаплахите в началото на деня и предоставя насоки за действие за предотвратяването им. GRC предоставя, също така и достъп до специализираната система „Електронно защитена приложна платформа за сътрудничество между експерти" (Electronically Secure Collaborative Application Platform for Experts - ESCAPE). ESCAPE дава възможност на IMPACT GRC да действа като център за координиране и реагиране при извънредни ситуации, което позволява бързото идентифициране и споделяне на наличните ресурси зад граница.

III. Международни законови, нормативни и регулаторни изисквания споразумения в областта на информационната/киберсигурността, използвани в държавната политика

Утвърдени стандарти за мрежова и информационна сигурност и най-добри световни практики са серията международни стандарти: ISO/IEC 27000: ISO 27000 – Принципи и речник; ISO 27001 – ISMS изисквания (BS7799 – Част 2); ISO 27002 – (ISO/ IEC 17799:2005) ISO 27003 – ISMS Ръководство за приложение (2007) ISO 27004 – ISMS Метрики и измерване (2007) ISO 27005 – ISMS Управление на риска

ISO 27006 – 27010 – за бъдещо ползване; CoBit и др. намиращи отражение в дейностите на експертите по информационна сигурност.

ISO 27001:2005 е основният международен стандарт за осигуряване на модел за създаване, изпълнение, функциониране, наблюдение, преглед, поддържане и подобряване на системата за управление на сигурността на информацията (СУСИ).

В заключение, в условията на глобално развитието на информационните технологии за мениджърите и експертите, отговорни за информационната/ киберсигурността е от важно значение добрата информираност за актуалните технологични подходи и решения, които ще им помогнат да вземат най-правилните решения за постигане на по-голяма сигурност и изграждане на доверие в „дигиталния" свят.

ДЪРЖАВА И СИГУРНОСТ

ИНФОРМАЦИОННИЯТ ДИЗАЙН – НЕОБХОДИМОСТ И ЗНАЧЕНИЕ ЗА БИЗНЕСА И СИГУРНОСТТА И ОТБРАНАТА

Ваня К. Банабакова, Марин Т. Петков, Атанас Г. Панев

Национален Военен Университет, Велико Търново,
e-mail: v_banabakova@abv.bg

INFORMATION DESIGN – NECESSITY AND IMPORTANCE FOR THE BUSINESS AND SECURITY AND DEFENCE

Vania K. Banabakova, Marin T. Petkov, Atanas G. Panev

ABSTRACT: *The activity of the Information design consist in a process of precise structure of the information, its organizing in clear navigation scheme and its attractive presentation by intuitive and unambiguous visual elements. The final aim is to allow the information to be easy to understand, reach and control. The aim of the present development is to analyze the special features of the information design and on that ground to recover its significant for business, for security and for defense and also the methods and the rules for its effective functioning.*

KEY WORDS: *information design, information system, consumer, business, security, defense.*

Достъпът до различни информационни източници, трансформиране и мигриране на данни са основните причини, определящи необходимостта от интеграция на информацията. За да не се губи от стойността и информацията, се изисква времето между съответното действие и реакция да бъде минимално, което налага интеграцията на данните да бъде в реално време. „Когато се ползват компютри, всяко нещо е информация”[1]. Да се предоставят подходящите данни и необходима информация синтезирано, в добър визуален вид и в подходящия момент на потребителите, изглежда лесно, но реално се превръща в непреодолим проблем за все повече организации. През последните години, с развитието на науката за управлението, концепцията за информацията бележи съществено развитие. Трактовката на кибернетиката, че информацията е средство за отстраняване на неопределеността на системата, се развива и се свързва с процеса на вземане на решение. Подчертава се, че информацията всъщност представлява съвкупност от данни, съответстващи на дадено управленско решение, т.е. данни, обработени с определена цел. Както става ясно, информацията се свързва с нейното подготвяне (преработването на данните) за удовлетворяване на потребителите. По този начин се акцентира върху предназначението ѝ, като крайният потребител определя доколко обработените данни съдържат информация. Очевидно, превръщането на данните в информация в

резултат на обработването им с определена цел зависи пряко от изискванията на управленското решение. Измененията в природата на информационната дейност в мениджмънта през последните години са свързани с широкото разпространение на информационните технологии. Прилагането на компютри за предоставяне на необходимата в бизнеса информация революционизира мениджърската дейност.

Ефективната организация на информацията е необходима не само за бизнеса, но и в сферата на сигурността и отбраната.

В Министерството на отбраната (МО) и Българската армия (БА) се цели изграждане на единна информационна среда, която следва да се разглежда като неотменима част от процеса на трансформация, осигуряваща ефективно функциониране на системата за командване и управление. [5] Във въоръжените сили са стартирали проекти за развитие на информационните системи, свързани с автоматизиране на управленската дейност и повишаване на информационната осигуреност. Завършването на тези проекти до 2014 г. следва да осигури използване на единна информационна среда, съкращаване на времето и разходите за документооборота. Изграждaната информационна среда на МО и БА си базира на съществуващите сегменти на публичната мрежа „Интернет" и ведомствената мрежа „Автоматизирана информационна система на Българската армия" (АИС на БА) за обмен на класифицирана информация, осигуряваща набор от стандартни услуги за общ достъп (електронна поща, WEB и други), както и достъп до вътрешноведомствени информационни системи.

От 2011 г. в АИС на БА има готовност да се поддържа инфраструктура с използване на публичен ключ, поддържаща всички стандартни функции, базирани на цифрови сертификати и електронния подпис.

Планира се и развитие на системата за обмен на военни съобщения по стандарт на НАТО, в основата на която е стандартната електронна пощенска услуга в своята пълна функционалност.

Автоматизираната информационна система на Българската армия има за цел а осигурява разчетните, разчетно-аналитичните и справочни информационни системи на индивидуални и групови информационни услуги на голям брой поделения от състава на БА. В момента АИС на БА обхваща над 60 възела в различни поделения. [6] През настоящия период работата по АИС на БА е фокусирана върху поддръжката и експлоатацията на вече изградената инфраструктура и информационни подсистеми от една страна, а от друга – върху нейното развитие и модернизация. При поддръжката на част от съществуващата инфраструктура се използва аутсорсинг, на базата на сключените договори с външни фирми.

Експлоатацията на съществуващите системи – автоматизирана система за управление „Човешки ресурси", информационните системи „Логистика", „Труд и работна заплата", „Документооборот", „Информационни рубрики", „Оперативен архив", „система за наблюдение и управление" и други, до голяма степен облекчават и улесняват администрирането на процесите, управлението на движението на информационните потоци и изготвянето и разпространението на актуални и точни анализи за подпомагане на управленските решения.

В този смисъл като потребители на информация следва да разглеждаме както организациите в сферата на бизнеса, така и тези, свързани със сигурността и отбраната на страната.

Целта на настоящата разработка е да анализира особеностите на информацион-

ния дизайн и на тази основа да разкрие неговото значение за бизнеса и сигурността и отбраната, както и методите и правилата за ефективното му функциониране.

В съвременното общество все по-често се използва термина „Информационен дизайн", като под това понятие най – често се разбира електронните технологии и погрешно се идентифицира с Уеб дизайна, но това виждане е неточно. Информационната архитектура, наричана още "Информационен дизайн", „Информационно проектиране" или "Инфодизайн" е най-бързо развиващата се част от науката за Интернет. Информационната архитектура формира ядрото, около което се изграждат всички останали компоненти: общата визия, функционалностите, навигационните схеми, потребителския интерфейс и други. Дейността на Информационния дизайн се състои в процеса на прецизно структуриране на информацията, нейното организиране в ясни навигационни схеми, и атрактивното й представяне, чрез интуитивни и недвусмислени визуални елементи. Крайната цел е да позволи информацията да бъде лесно достъпна, разбираема и управляема. Той е фокусиран върху проектирането и разработването на софтуерни решения, Уеб базирани решения и системи, интерактивни приложения с приятелски интерфейс и оптимизирана информационна архитектура. Днес, дизайнът на информация се занимава с най-сложните проекти, които включват комуникация с потребители, доставчици, партньори и граждани. Проектирането е ключов момент в Информационния дизайн и разработването на всяка една информационна система и проект като цяло. Той придава ново качество на цялостния процес от създаване до крайно оформление на информацията. Можем да обобщим, че **информационният дизайн е процес на подробно планиране на хардуер инфраструктура и софтуерното обезпечаване, чрез които да се достигне до обработване на конкретни данни. Така обработените данни се превръщат в информация, която трябва да бъде предоставена на конкретна целева аудитория по определен начин и да отговарят на предварително зададени цели.** Много важна цел на Информационния дизайн е да създаде качествен краен продукт, като преработи наличните данни и структурира и формира информация с подходяща потребителска визуализация. Тази метаморфоза трябва да създаде определено качество на информацията, тоест това качество е знанието. И тук се заражда проблема, че повечето ИТ специалисти и дизайнери не дооценяват полезността на знанието. Това е фундаментален проблем, който стои за разрешаване пред информационния дизайн като научна дейност и практика. Някои специалисти определят информационния дизайн като подмножество на графичния дизайн, но можем да кажем, че дълбоко грешат. Информационният дизайн съдържа в себе си графичния дизайн за нуждите на естетическото оформление на дадено визуално изображение, като резултат от обща визия или действие на информационна система. Възможна е и употреба в по-широк смисъл засягащ и архитектурата (конструкцията) на дадена информационна система. Ето защо, можем да разглеждаме информационния дизайн като смесено направление между дизайна и информационните технологии, което създава „мост" между ИТ и медиите за нуждите на потребителите на информация. Следва също така да отбележим, че в условията на съвременната среда, отличаваща се с динамика и глобализация се търсят иновативни решения, ориентирани към дизайна на информация. Водещата световна компания в производството на софтуерни продукти за дизайн Autodesk формулира накратко корпоративната си визия така: **"Да предоставим на нашите потребители иновативни софтуерни решения и услуги, подпомагащи тяхната креативност**

и реализацията на техните идеи". [2] Информационният дизайн, базиран на високите технологии може да очертае насоките за развитие и да определи правилата при проектиране и изграждане на софтуер. Той може да положи основите, като се формулира **„Правилото 5Д",** което да бъде водещо при проектиране на софтуер и приложения:

- Добра софтуерна архитектура и дизайн.
- Добра съвместимост с различните операционни системи.
- Добра функционалност и резистентност.
- Добра оперативност и поддръжка.
- Добра визия с улеснен интуитивен интерфейс.

Приложната дейност на информационния дизайн е обвързана и с изграждането на софтуерната архитектура (софтуер дизайн) на Уеб приложението. Тя се отнася до общата структура на софтуера и начините, по които тази структура създава целостта на системата. Правилното функциониране на софтуера зависи от добре организираната архитектура - хоризонтална и вертикална; позиционирането на модулите и инструментите; и обвързването на данните. В този смисъл следва да разграничим следните два вида архитектура:

- **Хоризонтална архитектура** – създава връзка между отделните системи и данните съдържащи се в базата данни.
- **Вертикална архитектура** – изгражда информационни канали, контролирани от горе на надолу в програмната структура.

Друга насока на информационния дизайн е ергономията на информационните системи, разглеждаща взаимодействието човек-компютър и обединяваща в себе си два раздела: **хардуерна ергономия** и **софтуерна ергономия**. Хардуерната ергономия обхваща влиянието на физическите свойства на компютърните устройства, мрежи и периферия, използвани при работа на информационната система. **Софтуерната ергономия** изследва възможните ергономични аспекти от цялостната реализация на информационната система. Тя обхваща всички ергономични аспекти на разработването и използването на софтуера на информационните системи, включително ергономията на труда на ИТ специалистите и информационните дизайнери. **Ползваемостта** (usability) е част от софтуерната ергономия, която изследва взаимодействието между информационните системи и тяхното въздействие върху крайните потребители. **"Ползваемостта на дадена информационна система е показател за ефективността на системата от гледна точка на целите, знанията и уменията на потребителите"**.[3]

Ползваемостта обхваща три класа характеристики на информационните системи, фокусирани върху три различни типа отношения към крайните потребители на информационната система:

- **Потребителска ефективност** (effectiveness) - този аспект акцентира на това, доколко функционалният обхват и начинът на работа със системата съответстват на нуждите, целите и субективните умения на потребителите.
- **Потребителска производителност** (efficiency) - този аспект акцентира на количеството полезни действия, които потребителят може да извърши за определено време.
- **Потребителска удовлетвореност** (satisfaction) - субективната емоционална и естетическа оценка на потребителя за работата на системата и неговата лична

удовлетвореност или неудовлетвореност от начина на работа и получените резултати.

Следва да подчертаем, че продуктът от дейността на информационния дизайн и в частност софтуерната ергономия е отново информация, която е подходящо обработена за нуждите на потребителите. Така информационния дизайн може да се разглежда и в качеството си на активен двигател и медиатор на циркулацията на всички данни, информация и знания в глобалната и специализираните (частни) информационни среди. Под интерфейс на информационната система следва да се разбират средствата за взаимодействие между потребителя и системата. Графичният интерфейс представлява система от графични елементи, които реагират на определени сигнали, насочени към тях от потребителя. Интерфейсът, предоставен на потребителя, значително се различава от интерфейса, с който разполага програмиста. Той е с редица ограничения - например таблиците, заявките и редица системни команди, обикновено остават скрити за крайните потребители. Това се прави от съображения за сигурност и защита на данните, както и за избягване на излишна информация, от която потребителите биха се объркали (те обикновено не са запознати със системата за управление на базата данни (БД)). При една завършена информационна система, предназначена за употреба от крайните потребители, общуването с базата данни се извършва, чрез система от менюта, ленти с инструменти, формуляри и отчети, диалогови кутии, системни съобщения и др. От този интерфейс в значителна степен зависи удобството при работа със съответната информационна система и нейните шансове да се наложи на пазара. Не е за подценяване и естетическото оформление на графичния интерфейс. Това означава, че програмистите следва да бъдат научени отрано, още като обучаеми, правилно да проектират и изграждат потребителския интерфейс. **Дизайнът на съвременните информационни системи или друг софтуер е целесъобразно да бъде потребителски ориентиран и с приятелски интерфейс, което поставя потребителите в основата на концепцията**. Универсална рецепта за изграждане на интерфейса на ИС няма и не може да има. Той се влияе от редица фактори като: специфика на предметната област и степен на нейното познаване, квалификация и владеене на програмния продукт, минал опит, лични предпочитания и други. Въпреки това, информационният дизайн може да допринесе значителна практическа полза при проектирането на потребителския интерфейс. Информационният дизайн следва да има задачата да създаде възможност за **самоконфигуриращ се интерфейс** на потребител с легитимен достъп до БД на сървърите с цел удобство да търси необходимата информация и организира представянето й, съобразно собствения си стил на работа. За разлика от стандартните средства за достъп до БД, тук не се изисква познаването на релационната структура на представените данни. Това става възможно, защото се използват ефикасно средства за управление на данните, като методите за навигация са многообразни и могат да се комбинират помежду си.

С приложение са следните **навигационни методи:**

o Чрез използване на групи сродни данни или съвкупности - Този метод най-често се използва в статистиката, защото там почти всички изследвания се свеждат до изследване на съвкупности.

o Използване на синоними на обекти от БД и задължително на релациите между тях (таблици, заявки).

o Третият метод е подобен на втория, но се използват синоними на отделните

информационни елементи, а не на обекти. Тези елементи, в масовия случай са атрибутивните записи на частите в БД.

o Навигация по агрегационни нива (степени на агрегационно ниво) и на обектите в БД. Това се свежда до използването на логически идентификатори или на някаква комбинация на логически идентификатори.

o Използването на имена или символи на интегрирани програми, на интерфейси, на отчети и други.

Всички навигационни методи могат свободно да бъдат комбинирани помежду си, така потребителят има пълна възможност да приложи свой собствен стил на търсене на данните и на използване на различни начини за представяне на данни. Информацията, намерена чрез средствата за навигация, винаги се извежда на отделен прозорец за данните. В него се разполагат таблици и за предпочитане съответните ергономични форми, създадени за различни цели за представяне. Тъй като на практика не е възможно ясното разграничаване между оперативните и информационните данни, **потребителят задължително трябва да има възможност сам да въвежда и визуализира информацията**. Изискването в това отношение е системата да се грижи нововъведените данни да са винаги интегрирани.

Доброто проектиране на информацията е целесъобразно да се придържа към следните седем правила:

1. Подчертаване на възможностите: **целесъобразно е** информацията да се проектира по начин, който да помогне да се видят тенденциите в данните и да се дадат насоки за действие. Например, ако се проследи развитието на Програмата по бизнес администрация в Харвард се вижда, че престижното учебно заведение е въвеждало големи промени в учебната програма приблизително на всеки 10 години. Въпреки това, събирането на тази информация не е представлявало сложен и изтощителен процес. Изготвянето на схемата е отнемало един ден, а на персонала му трябвали още няколко седмици, за да осъзнае, че отново е време за промяна в програмата – повечето организации биха характеризирали този темп на промяна като "с бясна скорост". [3]

2. Определяне на приоритетите: добрите дизайнери на информация започват със задаване на въпроси. Кое е най-важното тук? След това оставят отговорите да ръководят процеса на проектиране. Тъй като подреждането на данните променя тяхното значение, този подход се съсредоточава върху основните принципи и оставя данните сами да разкажат своята история. Ефектът от анализа се засилва и чрез заместване на необработените данни с проценти и съотношения така, че да се поберат на една страница. Хаосът от числа може да послужи за добра база за сравнение, ако е представен във времето на фона на поставени цели или е събран в една добре обмислена графика.

3. Постигане на единодушие: експертите следва да разглеждат дизайна на информацията не само като процес, но и като продукт, осигуряващ обща платформа, на базата на която хората могат да сравняват идейните си модели и бързо да ги синхронизират. Например, членовете на един високо технологичен екип са смятали, че знаят какво искат за сайта си. Все пак те са се консултирали с професионалист в областта на дизайна на информация. По време на срещата с него идеите на всеки са скицирани набързо в реално време. Оказва се, че вижданията им доста се различават. В бъдеще време тези различия са щели да изплуват на повърхността и да подкопаят ефективността на проекта. [3]

4. Разрешаване на правилните проблеми: ръководните органи не могат да разрешават проблеми с ефективността или да се възползват от бизнес възможностите, ако не ги виждат ясно. Например, една фармацевтична компания не можеше да разбере защо губи пазарен дял въпреки, че разполагаше с огромен обем от данни за предписваните рецепти. Когато дизайнерите на информация обобщиха наличната информация в две страници, проблемът излезе наяве. [3]

5. Помощ при ориентацията: **п**рофесионалистите използват дизайна на информация, за да помогнат на клиентите си да разберат как да използват даден продукт или да се ориентират в даден уеб сайт. Добрата навигация може да е онзи ключов фактор, който или ще удовлетвори потребителите, или ще ги отблъсне. [3]

6. Ускоряване на процеса на взимане на решения: една голяма верига ресторанти постигнала значителни подобрения в дейността си, като изготвила оценка в графичен формат – доклад от 40 страници бил сведен до две страници, описващи графично различната ефективност по обекти. Освен че веднага били засечени "двойкаджиите", мениджърите можели бързо да видят дали пилотните програми за подобряване на дейността дават очакваните резултати. [3]

На основата на представения анализ на особеностите на информационния дизайн следва да направим следните **изводи:**

o Дизайнът на информация може да помогне на организацията да намира и използва провокативни данни – нови тенденции, „смахнати" идеи или странно противоречиви факти – които да родят революционно нови решения. [4]

o Дизайнът на информация следва да се превърне в част от ежедневното управление на данни, свързани с бизнеса или със сигурността и отбраната, което се изразява в интегриране на ИТ и управлението на данни - т.е. възползване от комбинирането на възможността за бързо обработване на транзакции, управляване на изчистени, точни и последователни данни и проектиране на информация, която да предава правилното послание за части от секундата.[4]

В заключение можем да обобщим, че информационният дизайн подпомага създаването на полезна информация. Изпълнявайки тази функция, той се явява основна част от информационния мениджмънт като пред него са изправени предизвикателствата, създавани от лавинообразното развитие на информационното общество.

Литература:

1. Томас Ж. и В. Джамбазов, „Уеб Дизайн"- Как да създаваме успешни уеб сайтове, Част II, Страница 69, Изд. къща Сиела, С., 2010 г., стр. 69.

2. idg.bg/wp/11_dizajnat__osnova_na_uspeshnata_biznes_strategiya_dnes - **Дейвид Палаш**, Търговски директор за региона Autodesk s.r.o

3. Лазарова, Ваня и Д. Петров, Потребителската ефективност на информационните системи в интернет: методологични проблеми при потребителски ориентираното проектиране, С., 2007 г., стр. 190-208.

4. ww.cio.bg/1008_informacionen_dizajn__neshto_poveche_ot_danni_i_dostap_do_tyah.1

5. План за развитие на въоръжените сили на Р България, МО, С., 2010 г., стр. 23-24.

6. Доклад за състоянието на отбраната и въоръжените сили през 2010 г., МО, С., стр. 44.

СЪЩНОСТ И ФУНКЦИИ НА ОРГАНИЗАЦИОННИТЕ СТРУКТУРИ

Христо Д. Бонев

гр. Шумен -9700, ул. ДедеАгач"1,вх.1,ап.75, ет. 15, rino_71@abv.bg

THE ESSENCE AND FUNCTIONS OF THE ORGANISATIONAL STRUCTURES

Hristo D. Bonev

ABSTRACT: *The paper focuses on the essence and functions of the organisational structures.*

KEW WORDS: *essence, functions, organisational structures*

На сегашния етап от развитието на обществото няма и не може да има човешка дейност, която се осъществява вън и независимо от обществото. Колкото и самостоятелна и независима да изглежда някоя от дейностите, дори и на художника, поета или учения, пряко или опосредствено всяка една от тях е обвързана с обществото. То винаги се появява както в ролята на заявител, така и като потребител и във всички случаи като условие, без което не може да се осъществи нито едно действие. Това е така дори и поради факта, че съвкупният човешки опит е на индивидуален и неговото функциониране - предаване и приемане между индивидите се извършва единствено в обществена среда. За улесняване на процесите на обмяна на опит, както и за оптимизиране действията на отделния индивид и на обществените групи се изграждат организационни структури. Тяхното изграждане и функциониране се ръководи от определени принципи и във всеки един момент от съществуването им се съгласува с редица критерии за ефективност. Това осмисля съществуването и необходимостта от развитие на дадена организация или служи като предпоставка на решението за нейното преустройване.

Терминът "организация" означава съзнателна и целенасочена координация между усилията на двама или повече човека с оглед постигането на обща цел, чрез разделение на труда и структуриране на дейността им.

Могат да се очертаят някои съществени характеристики, присъщи на организацията, които я отличават от другите обществени формации. По-важните от тях са:

1. **Координация**. Тя се осъществява чрез правила за функциониране на организацията. Правилата могат да бъдат:

- **писани** - нормативни и поднормативни актове, въз основа на които е създадена и функционира организацията. За армията това са ЗОВС, ПКВС, уставите, наставленията, правилниците, заповедите, разпорежданията и другите документи, които регламентират структурата, взаимодействието и отговорностите на елементите от армейската организационна структура;

- **неписани** - норми и правила, съществуващи в живота на всяка организация, които се формират и предават устно, обикновено чрез традициите. Те са относително трайни във времето и наред с писаните правила осигуряват устойчивост на

организацията във времето.

За организации от типа на армейската, където се решават задачи, понякога свързани с опасност за живота на хората или със състоянието на националната сигурност, правилата за функциониране са разширени (обхващат прекалено много области) и задълбочени (стигат до най-малките детайли), а от неспазването им произтичат сериозни последици (военен съд).

2. **Разделение на труда**. Тази характеристика предполага постигането на общата цел (организационната цел), посредством изпълнението на различни, но взаимосвързани задачи. При съществуващите около 2 000 специалности в армията е ясно, че само чрез едно ясно разделение на труда между военнослужещите и доведено до крайност съгласуване на усилията и резултатите по време, място и други специфични критерии, може да се постигне краен оптимален резултат;

3. **Йерархия на властта**. Формулирана по този начин, тази характеристика на организацията осигурява функционирането на механизма за ръководство и контрол, чието прилагане гарантира изпълнението на задачите от подходящи хора по адекватен начин и в подходящо време;

В литературата са известни няколко основни класически принципа по които се структурира властта, някои от които с успех се прилагат и в армията. Те са:

- **скаларен принцип** - всички ръководни длъжности се ранжират във възходящ ред, който гарантира по-ефективно осъществяване на комуникацията и вземането на решение;

- **принцип на делегиране** - осигуряване на достатъчно пълномощия на всеки подчинен от ръководителя му за постигане на очакваните резултати;

- **принцип на абсолютната отговорност** - ръководителят не може да отклони отговорността за организиране на дейността на своите подчинени. Подчинените носят отговорност за резултатите от тяхната дейност;

- **принцип за паритет на права и отговорности** - поемане на отговорност според предоставените права;

- **принцип на единоначалието** - всеки подчинен има един началнник. Основен принцип при изграждането на армията;

- **принцип на равнището на пълномощията** - изисква вземане на решения според предоставените пълномощия, а не посочването им на по-горното равнище ръководител.

4. **Съгласуване на целите**. Въпреки че се преплита с някои от останалите характеристики, тази е изведена отделно, за да се подчертае нейната важност и голямата зависимост на функционирането на организационната структура от нея.

Посочените главни характеристики определят динамичното цяло, което беше означено с понятието "организация".

Литература:

Шопов Д., М. Атанасова. Управление на персонала, УНСС, София, 1995
Армстронг М., Управление на човешките ресурси, Делфин прес, Бургас, 1993
Кендал Б., Управление на човешките ресурси, УНСС, София, 1994
Galbraith, J.R. Organization Design, in Jay W. Lorsch, ed., Handbook of Organizational
Behavior. Englewood Ccliffs, N.J.: Prentice-Hall, 1987, pp. 343-357
Христова, Т. Мениджмънт на човешките ресурси",с. 209

Milkovich G., PersonelManagement, IRWIN, Illinois,1988
Fisher C., L. Schoenfeldt., J. Shaw. Human Resourse Management, Houghton Mifflin Company, Boston, 1990; Flippo E., Personel Management, McGrow-Hill, N.Y.1991

НЯКОИ ОРГАНИЗАЦИИ С ОСОБЕН СТАТУТ

Христо Д. Бонев

гр. Шумен -9700, ул. ДедеАгач"1,вх.1,ап.75, ет. 15, rino_71@abv.bg

SOME ORGANISATIONS WITH SPECIAL STATUS

Hristo D. Bonev

ABSTRACT: *The paper presents some organisations with special status.*

KEY WORDS: *organisations, special status, human resources*

Успешното управление на организацията като цяло и на човешките ресурси в частност изисква познаване на индивидуалните различия на хората в организацията. Това гарантира разбирането на специфичните реакции и поведението на подчинените. Познаването на стабилните индивидуални различия дава възможност както за по-добър и ефективен подбор, така и впоследствие за оптимално мотивиране, контрол, анализ, оценка, предвиждане и насочване на тяхното поведение.

Установени са няколко групи индивидуални характеристики, които обуславят различията в поведението на хората в организацията. Те имат специфична роля в динамиката на поведението. Предмет на анализ са следните индивидуални особености:

1. Ценности - те имат ориентационна функция спрямо поведението.
2. Нагласи - те определят спецификата на поведението в различни ситуации.
3. Способности - те играят роля на предпоставки за осъществяване на поведението.
4. Личностни характеристики - те определят спецификата на поведението при отделни индивиди.

По-подробното им разглеждане ще даде възможност да се очертае мястото и ролята им за функционирането на човешките ресурси в организацията, както и за оптимизиране на управлението им.

1. Ценности

Ценностната система на човека представлява устойчива съвкупност от глобални убеждения за субективно значими условия и начини на действие и резултати във връзка с труда. Ценностите във връзка с труда са елемент на цялостната ценностна система на човека. В рамките на организационната психология ценностите се определят като желани резулатати във връзка с труда, които допринасят за личното благополучие на човека в организацията. Ценностите се проявяват чрез разнообразни желания, които могат да бъдат групирани в следните категории:

- яснота, хармония и справедливост;
- предизвикателство, независимост и отговорност;

- улесняване протичането на работата, подкрепа, признание;
- топлота и приятелски връзки.

Посочените категории могат да се възприемат и като рамка за тълкуване на събитията в организацията, както и за насочване на организационното поведение по съответен начин.

Наблюдават се известни влияния на някои индивидуални фактори върху ценностите, като:

- **възрастови различия** - по-възрастните лица изразяват по-силна протестантска етика в сравнение с по-младите. Ценности като признание от колегите, професионално развитие и постигане на високи резултати в работата не се променят с възрастта.
- **полови различия** - за жените е по-силна значимостта на организационните ценности и на различни социални референти.

2. Нагласи

За разлика от ценностите като по-глобални убеждения, нагласите като специфични убеждения спрямо обектите в организацията определят поведението в разнообразни ситуации. Айзен и Фишбайн определят нагласата като "научена предразположеност за реагиране по консистентно положителен или отрицателен начин на даден обект".

Следователно нагласите могат да съответстват на ценностите в различна степен. Например някой ръководител може да цени високо независимостта, но да има негативна нагласа към проявата на самостоятелност когато няма достатъчно делегирани пълномощия за определени действия.

Данните от различни изследвания показват, че нагласата влияе по-силно върху намерението за напускане в сравнение със субективната норма. Тези два компонента влияят по-силно върху намерението, отколкото върху реалното действие на напускане.

Към посочения модел могат да се включат още два компонента с определени ефекти върху поведението. Идентификацията с организацията влияе по-силно върху намерението за напускане, отколкото удовлетвореността от труда, освен това по-силно е влиянието на удовлетвореността от организацията като цяло в сравнение със специфичните оценки на удовлетвореност (заплащане, съдържание на труда и ръководство).

3. Способности (Интелигентност и познавателни процеси)

Способностите влияят значимо върху равнището на изпълняваните задачи и постигнатите резултати в организацията. Тяхното предварително измерване се разглежда като много важно и се осъществява като процедура на подбора на персонал в различни организации.

Интелигентността представлява способност за конструктивно мислене и откриване на закономерности. Разграничават се две разновидности на интелигентността: 1) Обща психична способност, необходима за решаване на разнообразни задачи, изискващи преработка на информация; 2) Специфични способности за решаване на конкретни проблеми. Интелигентността също може да присъства като критерий при подбора на персонал и се препоръчва от водещите агенции, като предсказваща бъдещата дейност в организацията.

4. Личностни характеристики

Доказан факт е, че комплексът от подходящи за определена дейност личностни

характеристики предопределя функционирането на хората в организацията. В рамките на тази разработка естествено ще бъдат разгледани само някои от тях, смятани за най-важни и универсални, т.е. отнасящи се до преобладаващата част от дейности.

а/ Локализация на контрола

Тази личностна променлива отразява различията между хората в начина им на интерпретиране на връзката между изразходваните лични усилия и постигнатите резултати. Лицата с вътрешен контрол (интернали) споделят убеждението, че постигнатите от тях резултати се дължат на техните лични усилия, а лицата с външен контрол (екстернали) са убедени, че постигнатите резултати произтичат от действието на други хора, външни фактори и обстоятелства.

б/ Екстраверсия и интроверсия

Тези различия са свързани с възбудните процеси на мозъчната кора. Равнището на оптимална възбуда се определя от външната стимулация и индивидуалното равнище на възбуда. Екстравертите и интровертите се различават по равнището на възбуда: екстравертите имат по-ниско равнище на възбуда и затова се нуждаят от по-силна външна стимулация, за да постигнат оптимално равнище на възбуда, докато интровертите имат по-високо равнище на възбуда и затова се нуждаят от по-слаба външна стимулация (вж. табл. 1).

Таблица 1. Различия между екстраверти и интроверти

Предпочитания	Екстраверти	Интроверти
Високо равнище на възбуда	след обяд	сутрин
За работа	с хора и неща	с идеи
Изразяване на идеи	лесно	трудно
Изпълнение при конкурентен стимул	най-добро	слабо
Стратегия за оптимална възбуда	взаимодействия с хора, нови и по-силни чувства	сами или с близки познати начини на действие
Отношение към хората	разговорчиви, конкурентни	подозрителни, внимателни

Екстроверсията и интроверсията влияят върху предпочитанията към задачите. Екстравертите предпочитат по-високи равнища на изисквания на задачите за преработка на информация, бърз темп на работа, повече вътрешни и външни награди. Интровертите имат обратните предпочитания.

Отбелязват се и различия в отношението към работата. Екстравертите докладват по-ниска удовлетвореност от съдържанието на труда, от ръководството и от колегите, в сравнение с интровертите. Следователно по-благоприятни са реакциите когато възприятията и оценките на характеристиките на трудовата среда са по-близки до предпочитанията. Други изследвания показват, че екстравертите посочват по-висока удовлетвореност от заплащането и от труда като цяло в сравнение с интровертите.

Екстраверсията е свързана с някои атрибутивни отклонения. Тя е свързана с приписване на положителните събития на вътрешни, стабилни и глобални причини в по-голяма степен. Това означава, че екстравертите изразяват по-силна склонност

за употреба на защитен атрибутивен стил в сравнение с интровертите.

в/ Поведение от коронарен тип А

Това поведение е рисково за здравето. То е стабилна личностна характеристика, наред с другите рискови фактори - тютюнопушене, високо кръвно налягане, затлъстяване, високо равнище на холистерол в кръвта, физическа пасивност. Съществуват данни, които показват, че поведението тип А мултиплицира рисковите ефекти на посочените фактори.

Поведението от тип А е комплексно. То представлява емоционално-поведенчески комплекс. То се проявява чрез следните характеристики:

- забързана реч, акцентиране на ключови думи;
- склонност към бързо хранене и движение;
- постоянно нетърпение спрямо събитията, напр. раздразнение от скоростта на протичане на нещата;
- силно предпочитание към извършване на две или повече неща;
- тенденция към насочване на разговора към лично значими обекти или теми;
- прекъсване на друг човек докато говори за вмъкване на собствена гледна точка;
- чувство на вина по време на почивка;
- тенденция на забравяне на други неща извън основното занимание;
- по-силна заинтересованост от неща, които си заслужава да имаш в сравнение с качества, които си заслужава да бъдеш;
- тенденция за планиране на все повече и повече неща за все по-кратко време;
- преживяване по-скоро на конкуренция, отколкото на сравнение при контакт с друг човек с поведение тип А;
- използване на характерни жестове, нервни тикове;
- убеждение, че успехът се дължи на способност да се постига по-бързо от другите;
- тенденция да се разглежда и оценява дейността, личната и на другите "на бройки", например брой срещи, брой обаждания по телефона и др.

Макар и разгледани фрагментарно, посочените личностни характеристики по ясен и недвусмислен начин демонстрират влиянието на личността върху трудовата реализация. Ето защо отчитането им при подбора на персонал е задължително.

Литература:

Владимирова, К., К. Спасов, Н. Стефанов. Управление на човешките ресурси. Университетско издателство “Стопанство. С., 1998

Андреева М., Управление на персонала, ИК “Галактика”, Варна, 1995

Савов, В. Основи на управлението. Университетско издателство “Стопанство. С., 1996

Мениджмънт на човешките ресурси. Princeps, Варна, 1996

Milkovich, G., J. Boudreau. Personnel Human resource management. A diagnostic approach. BPI, 1988

Byars, L., L. Rue. Human resource management. IRWIN, 1987

СИГУРНОСТТА В ГЛОБАЛИЗИРАЩИЯ СЕ СВЯТ

Маргарита К. Бонева

Шуменски университет „Епископ Константин Преславски", Педагогически факултет

SECURITY IN A GLOBALIZING WORLD

Margarita K. Boneva

Konstantin Preslavsky University of Shumen, Faculty of Education

Abstract: Enriched is a theory about the nature of security in a globalizing world.

Key words: security, globalizing world.

В националната и световната литература понятието сигурност се дефинира по различен начин.

Сигурността е цел и потребност на обществото и е обект на дългогодишни и разностранни изследвания.

Социално-екологичните проблеми на глобализиращия се свят са своеобразна съвкупност от традиционните проблеми на човечеството, към които се прибавят и опасностите от глобалната екологична криза.

Налага се всички проблеми да се решават заедно, т.е. заедно с традиционните проблеми трябва да се решават проблемите, свързани с глобалното антропогеннно замърсяване и изчерпване на природните ресурси, с международния тероризъм, организираната престъпност, с корупцията, с неконтролираната миграция, с етническите конфликти, с опустошителните природни бедствия, опасните епидемии, разпространяващи се в целия свят, с пълните с напрежения конфликти на страни, притежаващи ядрено оръжие и пр.

С други думи в съвременния глобализиращ се свят основен проблем става неговата сигурност.

Не трябва да се отминава и фактът, че структурите на световната сигурност са недостатъчно на брой и имат ограничени възможности.

Съвременното състояние е такова, че приоритет по въпросите на световната сигурност, която е най-близка до човешката сигурност имат националните държави.

Състоянието на световната сигурност е най-сигурният инидикатор за развитието на човечеството, а равнището на личната сигурност е индикатор за състоянието на сигурността на обществото.

Според Н. Слатински първите три нива на сигурността – съответно на инидивида, на групата от индивиди и на държавата – определят Националната сигурност. Последните три нива на сигурността – на държавата, на общността от държави и на света – определят Международната сигурност.

Според Д. Йончев «В променените условия на глобализиращия се свят трябва

да се мисли с категориите на всички равнища на сигурност».

Нарастващата взаимозависимост в глобалните, континенталните, регионалните и националните процеси размива границите между различните нива на сигурността.

«Меките аспекти» на сигурността – здравеопазване, образование, наука, качество на живота, качество на човешкия капитал, качество на екологичната среда са свързани със социално-екологичните проблеми на глобализиращия се свят.

Въвеждането на понятието регионално равнище на сигурност като «някакво състояние на отношенията между държави и общности в региона от гледна точка на споделения между тях контрол над вредните въздействия върху региона» е обвързано с международната сигурност.

Според Бари Бузан «изучаването на сигурността трябва да надхвърли чисто военните въпроси и затова той предлага следните пет сектора, имащи потенциал за въздействие върху сигурността:

- военна сигурност;
- политическа сигурност;
- икономическа сигурност;
- социетална сигурност;
- екологична сигурност.

В статията си «Що е сигурност» Ема Ротшилд твърди, че «през 90^{те} години на XX век схващането за сигурността се разширява:

- от сигурност на държавите към сигурност на групите от индивиди и сигурност на индивидите. Това е разширяване «надолу» - от държавите към индивидите;
- от сигурност на държавите към сигурност на международната система. Това е разширяване «нагоре» - от държавата към биосферата;
- хоризонталното разширяване на сигурността е свързано с разширяване от военното измерение към политическата сигурност, икономическата сигурност, социалната сигурност, свързаната с околната среда сигурност или човешката сигурност.

Според Доклада за развитието на човека на ООН (1994 г.) най-важните компоненти на човешката сигурност са:

- икономическа сигурност;
- продоволствена сигурност;
- здравна сигурност;
- екологична сигурност;
- лична сигурност;
- общностна сигурност;
- политическа сигурност.

Според група български изследователи «човешката сигурност е концепция, фокусирана върху човека, в чиято основа залягат животът и социалните възможности на обикновените хора».

Според Джордж Неф човешката сигурност се състои от :

- екологична, персонална и физическа сигурност;
- икономическа сигурност;
- социална сигурност;
- политическа сигурност;
- културна сигурност.

Гари Кинг и Кристофър Мъри идентифицират 5 ключови индикатора, свързани с благосъстоянието, чрез които се измерва нивото на човешката сигурност: бедност, здраве, образование, политическа свобода, демокрация.

В петте базисни критерии към Системата за колективна сигурност разглеждана в четвъртото ниво на сигурност, а именно: повече сигурност, повече демокрация, повече жизнен стандарт, запазване правото на глас, съхранение на националната идентичност прозират социално-екологичните проблеми на глобализиращия се свят, които трябва да бъдат решени.

Основавайки се на въведеното от Н. Слатински пето ниво на сигурността, което е Сигурност на света, сигурност на планетата, т.е. обща, всеобща, глобална, универсална сигурност и на базата на изследванията на Oxford Research Group, според които най-сериозните предизвикателства към глобалната сигурност са:

- промените в климата и глобалното затопляне;
- конкуренцията за все по-ограничените стратегически суровини;
- нарастващото социално-икономическо разделение (т.е. пропастта "Север"-"Юг") и маргинализацията на все повече хора;
- засиленото разпространение на оръжия и военни технологии, включително оръжия за масово унищожение (глобалната милитаризация).

Може да се направи извода, че социално-екологичните проблеми на глобализиращия се свят, които са обект на социалната екология имат съществено значение за глобалната сигурност на планетата.

Прибавяйки към това дефинираните от Ал Гор глобални заплахи:

- глобалната екологична криза, която може да обезмисли целия ни напредък в други насоки, ако не се справим с нея;
- водната криза, която се дължи на рязко нарасналото търсене на сладка вода и разрушителното влияние на глобалното затопляне върху естествените водни запаси в природата – снежни върхове и ледници, както и на влошеното качество на водата, причинено от нейното замърсяване и незадоволително пречистване;
- глобалната заплаха от тероризма, която става още по-сериозна с нарастващия достъп до нови видове оръжие за масово унищожение;
- наркотиците и корупцията в световен мащаб, чието разпространение никога не е било по-голямо, защото международната организирана престъпност усъвършенства своите методи и засилва мощта си с невиждани досега темпове;
- новите пандемии от рода на ХИВ/СПИН, които погубват цели общества и се задълбочават като проблем с появата на нови щамове на стари болести, ужасяващо резистентни спрямо антибиотиците, се налага извода за приоритетното значение на социално-екологичните проблеми за сигурността на планетата.

Изхождайки от факта, че глобализацията изтощава ресурсите на държавата за въздействие и власт, че светът все повече става свят на транснационални компании и универсификацията на мисленето и целите, на ценностите и морала, на критериите за успех, стандарт и просперитет, на преструктуриране на геополитически пространства и интереси, на всички основни политически, икономически, социални, културни и други процеси, на търговията, паричните потоци и инвестициите, на «трудовите ресурси» и «сивото вещество», на комуникациите, информацията и интелектуалната собственост, на културата, екологичните беди, престъпността и порнографията, може да се твърди, че всичко това намалява сигурността на света като цяло.

Високите технологични и конструктивни достижения на човека, както и ескалиращото му и ненаситно потребителско отношение към природата, концентрацията на огромни по мащаби енергия или сложни химически и биологически производства, експериментите на генно свръхмикроравнище, както и растящото безразсъдство на тероризма могат да променят изцяло представите ни за кризи и кризисни ситуации и да доведат до качествено нова структура на цялата система за управление на кризи и при кризи.

Разпространението на пандемични болести от типа на SARS (тежък респираторен синдром) би могло да нанесе опустошителни човешки и икономически загуби, ако не се овладее с адекватни и понякога безкомпромисни мерки.

Развитието на демографските тенденции, постепенно променящи етническия, религиозния и расовия баланс в глобален мащаб са също проблем на сигурността.

През второто хилядолетие на планетата Земя се реализира крупна демографска революция, за която свидетелства динамиката на растеж на населението в исторически план. По-голям е прирастът на населението в най-бедните страни като съществено влияние оказват морално-етичните и религиозните възгледи.

90% от прираста на населението е в развиващите се страни и страните от Третия свят, т. е. от най-бедната част на човечеството, а това усложнява икономическото развитие и снабдяването с продукти. В цялата история на човечеството производството на храни е основната или една от основните съставящи на всяка обществена формация. Решението на този проблем зависи от производствените отношения и тяхното ниво, от разликата между нивото на производство на храни и прираста на населението.

Експертите определят четири групи население: население на икономически развитите страни (25%); население, което се храни задоволително (25%); население, което се храни лошо (24%); население (26-30%), за което енергоемкостта на храната лежи на границата между живота и смъртта.

Понастоящем учените от цял свят се обединяват в разбирането си, че особено важна страна от т.нар. нови проблеми в сферата на сигурността са тези, свързани с продължаващото нарастване на броя на хората на Земята.

Прогнозите за 2025 г. са, че мнозинството от градското население в света ще попадне сред бедната част от хората на Земята, а това води до сериозни рискове. Във все по-глобалния съвременен свят националните демографски проблеми надхвърлят рамките на отделните държави и региони и постепенно се превръщат в проблеми на цялото човечество. Дестабилизиращият потенциал на динамиката в нарастването на населението, потребността от осигуряване на храна, подслон, възможности за социална реализация и защита на човешки живот може да се превърне в сериозен глобален въпрос на сигурността.

Друг глобален проблем е миграцията.

Най-важните причини за съществуващия мощен миграционен поток днес са:

- растящата глобализация;
- ускорената интернационализация на производството;
- разпределението и пазарите на труда;
- качествено новата международна среда в Европа;
- приемащите държави, които имат потребност от допълнителна работна ръка;
- демографският взрив;

• безработицата и отчаянието от бедността в развиващите се страни предизвиква огромен излишък от работна ръка и желание да се напусне собствената страна;

• чисто политически явления – неспазване на основните политически права и свободи на хората, политическа дискриминация и сагрегация.

Предотвратяването на възможната екологична катастрофа на човечеството – в наше време това вече не е потенциална, а реална опасност, която се отнася за цялата планета.

Проблемът "биосфера – човек" привлича вниманието на световната общественост. В глобален мащаб все по-актуални стават изследванията, които доказват необходимостта от приемане на конкретни мерки за опазване на биосферата и за рационално използване на природните ресурси.

В съвременния глобализиращ се свят е повече от актуална фразата на Ал Гор: «Време е да променим начина, по който живеем заедно на тази планета».

Литература

1. Бауман, З., Глобализацията. Последиците за човека, София, 1999.
2. Бейнс, Д., Морал за 21 век, С., 2001.
3. Бекярова, Н., Демография и сигурност, С., 2004.
4. Владимиров, Л., Рискметрия в екологичната сигурност, В., 2009.
5. Доклад на Програмата за развитие на ООН „Новите измерения на човешката сигурност", 1994.
6. Йончев, Д., Равнища на сигурност, НБУ, С., 2008.
7. Недев, Т., Глобализирующийся мир: бедность, богатство, тероризм, В., 2005.
8. Петров, А., Тероризъм и системи за сигурност, С., 2005.
9. Проданов, В., Глобалните промени и съдбата на България, София, 1999.
10. Сандев, Г., Система и политика на националната сигурност, Ш., 2003.
11. Слатински, Н., Измерения на сигурността, С., 2000.
12. Слатински, Н., Националната сигурност – аспекти, анализи, алтернативи, С., 2004.
13. Слатински, Н., Петте нива на сигурността, С., 2010.
14. Томов, В., А. Ненова., Индустриална и екологична сигурност, В., 2002.
15. Хотянцев, Ю., Экология и экологическая безопасность, М., 2002.
16. Хънтингтън, С., Сблъсъкът на цивилизациите и преобразуването на новия световен ред, С., 1999.

ГЛОБАЛИЗАЦИЯ - НАЦИОНАЛНА СИГУРНОСТ - СОЦИАЛНА ЕКОЛОГИЯ

Маргарита К. Бонева

Шуменски университет "Епископ Константин Преславски", Педагогически факултет

GLOBALIZATION, NATIONAL SECURITY AND SOCIAL ECOLOGY

Margarita K. Boneva

Konstantin Preslavsky University of Shumen, Faculty of Education

Abstract: Analyzing the socio-environmental problems is found a relationship "globalization, national security and social ecology. "

Key words: globalization, national security, social ecology

В настоящата работа се представя релацията "глобализация – национална сигурност и социална екология". Взаимодействието между икономическите, социалните и екологичните цели представлява сърцевината на последователния подход към политиката, и въпреки че много въпроси на околната среда изискват глобални действия, на национално равнище е необходимо да се подготви голям резерв за устойчивото развитие. Глобалните социални и екологични предизвикателства носят в себе си всички аспекти на проблемите и противоречията на взаимодействията на човека и обществото с природата – на ниво човек (личност, гражданин), на ниво страни (отрасли, производства и структури на обществото), а така също в регионални и глобални мащаби, застрашаващи съществуването и устойчивото развитие на цивилизацията. Тези три нива на противоречия (човекът природоползвател и природа на региона, общество и природа на страната, човечество и природа на биосферата на Земята) са в основата на трудно прогнозируеми и даже непредсказуеми конфликти в национален, регионален и глобален мащаб. Те се изучават от социалната екология, съществуваща в общата система от науки като ноосферен феномен на развитие на мислите на човечеството.

Осигуряването на световния мир, като върховна жизненоважна човешка потребност, предполага решаване на редица проблеми:

- екологичен проблем – реално следствие от взаимодействието между обществения характер на това взаимодействие, обект на научен анализ и изследване, индикатор на неблагоприятната днес взаимозависимост между материалната производствена дейност и потребност;
- енергиен проблем – необходимост от мощен енергиен поток за по–нататъшното развитие на цивилизацията;
- демографско развитие и прехрана на човечеството – релация, водеща преди всичко до екстензивно биотехнологическо развитие на селското стопанство;
- усвояване богатствата на световния океан.

Глобализацията води до появата на ново качество на съвременната социална система, определяна като постиндустриално, информационно, глобално общество, което често се оприличава с популярната метафора "глобално село".

Многобройните взаимозависимости, в които днешният човек е включен, изграждат няколко относително обособени системи, едновременно пораждащи и понасящи натиска на глобализацията. Това са политическата, икономическата, технологичната и екологичната глобална система.

В рамките на световната политическа система се глобализират и редица други проблеми като:

- зачитането и спазването на правата на човека;
- правните и нравствените измерения на информационните технологии;
- национализмът, фундаментализмът, расизмът;
- престъпността и тероризмът;
- наркотрафикът;
- корупцията.

Изострянето и сложното преплитане на глобалните проблеми е една от най-важните особености на нашето съвремие. Те имат разнообразен характер – културно-политически, социално-икономически, демографски, природно-ресурсен, екологичен, военно-политически, юридически и пр. Същевременно те са провокирани от хронологичното единство и бързите темпове на разрушаване на баланса между природата и обществото, поради което трябва да се разглеждат като единна система от динамично променящи се взаимно зависими явления.

Редица от самостоятелно дефинираните социални или природни глобални проблеми имат индиректно отношение към съвременните тенденции.

Сред най-значимите за бъдещето на човешката цивилизация са хидроатмосферните изменения, водещи до глобално затопляне на климата, повишаване нивото на Световния океан и промени в зоналните природни закономерности.

Реален шанс за функциониране на природата в оптимални пропорции би имало само, ако се овладеят тенденциите, породени от антропогенния натиск. Първостепенна задача в това отношение е стабилизирането на броя на населението в глобален мащаб.

Главна черта на глобалния икономически модел е стремежът за контрол върху невъзстановимите природни ресурси и за безпрепятствено функциониране на снабдяването с тях.

Новите технологии създават огромни възможности за лична изява и електронна търговия, но създават нови рискове за обществената безопасност и националната сигурност. Затова първият стълб в новата парадигма трябва да бъде повишаването на сигурността и тайната на информацията – да се гарантира сигурност и поверителност на съхранените и разпространяваните данни от неоторизиран и незаконен достъп.

Над социалните аспекти преобладават мерките за отваряне на пазарите, както и финансовите и икономическите съображения.

Голяма част от проблемите на глобализиращия се свят – бедността, липсата на достоен труд и неуважението на човешките права съществуваха много преди настоящата фаза на глобализация. Непостоянният характер на глобализацията обаче застрашава както богатите, така и бедните. Произвеждат се огромни богатства, но проблемите на бедността и неравенството продължават да съществуват. Корупция-

та е широко разпространена. Отворените общества са застрашени от глобалния тероризъм, а бъдещето на отворените пазари все повече се поставя под съмнение.

Безработицата и непълната заетост продължават да са жестока действителност за по-голямата част от населението на света.

Глобализацията трябва да поставя на първо място хората и не трябва да се разглежда като нова версия на предишните форми на господство и експлоатация. Тя трябва да има социално измерение, което подкрепя човешките ценности и увеличава благосъстоянието на народа от гледна точка на човешката свобода, процъфтяване и сигурност. Глобализацията се възприема през погледа на обществото от гледна точка на възможностите, които тя създава за достоен труд, за удовлетворяване на основните им потребности от храна, вода, здравеопазване, образование, дом, защита на околната среда. Без такова социално измерение глобализацията е немислима.

Действащият икономически модел "изяжда" невъзстановимите ресурси и околната среда и изостря противоречията между петте типа различни в материално и морално състояние държави: свръхразвити, развити, развиващи се, изостанали в развитието си и деградиращи.

Бедността става нетърпима, безработицата расте.

Определени аспекти на общопризнати принципи и ценности нееднократно намират отзвук в хода на обществените дебати за глобализацията. Те изразяват тревогата на хората по следните въпроси:

- зачитане правата на човека и човешкото достойнство, включително равенството на половете;
- зачитане на разнообразието на културни, религиозни, политически и социални виждания при пълно спазване на всеобщите принципи;
- зачитане на справедливостта;
- зачитане на солидарността, защото тя се основава на признаването, че във взаимно зависимия свят бедността или потисничеството, на общата човечност и глобалното гражданство независимо от това къде се проявяват, са заплаха за процъфтяването и стабилността в целия свят;
- уважението към природата изисква глобализацията да има екологически устойчив характер и да зачита природното разнообразие на живот на Земята и жизнеспособността на планетарната екосистема, както и да осигурява справедливост между днешните и бъдещите поколения.

Глобализацията е резултат от човешката дейност, т.е има антропогенен произход, а по своята същност и характер е социално явление. Тя поражда проблеми, надхвърлящи границите на отделните държави, които не могат да бъдат решени от една или няколко страни, а изискват обединяването на усилията и волята на цялото човечество.

Глобализацията обхваща "целия свят от човешки същества като мигновена и постоянна реалност". Тя е свързана с множество явления, пораждащи нееднозначни последствия, от които по един или друг начин зависи нашето бъдеще. Глобализацията като процес влияе върху сигурността във всичките й измерения.

Многобройните взаимозависимости, в които днешният човек е включен изграждат няколко относително обособени системи, едновременно пораждащи и понасящи натиска на глобализацията. Това са политическата, икономическата, технологичната и екологичната глобална система.

В руския Енциклопедически речник "Политология", националната сигурност е дефинирана така: “Състояние, при което се обезпечава защитата на жизнено важните интереси на държавата и гражданското общество в икономическата, политическата, военната, екологическата, хуманитарната и други области”.

Джесика Тучман Метюс изказва твърдението, че «Глобалните развития подсказват необходимостта в националната сигурност да бъдат включени въпросите на ресурсите, екологията и демографията».

На националната сигурност са присъщи специфични политически, икономически, социални, етнически, духовни, военни, информационни и екологични компоненти, всеки от които самостоятелно или в съчетание с другите както и с редица странични фактори, може да се окаже критичен за държавата.

Тя отразява връзката на сигурността на нацията, с определена териториално-държавна общност.

• Първото ниво е сигурност на индивида (на личността, на отделния човек) - наричана различно: лична, индивидуална, персонална сигурност. Тя излиза все повече на преден план, защото е свързана пряко не просто с правото на живот, а с правото на по-добро качество на живот, с другите основни човешки права и задължения, свободи и отговорности.

• Второто ниво е сигурност на групата (от хора) - групова сигурност. Групата може да се обособи по различен признак: етнически, религиозен, социален, професионален, сексуален. обществени прослойки, като краен вариант - самото общество. Групата носи в себе си материални и духовни ценности, идентичност, памет, език, традиции, обичаи. Опазването и зачитането им е важен аспект на сигурността й.

• Третото ниво е сигурност на държавата - държавна сигурност. Терминът "държавна сигурност" е натоварен с много негативно съдържание по названието на съответната тоталитарна институция и това ни кара да усложняваме систематизацията, само и само да избегнем прекомерната му употреба. Тя е свързана със защитата на изконни ценности: териториална цялост, независимост, суверенитет, конституционен ред и др.

• Четвъртото ниво е сигурност на общността от държави - колективна, коалиционна сигурност. Терминът "общност" обхваща различни форми на сдружаване на държави: двустранни и многостранни договори и пактове, общности за сигурност, коалиции, съюзи и др.

• Петото ниво е сигурност на света (на планетата) - глобална, универсална, обща, всеобща сигурност. При нарастващата взаимообвързаност, проблемите на глобалната сигурност постепенно излизат на преден план.

Ръководената от Улоф Палме Независима комисия по въпросите на разоръжаването и сигурността към ООН първа разработи в началото на 80-те години концепцията за обща сигурност съгласно, която не може да има трайна сигурност, ако тя не бъде споделена от всички и че обща сигурност може да бъде постигната само чрез сътрудничество, основано на принципите на равенството, справедливостта и реципрочността.

Първите три нива на сигурността - на човека, на групата, на държавата определят националната сигурност.

Последните три нива на сигурността - на държавата, на общността, на света определят международната сигурност.

Познавайки същността на петте нива на сигурността, дефинирани от Н. Слатински може да се стигне до извода, че сигурността е пряко свързана с обектите на социалната екология – човека, групата, обществото.

В контекста на равнищата за сигурност «Лична сигурност има онзи, който се радва на здравословни условия на живот, чиято среда на обитаване не поражда заплахи за физическото и психическото му здраве, има възможност да планира бъдещето си и притежава някаква общоприета степен на свобода, за да взема сам решенията за себе си»

Личната сигурност е някакво състояние на равновесие между различните въздействия върху човека в определено време. Хората са много чувствителни към условията на своя живот. Една значителна част от условията са продукт на обществото. Друга част се дължат на климата и на географските особености, а третата – на личностните особености на човека.

Личната сигурност може да се разглежда като точен и верен индикатор на състоянието на сигурността в обществото.

Групата е инструмент на присъствието, човешка среда, която създава подходящи условия за живот. "Групата според Н. Слатински "носи в себе си материални и духовни ценности, идентичност, памет, език, традиции, обичаи. Опазването и зачитането им е важен аспект на сигурността ѝ". Груповата сигурност е показател за зрелостта на обществото и на неговата организация.

Държавната сигурност е сигурност на държавно равнище. Тя е рамка на личната сигурност на гражданите и на груповата сигурност на общностите и организациите. Тя е не само ясно осъзната дейност на обществото, но е и предмет на непрекъснат изследователски, законодателен и обществен интерес. Пораждането и поддържането на държавната сигурност е основна, ежедневна, осъзната, институционализирана грижа на съвременната държава.

Системата за национална сигурност отчита националните, регионалните, континенталните и глобалните аспекти на външната политика, отбраната и сигурността.

Отчитането на националните аспекти на сигурността означава да се очертаят българските интереси, цели, приоритети и идеали. Това изисква неимоверно усилие на нашия народ за:

- малко повече суверенитет и достойнство;
- за повече сцепление и заедност;
- за повече обща воля и разум.

Националната сигурност се основава на един своеобразен закон: в колкото по-голяма криза е една държава, колкото по-нестабилна е тя, толкова повече проблеми стават проблеми на сигурността, т.е. секюритизират се. Не всеки проблем е задължително проблем на сигурността, но той става такъв тогава и от момента, в който не може да бъде овладян без структурни трансформации в системата за национална сигурност, в държавата и обществените отношения. Сериозни проблеми вече се превръщат в проблеми на националната сигурност, например изтичането на мозъци, образованието и здравеопазването, демографията и бежанците.

Отчитането на глобалните аспекти на сигурността изисква размисъл:

- за преструктурирането на геополитическите пространства, сили и интереси;
- за нарастващата трансграничност на информацията;
- за културата;
- за интелектуалната собственост;

- за паричните потоци, инвестициите, търговията;
- за трудовите ресурси;
- за "сивото вещество";
- за екологичните проблеми,;
- за престъпността и порнографията;
- за утвърждаването на колективни системи за сигурност.

Тероризмът, международната организирана престъпност изискват обединените усилия на цялата международна общност и нетърпимост от страна на всеки човек. Нито една държава вече не разполага с абсолютната привилегия да остане затворена в собствените си географски очертания. Все повече държавите се стремят да се приобщят към различни регионални или международни организации за колективна сигурност, опитвайки се да установят някакви универсални, стандартизирани правила, с надеждата, че те ще се превърнат във всеобща норма за поведение.

В днешния свят без граници повече от всякога трябва да се познават и уважават националната култура и традиции, да се съхранява родния език. Днес повече от всякога трябва да се изисква уважение към историята и със самочувствие да се отстоява нейния автентичен прочит.

Сред главните рискове за националната сигурност е опасността от демографски колапс на всеки етнос и оттук – на коренна промяна на демографската и етническа картина на всяка нация. Броят и относителният дял на лицата на възраст до 15 години непрекъснато намалява, а се увеличават броят и делът на населението над 65 години.

За застрашителната депопулация допринасят: масовата бедност и безработицата, колосалното натоварване на работещите хора от големия брой пенсионери и неработещи.

Към това може да се добави увредената природна среда, ниското качество на храната, стресът, агресията, насилието, личната несигурност, все по-влошаващият се в здравен, в образователен и квалификационен разрез качествен състав на населението.

Понастоящем учените от цял свят се обединяват в разбирането си, че особено важна страна от т.нар. нови проблеми в сферата на сигурността са тези, свързани с продължаващото нарастване на броя на хората на Земята.

Прогнозите за 2025 г. са, че мнозинството от градското население в света ще попаднат сред бедната част от хората на Земята, а това води до рискове за сигурността.

Най-важните причини за съществуващия мощен миграционен поток днес са:

- растящата глобализация;
- ускорената интернационализация на производството;
- разпределението и пазарите на труда;
- качествено новата международна среда в Европа;
- потребност от допълнителна работна ръка в приемащите държави;
- демографският взрив,;
- безработицата и отчаянието от бедността;
- неспазване на основните политически права и свободи на хората, политическа дискриминация и сагрегация.

Във все по-глобалния съвременен свят националните демографски проблеми

надхвърлят рамките на отделните държави и региони и постепенно се превръщат в проблеми на цялото човечество. Дестабилизиращият потенциал на динамиката в нарастването на населението, потребността от осигуряване на храна, подслон, възможности за социална реализация и защита на човешки живот може да се превърне в сериозен глобален въпрос на сигурността.

Предотвратяването на възможната екологична катастрофа на човечеството – в наше време това вече не е потенциална, а реална опасност, която се отнася за цялата планета. Оттук и прерастването на екологичният проблем от икономически и технологически в екзистенциален.

Няма съмнение, че понастоящем протича коренно преустройство на биосферата, на нейния животински и растителен свят. Съвършено вярно е, че са налице признаци на загуба на способностите на биосферата за възстановяване на природното равновесие – признаци, много опасни по своите бъдещи последствия. Ето защо абсолютно закономерно, проблемът "биосфера – човек" привлича вниманието на световната общественост. Все повече са задълбочените изследвания, които доказват необходимостта от приемане на конкретни мерки за опазване на биосферата и за рационално използване на природните ресурси.

Според Jeremy Rifkin светът е на края на възможностите си в производството на енергия и това изисква радикален, нов световен възглед за спасяването на света".

Литература

17. Бауман, З. Глобализацията. Последиците за човека, София, 1999.
18. Бейнс, Д., Морал за 21 век, С., 2001.
19. Бекярова, Н., Демография и сигурност, С., 2004.
20. Будыко, М., Глобальная экология, М., 1977.
21. Владимиров, Л., Рискметрия в екологичната сигурност, В., 2009.
22. Гирусов, Э.В., Основы социальной экологии. М., 1998.
23. Горелов, А., Социальная экология, М., 1997.
24. Данило, М., Социальная экология, М., 1989.
25. Доклад на Програмата за развитие на ООН „Новите измерения на човешката сигурност", 1994.
26. Йончев, Д., Равнища на сигурност, НБУ, С., 2008.
27. Комаров, В .Д., Социальная экология. Философические аспекты, Л., 1990.
28. Малофеев,В. И., Социальная экология. М., 2003.
29. Марков, Ю. Г., Социальная экология. Новосибирск, 1986.
30. Маркович, Д. Ж., Левин А. С., Введение в социальную экологию. М., 1999.
31. Недев, Т., Глобализирующийся мир: бедность, богатство, тероризм, В., 2005.
32. Никоноров, А., Глобальная екология, М., 2001.
33. Петров, А., Тероризъм и системи за сигурност, С., 2005.
34. Проданов, В., Глобалните промени и съдбата на България, София, 1999.
35. Сандев, Г., Система и политика на националната сигурност, Ш., 2003.
36. Ситаров, В. А., Социальная экология. М., 2000.
37. Слатински, Н., Измерения на сигурността, С., 2000.
38. Слатински, Н., Националната сигурност – аспекти, анализи, алтернативи, С., 2004

39. Слатински, Н., Петте нива на сигурността, С., 2010
40. Стиглиц, Дж., Глобализацията и недоволството от нея, С., 2003.
41. Томов, В., А. Ненова., Индустриална и екологична сигурност, В., 2002.
42. Хотянцев, Ю., Экология и экологическая безопасность, М., 2002.
43. Хънтингтън, С., Сблъсъкът на цивилизациите и преобразуването на новия световен ред, С., 1999.
44. Goudie, D., Енциклопедия на глобалните промени. Промяна на околната среда и човешкото общество, т.1 и т. 2, Оксфорд, 2001.

СОЦИАЛНО-ЕКОЛОГИЧНИ ПРОБЛЕМИ НА ГЛОБАЛИЗИРАЩИЯ СЕ СВЯТ

Маргарита К. Бонева

Шуменски университет „Епископ Константин Преславски", Педагогически факултет

SOCIO-ENVIRONMENTAL PROBLEMS OF A GLOBALIZING WORLD

Margarita K. Boneva

Konstantin Preslavsky University of Shumen, Faculty of Education

***Abstract**: It the presents current but not enough investigated socio-environmental problems of a globalizing world. Created conceptual theoretical model to address socio-environmental problems in accordance with the conditions and Circumstances in the country and globalizing world.*

Key words*: *socio-environmental problems, globalizing world

От гледна точка на хронологията глобализацията е емблематична характеристика на двадесетото столетие. Същевременно проблемите, които се описват като глобални не могат да бъдат решени с еднократни действия, а тяхната продължителност може да засегне няколко поколения.

Глобализацията обхваща "целият свят от човешки същества като мигновена и постоянна реалност". Тя е свързана с множество явления, пораждащи неоднозначни последствия, от които по един или друг начин зависи нашето бъдеще.

Социално-екологичните проблеми на глобализацията се свеждат до:

- високо равнище на безработица;
- нарастващ брой финансови кризи;
- засилващо се неравенство в равнището на работната заплата на пазара на труда;
- нестабилност и недостатъчна съгласуваност между икономическата, финансовата, търговската, екологичната и социалната политика;
- недостатъчна заетост на населението в трудоспособна възраст;

• неспазване правата на работниците и трудовите норми в глобалната икономика;

• детският труд;

• жестока бюджетна политика, насаждана от Международния валутен фонд и Световната банка;

• нелегална икономика;

• широко разпространена корупция;

• промяна в традиционното селско стопанство на страните;

• липса на ефективно и демократично управление;

• неравенство на бедни и богати нации;

• нови форми на национализъм;

• етнически и религиозни конфликти;

• накърняване на основни човешки права;

• бедност;

• неравенство на половете;

• несъвършени системи на социална защита;

• отсъствие на подреден режим и правила за трансгранично движение на хора;

• социална несправедливост;

• миграция;

• маргинализация на страни от Близкия Изток и Африка;

• социална поляризация;

• тероризъм;

• пандемия на ХИВ/СПИН в африканските страни;

• търговия с хора и наркотици;

• демографска криза;

• неравен достъп до образование;

• неграмотност и ниска квалификация;

• недостатъчни инвестиции в образованието и професионалното обучение;

• неефективно здравеопазване;

• негативни последици от урбанизацията;

• недостатъчна защита на националните култури;

• изчерпване ресурсите на планетата;

• прогресираща загуба на устойчивостта на екосистемите вследствие тяхното разрушаване;

• глобално антропогенно замърсяване;

• климатични промени.

В Доклада на Световната комисия по социалните измерения на глобализацията се посочва, че за превръщането на глобализацията в «ключ» за по-сигурен живот, в процес, който отчита общопризнатите ценности и правата на човека е необходимо:

• Съсредоточаване на вниманието върху хората - съобразяване с потребностите, правата, културната самобитност, за достоен труд и равенство на половете.

• Изграждане на демократична и ефективно действаща държавна система, притежаваща широки възможности за управление на процеса на интеграция в глобалната икономика, за укрепване на социалния и икономическия потенциал и осигуряване закрила на населението.

• Постигане на устойчиво развитие – глобализация, която се опира на взаимно зависими и взаимно подкрепящи се стълбове на икономическо и социално развитие с приоритети за защита на околната среда на местно, национално, регионално и глобално равнище.

• Създаване на производителни и справедливи пазари в условията на непрекъснато работеща пазарна икономика.

• Разработване на справедливи правила, които да откриват равни възможности за всички като се признават разнообразието от национални потенциални възможности и потребности в областта на развитието.

• Глобализация, основана на солидарността – с необходимата отговорност да се помогне за преодоляване на неравенството както вътре в страните, така и между тях, с цел изкореняване на бедността.

• По-голяма отговорност пред хората - всички държави, трябва да бъдат демократично подотчетни за политиката, която провеждат и за мерките, които приемат.

• По-задълбочено партньорство - диалогът и партньорството да бъдат най-важните демократични инструменти за създаването на по-справедлив свят.

• Усъвършенстване дейността на Организацията на обединените нации - важен залог за създаването на демократични, законни и здрави основи на глобализацията.

• Промяна в съвременната международна политика, която не е способна адекватно да реагира на задачите, възникващи в процеса на глобализация, защото над социалните аспекти преобладават мерките за отваряне на пазарите, както и финансовите и икономическите съображения. Официалната помощ за целите на развитието (ОПР) далеч не покрива дори минималните норми, които са предвидени в Целите в областта на развитието, формулирани в Декларацията за хилядолетието (ЦРТ) и не може да реши изостящите се глобални проблеми.

• Повишаване ефективността на функциониране на многостранната система, отговаряща за разработването и осъществяването на международната политика. Тя страда от политическо късогледство като цяло и освен това е недостатъчно демократична, прозрачна и подотчетна.

Поведението на националните държави като глобални участници в процеса на управление се явява предопределящ фактор за качеството на глобалната мрежа на управление. Степента на тяхната привързаност към идеите на многостранността, универсалните ценности и общите цели, способността им да реагират на междудържавните последици от тяхната политика, както и значението, което те придават на глобалната солидарност, са жизнено важни фактори, предопределящи качеството на глобалната система за управление.

Обобщавайки информацията в редица публикации, доклади и нормативни документи може да се направи извода, че ***социалното измерение*** на глобализацията я представя като:

• Процес, основан на универсално споделени ценности, който изисква всички участници (държавите, международните организации, бизнесът, гражданското общество и медиите) да поемат своята отговорност, като икономическото развитие се основава на спазването на човешките права.

• Духовна и културна глобализация, налагана чрез общи нравствени, духовни и ценностни принципи и общи културни кодове, които проникват на всички нива на обществото, включително до нивото на вярата, ценностите, поведението и възприятията на отделния индивид.

• Международно задължение за осигуряване на основните материални и други искания, гарантиращи човешко достойнство за всички, закрепени във Всеобщата декларация за правата на човека, ликвидирането на бедността и постигането на Целите за развитие през хилядолетието.

• Устойчива траектория на развитие, която създава възможности на всички, за устойчив начин на прехрана и заетост, съдейства за равенството между половете, съкращава неравенството между страните и народите, и гарантира по-голяма съгласуваност на икономическата, социалната и екологичната политика.

• По-демократично управление, гарантиращо по-голямо право на глас и участие като едновременно с това се осигурява пълно зачитане на правомощията на институтите на представителната демокрация и върховенството на закона.

• Уважение към природата с изискване глобализацията да има екологически устойчив характер, да зачита природното разнообразие на живот на Земята и жизнеспособността на планетарната екосистема.

Социално-екологичните проблеми поставят на дневен ред пред цялата международна общност за решаване много въпроси:

• За осъществяване възможностите на глобализацията всички страни трябва да инвестират в реформиращо се образование, професионално обучение, натрупване на технологични възможности и борба с неграмотността.

• Вътрешната политика, трябва да се насочи към увеличаване на стимулите и разширяване на възможностите с оглед хората с висока квалификация да останат в родината си, а това ще реши проблема с трансграничното движение на хора.

• Урбанизмът е не само част от обществото, а е израз на влияние върху същността на по-широката социална система. Градът е концентриран израз на противоречия, конфликти и проблеми (бедност, етническо разделение, противопоставяне между бели и чернокожи, престъпност, несигурност).

• Сред ключовите цели на социалното развитие международната общност обръща особено внимание на здравеопазването. Концепцията "здраве за всички" е важна тема на последните дебати за повишаване достъпността на лекарствените средства. Бързото разпространение на инфекциозни болести е една от глобалните беди на нашия взаимосвързан свят.

• Глобализацията насърчава научния и технологичен процес, правейки европейското измерение още по-важно за развитието на знанието, мобилността, конкурентноспособността и иновациите. Основна цел на Европейския съюз след 2020 г. ще бъде икономиката да се трансформира в икономика на знанието, за да стане по-конкурентноспособна, свързана и екологична. Това означава, че ще продължат усилията за ограничаване на изчерпването на ресурсите, без да се спира модернизацията на промишлените сектори, при по-ефективно използване на материалните фактори за постигане на по-голяма производителност. Намаляването на риска от нарастване на социалната поляризация в регионите и справянето с отрицателните ефекти на глобализацията изисква образователните системи да се адаптират към нуждите на пазара на труда и да се повиши ефективността на квалификациите и преквалификациите.

• Второто десетилетие на XXI в. ще наложи справяне с неравномерната концентрация на населението в ЕС и миграционните процеси в него. Очаква се населението в работоспособна възраст да намалее, както и демографски срив в някои райони. Това ще доведе до намаляваща работна сила, по-високи разлики в доходи-

те и регионална политика, която цели териториално сближаване и справяне с негативните последици от урбанизацията.

• Икономическият растеж на регионите след 2020 г. ще означава и повишаване на уменията на хората, запазване на конкурентноспособността на пазара на труда, подобряване на регулаторната среда, с цел постигане на териториално сближаване и по-добри условия за предприемачество.

• Друго сериозно предизвикателство пред ЕС след 2020 г. ще бъде справянето с последиците от климатичните промени, които влияят върху икономическите, социалните и екологичните системи. За районите, изложени на риск от наводнения, крайбрежна ерозия, изтощение на почвата и сушата, ЕС трябва да изработи стратегия за диверсикация на традиционните икономически дейности.

• Революцията в информационните и комуникационните технологии (ИКТ) в съчетание с намаляването на транспортните разходи създава както технически, така и икономически възможности за увеличаване на производството на стоки и услуги, широко разпръснато в много страни. Стана възможно производствените процеси и техните елементи да се разположат по целия свят, използвайки икономическите предимства, свързани с разликите в разходите, наличието на производствени фактори и инвестиционния климат, както и да се контролират благодарение на съвременните средства за комуникации.

• От една страна, новите технологии променят международните сравнителни преимущества, в резултат на превръщане на знанието във важен фактор на производството. Наукоемките и високотехнологичните отрасли на промишлеността като най-бързо развиващите се сектори на глобалната икономика изискват по - големи инвестиции в образованието и в професионалното обучение.

• Бурният растеж на Интернет рязко ускори глобализацията на свободния пазар. С появата на глобалните производствени системи, които съдействат за увеличаване на потока от преки чуждестранни инвестиции, възникват нови възможности за растеж и индустриализация в развиващите се страни. Около 65000 многонационални предприятия с приблизително 850000 техни чуждестранни дъщерни компании играят ключова роля във функционирането на тези глобални производствени системи.

• Икономическите изгоди и социалната цена на глобализацията се разпределят неравномерно между социалните групи.

• Ключови елементи на глобалната икономика са образованието, професионалните навици и знания, които имат все по-нарастващо значение за икономическото оцеляване, но равнището на инвестиции в образованието е крайно недостатъчно. Статистическите данни показват, че от 680 милиона деца на ранна училищна възраст в развиващите се страни 115 милиона не ходят на училище, а от тях 65 милиона са момичета. От всеки две деца, които посещават училище, само едно завършва.

• Едно от важните изменения е свързано с повишаване равнището на глобалното съзнание.

• Основните принципи, които трябва да ръководят процеса на глобализация, са демокрация, социална справедливост, уважение на правата на човека и върховенство на закона.

• Всички страни страдат от лошо управление, независимо от формата. Корупцията е широко разпространена в много развиващи се страни, като нанася особени

щети на най-бедните слоеве на населението, изключени от сферата на държавните услуги и подлагани на произвол.

- Световният демографски растеж, особено в Третия свят заплашва да се превърне в глобална катастрофа. Натискът върху ограничените ресурси на света, би могъл да доведе до глобален конфликт, който да завърши с големи войни. Небалансираната възрастова структура на неиндустриалните страни задълбочава техните социални и икономически затруднения. Младото поколение се нуждае от издръжка и образование и през това време е икономически непродуктивно. Много от страните на Третия свят нямат ресурси да осигурят всеобщо образование, в резултат на което децата започват целодневна работа или свързват двата края с улична просия. Порасналите "улични деца" стават безработни, бездомни или и двете заедно.

В настоящия момент, глобалните ресурси в света не са достатъчни, за да осигурят в Третия свят жизнен стандарт, сравним с този в индустриалните страни.

Държавата има важна роля в управлението на процеса на интеграция в глобалната икономика. Тя гарантира съответствието в управлението както на икономическите, така и на социалните цели.

На Срещата на високо равнище за хилядолетието държавните глави и правителствените ръководители утвърдиха осем глобални цели, свързани със социално-екологичните проблеми като всичките трябва да бъдат постигнати до 2015 година. Това са:

- Изкореняване на крайната бедност и глада.
- Осигуряване на всеобщо начално образование.
- Съдействие за равенство на половете и предоставяне правомощия на жените.
- Намаляване на детската смъртност.
- Подобряване на опазването на здравето на майките.
- Борба с ХИВ/СПИН, маларията и други болести.
- Осигуряване устойчивост на околната среда.
- Създаване на глобално партньорство за целите на развитието.

Литература

1. Василенко, В. Н., Экологические конфликты общества как предмет социологии и социальной экологии, Ноосфера,1998, с. 73- 79.
2. Гиренок, Ф., Экология. Цивилизация. Ноосфера, М., 1987, с. 22
3. Комаров, В. Д. Социальная экология. Философические аспекты, Л., 1990.
4. Коммонер, В., Замыкающийся круг. Природа, человек, технология, Л., 1994.
5. Корнеева, А., Общество и окружающая среда, М., 1985.
6. Лацко, Р., Икономически проблеми на жизнената среда, С., 1980.
7. Малофеев, В. И., Социальная экология. М., 2003.
8. Мармот, М. и др., Социални детерминанти на здравето, Оксфорд, Великобритания, 1999.
9. Моисеев, Н., Человек, среда, общество. Проблемы формализованного описания, М., 1982.

УПРАВЛЕНИЕ НА СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ

Цветлин Й. Йовчев

MANAGEMENT OF THE NATIONAL SECURITY SYSTEM

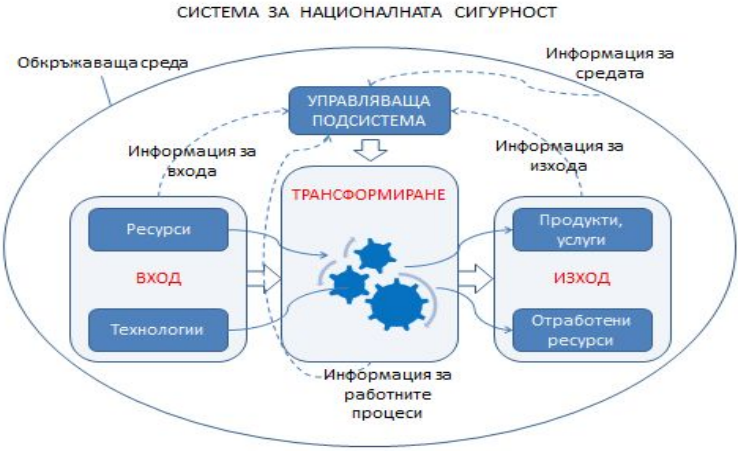
Tsvetlin Y. Yovchev

Abstract: The Management of the National security system needs a comprehensive, systematic and architecture approach with detailed assessment of the environment influence.

Key words: National security, management

„Национална сигурност“ е динамично състояние на обществото, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите, основните права и свободи на гражданите, устойчивото икономическо развитие и благосъстоянието на населението, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети“[1] .

Постигането на такова устойчиво, динамично състояние изисква изграждането на система от взаимосвързани и взаимно зависими елементи, които да бъдат организирани съгласно общи принципи, ред и правила и подчинени на общата цел. Всеки един от тези елементи по своята същност също представлява един вид социална система (или част от такава) на входа на която постъпват ресурси и технологии, а на изхода излизат продукти, услуги и отработени ресурси (фиг. 1).



Фиг.1

Създадените продукти и услуги въздействат върху обществените процеси и обкръжаващата среда, като по този начин предполагат определено състояние на обществото – национална сигурност.

Изхождайки от горното, системата за национална сигурност следва да се разглежда, като система от системи (подсистеми) функционираща в непрекъснато променяща се среда. Тя не бива да се разглежда като механичен сбор на елементи. Най-съществено в нея са изградените връзки и отношения между отделните части, като в резултат на това взаимодействие, тя придобива качества, които превишават сумата от качествата на отделните звена и изграждат способности, които са непостижими, ако отделните структурни единици са самостоятелни и независими – ***синергичен ефект*** [2].

Градивните й елементи – подсистемите, притежават няколко основни характеристики. Те са ***отворени*** и ***активни*** защото при своето функциониране пряко взаимодействат със средата (черпят свежи и изхвърлят отработени ресурси и въздействат върху нея посредством създадените продукти и услуги). Те са ***динамични***, защото се променят непрекъснато като функция от промените в обкръжаващата среда, както в резултат от прякото взаимодействие с нея, така също и в резултат на процесите на адаптация, с цел да гарантират съществуването и успешното си функциониране. Те са ***непълно определени*** поради непрекъснатия им процес на промяна, както и априорната неопределеност на средата. Те са ***сложни*** и ***неоднородни***, тъй като елементите им обединяват хора, ресурси, технологии, информация и др. За да оцелеят и да се развиват успешно те, също така трябва да бъдат и ***конкурентноспособни***.

Трансформирането и преработването на достъпните за системите ресурси практически е един производствен процес на създаване на продукти и услуги. В основата му, разбира се е вложения по определени технологии труд, но успешното реализиране и ефективност зависят и от съобразяването му с изградените обществени отношения и природните особености в обкръжаващата среда. В този ред на мисли производството на стоки и услуги може да бъде представено, като резултат от взаимодействието на няколко фактора: *Труд* на работещите в съответната организация; *Наличните технологии* за създаването на продукт или услуга; *Достъпните ресурси* – финансови, материални, човешки, информационни, време и др.; *Обществени отношения* – политически, икономически, социални и др.; *Природните особености* – климат, релеф, води, състав на почвите, сеизмична активност, слънчева активност, движение на въздушните маси и др.

Повечето от изброените фактори са извън системата и от гледна точка на функционирането й се явяват параметри на обкръжаващата среда. Вложения в производството труд представлява целенасочена човешка дейност и зависи от личностната мотивация. В този контекст той също е функция от средата, доколкото тя е съществен фактор при формиране поведението на индивида. От тук можем да направим извода, че ***съществуването и успешното функциониране на системата за национална сигурност зависи в значителна степен от процесите в обкръжаващата среда***. Тук под ***обкръжаваща среда*** разбираме всичко извън границите на системата, което взаимодейства с нея и в резултат на това взаимодействие се обменя маса, енергия и информация [3].

Адаптацията спрямо условията на средата, не само е важна, в съвременните условия тя е решаваща за всяка една човешка дейност. Обкръжаващата среда е в

състояние съществено да промени условията или силите, които въздействат върху системата. Голямата динамика изисква изключително бърза реакция в управлението й, за да я приведе в това състояние, което ще позволи достигане на поставените цели в новите условия.

Фиг. 2

В този контекст СНС следва да се разглежда като една непрекъснато променяща се система, функционираща в непрекъснато променяща се среда. Във всеки момент тя се намира в различно състояние, функция от което са и резултатите от дейността й. Наред с това съществуват функционални зависимости между процесите в средата и организационните способности на отделните й елементи, като тези зависимости също се променят във функция от времето. Изхождайки от това един от ключовите въпроси на управлението е изграждането на способности да се дефинира състоянието (взаимодействие система за национална сигурност – среда) и да се прогнозира бъдещото му развитие. Въздействието на глобалните процеси върху системата за национална сигурност винаги следва да оценява и в контекста на влиянието им върху процесите в страната (фиг. 2).

При прилагането на системния подход (***съставните части - организациите се възприемат като динамични, сложни, неоднородни, непълно определени, активни, отворени, самообучаващи се, конкурентноспособни системи, свързани от взаимодействащи си части, обединени от обща цел***[4]) отделните елементи трябва да бъдат изградени в съответствие със следните принципи [5]:

Синергизъм (значението е описано по-горе); *Гъвкавост* – способности да намира различни пътища и да прилага различни способи за постигане на желания резултат; *Условност* – конкретната ситуация (процесите в обкръжаващата среда, целите и ресурсите) е определяща за това как функционира системата; *Ефикасност* – желаният резултат се постига с изразходването на минимални ресурси; *Ефективност* – постигане на максимално възможни резултати с разполагаемия ресурс.

Същност на процеса на управление на системата за национална сигурност

Управлението е организиране, направляване на дейност [6]. Независимо от формата, под която е организиран процеса на управление той винаги е свързан с упражняването на власт на човек или група от хора над други хора. ***Властта*** е капацитет в отношенията, който дава възможност на личността да влияе асиметрично върху решенията на други хора по начин, който позволява на овластения да реализира интересите си или да извлече полза [7]. От тук в основата на ***управлението*** е правото и възможността да се вземат решения, а на основата на тях и да се предприемат действия за това как следва да бъде организиран централния работен процес, така, че да генерира в достатъчен обем стойност за потребителите, акционерите и членовете на организацията.

Разглеждайки организациите в контекста на управлението виждаме, че се появява нов значим елемент – ***ръководителя***. Посредством властта той получава права да взема решения от името на и отнасящи се до функционирането на съответната организация, като същевременно има възможност да реализира свои собствени интереси. Успешното управление е свързано и със способностите да се постигне синхрон и хармония в неговите и организационните интереси, а това е свързано пряко с формата, под която се упражнява властта.

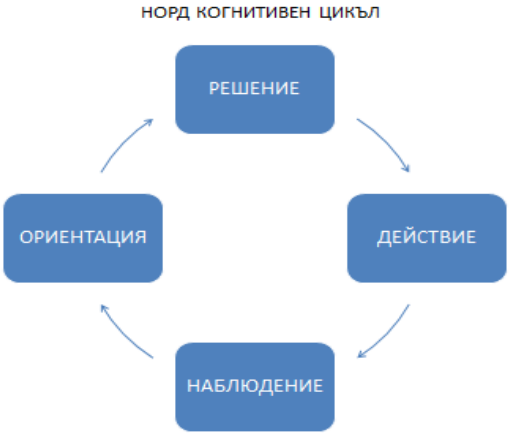
В началото на 20-ти век Анри Файол дефинира пет ***основни функции на ръководителя*** [8]: *Планиране* – процес на изграждане на мисия, визия, стратегия, цели, програми и обвързването им в йерархична зависимост; *Организиране* на ЦРП – технология на дейност, структура, функционални задължения на отделните звена, длъжностна характеристика на членовете на организацията; *Интегриране* – изграждане на организационна култура, създаване на организационно взаимодействие и комуникация между отделните звена; *Ръководство* – лидерство, мотивация, управление на конфликтите; *Контрол* – осигуряване на наблюдаемост и управляемост на процесите в организацията.

Можем да дефинираме две основни насоки в управлението на организациите:Организиране и поддържане на непрекъснат и ефективен централен работен процес;Успешно адаптиране на този процес спрямо промените в обкръжаващата среда.

Управлението може да се дефинира като съвкупност от анализи, решения и действия целящи създаването и поддържането на конкурентно предимство[9]. Под ***конкурентно предимство*** разбираме постигането на такива организационни способности, които позволяват при еднакви други условия организацията да доминира над опонентите си.

Постигането на конкурентно предимство в значителна, дори решаваща степен зависи от способностите на системата, а получава и обработва релевантна информация за случващото се в обкръжаващата среда и функционирането на централния работен процес.

През 1964 г. полковникът от армията на US Джон Бойд предлага концепция за управление, наречена ***НОРД когнитивен цикъл*** [10], целяща конкурентно предимство над опонентите посредством постигане на информационно превъзходство. Реализацията на този цикъл преминава през четири взаимосвързани и взаимно зависими етапа: *Наблюдение* на процесите в средата и организацията; *Ориентация* за причинно следствените връзки в тези процеси; *Решение* какво и как следва да се промени в дейността на организацията; *Действие*.



Фиг.3

Идеята в този модел, е че при рязко съкращаване на времето за реализиране на цикъла и значително увеличаване на обхвата му може да се постигне информационно превъзходство над опонентите. При едни и същи ресурси организацията може да получи информационно превъзходство, а от там и конкурентно предимство когато:*Разшири обхвата на НОРД когнитивния цикъл (областите, в които се осъществява наблюдение);Съкрати времето за реализацията на НОРД когнитивния цикъл.*

Разглеждайки управлението на системата, като съвкупност от анализи, решения и действия е важно да направим уточнението, че съществува определена ***последователност и йерархична зависимост*** между тях. Управлението винаги следва да се разглежда като ***процес*** или като действия, събития или промени, които са в причинно-следствена връзка. При този процес отделните съставни елементи изпълняват различни функции във времето, което предполага прилагането на архитектурен подход при управлението. ***Архитектурен подход*** имаме тогава, когато концептуалния модел на промяната се разглежда като съвкупност от градивни елементи, техните взаимовръзки, функциите на отделните компоненти и протичащите процеси[11]. Един от най популярните модели на организационна архитектура – аспекти и перспективи е разработен от Джон Захман – ***рамка на Захман*** [12] (табл. 1).

Табл. 1. Рамка на Захман

	Артефакти Какво?	Дейности Как	Разположение Къде?	Хора Кой	Време Кога?	Мотивация Защо?	
Планиращ							Обхват
Собственик							Орг.модел
Конструктор							Сист. модел
Изпълнител							Техн.модел
Доставчик							Компоненти
	Данни	Функции	Мрежа	Организация	График	Стратегия	

Както посочихме по-горе, промените в обкръжаващата среда влияят съществено върху процесите във всяка организация, а от там и върху резултатите от дей-

ността й. За да постигне успех организацията трябва да реагира адекватно на всяка една промяна и да се адаптира успешно спрямо новите условия. От тук и управлението винаги следва да се разглежда като ***цикъл***, при който решенията и действията на ръководителите са функция от промените в средата и от постигнатите резултати на съответната организация.

Създаването на стратегията е последователност от решения и изисквания от по-високите към по-ниските нива на управление, а реализирането й е процес на изграждане и свързване на отделните компоненти от по-ниските към по-високите (фиг. 4). Съвременните организации са сложни системи, при които създаването на крайния продукт или услуга е резултат от взаимодействието на различни по своите функции звена и управляването на различни по своя характер процеси, като ***успешното съгласуване и предотвратяването на колизии има ключово значение за ефективното и успешно функциониране на системата***. В този контекст трябва да съществува, както вертикална, така също и хоризонтална съгласуваност на процесите в управлението, която да се осъществява на няколко нива: *Парадигма за национална сигурност; Системен модел; Функционален модел; Технически модел; Компоненти*.

Фиг. 4

Стратегията може да се определи като технология на управленската дейност [13] Тя описва начина и пътя, по който да се изпълни мисията и по своята същност представлява набор от правила за вземане на решения [14]: Правила при използване на резултатите от дейността на организацията; Правила за изграждане на отношения на организацията с обкръжаващата среда; Правила, по които се установяват отношенията и процедурите в организацията; Правила, по които организацията извършва ежедневната си дейност.

Целта на тези правила е *да се организира и поддържа непрекъснат и ефективен централен работен процес, както и да се създадат възможности този процес*

да бъде адаптиран успешно спрямо промените в обкръжаващата среда.

Всяко едно организационно състояние има жизнен цикъл, който зависи от промените в обкръжаващата среда. Мисията, визията и стратегията дефинират технологията на преработване и/или трансформиране на ресурсите в продукти или услуги (централен работен процес) и нейното взаимодействие с обкръжаващата среда. Промяната в структурата, организационното взаимодействие и корпоративна култура задават определено състояние на системата, което позволява постигането на конкурентно предимство. Измененията в обкръжаващата среда въздействат в значителна степен и технологията на дейност (ЦРП) вече не е толкова ефективна в новите условия, което налага предефиниране на мисията, визията и/или стратегията, за да бъде постигането отново конкурентно предимство.

Този цикъл зависи изцяло от изградените способности за управление на информацията.

Фиг. 5

В заключение можем да обобщим, че успешното управление на системата за национална сигурност изисква от ръководителите цялостен, системен, архитектурен подход, който е изграден на основата на организационните способности за наблюдение и управление на процесите в системата и процесите в обкръжаващата среда.

Използвана литература

1. Закон за Държавна агенция „Национална сигурност“
2. Семерджиев Цв., Стратегическо ръководство и лидерство – среда, 2007, стр.35
3. Wikipedia
4. Семерджиев Цв., Стратегическо ръководство и лидерство - среда, 2007, стр. 38
5. Семерджиев Цв., Стратегия, 2007, стр. 24

6. Буров С., В Бонджолова, М. Илиева, П. Пехливанова, Съвременен тълковен речник на българския език, 1995, стр.947
7. Castells M., Communication Power, 2009, стр.10
8. Роббинз С., М. Коултер, Менеджмент, 2007, стр.38
9. Dess G., G. Lumpkin, A. Eisner, Strategic Management, 2008, стр. 8
10. Семерджиев Цв., Стратегически информационни системи, 2007, стр.222
11. Сариев Ив., Мениджмънт на информацията, 2008, стр.39
12. Federal Enterprise Architecture Framework – Version 1.1, 1999, стр.20
13. Семерджиев Цв., Стратегия, 2007, стр. 18
14. Семерджиев Цв., Стратегия, 2007, стр. 45

ПОДХОД КЪМ ОСИГУРЯВАНЕТО БЕЗОПАСНОСТТА НА ОБЕКТИТЕ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА

Христо А. Десев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ „ВАСИЛ ЛЕВСКИ” В.ТЪРНОВО
ФАКУЛТЕТ „АРТИЛЕРИЯ, ПВО И КИС”
ШУМЕН УЛ. КАРЕЛ ШКОРПИЛ №1 КАТЕДРА „ОУТП ОТ ПА”

APPROACH TO ENSURING SECURITY TO THE OBJECTS OF THE CRITICAL INFRASTRUCTURE

Hristo A. Desev

Abstract: The essence of the methodology is based on the planning of the index of the obejct risk, which depends on its rating in the factors scale, as well as, on the weight of every factor. This method can be applied as a mark on the vulnerability of the objects, which are caused by different kinds of threats.

Key words: crisis, management, threat, hazardous factors

В съвремието ни съществуват достатъчно обекти, чието поразяване може да нанесе достатъчно големи вреди на държавите и техните граждани. Това са не толкова военни обекти, а по-скоро обекти от гражданския сектор, при чието каскадно извеждане от нормалните параметри на работа могат да се получат щети сравними с резултатите от въоръжен конфликт. Болшинството от страните систематизират тези потенциално опасни обекти с термина “критична инфраструктура”.

Критичната инфраструктура е термин, използван от правителствата за описване активи, които са от съществено значение за функционирането на обществото и икономиката. Най-често се свързва с понятия, които са съоръжения за:

- производството на електроенергия, пренос и разпределение;
- производството на газ, транспорт и разпределение;
- петрол и петролни продукти, производство, транспорт и дистрибуция;
- далекосъобщителни;

• водоснабдяване (питейни води, отпадни води / канализация, произтичащи от повърхностни води (напр. диги и шлюзове);

• селското стопанство, производството на храни и разпространение;

• отопление (например, природен газ, мазут, централно отопление);

• общественото здраве(болници, линейки);

• транспортни системи (доставка на гориво, железопътната мрежа, летища, пристанища, вътрешните морски);

• финансови услуги (банки, клирингови);

• службите за сигурност (полиция, военни).

Най-общо те могат да се обединят в следните три групи:

• обекти осигуряващи националната безопасност;

• обекти необходими за решаване на задачи при осигуряването на националната безопасност;

• обекти намаляващи качеството на безопасността и икономическото състояние, банковия сектор, кредитно-финансовата система, енергетика, транспорт.

Ако анализираме различните подходи към организацията на осигуряването на безопасност на критичната инфраструктура различаваме няколко основни направления:

• разработване на национален план за осигуряването на безопасност на критичната инфраструктура с определяне на контролни точки за анализ на заплахите;

• изготвяне на програми за ликвидирането на заплахите във всеки сектор от промишлеността и икономиката;

• организация на сътрудничеството и взаимодействието между частния и държавния сектор;

• създаване на специализирани подразделения отговарящи за реализация на задачи по осигуряване на безопасността елементите от критичната инфраструктура;

• координация на такива подразделения с частните фирми;

• строга организация на системата за ранно предупреждение и оповестяване.

В качеството на основни заплахи се явяват: терористични действия, , природни явления, техногенни аварии и човешката дейност.

Осигуряването на приоритетна безопасност и реализацията на мерки за защита предполага постигането на:

• осъществяване на превантивни мерки насочени към недопускане на въздействия върху обектите от критическата инфраструктура;

• понижаване на нивото на уязвимост на тези обекти;

• стремеж за минимизация на загубите и вредите;

• създаване на възможност за бързо отстраняване на последствията и намаляване на вторични въздействия.

Като цяло тази предстояща задача може да се формулира в следния вид:

• водене на целенасочено разузнаване на обектите, характера и способите на заплахите;

• усилване на комуникациите, предпазните и превантивните мерки за следене на опасностите;

• защита на основни ключови обекти от които може да се наруши устойчивото функциониране на държавата;

• предотвратяване на достъпа на терористични организации до технологии и материали за създаване на оръжия за масово поразяване;

• създаване на национална система за реагиране на извънредни ситуации (планиране, снабдяване на специални подразделения, медицински екипи, противопожарни екипи и др.)

Съществен момент е определяне на оценката за уязвимостта на отделните обекти в зависимост от тяхната важност. Примерен модел с предложения в таблица 1.

Таблица 1

№ по ред	Фактори	Диапазон на оценката	Параметри на оценката	Тежестен коефициент	Ред за определяне на рейтинга
1.	Влияние върху реализацията на основното производство	1- 3	Оценката се определя от анализа на производството необходимо за икономиката на региона (страната). Количество, степен на участие и важност на реализираните и планираните програми.	15	1- най-маловажен 2 – междинен 3 – най-много важен
2.	Влияние върху възможностите на региона.	1-3	Оценката се определя от значимостта на производството за текущи задачи. Отчитат се цикличността на производство, запасите от определена продукция	14	също
3.	Влияние върху планираните възможности	1-3	Оценката се базира на важността на предприятието в производ-ството на продукция за перспек-тивни програми, аналитична оценка на технологичната готовност	13	също
4.	Корпоративен и финансов риск	1-3	Възможности за справяне с кризата. Оценката се базира на аналитична преценка на обема от информация за фирмата.	12	също
5.	Показател за икономическа жизненост на обекта.	1-3	Аналитична преценка с отчитане на численост на сътрудниците, дългове, дистрибуция, контакти с други производства, възможности за замяна на производството.	11	също
6.	План за възстановяване	1-3	Планирани мероприятия по ликвидиране на последствията. В основата лежи прогнозата за пълно възстановяване на производ-ството. Важи за обекти с непълни разрушения и не работили до 60 дни.	10	също
7.	Временни потребности за възстановяване	1-3	Отчитат се последствията от атаки на сигурността. Мероприятия за преодоляване на последствията, анализ на максимално допустимото прекъсване на производството и времето за пълно окомплектоване с персонал.	9	също
8.	Потребности за	1-5	Стойност на загубите по възстановява-	8	също

	възстановяване.		не на обекта.		
9.	Заплахи	1-3	Оценката се осъществява въз основа на заплахите в региона, а при отсъствие на сведения за такива от важността на региона.	7	също
10.	Отработеност на въпросите по обезпечаване на безопасността.	1-3	Оценката се осъществява на основата на проверката на готовността на населението (персонала) за действие при бедствие.	6	също
11.	Вероятност за опасност	1-3	Наличие на опасни вещества и тяхното състояние и оборудване.	5	също
12.	Вероятност от съпътстващи поражения	1-3	Оценява се риска от съпътстващи поражения при възникване на авария.	4	също
13.	Численост на населението в околностите	1-3	Този фактор представлява важен елемент като крайно число и като трудозаето население	3	също
14.	Реагиране на контролната дейност	1-3	Готовност на администрацията да координира и сътрудничи на общата защита на критичната инфраструктура.	2	също
15.	Оценка на уязвимост и безопасност при изпълнение на задачите.	1-3	Оценява се сложността и опасността на прилагането на плана по защитата.	1	също

Определянето на степените на уязвимост на обектите може да се извършва по предлаганата методика с основна тежест върху важността на обекта за разглеждания регион. Същността се заключава в разчета на индекса на риск за обекта, зависещ от рейтинга му от скалата с фактори и тежестта на всеки фактор. Приложения метод може да се използва за оценка уязвимостта на обекти от различни по характер заплахи.

Друг съществен елемент от осигуряването на безопасността е планирането на защитата на критичната инфраструктура. Тя трябва да предлага преди всичко създаване на инструменти за осигуряване на координацията, партньорството в интерес на безопасността, изпълнението на дългосрочни програми за снижаване на степента на риска, достигане на максимален ефект от използването на ресурсите отделяни за защитата на инфраструктурата на държавата.

Основни направления за планиране на защитата могат да бъдат:

- всестранен подход и обединяване на различни структури на властта, възможностите и ресурсите на страната и отделния регион;
- комплексна и достоверна оценка на състоянието на инфраструктурата с което се разпределят приоритетите по организацията на защитата и се приемат адекватни мерки за защита и възстановяване;
- организация и координация на партньорството на всички нива от висше държавно до частния сектор;
- интеграция на усилването на защитата на физическите обекти, киберпространството и населението;
- прилагане на сложна методология на анализ и моделиране при разработването на модели на защитата;
- повишаване на ефективността при противодействието на разрушенията.

Разгледания проблем структурира следните изводи

1. Успеха в глобалното осигуряване на безопасността е разработване на национален план за осигуряването на безопасност на критичната инфраструктура с определяне на контролни точки за постоянен анализ на заплахите;

2. Характера на кризите и процеса на тяхното развитие определят създаване на специализирани подразделения отговарящи за реализация на задачи по осигуряване на безопасността елементите от критичната инфраструктура и координация на такива подразделения с частните фирми;

3. Разработване на строги и интегрирани модели за защита и превантивни действия при осигуряване на безопасността на обектите.

Използвана литература:

1. National Infrastructure Protection Plans – октомври 2006 г.

2. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets – февруари 2003 г.

3. National Strategy for Homeland Security – юли 2002 г.

4. Решение 2004/277/ЕО, Евратом относно правилата за прилагане на Решение 2007/779/ЕО, Евратом на Съвета за създаване на механизъм на Общността за гражданска защита

ИНФОРМАЦИОННА СИГУРНОСТ И МЯСТОТО Й В СИСТЕМАТА НА НАЦИОНАЛНАТА СИГУРНОСТ

Николай Й. Досев

Шумен ул. „Карел Шкорпил" 1 Факултет „Артилерия, ПВО и КИС"

INFORMATION SECURITY AND ITS PLACE IN THE SYSTEM OF NATIONAL SECURITY

Nikolay Y. Dosev

Shumen, 1 Karel Shkorpil Str., Faculty of Artillery, Air Defence and CIS

Abstract: *This paper deals with the nature of the term informational security and analyses the main threats to information security in regard to individual, state and society. The author highlights the relation between national security and the other subsystems of the system of national security in The Republic of Bulgaria.*

Key words: *information security, national security, system of national security, information, information society*

Националната сигурност е една от основните категории на съвременната политическа наука. Тя е непосредствен спътник на обществения живот и един от неговите съществени признаци. Не случайно идеята за устойчивото развитие на чове-

чеството все по-вече се свързва със сигурността, разбирана в най-широкият смисъл на думата. За страна като нашата, която тепърва ще устоява мястото си на пълноправен член на Европейския съюз и НАТО изграждането на надеждна и ефективна система на национална сигурност вписваща се в регионалната и световната системи за сигурност е от съществено значение. В новите условия, стратегията ни сигурност не се ограничава в националните рамки, а представлява част от усилията на нашите съюзници. Рисковете и заплахите за сигурността на Република България и нейните граждани до голяма степен съвпадат или са сходни с тези, които застрашават и други страни от ЕС и НАТО. Ефективността на системата ни за сигурност зависи от взаимното доверие и сътрудничество между държавните институции, частния сектор, неправителствените организации и гражданите, а също така и със страните партньори за обмен на информация и съвместни действия. [1]

Понятието сигурност през последните години на миналия и в началото на новия век претърпя съществена еволюция. В условията на бурно развитие на информационните технологии и особено след събитията след 11.09.2001 г. ролята на информационния фактор в сигурността непрекъснато расте. Качеството на информацията, начините за нейното събиране, обработка, анализ и съхранение имат изключително важно значение за вземането на адекватни решения и своевременното им прилагане в сферата на сигурността. Поради тази причина наред с другите подсистеми – политическа, военна, социална, екологична и т.н. подсистемата за информационна сигурност става една от основните подсистеми от системата на сигурност на всяка държава без която не може надеждно да се гарантира мирното настояще и бъдещето на обществото.

За съжаление в България няма общоприето определение на понятието информационна сигурност. Редица други страни имат разработени различни документи в които е дефинирана информационната сигурност, разгледани са основните проблеми, източниците на заплахи и са разработени методите и държавната политика по осигуряването на информационна сигурност на държавата.

САЩ като държава с най-високо развити информационни технологии още през далечната 1906 г приема закон за защита на информацията. В настоящия момент в САЩ действат над 500 законодателни акта по отношение на компютърните престъпления и защитата на информацията. Проблемите на информационната безопасност се определят като един от ключовите елементи на националната сигурност. Според речника на военни термини, информационната сигурност се заключава в осигуряване на защита на информацията и информационните системи от неоторизиран достъп или изменение на информацията при нейното съхранение, обработка и предаване или противодействие на отказа от обслужване на оторизирани ползватели или осигуряване на обслужване на неоторизирани ползватели. Информационната безопасност включва необходимите мерки за определяне, документиране и предотвратяване на такива заплахи. [2]

Руската федерация има разработена доктрина за информационната сигурност в която информационната сигурност е дефинирана като състояние на защитеност на националните интереси в информационната сфера, характеризиращи се със съвкупността от балансирани интереси на личността, обществото и държавата. Според авторите й тя служи като основа за формиране на държавна политика за осигуряване на информационна сигурност, както и за подготовка на предложения за усъвършенстването на правовото, методическото, научно-техническото и организационно

осигуряване на информационната сигурност на Руската федерация.[3]

Както във всяка една сложна система, каквато несъмнено е и системата на националната сигурност, нейните подсистеми, елементи и връзките между тях са много сложни и непредсказуеми. В тази връзка, подсистемата на информационната сигурност оказва съществено влияние върху останалите подсистеми, но същевременно се влияе и зависи от тяхното състояние.

В политическата сфера това влияние се отнася до непрекъснато нарастване на ролята на информираността на отделните политически опоненти при тяхното ежедневно противопоставяне.

В икономическата сфера - икономическия потенциал на всяка държава все повече се определя от обема на информационните и ресурси и най-вече от нивото на изградената информационната инфраструктура и надеждността на функциониране и. Добиването на такава информация и изграждането на модерна инфраструктура обаче е свързано с изразходването на все по-вече финансови ресурси и използване на последните достижения на информационните технологии.

Не бива да се пренебрегва и ролята на информационния фактор във формирането и провеждането на балансирана и полезна за обществото външна политика. Без наличието на достоверна, актуална и пълна информация вземането на верни външнополитически решения и предотвратяването на използването на тази информация в ущърб на обществените интереси е невъзможно.

От своевременно добитата информация за бъдещи природни катаклизми (земетресения, изригвания на вулкани, унищожителни вълни цунами и др.) както и за размерите и характера на крупни промишлени аварии и катастрофи до голяма степен зависи сигурността на гражданите в цели региони, както и ефективността на взетите решения за своевременно ликвидиране на последствията от тях. Пример за това са опустошителното земетресение в Япония и авариите в ядрените й централи които създадоха опасност за целия азиатски континент. Решаването на екологичните проблеми и задачи е свързано със сбора и обработката на информация за състоянието на природната среда и с моделиране на мащабните глобални процеси протичащи в природата. Това е немислимо без наличието и използването на съвременните информационни средства и технологии. Изграждането на надеждна система за мониторинг, би позволило запазването на биологичното равновесие в природата, предприемане на превантивни мерки в резултат на прогнозиране на природните бедствия и създаване на нормални условия за живот на бъдещите поколения.

Може би най-съществена роля информационният фактор играе във военната сфера. Събитията през последните десетилетия, локалните военни конфликти, разработените стратегии за „мрежово-центрични войни", способите за добиване на стратегическа информация за евентуалния противник показват непрекъснато нарастване на ролята на информацията за постигане на планираните цели. Изхода от въоръжената борба вече пряко зависи от качеството на добиваната информация и информационните технологии с които са създадени средствата за разузнаване, системите за управление на войските, високоточните оръжия и другите средства за поразяване.

От казаното до тук е видно, че информационната сигурност се явява основна подсистема на националната сигурност, органически свързана с политическата, икономическата военната, социалната, екологичната и другите съставящи я подсистеми. Същевременно тя е относително самостоятелна сфера, предназначена да

осигури надеждна защита на информационните ресурси, системата за тяхното формиране и дейност, както и информационната инфраструктура на държавата.

Информационното въздействие, независимо от начините на неговото проявление все по-вече се превръща в основен способ за управление на хората, заменяйки физическото въздействие считано до сега като основно средство за управление. През последните години възможностите на средствата за масово осведомяване както и тези на социалните мрежи нараснаха толкова много, че те вече са в състояние да създадат политически сътресения на всеки политически режим, да провокират национални, социални и религиозни конфликти което да доведе до непредвидими последствия за мирното съществуване и демократичното развитие на цели региони. Пример в това отношение са събитията в началото на 2011 г. в държавите от северната част на Африканския континент – Либия, Египет, Тунис, Йемен които и до днес не са намерили своето мирно и цивилизовано решение. Подобни целенасочени информационни въздействия могат да доведат до сриване на извоювания авторитет на държавата, до снемане на доверието от страна на международната общност и пълната й изолацията в световен мащаб. Не бива да се подценява и ролята на информационния фактор в сферата на образованието, в процесите на формиране на личността, създаването на ценностна система на подрастващото поколение, изграждането на модел на поведение на отделния гражданин и отделни социални групи от обществото. Тази роля в следващите години непрекъснато ще нараства поради което и националната сигурност на страната все по-вече ще зависи от гарантирането на информационната й сигурност.

Основните субекти на националната сигурност са отделната личност, обществото и държавата. Какво е влиянието на информационната сигурност върху всеки от тях и какви задачи следва да се решат за гарантиране на сигурността им в това отношение.

Интересите на личността в информационната сфера се състоят в гарантиране на конституционните й права и лична свобода за достъп до информация, до използването на тази информация за осъществяване на дейности по духовното, нравственото, физическото и интелектуалното и развитие непротиворечащи на приетите в държавата закони. От съществено значение тук е гарантирането на защитата на личните данни на отделния гражданин от посегателства с престъпни цели. Тези права на българските граждани са отразени в конституцията на Р. България. В нея е записано че личният живот на гражданите, свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени. Всеки гражданин има право да търси, получава и разпространява информация.[4] В това отношение цялостната политика за национална сигурност в Р. България е насочена към повишаване на усещането за сигурност сред гражданите чрез създаване на необходимите условия и предпоставки за гарантиране на националните интереси, ограничаване на въздействието от рисковете и заплахите и оптималното разпределяне на ресурсите.[1]

Съвременните информационни технологии променят не само отношенията между гражданите в обществото но и облика им на живот, семейните отношения, обществените институции и органите на властта. В съвременни условия те се превръщат в движещ стимул за развитието на личността и обществото. Средствата за информационно въздействие върху хората са многообразни. Към тях можем да причислим, семейството, образователната сфера (детска градина, училище, уни-

верситет), улицата, книгите, радиото, телевизията, киното, пресата и т.н Съществено значение през 21 век върху информационната осигуреност има глобалната мрежа Интернет и нароилите се социални мрежи. В същото време използването на иновационните информационни технологии и някои действия на държавните органи и институции в това направление води до появата на нови заплахи за конституционните права и свободи на личността.

Като заплахи за информационната сигурност на личността могат да се посочат:

- предприемане на действия от страна на правителството накърняващи конституционните права и свободи на гражданите по отношение на информационното им осведомяване;

- нарушаване на правото на лична и семейна тайна, тайна на кореспонденцията и телефонните разговори както от страна на държавните институции така и от различни криминални структури;

- ограничаване по различни начини и поводи на достъпа до обществено достъпната информация;

- създаване на монопол върху получаването и разпространението на информацията от правителствени и неправителствени органи и организации.

Интересите на обществото в сферата на информационната сигурност се заключават в утвърждаването и развитието на демокрацията, гарантирането на информационната свобода на гражданите както и в създаването и поддържането на обществено съгласие.

Основните заплахи за обществото биха могли да бъдат:

- използване на средства за масово манипулиране на съзнанието на гражданите;

- разрушаване или нарушаване на нормалната работа на създадената система за събиране, обработка и съхранение на информация от всякакво естество и изтриване на създадената база от данни;

- ограничаване на достъпа на гражданите до държавните информационни ресурси несъдържащи класифицирана информация;

- манипулиране (изкривяване) на информацията насочено към подмяна значението на исторически факти и събития.

Като държавни интереси в информационната сфера могат да се посочат защитата на конституционния ред, суверинитета и териториалната цялост на страната, създаването на условия за реализиране на конституционните права и свободи на гражданите на дадената държава в областта на получаване на необходимата информация и използването и за поддържане на политическа и социална стабилност, както и за провеждане на международно сътрудничество на основата на партньорството и съблюдаване на интересите на страната.

Кои са източниците на заплаха за информационната сигурност на държавата. В зависимост от проявлението им заплахите условно могат да бъдат разделени на външни и вътрешни.[3] Към външните могат да се причислят:

- стремежа на други страни за установяване на информационно превъзходство и затрудняване на достъпа до нови информационни технологии с цел създаване на технологична зависимост в информационната сфера;

- дейността на редица чужди разузнавателни и специални служби, икономически и политически структури насочени против националните интереси на страната;

- използването от други държави на информация получена от космически, въз-

душни, морски и наземни разузнавателни средства в ущърб на националните интереси на страната;

- последиците от кибертероризмът във всичките му форми на проявление насочен към нанасяне на морални, психологически и финансови щети на отделния гражданин, обществото и държавата. Киберпрестъпността е глобална и анонимна заплаха за информационните системи.[1] ;

- разработката и прилагането на концепции за информационни войни имащи за цел използването на средства за масово въздействие върху психиката и поведението на противниковите бойци;

- престъпната дейност на различни терористически структури и отделни лица в информационната сфера и др.

По отношение на вътрешните източници на информационна заплаха като поважни такива могат да се посочат:

- съществуването изоставане в областта на информатизацията на обществото, ограничаващо възможността за равноправна интеграция с развитите в това отношение страни и получаването на икономически и социални ползи от това сътрудничество;

- сращване на организираната престъпност с държавните институции и органи на изпълнителната и съдебната власт в информационната сфера водещо до намаляване на защитеността на личните, обществените и държавните интереси в тази област;

- изоставане в технологично отношение по отношение производството на информационни и телекомуникационни средства и невъзможност за изграждане на собствена информационна инфраструктура. Зависимост от развитите в това отношение държави, създаваща заплаха за националната ни сигурност в условия на кризи и война;

- недостатъчно ясна и прозрачна държавна политика в страната по отношение на осигуряването на информационна сигурност;

- изоставане в областта на образованието на подрастващото поколение, затрудняващо подготовката на специалисти и ползватели на съвременните средства за достъп, обработка, съхраняване и анализиране на информацията;

- увеличаване на нивото на организираната престъпност в това число и на компютърните престъпления водещо до повишаване на несигурността на отделния гражданин и държавата в информационната сфера;

- недостатъчно финансово осигуряване на мероприятията по информационната сигурност.

В края на миналото и началото на новото хилядолетие сме свидетели на появата на един нов феномен–електронното общество (ИО). Информационното общество е резултат от промените, предизвикани от използването на новите информационни и комуникационни технологии (ИКТ) в съвременния живот. [6] Волю или неволю всички ние сме членове и реални субекти на това общество. Мобилните комуникации, развитието на телекомуникациите, електронните медии и не на последно място масовото навлизане в живота ни на Интернет технологиите доведоха до информационна революция в дома ни, в училище, на работното място и в обществените отношения. В подкрепа на тези факти, по данни на Националния статистически институт за последните 10 години броят на потребителите на Интернет в България се е увеличил от 450 000 през 2000 г. на 2 669 000 през 2010 г. Според същият източник близо 90% от потребителите имат достъп от дома си, 33% от

работното място и 14 % от училището или университета. Стойността на продажбите осъществени чрез Интернет мрежата е нарастнал от 234 млн лв. през 2006 г. на 2 493 млн лв. през 2010 г., а броят на предприятията имащи достъп до Интернет от 61.8% през 2004 г. се е увеличил на 85.1% през 2010 г.[7] Тези данни красноречиво говорят за масовото навлизане на ИКТ в нашата страна и необходимостта от интегрирането ни в световната е-общност.

Информационното общество е общество с качествено нова структура, организация и обществени отношения, основани на глобалния достъп и използване на информационни и комуникационни мрежи и услуги - без национални, географски или други ограничения, за обмен на информация, на научни, духовни, културни и други постижения. [8]

Сред основните цели и приоритети за развитието на ИО у нас, имащи отношение към информационната сигурност, са залегнали: [8]

- осигуряване на всички граждани на равнопоставен достъп до съвременни, ефективни и качествени телекомуникационни и информационни услуги, както и на равни възможности за придобиване на умения за използването им;
- създаване на нова среда на живот и работа чрез широко използване на нови ИКТ в обществената, политическата, икономическата и културната сфера.

По-важните мероприятия за реализацията на тези цели са: [7]

• въвеждане на европейски норми за осигуряване на достъп до информация при гарантиране сигурността на данните и основните човешки права;

• създаване на прозрачна и предвидима правна и регулаторна рамка за предоставяне на услугите на ИО за населението и бизнеса;

• развитие и обновяване на далекосъобщителната инфраструктура като основа за изграждане на национална информационна инфраструктура;

• предоставяне на телекомуникационни, медийни, мултимедийни и информационни услуги в либерализирана среда, при ясен механизъм за зачитане на правата на хората като граждани и потребители;

• въвеждане на съвременни ИКТ в управлението, икономиката, образованието, културата, здравеопазването, системата за националната сигурност и екологията;

• създаване на условия за всеобщо образование, непрекъснато и индивидуализирано обучение по ИКТ;

• широко осведомяване и подготовка на обществото за пълноценна реализация в ИО.

От казаното до тук е видно, че наред с редицата положителни резултати информатизацията на обществото поражда редица проблеми за информационната сигурност на отделния гражданин, обществото и държавата. В глобален план основните заплахи в това отношение са информационния тероризъм, киберпрестъпленията и осъществяването на концепциите за информационните войни. Последиците от тези заплахи могат да бъдат катастрофални не само за дадена държава, но и за населението на планетата като цяло. Всичко това потвърждава тезата, че значението на информационната сигурност, в контекста на националната сигурност, нараства неимоверно много. Информационната сигурност се явява основна подсистема на системата на националната сигурност от която в значителна степен зависят икономическата, социалната, политическата, екологическата и останалите подсистеми и пряко влияе на ефективната работа на органите на държавната власт и институциите имащи отношение към сигурността като цяло.

Използвана литература:
1. Стратегия за национална сигурност на Р. България
2. U.S. DOD. Dictionary of Military Terms
3. Доктрина информационной безопасности Российской федерации
4. Конституция на Република България (чл. 32 и чл. 34)
5. Петров В. П. Петров С. В. Информационная безопасность человека и общества
6. Национална програма за ускорено развитие на електронното общество в Р. България 2008-2010 г.
7. http://www.nsi.bg/otrasal.php
8. Стратегия за развитие на електронното общество в Р. България
9. Х. Тужаров Интернет технологии София 2007

ИЗПОЛЗВАНЕ НА ТЕХНИЧЕСКИ СРЕДСТВА ПРИ ОХРАНАТА НА ПРИРОДНИ ЗАБЕЛЕЖИТЕЛНОСТИ В ЗАПАДНИ РОДОПИ

Евгени М. Гавраилов, Тодор С. Тодоров

Варненски свободен университет „Черноризец Храбър", Юридически факултет, к.к. „Чайка", 9007 Варна
Пловдивски университет „Паисий Хилендарски", филиал Смолян,
Председател на туристическо дружество „Родопея", с. Ягодина

THE USE OF TECHNICAL MEANS FOR PROTECTION OF NATURAL SITES IN THE WESTERN RHODOPES

Evgeni M. Gavrailov, Todor S. Todorov

Varna Free University "Chernorizets Hrabar", Faculty of Legal,Department of Security and Safety;
Plovdivski University „Paisii Hilendarski", Smolyan Branch, Smolyan, Bulgaria; Chairman of the Tourist Association "Rodopeya", Yagodina

ABSTRACT**:** *The issue of preservation and restoration of the wealth of flora, fauna and unique landscape is the final date for the Western Rhodopes and Smolyan region. In the Rhodopes interaction between people and nature for centuries has formed a unique landscape, featuring important biological, cultural and material values.To protect these values is necessary restoration and conservation of nature and environment, which should be the primary goal when we touch it.*
KEY WORDS: *flora, fauna, unique landscape, karst formations, technical means of security, sensors, cameras.*

Общата дехуманизация на съзнанието е свързано с хищническото потребление на природните ресурси, обхваща в настоящото време много сфери от човешката дейност. Тя неизбежно води до унищожаване на многообразните биологически форми и оскъдната природа, която се явява източник на интелектуално и нравстве-

но развитие и материално благополучие.

Проблемът за съхраняването и възстановяването на богатствата на флора, фауна и уникален ландшафт се явява крайно актуален за Родопите и за Смолянски регион. В Родопите взаимодействието между хора и природа от векове е формирало уникален ландшафт, отличаващ се с важни биологични, културни и материални ценности.

Карстовите райони и най-вече пещерите в тях, са носители на разностранна информация за развитие на материалната и духовна култура на човечеството, животинският и растителния свят, населявали планетата в доисторическо и историческо време. Затова всяка непремерена човешка дейност в карста, включително и спелеоложката, може да доведе до нарушаване на естественото му състояние и да доведе до невъзвратими вреди за природата, науката и културата. За това опазването на карста има особена важност в системата на природозащитата в България.

Ето защо унищожаването на фауната на една единствена пещера може да доведе до изчезването на цели животински видове завинаги от лицето на земята. Редица български пещери са обявени за природни забележителности и паметници на природата, именно като обиталища на големи прилепни колонии и уникална безгръбначна пещерна фауна.

Логичен е въпросът: Защо трябва да се охраняват пещерите?

Отговорът на този въпрос може да се сведе до следното:

1. Пещерите представляват елементи на неживата природа, специфичен подземен ландшафт, който е съществувал много преди човека и има право да съществува в настоящето като съставна част от пейзажната обвивка на планетата.

2. Пещерите са местообитание на специфични представители на фауната, някои от които живеят в тях постоянно, а други – временно и са включени в Червената книга на Световния съюз за защита на природата (*IUCN*) и в Червената книга на България.

3. Пещерите са геоложки паметници на природата. Образуването на вторичните карстови форми трае сравнително дълго, а унищожаването им може да стане само за един миг. До момента са установени над *53* минерала, образувани в нашите пещери, което ги определя като важни за минералогията обекти.

4. Пещерите имат полеогеографическа стойност – в тях са се запазили следи от минали епохи, които обикновено са унищожени на земята.

5. Пещерите са с археологическо значение, защото са използвани от древните хора като подслон, заслони, светилища; в тях са запазени рисунки и скулптури на древните хора, предмети на бита и оръдия на труда.

6. В пещерите по особен начин протичат биологичните процеси, което позволява да се изучи влиянието на екстремните условия върху човешкото тяло и необичайния режим на работа, почивка и хранене.

7. Пещерите имат естетическа стойност, защото подземният пейзаж е необичайно красив, изразителен и величествен; много атрактивен и живописен карстов терен заради контраста, разнообразието и необичайността.

8. Посещението на пещерите стимулира любопитството, събужда интерес за научно познание на света, уважение към природата, желание човек да подобри своите физически способности и техническите умения.

9. Специфичните условия на пещерите намират разнообразно използване в живота на човека като спа клиники, лаборатории, съоръжения за отдих, музеи, кон-

цертни и ритуални зали, в отделни случаи и за укрития, складове, хладилни помещения и др.

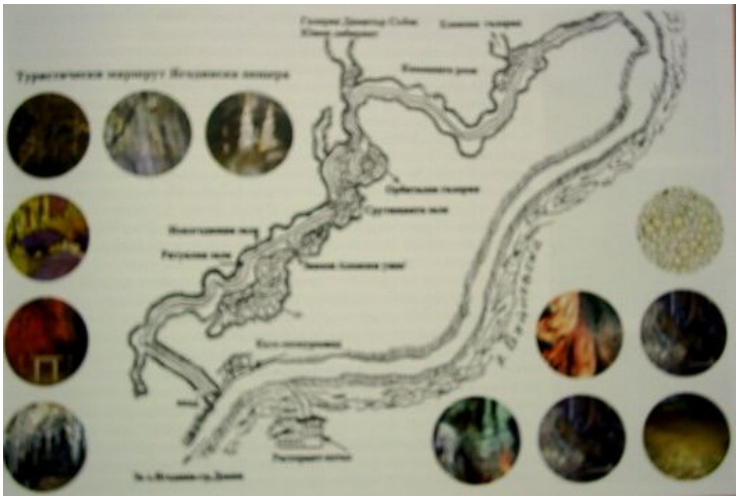
От разгледаното по-горе може да се заключи, че пещерите имат важно, научно, културно, естетическо и стопанско значение.

В България до сега в картотеката на Съюза на българските спелеолози към Българския туристически съюз (БТС) има планове на около *4500* пещери. Почти всички са изследвани и отворени за туристи — имащи познания в областта на спелеологията.

В Родопите са открити над *600* пещери, като по-известни са: "Снежанка", "Ягодинската пещера", "Дяволското гърло", "Ухловица", „Санчеста дупка", „Проходна Корудеренска пещера", „.Хаджийска ропка", „Горна Каранска", „Долна Каранска", „Мрачната дупка" и др.

Туристическо дружество (ТД) „Родопея" с. Ягодина е създадено през месец май *2002 г*. Дружеството стопанисва Ягодинската пещера и хижа Тешел. В района на село Ягодина и с. Триград има над *200* пещери, които са интерес за спелеологията и спелеотуризма. Към ТД е създаден пещерен клуб „Перла", който проучва и охранява пещерите и карстовото богатство на Ягодинския район.

Ягодинската пещера е сред Стоте национални туристически обекта на БТС. Намира се в Западни Родопите в землището на с. Ягодина. Дълга е *10,5 km* и е разположена на три етажа, от които само третият (най-ниският) е облагороден и електрифициран. За туристите в него е изградена *1100*- метрова пътека. Входът и изходът към този етаж са изкуствено прокопани тунели с дължина съответно *150* и *80 m* (фиг. 1.).



Фиг. 1.

От фигурата се виж-да, че пещерата е уникал-на със своите безброй сталактити, сталагмити, ста-лактони, хелектити, синт-рови езера, „завеси", „леопардови кожи" (различно оцветени скални слоеве), дендрити, драперии и най-уникалните образувания – пещерни перли. Общо *22* вида образувания от све-товно

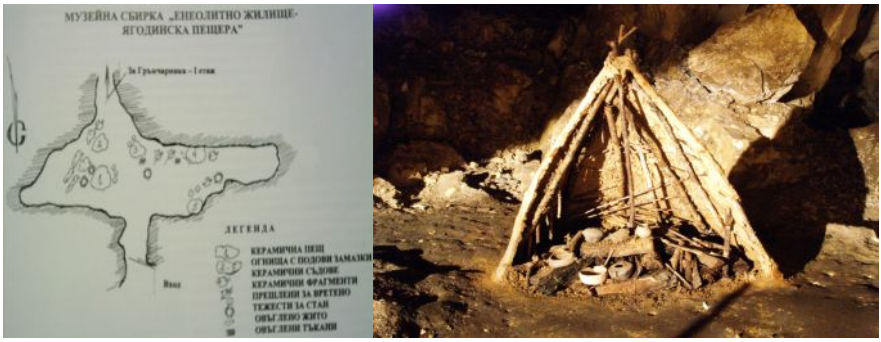
известните *28* вида.

Някои от вътрешните й оформления напомнят за Дядо Коледа, Снежанка и седемте джуджета, Богородица и Младенеца, Пижо и Пенда, форми на животни и фантастични фигури.

Тук край елха, която остава свежа няколко години, спелеолози честват Нова година. В ритуалната зала се са състояли *227* сватби.

Основният пещерен археологически паметник в района около с. Ягодина е пещерното жилище в Ягодинската пещера (Имамова дупка). В продължение на две последователни години (*1965, 1966 г.*) тук са извършвани археологически проучвания на площ около *100 m*^{2}. По време на проучванията са открити находки от най-различни епохи. Най-старите приналежат на поселниците от късният енеолит (IV хилядолетие пр.н.е.). По пукнатини в дълбочина се усеща силно течение, което подсказва за връзката на тази част от пещерата с повърхността или по-стари нива от по-долните етажи от пещерата.

Естественият вход на пещерата води към първия й етаж, където е открито древно жилище, обитавано около IV-то хилядолетие пр. Христа (фиг. 2.).



Фиг. 2.

Находките говорят, че то е било дом на умели майстори-грънчари. Особен интерес представляват Кръстовището и Грънчарника от I етаж на Ягодинската пещера – галерии, продължение от Предверието на пещерата.

В тези части на пещерата са открити редица материали – кремъци, кремъчни оръдия, фрагменти и цели керамични съдове, въглени, глина, която е била използвана за направа на съдовете (фиг. 3).

При детайлното изследване на пещерните наслаги се изясняват редица проблеми от морфологията и генезиса на пещерата.

Всички тези особености ха-рактеризират трудностите при физическа охрана и определят необходимостта от техническа такава.

Опитът показва, че за борба с тази тенденция е необходима целеустремена и стройна организация на процеса за осигуряване на сигурността. При това трябва активно да участват професионалните специалисти, администрацията на ТД, сътрудниците и потребителите на туристически услуги, което определя повишената значимост на организационните страни на въпроса.

От позицията на системния подход, сигурността трябва да бъде [8]:

- ✓ *Непрекъсната.* Това изискване произтича от това, че туристите търсят пос-

тоянна възможност да заобиколят защитата и да постигнат своите противоправни цели;

✓ *Планова*. Планирането се осъществява по пътя на разработката на детайлни планове за действия по осигуряването на защитеност на природната забележителност с всички компоненти от неговата структура;

✓ *Централизирана*. В рамките на структурата си ТД трябва да осигурява организационно-функционална самостоятелност на процеса по гарантиране сигурността на обекта;

✓ *Целенасочена*. Защитава се това, което трябва да се защитава в интерес на конкретни цели, а не всичко подред;

✓ *Конкретна*. На защита подлежат конкретни обекти, заплахата за които може да нанесе вреда на ТД и околната среда.

✓ *Активна*. Защитните мерки се претворяват в ежедневието с достатъчна степен на настойчивост;

✓ *Надеждна*. Методите, средствата и формите на защита трябва надеждно да прикриват всички пътища за проникване и възможните канали за отход. При това надеждността предполага не само прикриване, но и дублиращи средства и мерки за сигурност;

✓ *Универсална*. Счита се, че мерките за сигурност трябва да преграждат пътя на заплахите, независимо от местата на тяхното възможно въздействие;

✓ *Комплексна*. За осигуряването на защитата в цялото й многообразие от структурни елементи, заплахи и канали за нерегламентиран достъп, е задължително да се прилагат всички видове и форми на защита в пълен обем. Недопустимо е да се прилагат отделни форми или технически средства. Комплексния характер на защитата произтича от това, че тя е специфично явление, представляващо сложна система от неразривно взаимосвързани процеси, всеки от които на свой ред има множество различни взаимно обусловени едни от други страни, свойства, тенденции.

Фиг. 3.

Всичките технически средства за защита на обектите могат да се разделят на три категории – средства за откриване, средства за предотвратяване и средствата за ликвидиране на опасностите.

Инженерно–техническа защита на Ягодинската пещера е съвкупност от специални органи, технически средства и мероприятия по тяхното използване в интерес на гарантирането на сигурността на природната забележителност. Те се отнасят към първата категория, а именно средства за откриване (алармена сигнализация).

Средствата за *алармена сигнализация* са предназначени за разкриване на различни видове заплахи: опити за проникване в обекта, кражба на материални и финансови ценности и др. действия; оповестяване на сътрудниците от охраната или персонала на обекта за появата на заплахи и необходимостта от засилване на контрола на достъп до обекта, територията, галериите и залите. Използваните елементи на охранителната система са пасивни инфрачервени (*Pasiv InfraRed-PIR*) и сеизмични (*Seismic*) детектори. При охраната на административната сграда и командната зала се използват детектори за счупване на стъкло (*Glass-break*), фиг. 4.

Цифров датчик за движение с четворен *PIR* елемент *DGP2-60*

Акустичен детектор за стъкло *Glass Treak 456* (*Paradox*)

Фиг. 4.

Телевизионните системи за наблюдение и охрана са едно от най-разпространените средства за охрана през последните години. Главното положително качество на телевизионните системи се явява възможността не само да фиксират нарушението на режима за охрана на обекта, но и да позволят контрол на обстановката около него, да определят причините за сработване на алармената сигнализация, да позволят скрито наблюдение и видеозапис на охраняваните пространства, фиксирайки по този начин действията на нарушителите. По тази причина, когато говорим за доказателствени функции на алармените системи, това преди всичко се отнася за телевизионните системи за наблюдение.

При охраната на пещерата се използват два вида камери (фиг. 5).

Първите, със *CCD* преобразуватели, са за охрана на външния периметър на пещерата. Те са много по-леки и компактни; не се влияят от външни магнитни полета, поради което при тях липсват геометрични изкривявания на изображението и ефектите от типа „опашки”; камерите са готови веднага за работа след включването им; много по-устойчиви са на удари и вибрации, и притежават много по дълъг срок на експлоатация.

Фиг. 5.

Вторите, високо чувствителните, са способни да работят при много ниска осветеност. Използват се за охрана на галерии, зали, елементи на неживата природа, флората и фауната.

При пренасянето на сигнала се използва коаксиален кабел. За компенсиране затихването на видеосигнала, с което се губи детайлността на изображението в командната зала същият преминава през усилвател (фиг. 6).

Фиг. 6.

За паметниците на природата и природни забележителности могат да бъдат класифицирани редки, забеле-жителни пещери или части от тях (с околните райони) и карстови обекти, както и характерни обособени пред-ставителни или уникални райони на карстовите райони и ценни в научно, културно, образователно, естетическо и оздравително отношение.

За опазването на тези ценности е необходимо възстановяването и консервацията на природата и околната среда такава, каквато сме я получили от предходното поколение.

Специалистите в областта на проучването на карста и пещерите – географи, геолози, зоолози, археолози, спелеолози и пр. следва да обединят усилията си и да направят необходи- мото за обявяване на нови карстови райони и пещери за защитени територии.

Антропогенното влияние върху карста и пещерите в България предизвиква редица практически проблеми, отнасящи се до тяхната охрана и защита. На първо място това са несъвършенствата на правната уредба. Съществуващите закони гарантират, в повечето случаи теоретически, опазването само на онези карстови терени и обекти, които са защитени територии. Практическата охрана на всички пещери природни забележителности и значителна част от тези, които попадат на териториите на защитените местности и природните паркове в повечето случаи се свежда до поставянето на обозначителни табели.

Министерствата, ведомства, общини и неправителствени организации от природозащитата подпомогнати от експерти в областта на проучването на карста и пещерите следва да провеждат координирана и целенасочена образователна политика относно значението на карста и пещерите и необходимостта от тяхното опазване. Няма никакво съмнение, че най-ефективното средство за опазване е именно чрез образование и възпитание на членовете на обществото, като акцентът трябва да бъде поставен върху образованието на подрастващото поколение.

Използвана литература:

1. Конституция на Р България. Обн., ДВ, бр. 56 от 13.07.1991г. изм. и доп., бр. 12 от 6.02.2007г.

2. Закон за защитените територии. Обн., ДВ, бр. 133 от 11.11.1998г., изм., бр. 91 от 25.09.2002 г., в сила от 1.01.2003 г.

3. Закон за биологичното разнообразие. Обн. ДВ. бр.77 от 9.08.2002г., изм. ДВ. бр.33 от 26 Април 2011г.

4. Закон за горите. ДВ , бр. 19 от 8 март 2011 г., в сила от 09.04.2011 г.

5. Закон за частната охранителна дейност. Обн. ДВ. бр.15 от 24.02.2004г., изм. ДВ. бр.73 от 17.09.2010г.

6. Директива 92/43/ЕИО на Съвета за опазване на естествените местообитания и на дивата флора и фауна.

7. Бойчев П. Техническо разузнаване – оперативни способи и противодействие, Албатрос С. 2007.

8. Бурчак-Абрамович Н.И. Пещеры Кавказа - памятники природы и истории древней культуры, их изучение и охрана. Проблемы выявления, исследования и сохранения памятников природы, Воронеж, ВООП, 1983, с. 31-32.

9. Голод В.М., Мавлюдов Б.Р. Рекомендации по выявлению, учету, оформлению и организации охраны пещер и карстовых объектов в качестве государственных памятников природы, Москва, ВООП, 1984, 50 с.

10. Йорданова, М. Защитените територии в Смолянска област. Издателство ЕТ „Подмолова", Смолян, 2007.

11. Тодоров, Т., Е. Гавраилов. Теория, практика и методика на обучението по спелеология. Издателство ПУ „П. Хилендарски". Смолян, 2010.

12. Ganter J. Cave exploration, cave conservation: some thoughts on compatibility. NSS News, v. 49, № 10, 1989, p. 249-253.

13. http://bg.wikipedia.org/wiki.

ПРЕДИЗВИКАТЕЛСТВА ПРЕД УЧАСТИЕТО НА МВР В ОТБРАНАТА НА СТРАНАТА

Георги Гр. Гоцев

Министерство на вътрешните работи, гр. София, ул. "6-ти септември" № 29

THE CHALLENGES OF THE MINISTRY OF INTERIOR IN THE DEFFENCE

Georgi Gr. Gotsev

ABSTRACT: The main problems in the level of preparation of the Ministry of interior in the deffence of the country are covered in the report. The leading directions in preparing its structures in resolving the problems are shown, based on the aims of the Ministry in wartime.

KEY WORDS: security and deffence system, planning of deffence, civil deffence, alert system.

Целите на отбранителната политика на Република България, наред със създаването на благоприятна среда за гарантиране на националната сигурност, са насочени към изграждане и поддържане на модерна и ефективна система за отбрана на страната със способности и състав, съответстващи на националните интереси, динамичната среда на сигурност и наличните ресурси. Тя трябва да е в състояние, осигуряващо ефективното ѝ функциониране и оперативна съвместимост на националните институции с тези на НАТО и Европейския съюз.

Системата за отбрана, като част от системата за национална сигурност, се организира чрез взаимно свързани политически, икономически, военни, социални и други дейности с цел подготовка и осъществяване на въоръжена защита на териториалната цялост и независимостта на страната в условия на военнополитически кризи и във военно време. Тя включва органите за ръководство, командване и управление, въоръжените сили, силите и средствата на министерствата и ведомст-

вата от централната администрация, териториалната администрация, органите на местното самоуправление, юридическите лица и гражданите при единно ръководство и управление.

Основа на системата за отбрана на страната са въоръжените сили на Република България. Силите на държавните органи, в това число и МВР, органите на местното самоуправление и на местната администрация ги подпомагат, осигуряват и допълват по единен замисъл при подготовката и нейното осъществяване.

Отчитайки изменената среда на сигурност, съществуващите рискове и заплахи за сигурността и обществения ред и формулираните мисии на отбраната, могат да се определят основните функции и задачи, които МВР ще изпълнява при участие в отбраната на страната. По същество те няма да се различават значително от тези, възложени на министерството и неговите органи в мирновременния период, но ще се различават по обема им и условията, в които ще бъдат изпълнявани.

Основният фактор, определящ задачите на МВР, свързани с отбраната на страната, е моделът, по който ще се осъществява същата. Съгласно възприетите възгледи в зависимост от конкретната военнополитическа криза е възможно да се развият различни модели на отбрана, с различно съотношение на участващите в нея национални и съюзнически сили и средства. В съответствие с това дейностите по отбраната на страната могат да се реализират в съюзен, коалиционен или национален формат.

Макар и най-малко вероятно, изпълнението на отбранителни задачи на територията на Република България налага системата за отбрана да изгражда и поддържа способности за гарантиране на териториалната цялост и сигурността на страната до задействане на механизмите за колективна защита. Това ще бъде най-тежкия модел на отбрана, при който страната ни ще трябва да реагира сама на всички заплахи. Отчитайки и това, че съвременните конфликти, независимо от техния характер, ще бъдат предшествани и съпътствани от множество дестабилизиращи фактори, се очертава сложна и трудна за предсказване и управление ситуация, налагаща целият военен и невоенен компонент на системата за отбрана да бъде в състояние да се противопостави адекватно на възникващите заплахи.

Министерство на вътрешните работи като специализиран правозащитен орган на изпълнителната власт е ангажирано пряко с провеждане на държавната политика за защита на националната сигурност. Като система министерството и неговите органи имат за свой обект на въздействие обществените отношения, свързани с гарантиране на вътрешния обществен ред, разкриване и разследване на правонарушения в тази област с цел укрепване на законността и установения в страната конституционен ред.

Анализът на постановките в ЗОВСРБ за основните дейности, с които се реализира отбраната на страната и които определят нейното съдържание показват, че част от задачите по отбраната и основната част от задачите по отбраната на територията на страната ще се изпълняват изцяло или с участието на сили и средства на МВР. Основните структури на министерството ще изпълняват задачите самостоятелно или във взаимодействие с въоръжените сили, другите държавни органи и органите на местното самоуправление. Определените от Закона за МВР правомощия позволяват на органите му да изпълняват някои от задачите по отбраната още в застрашаващия период преди да е обявен военновременен правов режим на територията на цялата страна или на част от нея.

Главната задача на МВР в отбраната на страната е гарантирането на обществения ред и вътрешната сигурност извън зоната на военните действия, противодействие на престъпността и опазване на живота, здравето и имуществото на гражданите. Наред с това неговите структури ще участват в различна степен при решаването на следните задачи:

- охрана на държавните граници, въздушното пространство и териториалното море и евентуално прикритие на границата със съседни държави, не участващи във военния конфликт;
- охрана и отбрана на стратегически, особено важни и други обекти от критичната инфраструктура на територията на страната;
- борба с десанти, диверсионно-разузнавателни, терористични и други формирования за организирана съпротива;
- осигуряване сигурността и реда в обекти на националната икономика и непроизводствената сфера за действие при военнополитически кризи и при военен конфликт;
- организиране и осигуряване безопасността на населението и инфраструктурата при бедствия и разрушения;
- повишаване противопожарната устойчивост и безопасност на обектите на икономиката и тези, работещи в интерес на отбраната.

Освен задачите, изпълнявани от органите на МВР в отбраната на територията извън зоната на военните действия, част от тях ще изпълняват и задачи в нея. При неблагоприятно развитие на военно-политическата обстановка МВР трябва да има готовност да изпълнява и задачи на временно заета от противника територия на страната ни.

МВР се подготвя да участва в отбраната на страната в общия комплекс от мероприятия, регламентирани с Конституцията, Закона за отбраната и въоръжените сили, Закона за МВР, други закони и подзаконови нормативни актове. Както е известно подготовката за отбрана се провежда от органите за ръководство на отбраната, въоръжените сили, органите на централната и териториалната власт за организиране и всестранно осигуряване на отбраната. Тя включва подготовката на въоръжените сили, на националната икономика, на населението и на територията на страната и се осъществява чрез разработване и прилагане на съответна нормативна уредба, концептуални документи и планове за отбрана, изграждане на единна система за ранно предупреждение, информиране и управление на страната и въоръжените сили, всестранно осигуряване на отбранителни ресурси, поддържане на бойна, оперативна и мобилизационна готовност, както и организиране защитата на населението и икономиката във военно време.

При своята подготовка за участие в отбраната на страната съставът на МВР обръща основно внимание на изясняване на военновременните задачи на структурите му и планирането на тяхното изпълнение. В тази връзка приоритет в подготовката е конкретизиране задачите на отделните сили и създаване на условия за изграждане на способности на същите да ги изпълняват. От тази гледна точка силите на МВР съобразно задачите им във военно време се делят на:

- сили на МВР, които се включват във военновременния състав на въоръжените сили на Република България;
- сили на МВР за осигуряване на обществения ред и противодействие на престъпността на територията на страната;

• сили на МВР за участие в гражданската отбрана на страната.

Силите на МВР, които се включват във военновременния състав на въоръжените сили са тези, които съвместно с военния компонент на въоръжените сили допринасят за гарантиране на териториалната цялост и независимостта на страната при военен конфликт, възпират противостоящи сили и задържат заплахите отвъд границите на страната. За тази цел като невоенен компонент на въоръжените сили те участват в охраната на държавните граници с не участващите във военния конфликт съседни държави, участват в охраната и отбраната на стратегически и други обекти от критичната инфраструктура на страната, участват в борбата с десанти и диверсионно-разузнавателни групи, разкриват и неутрализират терористични групи и други формирования за организирана съпротива, поддържат обществения ред и сигурност в зоните за отговорност на въоръжените сили и съюзническите войски, оказват помощ при бедствия, разрушения и други извънредни ситуации.

Силите на МВР, които ще противодействат на престъпността и ще опазват обществения ред на територията на страната ще бъдат основната част от военновременния състав на министерството. Това са преди всичко органите с полицейски правомощия, които ще провеждат оперативно-издирвателна дейност за противодействие на престъпността чрез разкриване и разследване на престъпления. Голяма част от полицейските служители ще извършват патрулно-постова дейност за охрана на обществения ред и защита на обекти извън зоната на военните действия, ще спомагат за функционирането на икономиката, транспортната и комуникационната инфраструктура на страната. Тяхна задача ще бъде и опазването на живота, здравето и имуществото на гражданите в условията на усложнената във военно време криминогенна обстановка.

След закриването на Министерство на извънредните ситуации през август 2009 г. и възлагането на неговите функции и задачи на МВР, задачите по защитата на населението в мирно и военно време станаха основни за неговия състав. С последните промени в Закона за МВР съгласно чл. 52, ал. 2, т. 14 при обявяване на режими "положение на война", "военно положение" или "извънредно положение" ГДПБЗН ще извършва защита на населението в съответствие с разпоредбите на Женевските конвенции от 12 август 1949 г. и Допълнителните протоколи към тях от 1977 г. За действията на главната дирекция и другите структури на МВР във връзка с тази задача определящо значение има Допълнителен протокол I относно защитата на жертвите на международни военни конфликти, при окупация или гражданска война. По силата на чл. 61 от Глава VI на част IV на цитирания протокол "Гражданска отбрана означава комплекс от хуманитарни задачи, имащи за цел закрилата на гражданското население при военни действия или бедствия и да му помогнат да отстранят непосредствените последствия от тях, както и да осигурят необходимите условия за неговото оцеляване". Пак там като задачи на Гражданската отбрана са определени:

• предупреждаване (оповестяване) за видовете опасности;

• евакуация и разсредоточаване;

• предоставяне на скривалища и тяхното съоръжаване;

• провеждане на мероприятия за затъмнение (светомаскировка);

• спасителни работи;

• санитарно обслужване, включително оказване на първа помощ и религиозна помощ;

- борба с пожари;
- откриване и обозначаване на опасни райони;
- обеззаразяване и подобни защитни мерки;
- срочно осигуряване на подслон и храна;
- срочна помощ при възстановяването и поддържането на реда в района на бедствие или мащабни поражения;
- срочно възстановяване на дейността на необходимите комунални служби за осигуряване на населението;
- срочно погребване на мъртвите;
- помощ при съхраняване на обекти, необходими за оцеляването;
- допълнителна дейност, необходима за осъществяване на планирането и организацията им, без да се ограничава с тях.

От посоченото по-горе е видно, че Гражданската отбрана е част от системата за отбрана на страната. За това и българската държава винаги е разглеждала нейното организиране в общия контекст на отбранителната политика на страната. Още повече, че Гражданската отбрана не е задача на една или няколко организации в страната, а функция на цялата държава, обществото и всеки отделен гражданин.

Анализът на състоянието на дейностите по Гражданската отбрана на страната и необходимостта от тяхното осъществяване поставят въпроса кой държавен орган трябва да организира изпълнението на тези задачи. Изхождайки от техния характер и от държавното устройство е естествено това да е задължение на Министерския съвет. В сегашния формат на правителството при условие, че задачите по защита на населението са възложени основно на МВР, е естествено инициативата за решаването на този проблем да е в правомощията на министъра на вътрешните работи. За това вече се предприемат действия за цялостно нормативно уреждане на проблема с Гражданската отбрана на Република България.

Постигането на целите на отбраната на страната изисква добра съгласуваност между органите и силите от различните държавни органи и органите на местното самоуправление, участващи в нея. Взаимодействието между тях трябва да бъде постоянно: както при нормативното уреждане на всички дейности по отбраната така и при нейното планиране, подготовка и осъществяване. Тъй като сме приели отбраната да се провежда в рамките и с прилагането на механизмите на колективната отбрана на НАТО и общата политика за сигурност и отбрана на Европейския съюз с ефективно използване на националните отбранителни способности, взаимодействието трябва да е насочено към балансирано изграждане на военните и невоенните способности на страната за защита на националните интереси и изпълнение на съюзните и коалиционните ангажименти. Само така ще изградим модерна и ефективна система за отбрана на страната със способности, осигуряващи нейното успешно функциониране.

Взаимодействието на МВР със структурите на въоръжените сили и другите министерства и ведомства за постигане целите на отбраната се организира основно по задачи. Особено внимание се обръща на прикритието на държавната граница на незастрашените направления; борбата с диверсионно-разузнавателни и терористични групи, както и с формирования за организирана съпротива; охраната на стратегически и особено важни обекти; конвоирането и охраната на военнопленници. МВР съгласува действията си с формированията на въоръжените сили относно пунктовете си за управление, военновременните си места за разполагане, мобилизационните

райони, оценката на радиационната, химична, биологическа и епидемична обстановка в зоните за отбрана. С другите министерства и ведомства се съгласува охраната на транспортните комуникации, обектите за защита от държавната съобщителна система, провеждането на аварийно-спасителни и други хуманитарни операции, евакуацията и разсредоточаването, предоставяне на данни за метеорологичната обстановка, за състоянието на язовирите и водоизточниците, оборудването и поддържането на пунктове за добиване, пречистване и снабдяване с вода.

Взаимодействието на МВР с другите елементи на системата за вътрешна сигурност (ДАНС, НСО) се организира за съгласуване на задачите по водене на борбата срещу тероризма, борбата с формированията за организирана съпротива, провеждането на оперативно-издирвателна дейност срещу противоконституционни прояви, защита на стратегически и особено важни обекти от престъпни посегателства като диверсии, вредителство и др.

Взаимодействието между органите на МВР и органите на съдебната власт - следствие, съд и прокуратура, се организира за укрепване на законността и за повишаване на общата ефективност на дейността им за защита на националната сигурност, опазване на обществения ред и противодействие на престъпността. От голямо значение за ефективността на взаимодействието е хармонизирането още от мирновременния период на военновременната наказателна политика с очакваните форми на престъпна дейност и увеличаването на нейните размери във военно време за повишаване ефективността и бързината на наказателното правосъдие.

При организиране на взаимодействието на участващите в отбраната териториални сили на МВР усилията са насочени към съгласуване на действията с областните съвети по сигурност. На съответната територия се съгласуват въпросите по организирането и доставяне на ресурси от резерва-резервисти и техника от националното стопанство, заделени за специализираните формирования на министерството, осигуряване на сигурността и обществения ред в райони и обекти с важни военновременни задачи и повишени рискови условия. С органите на местната администрация и местното самоуправление се съгласува военновременната система за управление на МВР, особено пунктовете за управление, военновременните места и районите за оперативно-бойно използване.

Когато отбраната се осъществява в съюзен или коалиционен формат органите на МВР заедно с другите елементи от системата за вътрешна сигурност и обществен ред работят във взаимодействие със сродните органи на съюзните държави. Това взаимодействие се организира като продължение на сътрудничеството между тях в мирновременния период и се залага в съвместните планове.

Подготовката на МВР за участие в отбраната на страната в промененатa среда за сигурност и настъпилите промени в нормативната уредба очертават няколко основни направления, по които трябва да се работи. Те са свързани с планирането на участието на силите на МВР в отбраната и неговото управление във военно време, системата за оповестяване при възникване на различни по характер кризи по подготовката на състава за работа във военно време и в условия на кризи и ресурсното осигуряване на тази подготовка.

Планирането на развръщането и използването на силите на МВР при изпълнение на задачи по отбрана на страната е една от основните дейности, свързани с неговата подготовка за това. Целта на същото е да организира максимално ресурсите на министерството за опазването на вътрешната сигурност и обществения ред

в страната в условия на военно-политически кризи. Умението да се разработват и поддържат в актуално състояние военновременните планове в голяма степен зависи от ясното дефиниране на военновременните задачи на структурите на МВР, които по закон трябва да се възложат с акт на Министерския съвет. Това ще даде възможност да се определят с висока точност необходимите човешки, финансови и материални ресурси за изпълнение на задачите във военно време и управлението на тези ресурси съобразно създадената обстановка.

Динамичните промени на структурата на МВР и в средата на сигурност през последните години налага активна преоценка на подходите за планиране на участието му в отбраната на страната. Основните проблеми в тази насока са необходимостта от разработване на ръководни документи за работа на органите на МВР във военно време, включително нормативните актове, които трябва да бъдат въведени, изменени или чието действие се спира при въвеждане на военновременен правов режим, и тяхното отчитане при планиране на готовността за работа във военно време.

Оповестяването на структурите на МВР за привеждане в по-високи степени на готовност се извършва от оперативните дежурни и дежурните по системите и техническите средства за оповестяване с помощта на установени команди и пакети със сигнали. Основен елемент на системата до скоро беше автоматизираната система за оповестяване (АСО), но поради моралното и технологичното ѝ остаряване тази система постепенно отпада, което налага нови решения на проблема с оповестяването. Необходимо е да се използват за тази цел и възможностите на Националната система за ранно предупреждение и оповестяване приета с ПМС № 70/2009 г. Основното изискване към системата за оповестяване е тя да е многофункционална и да бъде съвместима с обединената система за оповестяване на страната.

При въвеждане в страната на военновременен правов режим ще се наложи цялата държавна машина да работи в синхрон, като единен механизъм. В този смисъл подготовката на служителите и органите за управление на министерството за работа във военно време е основен елемент от подготовката му за участие в отбраната. Планирането, организирането и провеждане на тази подготовка в МВР се извършва в системата на отбранително-мобилизационната подготовка, организира се от щатните звена "ОМП" и от служителите с възложени допълнителни задължения за работа по тези въпроси. В тази връзка е от съществено значение за ефективността на подготовката окомплектоването на тези звена със служители с добра обща професионална подготовка, преминали обучение и умеещи да планират, организират и провеждат този вид дейност. Това в още по-голяма степен се отнася за структурите без щатни звена "ОМП", в които тази дейност да се възлага на служители с доказан професионализъм и практически опит.

Проблемът с осигуряването на МВР с материално-технически средства за военно време безспорно е свързан със сериозните финансови ограничения, в които министерството работи през последните години. Независимо от това се организира планиране на необходимите материални и технически средства, с точни разчети и ясни правила как същите да бъдат осигурени в мирно време или в застрашаващ период. Този въпрос е пряко свързан и с осигуряването с финансови средства през военновременния период, което ще се извършва в рамките на планираните средства от военновременния проектобюджет на МВР.

Основната задача, която трябва да се реши при ресурсното осигуряване на МВР за работа във военно време е този с осигуряването на структурите на министерст-

вото с допълнителни човешки ресурси и техника за военно време. Законът за отбраната и въоръжените сили на Република България включи формирования на МВР във военновременния състав на въоръжените сили, което дава възможност чрез мобилизация да се получи допълнителен ресурс от мобилизационния резерв. Това поставя пред ръководствата на основните структури на МВР задължението да анализират военновременните нужди от допълнителен състав и да ги предвидят във военновременните организационни структури на звената. Заедно с това трябва да бъде планирано как и с какви средства ще се извърши приемането на ресурсите от резерва, тяхната подготовка и използване. Предстоящото приемане на Закон за резерва на Република България и подзаконовите актове за мобилизационната работа в Република България окончателно ще регламентират правилата на тази дейност и ще подпомогнат решаването на тези проблеми в структурите на МВР.

Цялостният анализ по подготовката на МВР да участва в системата за отбрана на страната, включително на съществуващите проблеми, предполагат организирана и целенасочена работа за нейното привеждане в съответствие с променената среда за сигурност. Необходимо е да се работи при пълно взаимодействие между институциите за усъвършенстване на нормативната уредба и организиране на нейното прилагане на всички управленски нива.

АРТИЛЕРИЙСКИТЕ ПОДРАЗДЕЛЕНИЯ В БОРБАТА С ТЕРОРИСТИЧНИ ФОРМИРОВАНИЯ

Иван А Гюргаков **Цветан Е Димитров,**

Военна академия „Георги С. Раковски”

ARTILLERY UNITS IN THE FIGHT AGAINST TERRORIST FORMATION

Ivan Gjurgakov, National Defense College**,** chair of land forces

Tsvetan Dimitrov, National Defense College**,** chair of land forces

Annotation. *Artillery units have specific role during planning and conducting of the Peace keeping operations. In use are guns, mortars and anti-tank weapons. Depending from the Peace keeping operational conditions, artillery units share different part in the operation – march, convoying, patrolling, proving military camp security, city battle operations and so on. Artillery reconnaissance and conducting of the Peace keeping operations.*

Key words: *artillery units, treats, artillery reconnaissance; military base, close fire support, convoy, columns, base, armed forces, peace keeping operation, peace enforcement, counter attack, fire support, multinational forces.*

Анализът на въоръжените конфликти през последните 10-15 г, показва, че те се характеризират, най-вече без ясно изразени граници по фронта и в дълбочина, даже

понякога и без наличие на ясно изразена фронтова линия на съприкосновение. Основа на бойните действия в тези случаи се явява борбата с терористичните формирования в различен състав и изпълнявани задачи.

В настояще време, наред с традиционните форми на действия се включват и широко мащабни настъпателни и отбранителни действия по овладяване и удържане на стратегически важни обекти. В тези действия най-често се противодейства на планирани терористични действия стигащи до открити въоръжени стълкновения с малки (до 15-20 души) и големи (до 500 и повече души). При това прилагането от терористичните групи на внезапност, решителност, дързост и действия за кратко време, налагат изменение в способите и формите за борбата с тях, както и привличането на различни сили и средства за тяхното неутрализиране.

Опита от воденето на борбата с терористични групи, потвърждава нарастващата роля на артилерията при поразяването на противника в хода на операцията особено, когато такива групи имат в състава си бронетанкова техника, артилерия, зенитни средства и друго тежко въоръжение.

При неблагоприятни климатични условия, артилерията се явява единственото огнево средство, което без ограничения може да се използва при всякакви климатични и метеорологични условия и по всяко време на денонощието да нанася точни удари за кратко време и да поддържа действията на маневрените формирования при ликвидиране на терористичните групи.

Лидерите на терористичните групировки, налагат основни организационни единици на тези формирования малки по численост отряди (групи), въоръжени с леко стрелково, противотанково и зенитно оръжие и силно развърната система от наблюдение в предполагаемия район за действие.

Най-ниското звено на такива формирования се явява бойната група, която най-често има численост от 4-5 до 15-20 души, имаща в своя състав снайперисти, гранатометчици, картечари и зенитчици. Групата има на въоръжение стрелково оръжие, противотанкови гранатомети, леки ПТРК, ръчни гранати, преносими зенитноракетни комплекси, различни видове мини и други.

Няколко групи могат да се обединяват в подвижен отряд, чиято численост, в зависимост от изпълняваната задача може да достигне до 150 и повече човека. Състава на такъв отряд, като правило включва:

- Една - две групи за управление и охрана;
- Две-три групи тежко въоръжение (при наличие на такова);
- Една-две броневи групи (при наличие на бронетехника);
- Една или няколко групи за връзка с местното население;
- Група за материално-техническо осигуряване.

За придвижване на групите могат да се използват товарни или леки автомобили с висока проходимост. За свръзка най-често се използват преносими радиостанции или средства използващи спътникови свръзки от най-различен тип и модел.

Ръководният състав на групите, отрядите и терористичните формирования, се готвят много старателно. Те изучават и познават като цяло силните и слабите страни в подготовката и начина на използването на силите срещу които ще действат, като най-често те имат и определена военна подготовка.

В състава на групите и отрядите се включват хора от различни националности, най-често като наемници или фанатици ислямсти, за които човешкия живот не представлява никаква ценност и са готови и самоубийствени действия. Тактиката на

действията на терористичните групи и отряди, съществено се отличава от действията на редовната армия. При воденето на бойни действия широко се използват рейдовите действия на малки по състав групи, диверсионни, диверсионно-разузнавателни или снайперски действия, предимно от засада с изненадващи удари от близко разстояние. Лидерите на такива малки терористични групи използват определени принципи, които могат да бъдат обобщени в следната последователност:

Тя се базира на следните основни принципи:

• Водене на бойни действия с малки по състав подвижни групи за кратко време (внезапно нападение на малки по състав наши подразделения в гарнизони или в райони, командни пунктове, свързочни възли, складове за материални средства, колони при извършване на марш в тесни или уязвими участъци, отделни групи военнослужещи и охранителни елементи, слабо охраняеми административни или държавни учреждения училища, в които има много хора, обществени сгради на културата при наличие в тях на много хора и др.)

• Избягване на стълкновение и напускане на местопребиваването, когато няма крайна необходимост от преки стълкновения с превъзхождащи сили, с изключение на отбрана на опорни базови центрове, населени места, проходи, превали и теснини;

• Преднамерено разполагане на елементи от бойните групи в населени места с много хора в тях, с цел прикриване на своите отряди с щит от мирното население, заемане на културни, култови и религиозни сгради, когато в тях има много хора;

• Периодично провеждане на диверсионни и терористични актове;

• Създаване на условия за бягство от затвори на осъдени лидери на терористични групировки, търговия с пленници (журналисти от различни медии, хуманитарни работници към световни организации, заложници) и тела на убити.

При воденето на бойните действия от терористичните групи умело се използва защитните свойства на местността, местните предмети, солидни здания в населени пунктове, църкви и джамии и др. в гориста и планинска местност се създава етажирана система на огъня. На господстващите височини се разполагат леки оръдия, ПТРК, големокалибрени картечници, зенитни картечни установки, леки преносими зенитно-ракетни комплекси и се оборудва система от опорни пунктове и съпротивителни възли, с широко използване на естествени и изкуствено създаване прегради и заграждения. Опорните пунктове се съединяват с ходове за съобщения, подготвят се пътища за извършване на маньовър и за заемане на запасни позиции. Максимално се използват маскировъчните свойства на местността (пещери, тунели, гъста растителност).

В населени места позициите на оръжията се избират в здания, от които има видимост и може да се простреля принадлежащото пространство, зад бетонни огради или в мазета на каменни постройки. Част от огневите средства, предимно картечниците и зенитно – ракетните комплекси се разполагат по покривите или на последните етажи на зданията и къщите. Най-голямо внимание се обръща на разполагането и действията на снайперистите и картечарите. Те най-често използват подземните комуникации за маньовър и за излизане в тил на нашите формирования, за унищожаване на командни пунктове, позиции на артилерийските подразделения и снабдителни складове. Много често, подстъпите към заеманите позиции се минират, а опорните пунктове се маскират.

При възникване на опасност от обкръжаване или пълно унищожаване, бойната

група се оттегля, като първи напускат снайперистите, които заемат запасни позиции, в дълбочина, на труднодостъпни места и прикриват оттеглянето на останалата част от групата. За прикритие на оттеглянето най-често се оставя малка, високоманеврена и добре въоръжена група от състава на бойната група.

Много често се използва и тактика на преднамерено оттегляне на част от бойната група в предварително избрано направление с цел въвличане на собствените подразделения за нейното преследване и попадането им в огневи чувал и унищожаване с огън от фланговете.

Значително място в действията на терористичните групи и отряди заемат диверсиите и терористичните актове. Обекти на диверсии могат да бъдат отделни автомобили, бронетранспортьори, БМП, танкове, преминаващи колони, свързочни и електропреносни мрежи, нефто - и газопроводи, държавни и културно-просветни учреждения, държавни и частни предприятия и др. Особен интерес по отношение на диверсионните актове извършвани както от мъже така и от жени представляват представители на прогресивната интелигенция и мирните жители. За извършване на диверсии и терористични актове терористите най-често се преобличат с униформи на местните или държавните силови структури.

За извършването на диверсии и терористични актове, отрядите от терористичните организации, използват засади, огневи налети и бързи атаки или миниране на даден обект и след това взривяването му.

В засада в зависимост от изпълняваната задача, обикновено действат 10-20 души, а понякога и повече от 100 човека, като се разполагат на един или няколко рубежа. Обикновено в състава на засадата има няколко групи: огнева; за отвличащи действия; за възпрепятстване на маньовъра и отхода на противника; резервна; за свръзки и информираност; зенитна и транспортна.

При подготовката за атаката си извършва пълно разузнаване, изучават се подстъпите към обекта, системата за свръзка, загражденията, наличието и мястото на огневите и другите средства. Групата обикновено напада с 20-30 души, като тя се разделя на подгрупи: за унищожаване на охраната; за извършване на проходи в загражденията; за прикритие и основни сили.

При борбата с терористичните формирования артилерийските, минохвъргачните и противотанковите подразделения на маневрените формирования имат готовност да поразят:

- Колони в състав отделение, взвод или рота, отделни автомобилни групи, пехотни подразделения в райони за съсредоточаване, снайперски групи и наблюдателни пунктове;
- Отделни огневи средства (минохвъргачки, гранатомети, картечници, противотанкови и зенитно ракетни комплекси), групите за огнева поддръжка на позиция, атакуващи пехотни подразделения и лекобронирана техника;
- Бойни групи на предварително подготвени позиции, отбранителни съоръжения, резервни групи (до рота) в райони за съсредоточаване, засадни групи;
- Автомобили и автомобилни колони, извършващи доставки на материални средства;
- Мостове, преправи на водни прегради, превали и тунели по пътищата;
- Опорни пунктове и огневи точки.

Артилерийските подразделения могат да се привличат за осигуряване охраната на собствените подразделения, когато те се разполагат в райони или когато блоки-

рат определен район. На тях се възлагат и задачи по огнево блокиране на терористичните групи, огнево прочистване на определени зони, създаване на огневи коридори за осигуряване придвижването на нашите подразделения по определени маршрути.

За изпълнение на тези задачи широко се прилагат поразяване на терористичните групи със смъртоносни и несмъртоносни средства и дистанционно миниране на заетите от тях райони или позиции.

За изпълнение на задачите по поразяване на терористичните групи могат да се привличат артилерийски дивизиони, реактивни дивизиони, минохвъргачни батареи, отделни оръдия, противотанкови батареи и взводове, установки ПТРК, взводове за звуково разузнаване и др. Огневите задачи могат да се изпълняват с право или спомагателно мерене, от закрити огневи позиции или чрез стрелба с право мерене. За водене на разузнаване за действията на терористичните групи се разгръща системата от артилерийски предни наблюдателни групи, по такъв начин, че прилежащата местност да се наблюдава напълно. Информация за състава и местоположението на терористичните отряди и групи се получава и от безпилотни летателни апарати и другите видове разузнаване.

При водене на огън с право или спомагателно мерене, част от самоходните артилерийски подразделения (в групи от 1 до 4 оръдия) заемат огневи позиции на господстващи височини със задача да водят контра оръдейна борба, да поразяват придвижващи се колони от терористи, атакуващи пехотни подразделения, огневи средства на бойна позиция и пунктове за управление. Огънят се води по наблюдаеми и надеждно разузнати цели, което позволява за 2-3 минути да се изпълнява задачата по унищожаване на разкритите цели с малък разход на боеприпаси и при осигурена безопасност за собствените подразделения.

При участие в борбата с терористичните формирования, действията на артилерията могат да се обособят в три етапа;

- ♦ Подготовка за водене на бойни действия и демонстрация на сила;
- ♦ Участие в нанасянето на изпреварващи огневи удари по терористичните групи и отряди и в обкръжаване на района, в който са разположени;
- ♦ Участие в операцията по ликвидиране на терористичните групи и отряди.

Изпреварващите огневи удари могат да се нанасят с началото на воденето на бойните действия по достоверно разузнати складове с военна техника и въоръжение, заети бойни позиции, райони за съсредоточаване на терористични формирования, пунктове за управление и снабдителни бази.

Подготовката за участие в изпреварващите огневи удари следва да се извършва в обстановка на строго спазване на скритостта в действията за постигане на внезапност и недопускане терористите да се разсредоточат или да напуснат заеманите райони.

За участие в огневите удари се привличат бойни вертолети, авиация, далекобойна и реактивна артилерия. Ударът се нанася предимно с високоточни боеприпаси по достоверно разузнати и наблюдаеми цели и при строго спазване на мерките за координиране на огъня и недопускане на жертви сред мирното население и разрушаване на обекти от инфраструктурата. Ударът започва с поразяване на огневите средства, пунктовете за управление и бойната техника на терористичните групи и отряди и продължава с поразяването на основните им сили.

След участието си в изпреварващия огневи удар, артилерията участва в операцията по ликвидиране на терористичните групи и отряди. За целта се извършва планиране на огъня на артилерията в следните периоди:

- Огнево осигуряване изнасянето на маневрените формирования към блокирания район;
- Огнева подготовка за въвеждане в бой на маневрените формирования;
- Огнево съпровождане на щурмовите групи и отряди;
- Огнево блокиране на терористичните групи в заетите от тях райони и позиции;
- Огнево възпрепятстване на маньовъра на терористичните групи и отряди.

При изпълнението на поставените задачи, артилерията може да се привлича за поддръжка действията на маневрените формирования при изпълнение на следните задачи:

- При разделяне на враждуващи групировки;
- Участие в рейдови бойни действия за прочистване на блокиран район;
- При устройване на засади;
- За пресичане на действия, водещи към нарушаване на установения ред;
- За охрана и отбрана на важни обекти;
- За поддръжка действията на маневрените формирования в зоната за отговорност;
- При охрана на комуникации и съпровождане на колони (хуманитарни конвои; представители на ООН, Европейския съюз, Червения кръст, Червения полумесец и др.) в зоната на конфликта;
- При осигуряване излизане от района на бойните действия на мирно население, преминаване на бежанци, освобождаване на заложници, възпрепятстване на провокативни действия, прилагане на съглашение за прекратяване на огъня и разоръжаване на терористични групи;
- При носене на комендантска служба и патрулиране в заповядани зони.

За решаване на посочените задачи артилерията използва известните видове огън: огън по отделна цел, съсредоточен огън, заградителен огън и съпровождащ огън по метода на последователното съсредоточаване на огъня.

Във всеки конкретен случай реда за изпълнение на огневите задачи, способа за обстрелване на целите, разхода на боеприпаси и количеството на привличаните артилерийски системи се определят в зависимост от обстановката на бойното поле. При това могат да възникнат за изпълнение нови понятия свързани със задачите на маневрените формирования по унищожаване на терористичните групи и отряди, такива като: отсечен огън, прочистващ огън, огън за блокиране, изтощителен огън, безпокоящ огън и др. Разходът на боеприпаси за изпълнението на всеки вид огън се определя в зависимост от задачата на стрелбата и необходимото време за небоеспособност на обстрелваните цели.

Управлението на огъня на артилерията при всички положения се извършва по

правилата за водене на съсредоточен огън, огън по отделни цели, съпровождаш огън и огневи наблюдения, по направленията за действия на маневрените формирования.

С началото на изнасянето на маневрените формирования към района на разполагане на терористичните групи и отряди, артилерията създава огневи коридори по протежението на маршрутите за движение на колоните. Тази задача може да се изпълнява в два варианта: първи - създаване на огневи блок и втори - комплексно използване на огневите средства по целия маршрут на движение на колоните. На схема № 1 е показан първият вариант на използване на огневите средства-създаване на огневи блок.

Превеждане на конвои и колони с „Огневи блок”

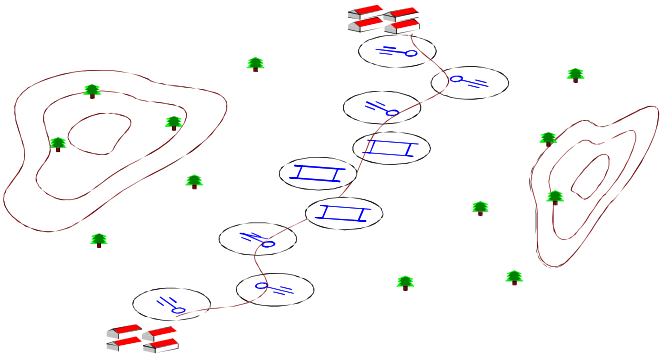


Схема №1.

„Огневи блок” се използва при превеждане на колони по сравнително къси и силно уязвими маршрути. Същността му се заключава в следното: встрани от маршрута за движение на колоната по цялата му дължина на отдалечение един от друг на разстоянието на правия изстрел се разставят танкове, БМП и самоходни артилерийски установки, а между тях през **300-400 m** - стрелкови средства (обикновено картечни групи). По този начин по дължината на целия маршрут има предварително развърнати и готови огневи средства. Този вариант предоставя голяма самостоятелност на командирите на маневрени формирования, на разчетите и екипажите за откриване на огън и прикриване движението на колоната.

Комплексното използване на огневите средства по целия маршрут на движение се прилага за съпровождане на колони при марш на големи разстояния. Той осигурява ефективното използване на артилерията за стрелба както от закрити огневи позиции, така и с право мерене. За целта се създават три групи артилерия, в състав като правило батареи (взводове) самоходни гаубици, а за коригиране на огъня им от закрити огневи позиции на всеки **10-15 машини** от съответната колона се изп-

раща артилерийска предна наблюдателна група. Първата група артилерия се движи в челото на колоната (в състава на охраната), втората - в състава на главните сили (след групата за управление) и третата - в края на колоната. Това построение осигурява огъня на артилерията и неговото коригиране дори в случай на разкъсване на колоната по време на марша. На схема № 2. е показан вариант на използване на този метод за превеждане на колоните по маршрутите им за движение.

Превеждане на конвои и колони чрез създаване на „Огневи коридори”

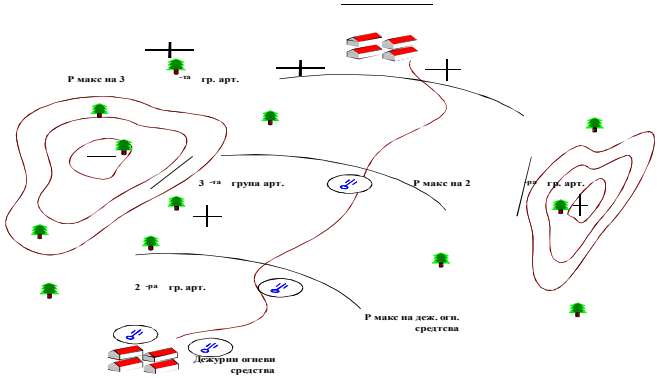


Схема № 2.

По протежението на маршрута за движение се определят: участъци на съсредоточен огън по места, в които е възможно разполагане на терористични групи и по позициите на техните огневи средства; рубежи на заградителен огън по направленията за възможни атаки на групите (т.н. „отсечен огън”). За изпълнението на огневи задачи по маршрута за движение на колоните последователно се развръщат артилерийските батареи (взводове), така, че колоната да бъде непрекъснато прикривана с огън, ако това е необходимо.

Същността на огневото блокиране се състои в блокиране на района, зает от противника (в някои случаи и от собствените войски), с огъня на артилерията, удари на бойни вертолети и дистанционни минни полета. Това не позволява на противника да реализира своите възможности за определено време, необходимо на настъпващите маневрени формирования за изпълнение на поставената задача. На схема № 3. е посочен вариант на огнево блокиране.

За „огнево блокиране” на терористичните групи и отряди в определен район в зоната на конфликта се планира и води заградителен и съсредоточен огън по възможните пътища за маньовър, за изолиране на резервите, за блокиране в заети позиции или населени места. При това се извършва дистанционно миниране, като се създават най-често сковаващи минни полета.

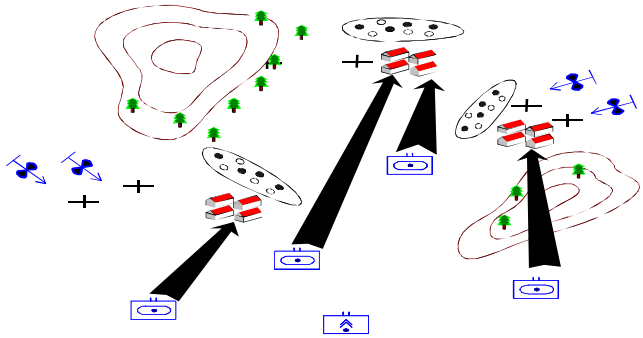


Схема № 3.

„Огневото блокиране” е целесъобразно да се провежда не само за изолация на противника в заетите от него райони, но и в хода на провеждане на огневата поддръжка. За целта се подготвят рубежи на заградителен огън в тилните граници и на фланговете на целите за атака, с цел предотвратяване оттегляне на противника, отразяване на флангови и фронтални контраатаки, възпрепятстване подхода на резерви на противника и др. Неподвижният заградителен огън се открива и води със серии методически огън или в течение определено време до изпълнение на поставената задача.

„Огневото прочистване” е целесъобразно да се планира и провежда по горски масиви с гъста растителност и други участъци от пресечена местност, на която могат скрито да се предвижват и съсредоточават терористични групи и огневи средства и да нанасят удари по нашите войски. То се използва най-вече за прочистване на блокиран район, в който има разположени терористични групи и отряди и има за цел тяхното ликвидиране или да се принудят да прекратят съпротивата и да се изземе оръжието им. Същността на огневото прочистване се състои в планиране и провеждане на огън на няколко рубежа, разстояние между които може да бъде до 200-400 м. На всеки рубеж се подготвят не по-малко от 5-6 участъци на съсредоточен огън. Участъците се избират на господстващи височини, на горски поляни, където терористичните групи могат да заемат бойни позиции или да разполагат на тях огневи средства. По всеки участък огъня се води със взвод или батарея. Едновременно с това се планира и води неподвижен заградителен огън по пътищата, с цел възпрепятстване оттеглянето на терористичните групи или подхода на резерви. Този метод на поразяване на терористичните групи и отряди много прилича на съпровождащия огън по метода на последователното съсредоточаване на огъня в съчетание със заградителен огън воден по фланговете, но тук воденето на огъня не е строго обвързано с времена за водене на огъня и темповете за настъпление на маневрените формирования.

В случаите, когато за воденето на „огнево прочистване” не могат да се опреде-

лят размери на целите, време за водене на огъня и разход на боеприпаси по всяка цел, то се планира и води по рубежи разстоянието, между които е 150-200 м, като се създава плътна зона на поразяване на всяко направление за действие на маневрените формирования. Широчината на зоната се определя от конкретната обстановка, условията на местността и се определя по 50 м на оръдие с калибър над 100 мм за един рубеж. Огънят се води като методически за определено време или от серии залпове през 15-20 секунди. Сигнала за пренасяне на огъня по следващия рубеж се подава по общите правила с отчитане на разстоянието за безопасност за собствените подразделения. При воденето на „огневото прочистване" по този начин се оставят 1-2 артилерийски взвода за дежурни, които имат задача при необходимост и при разкриване на огневи средства на терористичните групи да водят борба с тях.

Моралното въздействие върху терористичните групи и отряди с огъня на артилерията има особено важно значение. Това е така, защото в такива бойни действия са големи разрушенията и материалните щети за цивилното население, поради много честото пребиваване на терористи в населени места или пък използват цивилно население като жив щит.

Опитът от водене на борбата с терористичните групи и отряди показва, че степента и продължителността на моралното въздействие с огъня на артилерията по живата сила зависи от различни фактори: количеството на понесените загуби; общото състояние на терористите и издръжливостта в такава обстановка; личния пример на командирите и умението им да управляват подразделенията и да мотивират личния състав за водене на бойни действия срещу терористите; продължителността и интензивността на водене на бойни действия в операцията; реда за водене на огъня о огневите средства; възможностите за получаване на надеждна разузнавателна информация за целите на противника и тяхното своевременно обстрелване. Задачите за унищожаване на терористичните групи са скъпи от гледна точка на време и ресурси.

При отсъствие на точна информация за местонахождението на основните огневи средства на противника и неговата жива сила и с цел ликвидиране на блокирани или обкръжени терористични групи може да се провежда огнево прочистване на района. Използваната тактика на действие на принципа на скитащите оръдия, противника ще се стреми да действа практически по един и същ начин. Огневите позиции на огневите средства той ще определя близо до кръстопътища, окрайнини на гори, отделни здрави сгради в населените места, на превали и важни височини, координатите на които точки могат да бъдат предварително определени и по тях да се подготвят съсредоточени огньове.

Подготовката на бойното поле в разузнавателно отношение, непрекъснатото изучаване на действията на противника и времето през което той води огън, създава условия по него да се нанасят изпреварващи огневи налети и по този начин да се прочиства зоната от терористите.

В хода на бойните действия следва широко да се използва и воденето на „безпокоящ огън". Неговата същност се заключава във воденето на кратки 2-3 мин. огневи налети бърз или методически огън по разкрити цели на терористичните групи и отряди през интервал 15-30 мин. Целта на такъв вид огън е не толкова да се нанасят определени загуби на противника, колкото да се принуждава непрекъснато да маневрира и да избягва изпод ударите на артилерията и по този начин да се

изтощава и държи под непрекъснато напрежение и да се контролират неговите действия. Този вид огън може да се прилага във всякакви условия на денонощието, при всякакви метеорологични условия и на всякаква местност-равнинна, планинско-гориста и в населени места. При водене на огън нощем, се назначават оръдия за осветяване на местността в района на целите.

Такъв вид огън не само подтиска бойния дух на противника, но постига и друга по-важна цел – повдига духа на собствените формирования.

Когато се налага да се контролират големи по площ зони, да се отбраняват базови райони, важни стопански обекти, носене на служба от стражеви застави и постове с малко сили и средства се създава система от артилерийски бази. Основата на артилерийската база може да бъде артилерийска батарея или дивизион. Когато силите на терористите са в по-малък състава се назначава артилерийска батарея, а когато те са значителни се определя артилерийски дивизион в състава на артилерийската база. За тях се определя район за огневи позиции, който се подготвя за кръгов обстрел. Района за огневи позиции се избира в непосредствена близост до района за разполагане на маневреното формирование, до контролно-пропускателни пунктове, до базови райони на маневрените формирования и др., така че артилерията да бъде охранявана от тях. В зоната с радиус 2/3 от далекобойността на артилерийските средства се организира патрулиране и се води разузнаване от разузнавателни групи, а артилерийските предни наблюдателни групи се разполагат по периферията на зоната. За да се намали вероятността за разкриване на патрулите и разузнавателните групи в зоната, те трябва да са в малък състав, не повече от 3-4 човека и да са обучени да определят с достатъчна точност координатите на целите и да коригират артилерийския огън. В зоната се организира противовъздушна отбрана и наблюдение от въздуха за действията на противника. По този начин батареята (дивизиона) може да контролира зона с площ около 300-400 км^2. Следващите артилерийски бази се разполагат на 10-15 км една от друга, така че да се застъпват на разстояние 1/3 от далекобойността на артилерийските системи. В зоните на застъпване се определят и налагат мерки за координиране и се определя отговорник за координирането на огъня. Ако се направи анализ на използването на такива артилерийски бази, може да се направи извода, че те могат да играят съществена роля за контролирането на огромни територии, в които действат терористични групи и отряди и борбата с тях да бъде ефективна.

Опита от воденето на бойни действия срещу терористични групи и отряди, през последните няколко години показва, че ролята на артилерията в поразяването на противника непрекъснато нараства особено, когато в техния състав има на въоръжение бронирана техника, артилерия, зенитни средства и друго тежко въоръжение.

Бойните действия срещу терористични групи и отряди се характеризират с бърза и непредвидена промяна на обстановката, отсъствие на непрекъсната линия на съприкосновение, вследствие на което бойните действия най-често имат непредвидим характер, водят се по отделни направления с бърза смяна на бойните позиции. Това налага използването на нестандартни способи за водене на бойните действия в съответствие със създалата се обстановка и при голямо напрежение за личния състав, особено за командирите и щабовете.

Това е така защото, придържането към строго определените от ръководните документи и правила за водене на нестандартни бойни действия успех не може да се постигне. Вземането на решения при дефицит от време изисква командирите и

щабовете да прилагат на практика поуките от воденето на такива бойни действия и да усъвършенстват възприетите методи за вземане на решения и управление на бойните действия в нестандартна обстановка.

Използвани литературни източници:

1. Огнева поддръжка в съвременните операции – учебник – И. Гюргаков, 2007.
2. Тактическа доктрина на полевата артилерия, 2005 г.
3. Точилов, Годишник на Военна академия 2010 г. Военно научна конференция на факултет командно щабен, Доклад – Разузнавателна подготовка на бойното поле, основа на процесите на целеобразуване и целеразпределение.
4. STANAG 2484 "NATO fieled artillery taktikal doktrine".
5. STANAG 2934 "Artillery procedures".
6. STANAG 2285 arty (edition 1) – land targeting- AJP – 3.9.2 – 2007.
7. AJP-3 (b) allied joint doctrine for the conduct of operations.
8. Joint publication 3-60 – Joint targeting – 2007.
9. Brigade planning process – Center for army lessons learned 2006.
10. Field Artillery in Military Operations Other Than War: An Overview of the US experience Combat Studies Institute Press Fort Leavenworth, Kansas.

МОДЕЛИРАНЕ НА ДИНАМИКАТА ЗА РАЗПРОСТРАНЕНИЕ И ОТЛАГАНЕ НА АЕРОЗОЛНИ СТРУКТУРИ В ПРЕСЕЧЕН РЕЛЕФ НА РЕПУБЛИКА БЪЛГАРИЯ

Костадин Н. Костадинов

НВУ "В. Левски", koce_knk@abv.bg, тел.+359 62 61 611

MODELLING DYNAMICS DISTRIBUTION AND SEDIMENTATION OF THE AEROSOL STRUCTURES IN THE CROSSED RELIEF OF REPUBLIC OF BULGARIA

Kostadin N. Kostadinov

NVU"V. Levski", koce_knk@abv.bg, phone: +359 62 61 611

ABSTRACT: Modeling characteristics of the air reactivity of different types of aerosols landed to less pollution and cross-country average, deposition of aerosol clouds leading to the presence of undefined areas of concentrations above the exposure

KEY WORDS: aerosols, chemical activity, aerosol structures

Увод. Все по-често в практиката се налага да се моделират особеностите на въздушната химическа активност на различни видове аерозоли вадещи до замърсяване на слабо и средно пресечени местности в република България. Моделите преди всичко се приемат като за средни условия се предполага запазване на динамиката на отлагане на аерозолни структури, характерни за съответните процеси на

равнинни местности. Получените отрицателни резултати от отлагането на аерозолни облаци водещи до наличието на недефинирани зони на концентрации над допустимите, като правило се отписват, на случайни промени на посоката и скоростта на вятъра или от други локално определени метеорологически обстоятелства. [1,2]. При това не се разглеждат следствията на инверсия в атмосферния граничен слой в териториите на Република България – Дунавската равнина и Тракийското поле.

1. Постановка на проблема. Във връзка с горепосоченото се налага да се определи сравнително адекватен модел за разпространение и отлагане на аерозолни структури, който да позволи отчитане на динамиката в съответствие метеорологичните условия в даден терен от територията на Република България. За целта може да се използва математическият апарат задаващ уравнения от метеорологията с отчитане автономните зависимости и теория за сходството в слоя на постоянни турбулентни потоци и параметрите на приземният вятър на базата на пространствен модел [4,6]. При това водеща роля в тях се отдава на като компоненти на скоростта посоката на вятъра, значението на коефициента на турбулентност, както и височината на стабилен повърхностен слой, се използват при реализиране на пренасяне на примеси, което се основава на уравнението на преноса и турбулентната дифузия за концентрация в определен параметър изразен в обем в пространството от територията на Република България (x_d, y_d, z_d) и време за експозиция t_d задаващи коефициента на дифузия на аерозолите $K_{diff}^{aero}(x_d, y_d, z_d, t_d)$. Тогава при отчитане компонентите определящи вектора на скоростта на вятъра, а именно - u_p - атмосферно налягане - (Pa); v_α - направление, посока (азимут) на вятъра - $(0-360 \text{ deg})$; w_{sp} - скорост на въздушните маси (m/s), или (u_p, v_α, w_{sp}). При анализ или познаване физическите характеристика на типовете аерозолни структури, то е възможно да се определи скоростта на гравитационното утаяване на аерозолните примеси w_{send}. Тогава основната зависимост на влиянията на вятъра в пространството, дифузията се представя във следния вид:

$$\frac{\partial K_{diff}^{aero}}{\partial t_d} + \frac{\partial u_p K_{diff}^{aero}}{\partial x_d} + \frac{\partial v_\alpha K_{diff}^{aero}}{\partial y_d} + \frac{\partial (w_{sp} - w_{send}) K_{diff}^{aero}}{\partial z_d} = \tag{1}$$

$$= \alpha_{K_{diff}^{aero}} \frac{\partial}{\partial x_d} K_{x_d}^{turbo} \frac{\partial K_{diff}^{aero}}{\partial x_d} + \alpha_{K_{diff}^{aero}} \frac{\partial}{\partial y_d} K_{y_d}^{turbo} \frac{\partial K_{diff}^{aero}}{\partial y_d} + \alpha_{K_{diff}^{aero}} \frac{\partial}{\partial z_d} K_{z_d}^{turbo} \frac{\partial K_{diff}^{aero}}{\partial z_d} + In_{K_{diff}^{aero}}^{EM}$$

където $K_{x_d}^{turbo}, K_{y_d}^{turbo}, K_{z_d}^{turbo}$ - коефициенти на турбулентния обмен на въздушните маси с аерозолният облак в посоките x_d, y_d, z_d дефиниращи обема, пространството в определена територия на страната; $\alpha_{K_{diff}^{aero}} = \frac{1}{Sm}$; Sm - числото на Shmidt за базовата степен на аерозолен обмен; $In_{K_{diff}^{aero}}^{EM}$ - интензивност на емисиите на вещест-

вата влизащи в аерозолният облак в размерност $(\frac{kg^{-3}}{m^{-3}} s^{-1})$.

Основния набор от гранични условия за уравнение (1), се формулира в точката на източника на заразяването изразено на плоскост или пункт по границите на района, пространството от територията на местността в територията на страната, промените на коефициентите на дифузия на аерозолите могат да се представят във вида:

$$\frac{\partial K_{diff}^{aero}}{\partial x_d} = 0, \qquad \frac{\partial K_{diff}^{aero}}{\partial y_d} = 0;$$

При отчитане характера на местността - видът на релефа изразен със земните форми главно с надморската височина H_o^{elev}, или средната надморска височина на земните форми – хълмове, полупланинска местност, плата, поречия на реки и др.

$$K_{z_d}^{turbo} \frac{\partial K_{diff}^{aero}}{\partial z_d} = 0 \quad \text{при } z_d = H_o^{elev}$$

За получаване на модел на пренос и дифузия на примесите непосредствено на земната повърхност може да се приеме средната стойност на надморската височина $H_{o\_mean}^{elev}$ при дефиниране на (1). Тогава за концентрация на дифузията във височини за $K_{z_d}^{turbo}$ се задава със следния израз:

$$(2) \qquad K_{z_d}^{turbo} = N_k \left[e^{\left(-\frac{\left(H_{o\_mean}^{elev} - h_{diff}\right)^2}{2\sigma_{z_d}^2} \right)} + e^{\left(-\frac{\left(H_{o\_mean}^{elev} + h_{diff}\right)^2}{2\sigma_{z_d}^2} \right)} \right]$$

където h_{diff} - надморска височина на източника на аерозолни емисии над земята, m; $\sigma_{z_d}^2$ - стандартно отклонение (дисперсия) във височина на разположение източника на замърсяване спрямо $H_{o\_mean}^{elev}$; N_k - нормализиран множител на средната надморска височина в територията на Република България.

С цел извършване осредняване уравнение (2) се налага интегриране по z , използва се състояние на масата на вертикалния поток на горната граница в областта на земната концентрация, налагащо се върху контурите на релефа, генерирани със специална програма преди началото на основния разчет. Това позволява, промяна на интересуващите ни параметрит за да бъде решена задачата, анализира се характера на разпределение на концентрацията в контролната точка в разчетната област на Северна и Южна България.

2. **Проверка на модела в територията на Република България.** Нека определим работоспособността на модела (1) - (2) при описване на динамиката за разпространение и отлагане на аерозолни структури в пресечен релеф на Република България. За целта избираме параметрите на Дунавската равнина спрямо Тракийс-

ката низина ориентирани съгласно географски особености, а именно територия под формата на паралелепипед. Въвеждаме декартова координатна система (x_d, y_d, z_d) спрямо гр. Плевен и гр. Пловдив, в която оста z_d е насочена вертикално, оста x_d - на изток, а оста y_d - на север. Областта на решение се определя във вид на паралелепипед на неоднородната повърхност на релефа, хълмист с минимални параметри като

(3) $10\ km \le x_d \le D_x\ 10\ km \le y_d \le W_y,\ 100\ m \le z_a \le H_o^{elev}$,

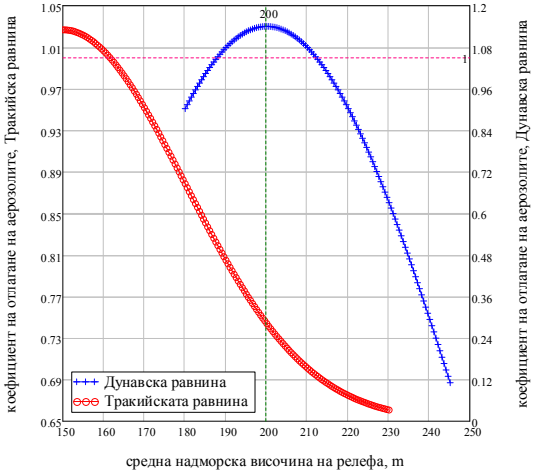
където D_x - дължината на региона km, W_y - широчина на региона, km ; приемаме функция $z_d = H_o^{elev}$ за определяне релефа на местността в двете равнини. При това е възможно да се формира област с параметри:

В дунавската равнина - район с размери ($D_x = 200\ km, W_y = 60\ km$ и предполага наличието на хълмове - 2 – 3 в km^2 при средна надморска величина $H_{o\_mean}^{elev} = 200\ m$ и величини $(u_p = 710\ Pa,\ v_\alpha = = 270 - 300\ \deg\ u\ w_{sp} = 5,\ 7u\ 10\ m/s)$ и с дължина на наветрения склон на хълмовете - 300 м разположени под прав ъгъл спрямо източника на аерозол.

В Тракийската равнина - район с размери ($D_x = 260\ km,\ W_y = 70\ km$ и предполага наличието на хълмове – 0.5 – 1 на km^2 при средна надморска величина $H_{o\_mean}^{elev} = 150\ m$ и величини $(u_p = 710\ Pa,\ v_\alpha = = 250 - 290\ deg\ u\ w_{sp} = 5,\ 7u\ 10\ m/s)$ и с дължина на наветрения склон на хълмовете - 200 м разположени под прав ъгъл спрямо източника на аерозол.

Реализацията на модела с посочените данни е демонстрирана на фиг. 1.

Коефициентите на отлагане на аерозоли - на фиг. 1 се демонстрира, че при равна интензивност на емисиите на веществата, влизащи в аерозолния облак , $In_{K_{diff}^{aero}}^{EM} \to const$ в двата региона. В Дунавската равнина хълмистата част в значителна степен задържа аерозолите. Така например, динамиката на отлагането при $H_{o\_mean}^{elev} = 200\ m$ бележи своя максимум $K_{diff}^{aero}(x_d, y_d, z_d) \to max$, а при останалите флуктуации на надморската величина на стандартно отклонение (дисперсия) във височина на разположение източника на замърсяване $\sigma_{z_d}^2 = 50\ m$ спрямо $H_{o\_mean}^{elev}$ съответно $0.12 \le K_{diff}^{aero}(x_d, y_d, z_d) \le 1.13$. Докато в Тракийската равнина с подчертаният си равнинен характер $H_{o\_mean}^{elev} = 150\ m$, $\sigma_{z_d}^2 = 30\ m$ съответно величината на коефициента $K_{diff}^{aero}(x_d, y_d, z_d)$ е в нормите на $0.62 \le K_{diff}^{aero}(x_d, y_d, z_d) \le 1.13$.



Фиг. 1. Коефициенти на отлагане на аерозоли в Дунавската равнина и Тракийската равнина на Република България

При отчитане на коефициенти на турбулентния обмен на въздушните маси с аерозолният облак $K_{x_d}^{turbo}, K_{y_d}^{turbo}, K_{z_d}^{turbo}$ в посоките x_d, y_d, z_d при данните и в двата региона $(u_p = 710\ Pa,\ v_\alpha = 250-290\ deg\ u\ w_{sp} = 5,\ 7u\ 10\ m/s)$ се наблюдават следните явления:

В Дунавската равнина, поради подчертано хълмистият си характер концентрация на избрания произволно аерозол по наветрената част от склоновете и фиксирана позиция на източник на емисии демонстрира различни параметри на аерозолното утаяване. Резултатите от него са демонстрирани в таблица 1.

Таблица 1.

Разпределение на параметрите на аерозола от скоростта на вятъра в хълмиста местност в приземния слой на атмосферата в Дунавската равнина

Скорост на вятъра в приземния слой, m/c	Параметри на подножието на хълмовете с размери, m	Структура на аерозолното образование, диаметър на капката -% в подножието на хълмистата местност
5	500	70 mkm -20%, 100 mkm -50% 120мкм -30%
7	700	100 mkm -30%, 160 mkm -40% 180мкм -30%
10	900	170 mkm -20%, 190 mkm -20% 220 mkm -60%

Разпределение на земната концентрация в указаната по-горе област, при 2–3 хълма (Таблица 1.) динамиката на разпространение и отлагане на аерозоли, при скорост на вятъра 5 m/s обхваща - 120 mkm -30% докато при 10 m/s с размери 220 mkm -60%. В този случай, концентрацията се увеличава от началната стойност 30 -

32%, като по този начин затруднява намаляването въздействието на аерозолите особено в силно хълмистата част на Дунавската равнина.

В Тракийската равнина, поради преобладаващо равнинният си характер концентрация на избрания произволно аерозол по наветрената част на склоновете и фиксирана позиция на източник на емисии демонстрира различни параметри на аерозолното утаяване. Резултатите от него са демонстрирани в таблица 2.

Таблица 2

Разпределение на параметрите на аерозола от скоростта на вятъра в хълмиста местност в приземния слой на атмосферата в Тракийската равнина

Скорост на вятъра в приземния слой, m/c	Параметри на подножието на хълмовете с размери, m	Структура на аерозолното образование, диаметър на капката -% в подножието на хълмистата местност
5	300	60 mkm -20%, 80 mkm -50% 100мкм -30%
7	400	100 mkm -30%, 140 mkm -40% 160мкм -30%
10	600	180 mkm -20%, 190 mkm -20% 200 mkm -60%

Разпределение на земната концентрация (таблица 1) динамиката на разпространение и отлагане на аерозоли, при скорост на вятъра 5 m/s обхваща - 100 mkm -30% докато при 10 m/s с размери 200 mkm -60% . В този случай, концентрацията се увеличава от началната стойност 30 - 32%, при намаляване на параметрите на размерите на аерозола с 10 -20 % като по този начин благоприятства намаляване въздействието на аерозолите особено в силно равнината част на Тракийската равнина.

Заключение. Горепосочените резултати показват, че дори и леко, невисоки, хълмове $H_{o\_mean}^{elev} = 200\ m$ водят до съществени промени в характера на разпространението и отлагането на въздуха и образуването на аерозоли в пресечен терен особено важно за Дунавската равнина. Докато в Тракийската равнина липсата на хълмове оказва положителен ефект при намаляване вредните концентрации при техногенни катастрофи. Например при разработването на сценарий с АЕЦ „Козлодуй" образуването на аерозоли в пресечен терен за Дунавската равнина ще води до негативни резултати. А при химически аварии в Тракийската равнина тяхното локализиране ще бъде ефективно за кратко време.

Литература

1. Леженин, А. А. Численная модель миграции аэрозоля, образовавшихся в зоне лесных пожаров, А. А. Леженин, В. А. Мальбахов, В. А. Шлычков, Оптика атмосферы и океана, 2008.

2. Меньшов, М. В. О математической модели миграции и осаждения полидисперсного аэрозольного образования, М. В. Меньшов , Вестн. Сам. госуд. ун-та. Естественнонаучная серия, 2006.

3. Шлычков, В. А. Численная модель пограничного слоя атмосферы с детали-

зацией конвективных процессов на основе вихреразрешающего подхода, В. А. Шлычков ,Новосибирск: Изд-во СО РАН, 2005.

4. Breitung W., Redlinger R. Containment pressureloads from hydrogen combustion in unmitigated severe accidents, Nuclear Technology, 1995.

5. Chrosciel St., Instructions for standard calculations of emission parameters for industrial, sources in Polish, Technical University of Warsaw Publ., Warszawa, 1983.

6. Smagorinsky J., Numerical results from a ninelevel general circulation model of the atmosphere, J. Smagorinsky, S. Manabe, J. Hollway , Month. Weather Rev, 1993.

ИНФОРМАЦИЯ И МАТЕМАТИЧЕСКИ МОДЕЛ, ОПИСВАЩ РАЗПРОСТРАНЕНИЕТО НА ЗАМЪРСИТЕЛИ В АТМОСФЕРАТА

Костадин Н. Костадинов

НВУ"В. Левски", koce_knk@abv.bg, тел.+359 62 61 611

INFORMATION AND MATHEMATICAL MODEL DESCRIBES SPREAD OF CONTAMINANTS THE ATMOSPHERE

Kostadin N. Kostadinov

NVU "V. Levski", koce_knk@abv.bg, phone: +359 62 61 611

ABSTRACT: A method is proposed to construct horizontal and vertical profile, the height of the upper atmosphere. Featured are differential equations describing the spread of pollutants to certain meteodanni.

KEY WORDS: horizontal and vertical profile, atmosphere pollutants, information system failures.

1. Увод. През последните години все по-голямо внимание се отделя на екологията като резултат от бурното развитие на химията в промишлените производства в националните икономики на множество страни. Поради това прогнозирането на разпространението на замърсители във въздуха се явява важен проблем за повишаването качеството на безопасност на населението живеещо в тези региони. Последното налага създаване на задоволителен физически модел, описващ замърсяването на атмосферата с различни замърсители. Част от такива модели свързани със замърсяване на атмосферата са представени в [1].

Ето защо възниква необходимостта от разработването на математически модел за прогнозиране на разпространението на замърсители в атмосферата в определени локални параметри наситени с промишлени предприятия от химическата промишленост. Математическият модел трябва да отчита степента на опасността, както и информационното осигуряване.

2. Постановка на задачата. Нека да предположим, че в определена локална

градска среда се намира индустриална зона Z_{ind} с правоъгълна форма с характерни размери M_R. Също така нека да са известни и метеорологичните особености на региона, в който е разположена тази Z_{ind}. При тези условия ние ще разгледаме влиянието на разпространяването на замърсяването с отлагания и окисляване на оксидите на сярата - SO_2 и SO_4, азотни окиси, прах както и други аерозоли подбирани по метода на подобието обединени под обобщените „условните аерозоли" - $A_{cond}^{aerosols}$. Предложеният модел предполага анализиране и на други видове замърсяване. За целта още в началото се определят метеорологичните елементи на параметрите на вятъра – скорост и посока, величината на турбулентността, а също така и други метеорологични данни. Те се явяват базисни за математическото моделиране, получени от метеорологични станции вътре в индустриална зона Z_{ind}.

Системата от уравнения, описващи преноса на замърсители в атмосферата, притежава сечения във височина, където означаваме: зоната за замърсяване $Z_{ind}^{pollution}$ за интервал от време $\Delta T^{poll} = 0, T^{poll}$ или $Z_{ind}^{pollution} \to 0, T^{poll}$; при условие, че замърсяването се реализира в пространствена зона възприета за паралелепипед, то заразената площ от земната повърхност $S_{ind}^{pollution}$ може да се опише с параметрите – дължина - $L_x^{pollution}$,m и широчина - $W_y^{pollution}$,m т.е $S_{ind}^{pollution} = L_Z^{pollution}.W_Z^{pollution}$ $H_{laers\_i}^{atm}$ - дебелина на i_{layers} -тия атмосферен слой от височината на заразяването на атмосферата, m. $C_{layer\_1i}^{aerosols}$ и $C_{layer\_2i}^{aerosols}$ концентрация на „условните аерозоли" - $A_{cond}^{aerosols}$ в два съседни слоя $i_{layer} \to 1 \; u \; 2$; $i_{layer} \to 1,...,nz$ - номер на слоя при сечението на стандартната атмосфера; представени в следния вид:

(1) $$\frac{\partial H_{laers\_i}^{atm} C_{layer\_1i}^{aerosols}}{\partial t} + H_{laers\_i}^{atm} C_{layer\_1i}^{aerosols} \overline{w}_{speed} - \left(K_{hor}^{diff} H_{laers\_i}^{atm} C_{layer\_1i}^{aerosols}\right) - D_{1,i} + \left(v_{d_1} + k_{trans}^{txim} H_{laers\_i}^{atm} + k_{trans}^{txim}, H_{laers\_i}^{atm}\right) C_{layer\_1i}^{aerosols} = \left(1 - \beta_{otn}^{\%}\right) H_{laers\_i}^{atm} \overline{Q}_{field}^{emiss}$$

(2) $$\frac{\partial H_{laers\_i}^{atm} C_{layer\_2i}^{aerosols}}{\partial t} + H_{laers\_i}^{atm} C_{layer\_2i}^{aerosols} \overline{w}_{speed} - \left(K_{hor}^{diff} H_{laers\_i}^{atm} C_{layer\_2i}^{aerosols}\right) - D_{2,i} + \left(v_{d2} + k_{\omega_1} H_{laers\_i}^{atm} + k_{\omega_1} k_{trans}^{txim}, H_{laers\_i}^{atm}\right) C_{layer\_1i}^{aerosols} - k_{\omega_1} H_{laers\_i}^{atm} C_{layer\_2i}^{aerosols} = \beta_{otn}^{\%} H_{laers\_i}^{atm} \overline{Q}_{field}^{emiss}$$

Където K_{hor}^{diff} - коефициент на хоризонталната дифузия, K_{vert}^{diff} - коефициент на вертикална дифузия, $\overline{w}_{speed}$ - скорост на вятъра, $\overline{Q}_{field}^{emiss}$ - поле на емисиите в заразеният участък , v_{d_1}, v_{d_2} - скорост на сухото отлагане на аерозолите , а $k_{\omega_1}, k_{\omega_2}$ - скорост на влажното отлагане на аерозолите, k_{trans}^{txim} - скорост на химическата трансформация на формирането на условните аерозоли в два съседни слоя, $\beta_{otn}^{\%}$ - относителна част от на всеки един аерозол в слоевете, спрямо общото на стойност-

та на „условните аерозоли” - $A_{cond}^{aerosols}$.

3. Условен физически модел на атмосферата. Известно е, че земната атмосфера е формирана от въздушни маси, които се характеризират от различни метеорологични параметри – температура на въздуха, налягане, влажност, посока и скорост на вятъра и др. Движението на въздушните маси има турбулентен характер и се характеризира с непостоянство на скоростта на вятъра $\overline{w}_{speed}$ в зоната за замърсяване $Z_{ind}^{pollution}$. Това води до силно смесване и взаимодействие между различните слоеве, които формирането на стойността на „условните аерозоли” - $A_{cond}^{aerosols}$ характеризират с коефициентите на дифузия, K_{hor}^{diff} K_{vert}^{diff}. Смесването води до формирането на стойността на „условните аерозоли” - $A_{cond}^{aerosols}$ с различна плътност, примеси и т.н.

Математическото описание на процеса на турбулентно смесване определя - скоростта на сухото отлагане на аерозолите v_{d_1}, v_{d_2}, а така също и скоростта на влажното отлагане на аерозолите $k_{\omega_1}, k_{\omega_2}$, k_{trans}^{txim} - скорост на химическата трансформация на формирането на условните аерозоли в два съседни слоя, където важна роля играе коефициента за турбулентност или коефициент на дифузия, тъй като стойността на „условните аерозоли” - $A_{cond}^{aerosols}$ използва изрази за турбулентни потоци на различни физически вещества. Например, вертикален турбулентен поток Fl_z^{aero} за формиране на „условните аерозоли” - $A_{cond}^{aerosols}$ може да се представи :

$$Fl_{vert}^{aero} = -K_z^{turbo} D_{atm}^{layer} \frac{\partial A_{cond}^{aerosols}}{\partial z} \quad (3)$$

където D_{atm}^{layer} - плътност на определен слой от атмосферата, а K_z^{turbo} - коефициент на турбулентност във вертикална посока.

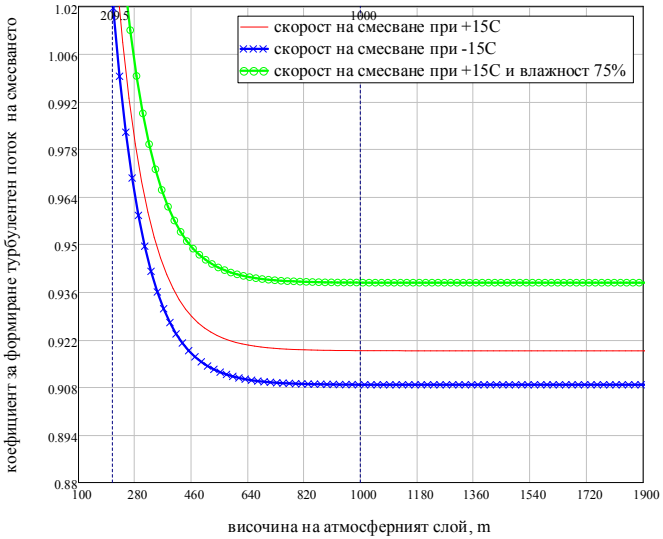
Решаването на (3) спрямо скоростта за формирането $\frac{\partial A_{cond}^{aerosols}}{\partial z}$ на „условните аерозоли” с отчитане на височината на условните слоеве z , се представя във вида:

$$\frac{\partial A_{cond}^{aerosols}}{\partial z} = K_z^{turbo} D_{atm}^{layer} - Fl_{vert}^{aero}$$

или

$$Fl_{vert}^{aero}(z) = A_{cond}^{aerosols}(z) = K_z^{turbo} D_{atm}^{layer} + e^z \quad (4)$$

Геометрическата интерпретация на $A_{cond}^{aerosols}(z)$ при плътност на въздуха за височин $100 \le D_{atm}^{layer} \le 3000\ m$ при различни метеорологични условия е представена на фиг. 1.



Фиг. 1. Коефициент за формиране вертикален поток на смесването на аерозоли с въздуха спрямо приземните слоеве на атмосферата.

Коефициентите за турбулентност в уравненията на турбулентните потоци Fl_z^{aero} (4),Фиг. 1. по правило не отразяват свойствата на преносимите субстанции с различни физични свойства т.е. не отразяват напълно стойността на „условните аерозоли" - $A_{cond}^{aerosols}$. Това е начално условие, поради което се допуска подобие в използването на едни и същи коефициенти K_z^{turbo} в (1) и (2), където от тяхната стойност се отчитат неравности на повърхността на земята, разпределение на температурата по височина (топлинна стратификация), влажност на въздуха, скорост на вятъра и др. За целта се приема, че K_z^{turbo} за получаването условните аерозоли при нормални условия и температура на въздуха $+15C^0$ в метри надморска величина се получава $820 \le K_z^{turbo} \le 1000\ m$; при температура $-15C^0$, $670 \le K_z^{turbo} \le 900\ m$; а при 75% влажност на въздуха - $520 \le K_z^{turbo} \le 800\ m$ - почти 25% по малко от нормалните условия фиг. 1.

4. Построяване модел на полето на вятъра - W_{field}^{aero} .

Проблемът по построяване полето на вятъра W_{field}^{aero}, създаващо площта на замърсяването $S_{ind}^{pollution} = L_x^{pollution}.W_y^{pollution}$, стойността на k_{trans}^{txim} в два съседни слоя, K_{hor}^{diff} - коефициентите на дифузиите $K_{vert}^{diff}, K_{hor}^{diff}$ при зададени стойности

на скоростта $\overline{w}_{speed}$ във височина, се явява основен за създаването на различни физически модели в атмосферата в приземният слой. За тази цел можем да се възползваме от уравнението за движение на въздушните маси. Тогава нека приемем, че определен обем V_{air} въздушна маса притежава тегло m_{air} и плътност ρ_{air} в различните слоеве на атмосферата под действието на различни сили. Полагайки силите, хоризонтална, вертикална, т.е $\vec{W} = (u, v, w)$ действащи на V_{air} и записвайки уравнението за движение в проекция на оси x, y, z в координатна система разположена на земната повърхност, ще получим система уравнения [1]:

$$\frac{du}{dt} = -\frac{1}{\rho_{air}}\frac{\partial D_{atm}^{layer}}{\partial x} + 2\omega_z v - 2\omega_y w + \frac{\partial}{\partial z}k_z\frac{\partial u}{\partial z} + K_{x,y}^{turbo}\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2}\right)$$

(5) $$\frac{dv}{dt} = -\frac{1}{\rho_{air}}\frac{\partial D_{atm}^{layer}}{\partial y} + 2\omega_x w - 2\omega_z u + \frac{\partial}{\partial z}k_z\frac{\partial v}{\partial z} + K_{x,y}^{turbo}\left(\frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2}\right),$$

$$\frac{d\overline{w}_{speed}}{dt} = -\frac{1}{\rho_{air}}\frac{\partial D_{atm}^{layer}}{\partial x} + 2\omega_y u - 2\omega_x v + \frac{\partial}{\partial z}k_z\frac{\partial w}{\partial z} + K_{x,y}^{turbo}\left(\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2}\right) - g$$

където $K_{x,y}^{turbo}$ - коефициент на турбулентност в хоризонтално направление, а $\vec{\omega} = (\omega_x, \omega_y, \omega_z)$ - ъглова скорост на въртене на Земята около своята ос за всяка една надморска височина (за един слой). Ще опишем граничните условия за система уравнение (5), където има пет неизвестни: $u, v, \overline{w}_{speed}, D_{atm}^{layer}, \rho_{air}$, поради това следва, да се определи влажността на въздуха. Влажността оказва влияние на топлообмена в атмосфера, на плътността на въздуха и т.н.

Система (5) описва движението на въздушната среда, на свободната атмосфера. Основна сложност при нейното решение се явява отсъствието на точна зависимост при определяне коефициентите на дифузиите $K_{vert}^{diff}, K_{hor}^{diff}$ и на турбулентност $K_{x,y}^{turbo}$, който зависи от температурата, влажността и скоростта на вятъра. Освен това - посоката и големината на вектора на топлинния поток зависи от разпределението на температурата по височина т.е. температурна стратификация на атмосферата. При построяване на модел на температурната стратификация ще вземем шест класа на временна стабилност на атмосферата със значение 3 - отговаря на дълбока инверсия, 2-силна устойчивост, и 0-безразлично състояние. Този параметър се използва за емпиричната формула за изчисляване на коефициентите на вертикална и хоризонтална дифузия $K_{vert}^{diff}, K_{hor}^{diff}$. Така, както коефициента за дифузия влиза

в уравнение (5), а полето на вятъра зависи от основните параметри на атмосферата, то процедурата за решаване на системи уравнения (1), (2) и (5) в общ вид е доста сложна, ще въведем ред от предварително дефинирани условия:

а) стойността на вертикалната компонента на скоростта на вятъра е $\overline{w}_{speed} = 0$;

b) движението, изменението на проекциите, „съставните" на вятъра върху земната повърхност $S_{ind}^{pollution} = L_x^{pollution}.W_y^{pollution}$ е постоянна величина при което, за хоризонталната - $\frac{du}{dt} = 0$ и вертикалната скорост $\frac{dv}{dt} = 0$;

c) коефициента хоризонталната турбулентност е $K_{x,y}^{turbo} = 0$.

При отчитане на посочените условия, системата за хоризонталните компоненти на вятъра придобива вида:

По дължината $L_x^{pollution}$ на зоната за време T^{poll} - $Z_{ind}^{pollution} \rightarrow 0, T^{poll}$

$$-\frac{1}{\rho_{air}}\frac{\partial D_{atm}^{layer}}{\partial x} + 2\omega_z v + \frac{\partial}{\partial z}K_z^{turbo}\frac{\partial u}{\partial z} = 0 \qquad (6)$$

По широчина на зоната $W_y^{pollution}$ за време T^{poll} - $Z_{ind}^{pollution} \rightarrow 0, T^{poll}$

$$-\frac{1}{\rho_{air}}\frac{\partial D_{atm}^{layer}}{\partial y} - 2\omega_z u + \frac{\partial}{\partial z}K_z^{turbo}\frac{\partial v}{\partial z} = 0 \qquad (7)$$

Решаването на посочените уравнения $\frac{\partial D_{atm}^{layer}}{\partial x}$ и $\frac{\partial D_{atm}^{layer}}{\partial y}$ при всички височини на слоевете позволява да се определят стойността на K_z^{turbo} в двете измерения на зоната $Z_{ind}^{pollution} \rightarrow 0, T^{poll}$.

При построяване областта $Z_{ind}^{pollution} \rightarrow 0, T^{poll}$ стойността на вятъра $\overline{w}_{speed}$ първоначално се приема за известна, което може да се определи по местонахождението на метеорологична станция (пункт), а във височина - чрез измерване. За провеждане на изследване приемаме, че вятърът не променя своите елементи за време $0, T^{poll} = 2\ hour$.

5. Определяне височината на границата на горния слой на смесване и формиране на условните аерозоли.

В представеният модел приемаме, че височината на горния слой на границата на смесване H_{max}^{layer} се променя в пространството и времето $0, T^{poll} = 2\ hour$. Следователно H_{max}^{layer} е резултат от функционална зависимост

$H_{max}^{layer} = f(K_{x,y}^{turbo}, D_{atm}^{layer}, \overline{w}_{speed}, K_{vert}^{diff}, K_{hor}^{diff}, T^{poll})$, която трябва да бъде диференцируема по координати в пространството и времето, и стойността й в точката в на мястото в метеорологичната станция с измерванията.

Нека в началото на всеки в момент от време t_n във време $0, T^{poll}$, където търсената величина удовлетворява уравнението:

$$H_{max}^{layer} = f(K_{x,y}^{turbo}, D_{atm}^{layer}, \overline{w}_{speed}, K_{vert}^{diff}, K_{hor}^{diff}, T^{poll})$$

Тогава последният слой H_{max}^{layer} може да запишем

$$H_{max}^{layer} = H_{topo} + \sum_{i=1}^{N_{measur}^{meteo}} \frac{k_{precis}^{long}}{1 + \Delta\varepsilon d_i(x,y)}, \quad (8)$$

при очакване площ $S_{ind}^{pollution} = L_x^{pollution} . W_y^{pollution}$, то

$$H_{max}^{layer} = \frac{1}{S_{ind}^{pollution}} \iint_{Z_{ind}^{pollution}} H_{max}^{layer}(x,y,t_n) dxdy, \quad (9)$$

където k_{precis}^{long} - коефициент на точността за измерване величините, зависещ от разстоянието до измерваната точка, N_{measur}^{meteo} - количество измерване от станцията за време $0, T^{poll} = 2\ hour$; $H_{max}^{layer}(x,y,t_n)$ - функция, значението на която в точка (x,y) в момент от време t е равна на значението H_{max}^{layer} в района; $d_i(x,y)$ - разстоянието от точка (x,y) до i-та метеостанция, $\Delta\varepsilon$ - градиент на измерването на величините от метеостанцията, регулиращ скоростта на изменение на търсената функция.

Посочените резултати позволяват по (9) да се определят данните $H_{\max}^{\text{layer}} = 3000\ m$, което представлява оптималното за територията на Република България, където средната височина на планинските масиви е около $H = 2000\ m$

6. Ентропия на информацията, описваща околната среда при разпространението на замърсители в атмосферата.

Средата за функциониране на тип информационна система локализирана в площта на замърсяването $S_{ind}^{pollution} = L_x^{pollution} . W_y^{pollution}$ по правило се дефинира с определена степен на неопределеност. Затова във времето за обработка на информацията, което съвпада с $0, T^{poll} = 2\ hour$ и цикли за предаване на информацията T_{cile}^{I} позволява стойността на информацията $-I_{raz}^{inf}$ условно да бъде възприета, като ентропия S_{entr}^{sys} в зоната за замърсяване $Z_{ind}^{pollution}$. Последното се определя

спрямо сумарното количеството информация $I^{sys}_{\sum_{I^{sys}_{pr}} V}$ налична в зоната и може де се запише във вида:

(10) $$\frac{dI^{sys}_{\sum_{I^{sys}_{pr}} V}}{T^{I}_{cile}} = -I^{inf}_{raz} = \frac{dS^{sys}_{entr}}{T^{I}_{cile}}$$

От тук

(11) $$\frac{dS^{sys}_{entr}}{T^{I}_{cile}} = -I^{\inf}_{raz}$$

Така цялата стойност на $-I^{inf}_{raz}$ в (11) се задава със средното време t^{func}_{sr} на информационната дифузия U^{Inf}_{diff} и предава екзоинформационният характер Δ_{ex} на информацията представена за обработка в един работен цикъл на системата T^{I}_{cile}. Следователно, S^{sys}_{entr} може да се изрази чрез:

(12) $$\Delta_{ex} S^{sys}_{entr} = \frac{I^{inf}_{raz}(0, T^{poll})}{T^{I}_{cile}}$$

Представяйки в (12) значение (10), определяно (11), за същността на I^{sys}_{stac} представяме „максималното количество" ентропия на средата за зоната за замърсяване $Z^{pollution}_{ind}$, което приема вида:

(13) $$\Delta_{ex} S^{sys}_{entI\_max} = -\frac{I^{inf}_{raz}(0, T^{poll}) N^{sys}_{inf} U^{pot}_{V}}{T^{I}_{cile}}$$

Максималната стойност на $\Delta_{ex} S^{sys}_{entI\_max}$ в (13) преди всичко е силно чувствителна от стойността на величините $I^{inf}_{raz}(0, T^{poll})$ и T^{I}_{cile}. Освен това се вижда, че ентропията S^{sys}_{entr} се явява екстензивна величина в стационарния режим на I^{sys}_{stac}. Екстензивността се характеризира с индивидуалната способност на системата да „губи" информация, извън площта на замърсяването $S^{pollution}_{ind} = L^{pollution}_{x}.W^{pollution}_{y}$ и може да се определи с коефициента на загубите ξ_{zag}. Той косвено определя S^{sys}_{entr} на стационарното състояние и конкретизира физическо съдържание на информационната система обслужваща информационната работа при ликвидиране на аварии от техногенен характер.

Заключение

Математическият модел може да се използува при замърсители в атмосферата в зависимост от наличието на вятър, турбулентност, влажни и сухи отлагания и трансформация на вещества за създаване на категория „условните аерозоли" -

$A_{cond}^{aerosols}$. За тази цел, е построен математически и физически модел на атмосферата. Предложен е метод за построяване на хоризонтален и вертикален профил, височината на горната граница на атмосферата, вятъра на базата на метеорологични измервания. Препоръчани са диференциални уравнения, описващи разпространението на замърсители, спрямо определени метеоданни във височина 200 – 3000 m и време от 2h. Описан е оригинален метод за работа на информационна система при определяне ентропията на информацията при ликвидиране на аварии от техногенен характер.

Литература

1. Берлянд М.Е. Прогноз и регулирование загрязнения атмосферы. — Л: Гидрометеорологическое издательство, 1985..

2. Кухарец В.П., Цванг Л.Р. Некоторые результаты натурного моделирования воздействия подстилающей поверхности на характеристики турбулентности в приземном слое атмосферы, Изв. РАН. Физика атмосферы и океана, 1994.

3. Плющев СИ., Самарская Е.А., Сузан Д.В., Тишкин В.Ф. Математическая модель распространения загрязнений в атмосфере., Препринт N 23, 1995.

4. Тверской И. Н., Курс метеорологии, Физика атмосферы, Гидрометеорологическое издательство, 1962.

5. Chrosciel St., Instructions for standard calculations of emission parameters for industrial sources in Polish. Technical University of Warsaw Publ., Warszawa, 1993.

6. Schnepf R., Lifecycle emissions include emissions from all stages of fuel production and use, as well as both direct and indirect changes in land use from farming crops to produce biofuels, 2007.

7. Tom Socha, Air Pollution Causes and Effects, http://healthandenergy.com/air_pollution, 2011

8. Causes of Air Pollution, http://www.buzzle.com/articles/causes-of-air-pollution.html, 2011.

9. Atmospheric Pollutants, http://www.tutorvista.com/content, 2011.

ИНФОРМАЦИЯ ПРИ ВЗРИВ НА ВОДОРОДНА СМЕС В ЗАЩИТНАТА ОБВИВКА В РЕАКТОРНАТА ЗАЛА АЕЦ

Костадин Н. Костадинов

НВУ"В. Левски", koce_knk@abv.bg, тел.+359 62 61 611

INFORMATION IN AN EXPLOSION HYDROGEN OF CLEARANCE ENVELOPE IN THE REACTOR HALL NPP

Kostadin N. Kostadinov

NVU"V. Levski", koce_knk@abv.bg, phone: +359 62 61 611

ABSTRACT: The question is a basic scenario of an accident in a nuclear reactor. Described are the consequences of possible damage and the formation of explosive hydrogen mixture. Attention is drawn to possible situations related to the problem of hydrogen released at high temperature fusion.

KEY WORDS: explosion, hydrogen, clearance envelope, reactor

Увод. Ядрените катастрофи в АЕЦ Три-Майл-Айленд, Чернобил и Фукушима през 2011 година са вследствие разхерметизирането на реакторния блок и взрив на водород вътре в защитната обвивка. Ето защо се обръща внимание на хипотетично малко вероятни ситуации, в това число свързани с проблема с водорода отделян при високата температура при ядреният синтез. При проектиране защитната обвивка на реакторите на почти всички АЕЦ много важно е определянето на максималната заплахата при проектни аварии. В държавните и задгранични центрове се извършват детайлни изследвания във връзка с този проблем и са предложени ефективни инженерни решения [3,4,5,9].

Спецификата на прогнозата за тежка авария се явява принципно невъзможна, както при провежданите крупномащабни експерименти, така и прекия пренос на резултатите от лабораторните експерименти в реални условия на действия при аварии. В тази ситуация нараства ролята на изчислителните експерименти и се повишават изискванията към качеството на численото моделиране на физическите явления. Особеността при изследване на процесите се заключава в характерните съществени различия при пространствено-временни газодинамични течения и химични реакции, а също така в значителното влияние на геометричните фактори на характеристиките на газодинамическите смущения и определените за тях условия в прехода на горене в детонация. Това предизвиква значителни трудности при математическото моделиране, като:

A. се разглеждат съществено многомерните задачи;

B. поради различията в мащабите водещи процеси системата уравнения се явяват доста тежки;

C. голямо количество физико-химични фактори, влияещи на възбуждане и

разпространение на детонацията на взривните смеси.

Отчитайки изчислителните особености на проблема, за числения анализ на процесите на детонация и взрив, е разработен комплекс програми, позволяващи да се провеждат разчети с приложение на широк набор числени алгоритми. Това дава възможност да се повишат надеждните резултати от разчетите и да се избере за решение конкретния най-адекватен алгоритъм.

1. Постановка на задачата и избор на базов сценарий за ядрена авария

Най-често инцидентите в ядрените реактори на централите $Acc^{H}_{Nuclear}$ по света обикновено могат да бъдат свързани с нарушение на:

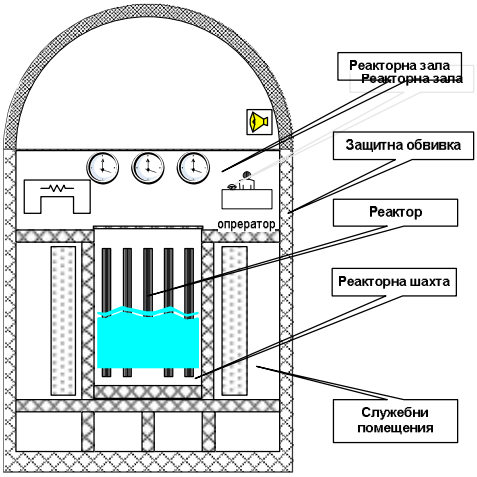
a) системата на термичното отвеждане на топлоносителя от активната зона на реактора към контура на парогенератора;

b) механически повреди на тръбопроводите на топлоносителя, което като правило води до загряване и последващо разрушаване на реактора $R_{Nuclear}$.

Последствията от реализирането на посочените повреди (a) и (b) следва приблизително следният сценарий за развитие на ситуацията: при повишаване температурата във вътрешният обем $T_{Nuclear}$ поради невъзможност да се контролира ядрената реакция в нормите $1100 \le T_{Nuclear} \le 1500\ K$ вътрешната облицовка започва да се окислява от прегретите водни пари, което е съпроводено с разлагане на водата на водород H и кислород 0_2, и значително отделяне на топлина. Понататъшното развитие на ситуацията се предизвиква от разрушение в активната зона на реактора, навлизане на част от горивото в долната част на корпуса и попадане образуваща се течна маса в бетонната шахта на реактора. Топлината и химическото взаимодействие на течната маса с бетона се съпровожда с интензивно отделяне на газове, в това число H и оксиди на въглерода, явяващи се, както водорода горящи компоненти, образуващи газови смеси. Освен това и в стадия разрушение но охлаждащите контури, и при попадане течната маса в шахтата на реактора протича интензивна генерация на водна пара. Всичко това съществено изменя състава на атмосферата под защитната обвивка. Попадането на водород във въздушната атмосфера води до образуване взривоопасна смес, което създава условия за горене, взрив, разрушаване на защитната обвивка и освобождаване на радиоактивност радионуклиди извън реакторното помещение.

Нека приемем за моделиране на процесите в реактори при инцидент $Acc^{H}_{Nuclear}$ - реактор ВВЕР-1000. Същият притежава основните параметри на защитна бетонна обвивка на реакторната зала: височина на сферичния купол $H^{cup}_{Nucl} = 51\ m$, височина на шахтата на реактора - $H^{shaft}_{Nucl} = 22\ m$, радиус на долната цилиндрична част на купола - $R^{cylinder}_{Nucl} = 23\ m$, нейната височина - $H^{cylindert}_{Nucl} = 10\ m$. Основна архитектурно-функционална схема на реактор ВВЕР-1000 по отделни елементи обособени от бетонна обвивка е представена на (фиг. 1).

Обособените елементи в посоченият реактор фиг.1 се явяват класически и за останалите типове реактори от този тип, при което по метода на подобието можем да причислим всички реактори по света.



Фиг.1. Архитектурно-функционални елементи на ядрен реактор ВВЕР-1000

3. Динамиката на процесите формиращи околната среда на ядрен реактор при инцидент.

Нека разгледаме инцидент $Acc^{H}_{Nuclear}$ с реактор, при който околната среда се разглежда като динамична и притежаваща следните характеристики: едноскоростна, еднотемпературна, многокомпонентна газова смес. Уравненията от газовата динамика с отчитане вискозитет, топлопроводимост и отделяне на енергия за сметка на химични реакции в интегрална форма, могат да бъдат използвани за описване на процесите на детонацията представени във вид:

(1) $$\frac{d}{dt}\int\limits_{V^{gas}_{volume}} \rho^{\%}_{gas}\, dV^{\,gas}_{volume} + \int\limits_{S} \rho^{\%}_{gas}\left(u^{det}_{speed}\, n^{norm}_{surf}\right)dS = 0$$

(2)

$$\frac{d}{dt}\int\limits_{V^{gas}_{volume}} \rho^{\%}_{gas}\, u^{det}_{speed}\, dV + \int\limits_{S} \rho^{\%}_{gas}\, u_i \left(u^{det}_{speed}\, n^{norm}_{surf}\right)dS = \int\limits_{S} \prod (x,y,z) n^{norm}_{surf}\, dS$$

Тук $\rho^{\%}_{gas}$ - плътност на газовата смес – водород, водни пари, въздух, ρ_H - парциална плътност на k-тия газов компонент, спрямо общият обем на газовата смес; V^{gas}_{volume} - обем на водородната смес в купола на реактора; $S^{gas}_{contact}$ - площ на контакта на водородната смес с вътрешната част на купола на реактора; E^{mix}_{gas} – вътрешна енергия на газовата смес, в зависимост от нейният състав T^{mix}_{comp} - температура, приета еднаква за всички компоненти формиращи газовата смес, $\prod(x,y,z)$ - тензор на напрежение върху бетонният купол, поради действието на

ударната вълна с пространствени координати (x, y, z); p - термодинамично налягане, u_{speed}^{det} - масова скорост на детонацията, N^{mix} - пълния брой компоненти в газовата смес, n_{surf}^{norm} - вектор перпендикулярно налягане на повърхността на купола; $i, j(i, j = 1,2,3)$- индекси, обозначаващи пространствените координати (x, y, z) на водородната смес спрямо началото на детонацията.

Уравненията от газовата динамика (1), (2) са изведени в правоъгълни координати с цел моделиране на разпространението на взривни и детонационни вълни в обема в купола, при което (1), (2) могат да се решат в двумерно и тримерно пространство.

За решаване на задачите по определяне параметрите на детонацията в тримерно пространство е избран метод, където налягането на ударната вълна изразява структурата на вълновите полета и съответства на значително по високи градиенти термодинамични величини на фронта на ударната вълна. За целта за интегралните характеристики на процеса, в това число на импулса на налягане, на всяка стъпка по време е използван методът на приближена факторизация, на параметрите на ударната вълна, въздействащи на стените на обвивката.

Пресмятането на многомерните задачи се извършва с прилагането на физични модели на реакциите на горене в затворен обем водещ до детонация. Уравнението на горене, скоростта на горенето, детонацията на горящата компонента W_{burn}^{gas} - водородната смес, може да се определи от уравнението

$$\frac{dW_{burn}^{gas}}{dt} = -W_{burn}^{gas} Z_{det\,on} e^{-\frac{E_{activ}^{deton}}{E_{Internal}^{gas}}} \tag{3}$$

Където решението е

$$W_{burn}^{gas} = e^{-Z_{det\,on} e^{\frac{E_{activ}^{deton}}{E_{Internal}^{gas}}} tC} \tag{4}$$

където E_{activ}^{deton} - енергия за активиране, горенето - детонационният процес; $E_{Internal}^{gas}$ - вътрешна енергия, калорийност на водородната смес; $Z_{det\,on}$ - експоненциален коефициент на скоростта на детонацията в зависимост от количеството на водорода във водородната смес. Степента на изгаряне на водородната смес се изменя от 1- наличното количество до 0 – пълното му изгаряне. Времето за горене T_{burn}^{gas} и това за детонацията спрямо T_{deton}^{gas} потенциалната вътрешна енергия на водородната смес е представено фиг. 2.

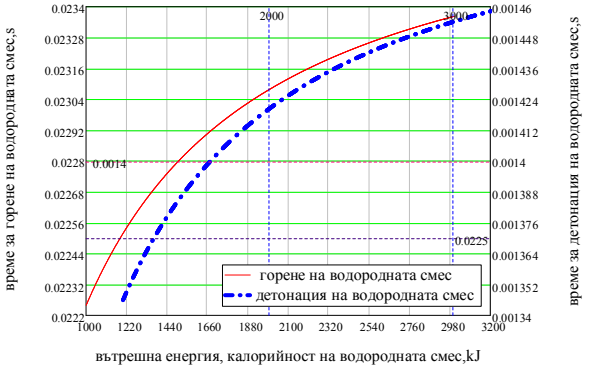
Времето за горене фиг. 2 на водородната смес в реактора е в рамките $0.0222 \le T_{burn}^{gas} \le 0.234\ s$ при вътрешна енергия $1000 \le E_{Internal}^{gas} \le 3000kJ$, а времето за детонация $0.00134 \le T_{burn}^{gas} \le 0.00146\ s$ съответно, намаляване на времето

почти 90- 95%.

При горенето и детонацията съществува време на забавяне. Тогава в уравнение (4) трябва да се допълни и отчете условието:

(5) $$t - t_0 > \tau$$

където τ - ефективно време за забавяне възпламеняването, t_0 - момент от време, при което смущението на термодинамичните величини достига дадения елемент на горящата смес, контактуващ с вътрешната стена. В практиката се използва следния метод за задаване на параметъра τ .



Фиг. 2. Време за горене и детонация спрямо потенциалната вътрешна енергия на водородната смес

(6) $$\tau(t) = \tau_0 \, exp \frac{p_h}{p(t)},$$

където τ_0 - емпирическа константа, p_h - налягане в точката на Чемпен-Жуге, $p(t)$ - налягане в газовата смес, намираща се в затвореният обем на реактора.

Нека да разгледаме няколко схеми за химическо окисление на водород - в модел на разклонена схема на химически трансформации от 3 уравнения, независимо от конкретния вид, която дава качествено подобна картината на хидродинамичните процеси, а именно:

(7) $$H_2 + O_2 = 2OH, \qquad 2OH + M = H_2O_2 + M,$$
$$O + H_2 = OH + H, \qquad H + O_2 = OH + O,$$
$$H + HO_2 = 2OH, \qquad HO_2 + H_2O = H_2O_2 + OH$$

Ефектът на взрива поради водните пари в (7) се характеризира с значително увеличение $R_{Nuclear}$, а за водородно-въздушни смеси, азота в схема на химическа реакция горене се отчита като неутрална съставна.

4. Модел на взрив на водородна смес в ядрен реактор

Разрушението в активната зона на ядрения реактор $R_{Nuclear}$ при авария предс-

тавлява физико-механични процеси, съпровождащи се от отделяне на голямо количество водород и въглероден окис, а така също нагряване на околната среда за сметка на отделящата се енергия. Най-голяма опасност представлява натрупването на водород в пространството под предпазната (задържаща) полусфера купола (Фиг.2.). Водорода в съчетание с кислорода във въздуха формира водородната смес в реакторната зала. Анализа от ядрените катастрофи показва, че количеството водород, отделящо се за сметка взаимодействието на цирконievата обвивка с водата и течната маса от бетонната шахта на реактора, може да надхвърли 2.5 тона. Процеса отделяне на водород $R_{Nuclear}$ е достатъчно бавен, и критичното количеството в залата се натрупва в продължение до 20 - 40 часа след аварията. Това време е достатъчно за вземане на необходимите мерки за понижаване на температурата, налягането и концентрацията на водорода под защитната обвивка, например, най-често с включването на резервна охладителната система. Значителна опасност в за натрупването на водорода е след 1 – 2 часа от началото на аварията. В този случай масата на отделения водород не превишава 300-500 килограма. При това детонационния режим на горене на водородосъдържащи смеси се реализира само в отделни области под защитната обвивка при незначително превишаване на налягането от $1.3 \le N^{\mathrm{H}}_{\mathrm{pressure}} \le 3.3\ atm$. Във всички сценарии налягането на ударна вълна, въздействаща на обвивката, е в пределите от $55 \le N^{deton}_{pressure} \le 85\ atm$, а съответстващия импулс на налягането не надвишава 0.4 – 0.6 atm.

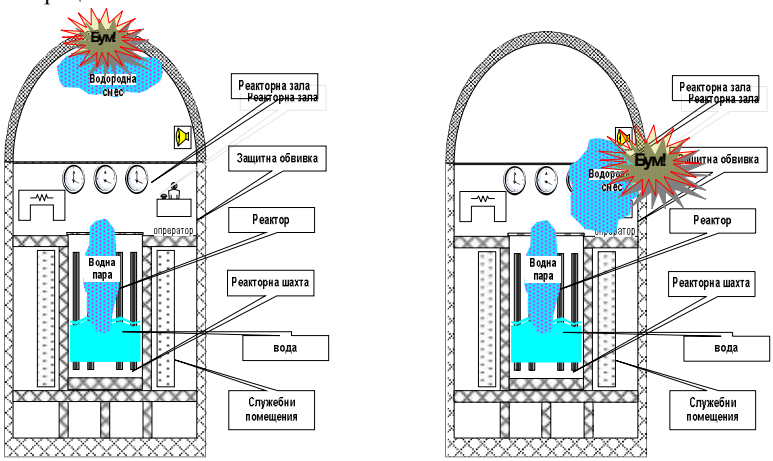
Взрива на водородната смес в пределите на реакторната шахта вътре в защитната обвивка зависи от много фактори, водещи до инцидентно разрушаване на активната зона на реактора, охладителни системи и други компоненти. Разпределението на концентрация на водорода и водните пари, до голяма степен се определя от ефектите на хаотичния характер и не може да се предвиди предварително с определена степен сигурност. Вариантите за формиране на взрива са демонстрирани на фиг. 3.

Възпламеняване и детонация на взривни смеси под защитната обвивка е представено на база на триизмерни модели фиг. 3., с описание на реакция на водородно-въздушната смес. Общият вид разчетни области е показан на фиг. 3, където са представени два различни базови сценария на възникване на взрив под защитната обвивка на реактора. Детонацията генерира устойчиви вълни на детонация във вариант **„A”** водородно-въздушната смес запълва целия обем, което може да доведе до възбуждане интензивни високочестотни колебания на защитната обвивка. А във вариант „**B”** - само страничната част на обема под защитната обвивка, където разпределението на натоварването е странично. При това се приема, че долната част на обема се запълва с въздух.

Направеният анализ на влиянието на концентрацията на водородно-паровъздушни смеси на развитието на детонацията под защитният купол показва, че тя се прекратява при падане на концентрацията под 15% от обема на вътрешната част на реактора.

Влиянието на турбулентността на разпространението на взривната вълна под защитната обвивка се изразява в това, че в начална нетурбулентна среда предизвикана от екзотермична реакция на предната част на горене турбулентност при нуле-

во или малко време не оказва почти никакъв ефект на динамиката на детонационната вълна. Обаче за времето на забавяне $\tau_0 = 30$ мкс, съответстващи на най-близкото значение до точното описание на реакцията във водородно-въздушна смес, ролята на турбулентните фактори започва качествено да влияе на развитието на взривния процес.



Фиг. 3. Базов сценарий на възникване на взрив под защитният купол на реактора

7. Точност на информацията при определяне състоянието на атомният реактор след авария

При получаване на авария в реактора се налага получаване на постоянен зададен ансамбъл от информационни величини за състоянието на вътрешната част на херметичният купол и състоянието на водородната смес. От концептуална гледна точка ние трябва да получаваме възможно максимално количество информация за промените, оценявани на основание относителната честота на подаваните величини от датчиците с определена вероятност на точността, до началото на аварията намиращи $I_{R_{Nuclear}}^{primary}$ и след нейното получаване $I_{R_{Nuclear}}^{breakdow}$ се във вътрешната част на реактора , т.е. величини

$$I_{R_{Nuclear}}^{primary} = -\sum_{primary} p_j \ln p_j \qquad (8)$$

$$I_{R_{Nuclear}}^{breakdow} = -\sum_{breakdow} p'_k \ln p'_k \qquad (9)$$

където p_j и p'_k вероятност получаване на информация от вътрешната част на реактора преди и след аварията.

Известно е, че при изправна информационна система $\sum_j p_j = 1$, но след началото на аварията, винаги вероятността на точността на информацията за състояни-

ето на реактора е $\sum_k p'_k < 1$, т.е имаме недостатъчност на информация.

За компенсиране на негативните последствия от недостига на информация се налага да се търсят методи за увеличаване на нейната точност. Това се постига чрез въвеждане предварително моделирана функция $f^{break\_model.}_{R_{Nuclear}}$ на информацията при определена аварийна ситуация в реактора $I^{break\_model}_{R_{Nuclear}}$; Тогава $I^{break\_model}_{R_{Nuclear}}$ може да се интерпретира като средно по $f^{break\_model.}_{R_{Nuclear}}$, а именно

(10) $$I^{break\_model}_{R_{Nuclear}} = \sum p_j f^{break\_model.}_{R_{Nuclear}}$$

Следователно моделната функция $f^{break\_model.}_{R_{Nuclear}}$ може да се определи по

(11) $$f^{break\_model.}_{R_{Nuclear}} = -K^{break\_model}_{mod}\, ln\, p_j, \quad \text{при} \quad p_j \neq 0 \quad ,$$

където $K^{break\_model}_{mod}$ - коефициент на адекватност на модела с действителната ситуация в реактора , (0.6 - 0.99).

Точността на информационно съдържание на (11) предполага, че множеството измерения на състоянието на водородната смес в ректора ни води към относителна честота на измерването, водещо до формиране на вероятност p'_j. Това предполага необходимостта от измерване на съответстващото изменение на информацията $I\Delta_j$ между началното състояние и текущото състояние в ядреният реактор по съотношението:

(12) $$I\Delta_j = K^{break\_model}_{mod}\, ln\, p'_j - K^{break\_model}_{mod}\, ln\, p_j$$

Следователно по (12) можем да получим средното изменение на информацията, което е условието за получаване на възможност за нейното увеличение и вземане на адекватни мерки за адекватна реакция по локализиране на аварията. Последното се интерпретира, като получаването на максимума информация, където се прави смесена оценка за разпределение вероятността на състоянието на системите за контрол на информация присъщи за неравностойните системи, такива каквито са ядрените реактори.

Заключение. Разгледан е базов сценарий на авария в ядрен реактор като са описани последствията от реализирането на възможни повреди и образуване на взривоопасна водородна смес. Описана е динамиката на процесите, формиращи околната среда на ядрен реактор при инцидент чрез уравненията от газовата динамика с отчитане на вискозитет, топлопроводимост и отделяне на енергия за сметка на химични реакции в интегрална форма. Определено е времето за горене и детонация спрямо потенциалната вътрешна енергия на водородната смес чрез разработване на модел на взрив на водородна смес в ядрен реактор. Допълнително е изведена зависимостта от точността на информацията при определяне състоянието на атомният реактор след реализиране на авария.

Литература

1. Белоцерковский О.М. Давыдов ЮМ. Метод крупных частиц в газовой динамике. -М.: Наука, 1982.

2. Ганьжа Д.Х., Музафаров И.Ф. Утюжников СВ. Применение подвижных адаптивных сеток в алгоритмах с компактными аппроксимациями, Ж.выч. мат. и матем. физики, 1995.

3. Годунов С.К., Забродин А.В. Иванов М.Я. и др. Численное решение многомерных задач газовой динамики. -М.: Наука, 1976.

4. ИвановМ.Ф.,ПаршиковА.Н. Моделирование микромеханики композиционнго материала при импульсном нагружении, Препринт ФИ РАН, №6, 1992.

5. Самарский А.А., Попов Ю.П. Разностные методы решения задач газовой динамики. -М: Наука, 1992.

6. Dorofeev S.B., Bezmelnitsin A.V. et al Experimental study on combustion behavior of hydrogen air mixtures with turbulent jet ignition at large scale, RRC "Kurchatov Institute" Report, RRCKI-80-05, NUREG,CR-6072, 1993.

7. Baker W.E., Cox P.A., Westine P.S. Kulesz J J., Stehlow R.A. Explosion Hazards and Evaluation. Amsterdam - Oxford - New York: Elsevier Scientific Publishing Company, 1983.

8. Breitung W., Redlinger R. Containment pressureloads from hydrogen combustion in unmitigated severe accidents, Nuclear Technology, 1995**.**

9.Eibl J., Schlutter F.H., at al. Containments for futher PWR-reactors, Proc. SMIRT 11 Post Conference, Kyoto, Japan, August 26-27, 1991.

10. Harlow F.H., Narayama P.I. Transport of Turbulence Energy Decay Rate, LA-3845 Los Alamos Sci. Lab., University of California, 1968.

11. Nettleton M.A. Gaseous Detonations: their nature, effects and control. London, New York: Chapman and Hall, 1987.

12. Yamano N., Maruyama Y., Moriayma K., Sugimoto J. Technical note on ex-vessel core melt debris coolability and steam explosions. - Committee on the safety of nuclear installations OECD NEA, December 1996.

13. Yee H.C., Warming R.F., Harten A. Implicit total variation diminishing (TVD) schemes for steady-state calculation, J. of Comput. Phys., 1985.

ОСОБЕНОСТИ В ПОВЕДЕНИЕТО НА РЪКОВОДИТЕЛЯ В ЕКСТРЕМАЛНИ УСЛОВИЯ

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски"
Катедра „Психология"

SPECIFICITIES IN LEADER BEHAVIOR UNDER EXTREME CONDITIONS

Krasimir M. Markov

ABSTRACT: *This paper deals with some specificities in leader behavior under extreme conditions defined by the specific features of his or her individuality.*
KEY WORDS: *individuality, leader, behavior, extreme conditions*

Прието е да се смята, че психологията на управлението в екстремални условия изучава процеса на оптимизация на живота и дейността на специалистите, функционалните групи и тяхното състояние и психически изменения в резултат на управленско взаимодействие на ръководителите с подчинените в опасни за живота и здравето ситуации, свързани с въздействието на силни и извънредни стресови фактори /2, с. 6/. Това налага да бъдат разгледани няколко аспекта на психологията на управлението в екстремални условия:

Личност на ръководителя в екстремални условия. Столяренко А. М. (2003) отделя в структурата на личността три важни подструктури или сфери: сфера на насочеността, операционна сфера и модулационна сфера. /цит. по 2, с. 34/

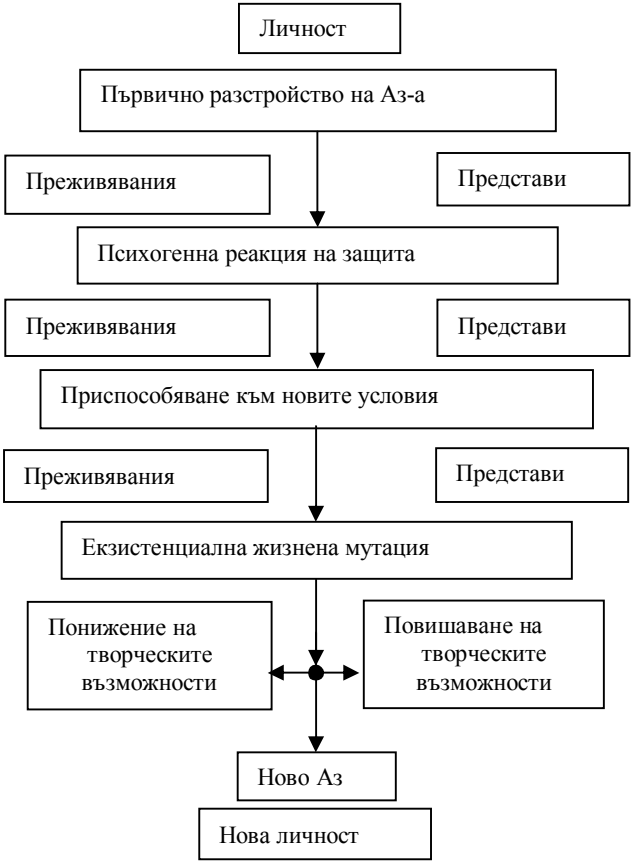
Сферата на насочеността, наричана още ценностно-мотивационна сфера определя личностовата активност и отношение, дава отговор на това към какво се стреми личността и в каква степен да се привлекат другите подструктури за успешна реализация на психичната дейност на личността. Това означава че тя включва идеалите и убежденията, плановете, потребностите, мотивите, целите, интересите, склонностите и нагласите на личността. От тях важна роля за успеха в управленската дейност играе развиването на такава интегрална личностова характеристика като индивидуалната управленска концепция.

Операционната сфера включва елементи представляващи начини и опит, които има личността и които тя използва за достигане на поставените цели. Естествено тук ще влязат нейния образователен и квалификационно професионален опит, интелектуалните и творческите, емоционално-волевите, комуникативните и организаторските способности. Тяхното развитие, балансът между тях представлява потенциала на професионална компетентност на личността на ръководителя.

Модулационната сфера отразява наличието в личността на специфичните свойства на нервната система и психофизиологичните функции, които оказват динамично, но несъдържателно влияние на психичните процеси, състояния и свойства на личността. Дотолкова, доколкото тези компоненти предопределят психофизиологичните ресурси и се проявяват в частност в работоспособността и

издръжливостта, те трябва да бъдат разглеждани като психодинамичен потенциал на личността на ръководителя.

За да може да се осъществява управление и оказва помощ е необходимо да се познава динамиката на преминаването през криза.



Фигура 1. Динамика на измененията в самосъзнанието на личността, възникващи в екстремални ситуации

На фигура 1 е изобразена динамиката на измененията в самосъзнанието на личността, възникващи в кризисни и критически ситуации. Тази схема е разработена в лабораторията за социалнопсихологическа рехабилитация на личността към Института за развитие на личността (Москва, Русия) от колектив под ръководството на А. Ф. Шадура при участието на Н. Г. Осухова през 1999 г. Схемата се цитира по /1., с. 128/.

В екстремални условия от ръководителите се изискват съвършено различни качества, отколкото в нормална обстановка, предпочитанията се насочват към такива качества като лидерство, ефективност, професионална подготовка и владеене на

обстановката. Изследванията в Русия показват, че на длъжност ръководител (командир) на организации работещи в екстремални ситуации от типа на Гражданска защита, БА, МВР, Спешна помощ и др., не трябва да се назначават специалисти с недостатъчно развити лидерски качества, независимо от идеята, че те могат да бъдат развити допълнително в процеса на професионалната, психологическата подготовка и на самата дейност, тъй като в този случай подготовката не само на ръководителя (командира), а и на цялата структура значително се усложнява [2, с. 36].

В екстремални условия индивидуалната управленска концепция на ръководителя (командира) се отличава значително от тази в нормални условия. Като елементи на индивидуалната управленска концепция на ръководителя в екстремални условия може да се определят следните:

- смислообразуване и целеполагане;
- замисълът за решаването на произтичащите и поставените задачи;
- предвиждания и прогнози за решаване на предполагаеми проблеми;
- активизация на управленските средства и функционалните единици, реализиращи тези средства;
- обработването и използването на оперативна информация за състоянието на групата, на всеки подчинен, за дейността, обстановката и техните изменения.

Професионалната компетентност в екстремални условия е следващия значим фактор за успешна дейност на ръководителя. Под професионална компетентност се разбира системата от вътрешни ресурси, необходими за ефективни действия в определени ситуации. При това управленската компетентност на ръководителя се представя като система от неговите вътрешни ресурси, необходими за реализация на ефективното ръководство на подчинените и групата, познаване на детайлите на изпълняваната задача, възможните начини и средства за постигане на набелязаните цели /2, с. 39/. Основа на професионалната компетентност на ръководителя е неговата адекватна организация в поставените цели и задачи, разглеждането им по приоритетност и съподчиненост. В екстремални условия ръководителят е длъжен бързо да реагира на всяко, даже незначително изменение в обстановката или в поведението на подчинените си. Ръководителят трябва да бъде готов за прогноза за развитието на събитията и перспективите за действие на подчинената му група, да има готовност за самостоятелно поставяне на цели пред групата и конкретизацията им за всеки човек. Затова в тази т.нар. съдържателна съставяща на професионалната компетентност, трябва да се включат не само поставените отвън цели, но и самостоятелното творческо формулиране, конкретизация и обезпечаване на тези цели, които самия той поставя. Това означава, че в процеса на своята дейност в екстремални условия, ръководителят едновременно осъществява и събиране, и анализ на оперативна информация необходима за вземане на управленско решение, изяснява проблемните ситуации, установява приоритети, определя необходимите ресурси за тяхното решаване, участва в реализацията на взетото решение. Но дори и при пълна яснота на поставените цели, приоритети, задачи и ресурси не може да се осъществи успешен изход и решаване на проблема без т.нар. ресурсна съставяща на компетентността. Тя включва информация за трудоемкостта, риска, сложността на решаваните задачи при отчитане на материално-техническите, времевите и човешките ресурси, които са необходими за решаване на задачата.

Може да се каже, че стабилността, ефективността и успешността в дейността на групата в екстремални условия изцяло зависи от нивото на професионална компе-

тентност на ръководителя, от неговия авторитет, от неговото право да поставя задачи, свързани с риск за живота, и от това как подчинените му го приемат като фактор можещ да поставя такива задачи, т.е. от взаимното доверие на хората един в друг [2, с. 41].

Това не може да се постигне ако ръководителят не се явява лидер на своите подчинени, т.е. ако те не се превръщат в негови последователи. Ефективността на лидерското положение на ръководителя зависи от развитието и баланса на два интегрални фактора:

1. структуризацията на дейността (т.е. от това как той определя своята роля и ролята на другите в постигането на целта);

2. от неговата загриженост към хората (Р. Стогдил, А. Кунс 1951) В екстремални условия нивото на доверие на лидера към себе си (вяра в собствените сили), към другите и обратно, доверието на групата и нейните членове към лидера би трябвало да се явява максимално високо, тъй като става дума за живота на хората. Това има пряко отношение към лидерския стил на управление, ако в нормални условия може да преобладава демократичният стил на ръководство, то в екстремални условия практиката показва, че подчинените имат по-голямо доверие на ръководител проявяващ авторитарен стил. Независимо от това би трябвало да се обърне внимание на проблема за ситуационното лидерство, тъй като и екстремалните ситуации не си приличат една с друга, рецепти за поведение и ръководство трудно биха се дали, следователно би трябвало лидерът да се ориентира от самата ситуация за това какъв стил на ръководство да прояви в нея. Затова обаче са необходими лидерски умения и натрупан опит.

В последно време, в литературата посветена на управление на персонала в екстремални ситуации се въвежда понятието "професионален екстремално-психологичен потенциал", който се отнася както до ръководителите, така и до функционалните групи и до техните членове. Той представлява не толкова набор от личностови и професионално значими качества, способности и опит, но което е по-важно, се явява генератор на професионалното и личностовото самоусъвършенстване и саморазвитие. В структурата на професионално-психологическия потенциал могат да се набележат две основни подструктури:

1. психотехнологична – която обезпечава рационалното изпълняване на задълженията, служи за показател на това до какво ниво може да се издигне като специалист дадения човек ако бъдат актуализирани определени психологически променливи при изпълнение на професионалните задачи.

2. личностова, която определя системата на смисловите съставящи на дейността и на живота като цяло, определя като каква личност може да се развие дадения човек и как това може да окаже влияние на неговата професионална дейност и на живота му.

В понятието екстремално-психологически потенциал следва да отчитаме не само личностовите характеристики, но и цялата съвкупност на външни фактори влияещи върху личността, тъй като в екстремални условия не само се актуализира екстремално-психологическия потенциал на човека, но и неговото развитие като специфичен психичен феномен. Следователно, под професионален екстремално-психологичен потенциал ще разбираме интегративната съвкупност от психични компоненти, имащи пасивно и активно съдържание, различни нива и пропорции, които се формират и развиват под влиянието на вътрешно личностовите условия и

външните условия, и следва да включва:

- индивидуално-управленска концепция;
- развити морално-психични качества;
- управленска подготовка;
- интелектуални способности;
- емоционално-волеви качества;
- комуникативни качества;
- развити организаторски способности и навици;
- високо ниво на доверие към себе си и функционалната група;
- способност да осъществява подпомагащи и обучаващи действия за усъвършенстване дейността на подчинените;
- развита подсъзнателна сфера на психиката и навици за управление на тази сфера;

Главно условие за повишаване на потенциала на ръководителя в екстремални условия е да се развие у него автопсихологична компетентност, която би следвало да се формира в процеса на професионалната екстремално-психологическа подготовка, самоподготовката, психоконсултирането и професионалната дейност.

Литература:

1. Осухова, Н., Психологическая помощь в трудных и экстремальных ситуациях. М., 2007
2. Смирнов, В. Н. Психология управление персоналом в экстремальных условиях. М. 2007

НЯКОИ ОСОБЕНОСТИ НА ОПИТА НА АРМИИТЕ НА ФРГЕРМАНИЯ И РАВСТРИЯ ПРИ ЛИКВИДИРАНЕ НА ПОСЛЕДСТВИЯТА ОТ ЕКСТРЕМАЛНИ СИТУАЦИИ

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Катедра „Психология”

SOME SPECIFICITIES IN THE EXPERIENCE OF THE ARMED FORCES OF THE FEDERAL REPUBLIC OF GERMANY AND THE REPUBLIC OF AUSTRIA

Krasimir M. Markov

ABSTRACT: *This paper deals with some specificities in Armed Forces practice in the Federal Republic of Germany and the Republic of Austria in* **liquidation of extreme situation consequences.**

KEY WORDS: *Armed Forces, civil management, extreme situations*

Правната основа за участието на Бундесвера в ограничаването и ликвидирането на последствията от природни бедствия, катастрофи и аварии съставлява чл. 35 от

конституцията на Федералната република:

(1) Всички служби на федерацията и провинциите си оказват взаимно правна и административна помощ.

(2) При природни бедствия или особено тежки катастрофи и аварии една провинция може да поиска съдействие от полицейски сили на други провинции, сили и съоръжения от други служби, както и от Федералните гранични войски и армията.

(3) В случай че от природни бедствия или особено тежки катастрофи и аварии е застрашена територията на повече от една провинция, федералното правителство може да инструктира правителствата на другите провинции (в случай, че е необходимо за ефективното овладяване на ситуацията) да предоставят полицейски сили, както и да се включат части от гранични войски или въоръжените сили на страната за да окажат подкрепа на полицията.

Мерките на федералното правителство по ал.1 могат да бъдат стопирани по всяко време по искане на Бундесрата (Федералния съвет – втората камара на парламента съставена от представители на провинциите), а в останалите случаи се прекратяват веднага след отстраняване на опасността.

Според военния министър на ФРГермания рисковете и опасностите, за които трябва да са подготвени въоръжените сили включват: природни бедствия, пожари, наводнения, а така също и нападения, катастрофи, защита на рискови инфраструктури, като напр. химически предприятия, ядрени електроцентрали, но също и големи летища, гари и др. големи съоръжения.

От една страна последствията от промяната на климата, а от друга асиметричните заплахи от терористи представляват сериозно предизвикателство за отговорните органи. Трите "наводнения на века" през последното десетилетие на XX век (например наводнението на Одер) показаха колко е важно синхронизираното сътрудничество между цивилните и военните сили. Без подкрепата на Бундесвера не би било възможно да бъде овладяна ситуацията.

В центъра на новото сътрудничество между военните и цивилните институции се намират резервистите от Бундесвера. 450 щата в новите окръжни и районни командвания са заети от резервисти.

Работната група „Подкрепа на Бундесвера при защитата от бедствия в провинциите" към Федералното министерство на вътрешните работи установи в своя доклад от 20.01.2005 г., че Бундесверът може да предложи помощ в следните области: специализирани действия при ЯХБЗ, масови случаи на ранени, в частност въздушен транспорт, възможност за осъществяване на комуникация, за инженерна и др. поддръжка.

Докато политическите дебати се водят основно на тема въздушна и морска сигурност, едновременно с това се посочват и все нови и нови опции за използване на военния потенциал: осигуряване на комуникационна техника, логистична поддръжка, осигуряване на транспортен капацитет (в частност хеликоптери), охрана на цивилни обекти (атомни електроцентрали, промишлени съоръжения и др.), осъществяване на екологични операции, борба с терористични групи и бойни операции във вътрешността на страната.

Операции на Бундесвера в страната.

Първата подобна операция е проведена през нощта на 16. срещу 17. февруари 1962г. при наводнението в Хамбург, където е имало общо 337 загинали. След като

е бил информиран на сутринта вътрешният министър на провинция Хамбург Хелмут Шмид установил, че за цивилната служба за защита от бедствия и аварии е свръх сили да се справи със ситуацията и нарежда – в разрез със закона- включването на 8 000 военнослужещи от Бундесвера. Въпреки че войниците дават 9 жертви, успяват да се спасят 1 117 жертви на наводнението. По-късно Шмид обяснява: Тогава ние съзнателно и преднамерено нарушихме конституцията на страната, конституцията на Хамбург, както и други закони. Едва по-късно е променен член 35 на конституцията, който позволява включването на армията в спасителни операции при бедствия и катастрофи.

През последното десетилетие на XX век военнослужещите са участвали в 68 спасителни операции при природни бедствия, аварии и катастрофи (на влакове, самолети и др.). Най-мащабна е операцията при наводнението на река Одер през юли 1997 г., в която участват 30 000 войници, 400 транспортни машини, 50 хеликоптера. С увеличаването броя и силата на природните бедствия в резултат от разрушаването на околната среда този вид операции ще се увеличават. Разбира се не трябва да се надценява приноса на Бундесвера в защитата от бедствия, катастрофи и аварии на фона на 1,1 милиона пожарникари, 600 000 участници доброволни организации (Червения кръст и др.) и 75 000 членове на техническата спасителна служба.

Шлезвиг-Холщайн, Нова година 1978/1979: Обилни снеговалежи. 3000 войници от Бундесвера са в действие. Те освобождават шофьорите от заседналите превозни средства, разчистват пътищата с тежки машини, доставят по въздуха провизии в изолираните населени места, транспортират с хеликоптери родилки до болницата.

Късното лято на 2002 г. 73 000 души от силите за борба с бедствия, катастрофи и аварии се борят с наводненията по поречието на Елба и Дунав. Сред тях са 44 000 военнослужещи – мъже и жени. Те подсилват застрашени от скъсване диги с чували с пясък, евакуират хора, доставят провизии на населението. Това е най-мащабната операция в историята на Бундесвера.

От създаването си Бундесверът е оказал помощ при повече от 160 бедствия, катастрофи и аварии в страната и в чужбина. Армията разполага с необходимия личен състав: 60% от участвалите през 2002 г. войници на сухопътни войски са наборни войници. Той разполага с необходимата техника: По време на наводнението ежедневно във въздуха са до 50 хеликоптера на Бундесвера. По време на 2100 –те летателни часа екипажите спасяват 778 души от смъртна опасност. На земята Бундесверът използва ежедневно 250 товарни камиона, 35 бронирани машини на инженерни войски, 50 понтонни лодки, 4 мостопоставача, 16 транспортни бронирани машини и около 25 автобуса.

Бундесверът разполага с необходимата организация: Командването в Кьолн ръководи всички операции в страната. Всяка провинция разполага със свое териториално командване за по ефективно сътрудничество между цивилните и военни сили. По принцип защитата от бедствия, катастрофи и аварии е в компетентността на провинциите.

Правна основа за участието на Бундесхера в ограничаването и ликвидирането на последствията от природни бедствия, катастрофи е Закона за отбраната:

В република Австрия, съгласно § 2 от Закона за отбраната Бундесхерът има задължението „б) освен военната отбрана на страната да защитава конституционните

институции и демократичните свободи на гражданите, както и опазването на реда и сигурността в страната изобщо; в) да оказва помощ при природни бедствия и катастрофи с особено голям мащаб; г) да оказва помощ в чужди страни при осъществяване на мероприятия по осигуряването на мира, хуманитарната помощ и помощ при природни бедствия";

Задачите по точки б) и в) (Assistenzeinsätze), които не са самостоятелна военна акция, се изпълняват само тогава, когато законните цивилни власти поискат участието на Бундесхера. Задачите по точка г) следва да се изпълняват само в случай че съответните компетентни органи вземат решение за изпращане на части на Бундесхера в чужбина.

Природни бедствия. Някои природни бедствия могат да бъдат предизвикани (напр. Опасност от заразяване, изкуствено предизвикване на лавини) или подсилени (увеличаване интензивността на наводненията поради извършени строителни мероприятия) от действия на човека.

Природните бедствия се обуславят предимно от атмосферни или геологични феномени и техните последствия. Възможни природни бедствия, имащи значение за Австрия са:

- бури;
- силни валежи, предизвикващи наводнения, свлачища, падане на камъни;
- пожари (горски пожари) и в трудно проходими райони;
- силен и продължителен снеговалеж (опасност от лавини);
- зарази (епидемии и пандемии);
- свлачища;
- изключителна суша.

Изискване на подкрепа от Австрийската армия. Съгласно § 2 (5) От закона за отбраната от 2001 г. властите и органите на федерацията, отделните провинции и общините в своя район на действие (отговорност/компетентност) имат право да изискат съдействия от Бундесхера за оказване на подкрепа при бедствия и катастрофи, доколкото това съответства на задачите на армията по§ 2 (1). Задължително се посочват:

- целта;
- предполагаемият мащаб;
- предполагаемата продължителност;
- обстоятелствата, поради което съответната задача може да се изпълни единствено със съдействието на Бундесхера.

Извършването на обикновени дейности като разчистване, пълнене на чували с пясък и др. може да се осъществява от всички сили на австрийския Бундесхер. Както показва досегашният опит за квалифицирани дейности са подходящи частите на ЯХБЗ, инженерните войски и военната авиация (за проучване, транспортни и спасителни работи и за погасяване на пожари).

Съвместни действия и координация между военните и цивилните служби. Връзката с цивилните служби в съответната провинция и действията на военната инфраструктура се осъществяват от военното командване.

Принципно сътрудничеството между военните и службите на съответното провинциално правителство, различните служби за защита на населението (пожарната, полицията и др.) в кризисния мениджмънт се осъществява от военното командване. В случай на нужда съответните централи за алармиране и оповестяване

подават сигнал за необходимостта от използване на военни сили и техника. Те отговарят за определяне на ситуацията и за координиране на всички участващи сили.

Необходима е допълнителна информация по следните въпроси:

- особености при провеждане на операцията, опасности, затруднени и др.;
- личен състав (функции) и организации (напр. Пожарна), средства и обслужващ персонал на мястото на операцията, вид и форма на съвместните действия, лица за контакт, упълномощени да вземат решения;
- представители на властите, упълномощени да вземат решения и дават указания, как да бъде осъществена връзка с тях, осигуряване на комуникация;
- представител на цивилните власти, който ръководи операцията;
- достъп до информационните системи;
- особености на района на провеждане на операцията и др.

Задачи на инженерните войски. Инженерните войски се използват на първо място за технически операции:

- за изграждане на преходи над наводнени участъци, както и за преминаване през опустошени райони с цел евакуация на цивилното население и осигуряване на бърз достъп на оперативните части;
- евакуация на хора, животни и имущество от наводнени региони с водни превозни средства;
- предотвратяване и/или ограничаване на щети в жизнено важни обекти и съоръжения, природни и културни забележителности;
- временно възстановяване на транспортната комуникация и приоритетно възстановяване на проходимостта с временни мостове;
- разрушаване на сгради, представляващи опасност по данни на цивилното ръководство;
- укрепване на скатове срещу свличане;
- подсилване или изграждане на диги при наводнение, съотв. взривяване на диги;
- измиване и почистване съоръженията на електроцентрали, като се предоставят водни транспортни средства и машини;
- извършване на всякакъв вид взривявания и инженерни дейности;
- поддръжка при операции при гасене на пожар.

Задачи на военната авиация. Военната авиация се използва:

- за бързо спасяване на хора и животни, както и за подслоняване на материални ценности;
- за транспорт на оперативни части, техника, продоволствие;
- за разузнаване (проучване) и свръзка;
- въздушни снимки за оценка на пораженията;
- транспорт и евакуация;
- гасене на пожари от въздуха;
- изкуствено предизвикване на лавини;
- изготвяне на най-точни метеорологични прогнози от метеослужбите.

Задачи на войските за ЯХБЗ. Войските за ЯХБЗ се използват предимно за технически операции, най-вече:

- деконтаминация (обеззаразяване) на хора и материална част след атомни, биологични или химични катастрофи;

- установяване границите на заразените, съотв. облъчени райони при ядрено и/или химично заразяване;
- гасене и борба с пожарите в заразените области;
- вземане на проби от квалифициран персонал и осигуряване на транспорта до съответната лаборатория.

Задачи на санитарни войски:

- осигуряване на първа медицинска помощ и по-нататъшно лечение съвместно с Червения кръст;
- изграждане на екипи за спешна медицинска помощ;
- осигуряване на леглова база и медицински грижи във военно-медицинските пунктове.

Задачи на другите родове и видове войски.

Други родове войски се използват в случай, че:

- инженерните войски или войските за ЯХБЗ нямат достатъчна численост в района на операцията;
- налага се използването на други специализирани войски (санитарно-медицински);

Други видове войски се използват в следните случаи:

- поддръжка при гасене на пожари (пехота, механизирани войски);
- транспорти от всякакъв тип (пехота, механизирани войски);
- поддръжка на инженерните войски при изграждането на диги при наводнения (пехота, механизирани войски);
- осигуряване подслон за транспортни средства и влакове (пехота, механизирани войски);
- метеосонди за прогнозиране на времето (артилерия);
- извършване на най-точни измервателни работи (артилерия);
- борба с лавини (пехота).

Примери за оказана подкрепа от Бундесхерът (австрийската армия) при природни бедствия:

През 2005 г. над 7200 военни са изработили 500 000 часа, участвайки в такива операции по ликвидиране на последствията от природни бедствия. Военната авиация е прелетяла 992 часа и е използвала 170 000 литра вода при потушаването на пожари. Изпълнявали са задачи, свързани с наводнения, обилен снеговалеж, ураганен вятър, потушаване на пожари, издирване на хора и взривни работи.

През 2006г. повече от 17 600 военнослужещи участвали в мисии в Австрия. Хеликоптерите на армията са пренесли над 4,2 милиона килограма. Тази година основната задача бе преодоляване на проблема с изключително голямото количество на падналия сняг. При това армията работи в тясно сътрудничество с цивилните организации.

Наводнения: В Австрия има специално понятие за операциите на армията в подкрепа на цивилното население Assistenzeinsatz.

Виена, 24.06.2009 г. Силните дъждове са причина за засиленото участие на Бундесхера. След обед 110 военнослужещи вземат участие в спасителните операции във Фелдбах, след като са призовани от Централата за своевременно алармиране на провинцията. Войниците извършват работи по разчистването на наводнена кожарска фабрика.

В Долна Австрия около 200 военнослужещи участват в спасителни работи след

наводнението. Войниците разполагат със специални превозни средства и участват в изпомпването на водата и работите по подсилването на предпазните диги.

Хеликоптери „Блек Хоук" хвърлят в Хафнербах чували с пясък от въздуха, за да бъде затворена отново една скъсана дига. Хеликоптери доставят материали и осъществяват връзка с бедстващите региони.

Военен самолет тип PC-6 заснема от въздуха крайдунавския регион, като предоставя на властите информация, въз основа на която се планират по-нататъшните спасителни операции.

Освен това една гвардейска рота и две инженерни роти от Мелк и Залцбург са в готовност да подкрепят по всяко време силите, участващи в операцията. В Горна Австрия шест роти за подкрепа на населението при бедствия са в готовност да се включат в операциите за ограничаване на щетите от наводнението. Армията оказва помощ на цивилното население при работите по разчистване в региона на наводнението след като реката постепенно отново се прибра в коритото си.

Редом с работите по демонтаж и отстраняване на временните съоръжения за ограничаване наводнението (напр. диги от чували с пясък) войниците на Бундесхера участват в дейности за предотвратяване на транспортни затруднения поради разкалване и затлачване. В някои общини са използвани тежки машини за разчистване на пътищата и възстановяване на проходимостта им.

В общините Шпиц и Вайсенкирхен във Вахау войници с тежка техника са заети основно с разчистване и възстановяване на все още затворения крайдунавски път. В операцията са участвали също и резервисти от инженерната рота в Долна Австрия със строителни машини и минибагери.

Повече от 40 години австрийската армия разполага с добре обучени военни кучета, които се използват и при чуждестранни мисии, терористични нападения, спасителни и издирвателни акции след природни бедствия в страната и чужбина.

Литература:

1. Интернет
2. Christine M. Pearson and Ian I. Mitroff . From Crisis Prone to Crisis Prepared: A Framework for Crisis Management *The Executive*, Vol. 7, No. 1 (Feb., 1993), pp. 48-59
3. Civil Military Planning Seminar for Crisis Management,Conflict Resolution and Prevention,ECSS "G. Marshall", Sofia, 10 – 14 Mai, 1999
4. Clarke, Thomas E., "**Management and Leadership of Scientists**", presentation to the 22nd Annual Conference of the Analytical Laboratory Manager's Association, League City, Texas, October 31st - November 2nd, 2001, Nanaimo, B.C.: Stargate Consultants Limited, November, 2001
5. Climate System Monitoring (CSM): Month. Bulletin. Issue No 1-12. Geneva: WMO, 1995
6. Cook S., Slack N. Making management decisions. Cambridge, 1984.

КОНФЛИКТ. ДЕФИНИРАНЕ, ХАРАКТЕРИСТИКИ И ДИНАМИКА

Генчо Б. Сандев

ШУ „Епископ Константин Преславски" Технически факултет.
Катедра „Управление на системи за сигурност"

CONFLICT: DEFINITION, CHARACTERISTICS AND DYNAMICS

Gencho B. Sandev

K. Preslavski University of Shumen Faculty of Technical Science, Department "Management of security systems"

Abstract: *A model of structure of a conflict is suggested in the paper – participants, disagreement zone, aim and function. A variant of conflict dynamics is formed, which gives opportunity to define the influence on the conflict situation.*

Key words: *conflict, structure, aim, function, characteristics, dynamics.*

I. Конфликт. Дефиниране и характеристики.

1. Дефиниции за конфликта - интеграция на различни постановки

А. Като състояние:

▪ Директна конфронтация между индивиди или групи, която обикновено възниква в ситуация, при която всяка от страните счита, че другата страна има вероятност да заплаши или вече е заплашила нейните основни интереси.

▪ Конфликтът като състояние може да бъде:

- определен случай на изостряне на противоречията;
- специфична форма на разрешаване на противоречията.

▪ Конфликтът е състояние, в което е нарушен хомеостатизма на взаимодействието между елементите в дадена система, при което става невъзможно:

- постигането на техните цели;
- удовлетворяването на основните им потребности;
- по-нататъшното им самосъхранение (оцеляване).

Б. Като процес:

▪ Конфликтът е процес, в който дадено усилие се прави от А с цел да противодейства на усилията на Б чрез някаква форма на блокиране, която ще осуети постигането от Б на неговите цели или задоволяването на неговите потребности (интереси).

▪ Конфликтът е процес на търсене на ново устойчиво състояние на системата (организацията) в пространството на състоянията, след като е била загубена устойчивостта й. Той съпътства опитите за постигане на синхрон между различните индивиди и групи от индивиди, заети в организацията, както и постигането на съгласуваност и компромиси между противоречивите елементи в нейната структура.

▪ Конфликтът е процес на взаимодействие, проявяващ се в дисхармония и противоречие в или между социалните субекти (индивиди, групи и организации) по отношение на социалното положение, цели, ценности, потребности (интереси) и

разпределяне на ресурси.

Обединяваща позиция – в основата на всеки конфликт лежи противоречие, което продължително време не е било разрешено и в резултат на неговото задълбочаване твърде често настъпва необратимо разрушаване на връзки и зависимости между отделни личности и/или групи (организации).

2. Структура на конфликта

Структурата на конфликта е съвкупност от устойчивите му елементи, отношения и връзки, които са композирани в цялостна система.

Основните елементи на структурата на конфликта са представени на фиг.1.

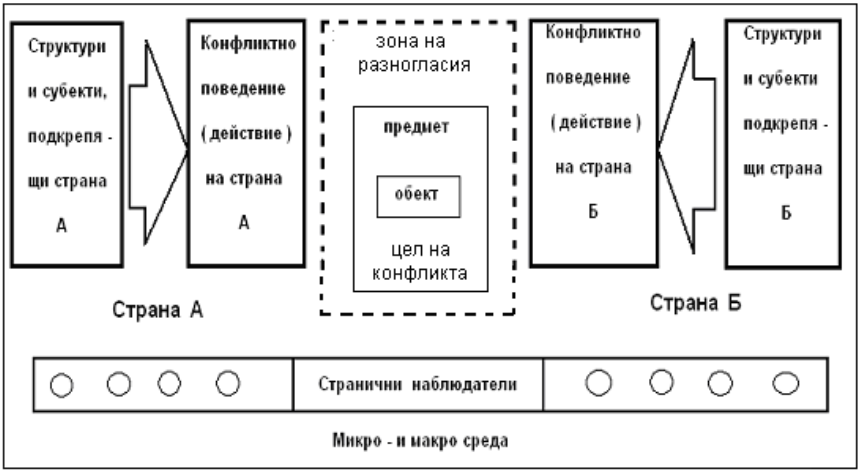
2.1. Участници в конфликта

Участниците винаги встъпват в конфликта със своите цели, ценности и интереси. Освен това, обществения живот не се свежда само до взаимодействие между отделните индивиди. В обществото действат различни социални групи, общности, политически формирования, юридически лица и др., които също могат да встъпят в противоборство. Разширявайки този кръг, участниците в конфликта, както и самите конфликти могат да бъдат голямо множество.

Съвременната конфликтология разделя всички участници на две групи:

- основни участници (преки);
- косвени (неосновни).

В реалната динамика на конфликта, границата между основните и неосновните участници често се оказва подвижна и относителна. Диалектиката се състои в това, че в процеса на развитие на конфликта, участниците често си разменят местата.



Фиг. 1

А. Основни участници. Във всеки конфликт има замесени пряко най-малко две взаимодействащи си страни, които са основните протагонисти на сблъсъка, наречени условно страна **А** и страна **Б.** Тези две страни могат да бъдат както отделни субекти, така и по-големи социални общности и организации.

Б. Косвени участници (структури и субекти, подкрепящи основните участ-

ници). Поначало всеки конфликт трудно може да остане, така да се каже, в „чист" вид - т.е. в него да бъдат непосредствено замесени само страна **А** и страна **Б**. На практика винаги около двете противоборстващи си страни възникват структури и субекти, които ги подкрепят. Тази подкрепа може да бъде както активна, така и пасивна. Както основните участници в конфликта, така и тук структурите и субектите могат да бъдат най-разнообразни като големина и специфичност.

Видове косвени участници:

▪ Инициатори са тези участници, които са взели инициативата в развитието на конфликта между други лица, групи или организации, като след възникването на конфликта, може и да не участват в него.

▪ Организаторите са група хора (или един човек), разработващи план за противодействието на опонентите с цел разрешаване на конфликта в своя полза. Те обмислят цялата динамика на конфликта, по начин, по който след приключването му, те да имат повече изгода, отколкото загуба.

▪ Съучастниците са лица, които помагат във възникването, организацията и развитието на конфликта. Те могат да са спонтанни или специално създадени групи, а така също могат да бъдат и отделни лица.

▪ Посредниците са третата страна в конфликта, т.е. те са косвени участници. Изпълняват ролята на авторитетни помощници, призовани от субектите в конфликта за разрешаване на проблема. Те могат да са както отделни лица, така и отделни организации и държави. Важна черта на посредника е неговия авторитет, признат и от двете страни. Целта на посредничеството е да се прекрати конфликта по пътя на намиране на компромис между опонентите.

2.2. Странични наблюдатели. Във всеки конфликт се откриват и т.нар. странични наблюдатели - т.е. субекти, групи или организации, които само наблюдават конфликта между страна **А** и страна **Б**, но не се намесват по никакъв начин - било то пряко или косвено. Казано иначе това е „мълчаливото мнозинство", което формира в индивидуалното или колективното си съзнание определено отношение към конфликтуващите страни, но не се намесва чрез целенасочени активни действия и пази мълчание.

2.3. Зона на разногласия. Обект и предмет на конфликта

В зоната на разногласия се очертават видимо или недотам ясно обектът и предметът на конфликта.

Обект на конфликта е тази конкретна ценност (материална или нематериална), към притежанието на която се стремят взаимодействащите си страни. Обект на конфликта по принцип може да бъде на практика всяка материална или духовна ценност от заобикалящия ни свят.

Предмет на конфликта е обективно съществуващото или субективно възприеманото противоречие (проблем), което е и причината за конфликтното взаимодействие между страните. Нерядко, предметът на конфликта между две взаимодействащи си страни е напълно идентифицируем (различим), но понякога можем да се сблъскаме с огромни трудности при откриването му. Често в конфликтологичната практика се откриват конфликти, предметите на които могат да бъдат открити единствено хвърляйки поглед далеч в миналото или чрез извършването на непрекъснато разслояване и сложни процедури.

2.4. Цел на конфликта

Целта на конфликта е свързана с промяната, която трябва да се извърши за да

се притежава някаква ценност. Всички конфликти са опит да се постигне или да се попречи на дадена промяна. Конфликтът не винаги води до промяна и не всяка промяна предизвиква конфликт. Но когато има конфликт, за да се разбере по-добре, трябва да се търси връзка с някаква промяна. Какво трябва да се промени, кой трябва да я извърши, каква трябва да бъде цената, кой трябва да плати цената на промяната, кога и как тя трябва да бъде платена - това са основните направления на конфликтното взаимодействие и цели за постигане. Всеки конфликт възниква, защото някой желае промяна, на която някой друг се противопоставя.

Промяната, като силен конфликтен агент, има две измерения - процесът на промяна и последиците от промяната. Те са вълнуващи за тези, които ги желаят и заплашителни и стресови за тези, които им се противопоставят.

2.5. Функции на конфликта - конфликтно поведение (действия)

Функциите на конфликта се определят, от една страна, от неговата социална същност и предназначение, а от друга страна, главно от вида, целите и силата на конфликтните взаимодействия между страните.

По своето съдържание функциите на конфликта обхващат както материалната сфера (свързана преди всичко с икономическите интереси, печалбата или загубата), така и духовната сфера (свързана главно с Аз - концепцията, активността и мотивацията).

Конфликтното поведение (действия) се характеризира със следните стратегии:

▪ **Взаимно примирение на страните (избягване).** Същото предполага игнориране на конфликтната ситуация, даване на вид че тя не съществува и не предприемане на никакви стъпки по нейното изменение. Тази стратегия е оптимална за ситуациите, които:

- не са особено значими за страните и те са преценили, че не си заслужава да се хабят сили и средства за внасяне на корекции в нея;
- независимо една от друга страните са стигнали до изводите, че шансовете им за успех в конфликта са близки до нула и в идеален план (най-често ценностно) са преобразували ситуацията;
- и двете страни притежават различен от обичайния за цивилизацията светоглед издигащ ги над всекидневните проблеми.

▪ **Приспособяване към опонента.** То най-често се осъществява чрез правене на отстъпки пред него, понякога стигащи дори до капитулация. Въпросните отстъпки могат да демонстрират добра воля и да служат за позитивен модел на другата страна. Не рядко те са преломен момент в напрегнатите ситуации към по-добро. Главната цел в приспособителната стратегия е да се съхранят силите и средствата за по-благоприятен момент. Тази стратегия е възможно най-приемливия изход от конфликта за една от страните в случаите, когато баланса на силите не е в нейна полза. Наред с това се допуска и възможността с течение на времето в резултат на външни или вътрешни фактори да настъпят такива изменения в зоната на разногласия, които коренно да трансформират актуалната конфликтна ситуация.

▪ **Съгласуване на интересите и позициите на конфликтуващите страни на нова основа (компромис).** Понякога той е единствено възможния и най-добър мирен вариант за разрешаване на проблемите. Чрез него всяка от страните получава по нещо вместо да продължава конфронтацията и да загуби всичко. Препо-

ръчително е компромисът да бъде в равна мяра, тъй като неудовлетворените в пълна степен интереси на страните крият риск за възобновяване на конфликта в по-остра форма.

▪ **Съперничество.** В редица случаи, то не само е допустимо, но и необходимо за развитието и прогреса. Не рядко, обаче съперничеството води до:

- впрягане на всички налични сили до границата на изтощение;
- не нормализация, а влошаване на отношенията с непосредствения опонент и с хора дори нямащи отношение към конфликта;
- пораждане на изкушение за победа на всяка цена (дори чрез използването на нечестни и жестоки методи) и т.н.

Употребата на сила е най-бързият тактически способ за разрешаване на конфликти, но същевременно и най-неефективния от стратегическа гледна точка. За да съхрани своето превъзходство победилата страна трябва постоянно да изразходва допълнителни материални, интелектуални, военни и други ресурси.

Освен това, конфликтът може да бъде завършен не само чрез налагане на пълно подчинение над по-слабия, но и чрез унищожаването му. В последния случай рано или късно винаги се стига до морално осъждане на победителите.

▪ **Сътрудничество.** Отличава се от останалите форми за разрешаване на конфликтите по стремежа да се постигне възможно най-пълно удовлетворяване на собствените и на опонента интереси. Често се разглежда като желан, но нереален вариант за завършване на конфликтите. За разлика от компромиса, при него е необходим преход от отстояване на собствената позиция към търсене на съвместимост на интересите. Сътрудничеството е единствения изход от конфликта, който позволява едновременното достигане на желания резултат и ненарушаване на отношенията между страните.

2.6. Среда на конфликта

Конфликтът винаги се развива и обективира върху някакъв социален фон (среда). Ако ние не отчитаме тази обективна даденост, рискуваме да разглеждаме конфликта откъснато и механистично, а самият той никога не е изолирано явление, тъй като протича в определена социална ситуация.

От гледна точка ниво на социална система се различават микро- и макросреда.

Микросредата е съвкупността от условията на взаимодействието между хората, непосредствено влияещи на междуличностните и междугруповите конфликти (мащабът е малка социална група).

Макросредата включва тези условия, които влияят на развитието на конфликта между големи социални групи и организации (държави).

3. Базови характеристики на конфликта и параметри.

Базови характеристики:

- биполярност - противопоставяне на два обекта (хора, групи, организации);
- активност (насочена към преодоляване на противоречията);
- многовариантност на състоянията и ситуациите;
- неповторимост на процесите;
- неуправляемост на мнозинството от факторите;
- съществена неопределеност на заплахите;
- слаба предсказуемост на последствията.

Основни параметри на конфликтуването:

а) обхват – измерва се с броя на участниците в конфликтуването. Този параме-

тър се различава от параметъра - брой на участниците в конфликта, защото е възможно не всички участници да реализират конфликтни действия. Но това се случва много рядко, в повечето реални конфликти двата параметъра имат равни стойности.

б) сила (С) – измерва се обикновено в степени чрез експертна оценка на критериите:

- вид и характеристики на групите (организациите) в конфликта;
- рационалните, волевите и афективните характеристики на личностите в конфликта;
- зависимост между страните в конфликта (степен на противоречивост);
- причини за конфликта и условия (фактори);
- въздействие на конфликтуването, както върху личността, така и върху дейността и развитието на социалната група (организация);
- управление на конфликта и др.

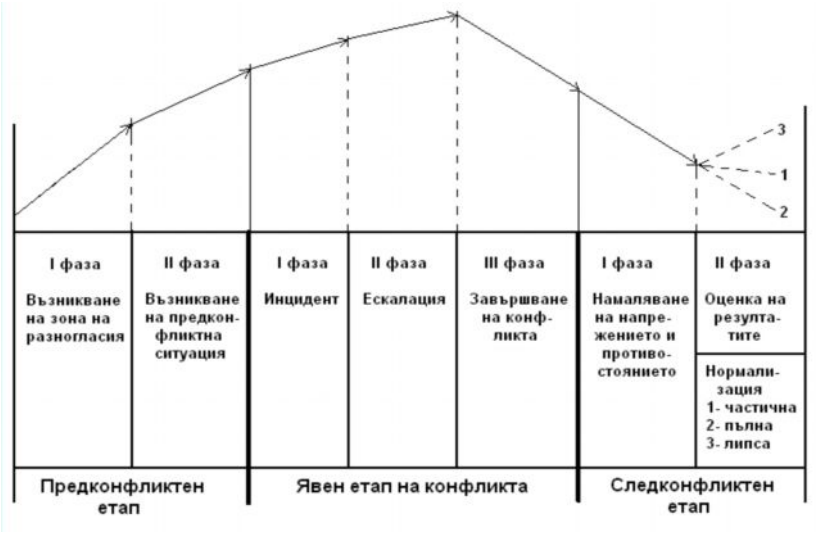
в) времетраене на конфликтуването **(В);**

г) мощност (М) – намира се по формулата: **М = С х В .**

Мощността зависи още и от убедеността в собствената правота на всеки участник в конфликта, от отстояването на позициите, от степента на тяхната несъвместимост, от ресурсите и др.

II. Динамика на конфликта

Конфликтът в темпорален план преминава през **три основни етапа.** По-долу са характеризирани етапите поотделно, заедно с включените в тях фази - фиг.2.



Фиг. 2

1. Предконфликтен етап

Той може да бъде описан със следните най-характерни особености: нарастване на социалното напрежение; открояване на взаимодействащите си страни; реално

накърняване на интересите на страните, което се осъзнава като такова (зона на разногласия); собствено възникване на реална предконфликтна ситуация.

Първата фаза от предконфликтния етап може да бъде наречена фаза на възникване на зоната на разногласия. Зоната на разногласията по принцип е обективна, макар и субективно възприемана реалност. Тя е пресечната точка, в която се вплитат противоположните интереси на двете взаимодействащи си страни, със съответните предмет и обект на конфликта. Разбира се, фазата на възникване на зоната на разногласия все още не е собствено конфликт, а само някакъв вид социално равновесно състояние - обстоятелство, което предшества открития сблъсък. Още в първата фаза на предконфликтния етап се наблюдават опити за решаване на обективно съществуващите проблеми (зоната на разногласия) чрез неконфликтни способи, а именно: по пътя на разясненията, молбите, осведомяване на взаимодействащите си страни с най-различен тип и вид информация. Ако всички тези начини не дадат конкретен, взаимоприемлив резултат, то предконфликтният етап преминава в следващата си фаза.

Втората фаза на предконфликтния период е възникване на предконфликтна ситуация. Най-важният белег на тази фаза е, че тук взаимодействащите си ясно и непосредствено осъзнават реалното нарушаване на интересите си, за разлика от първата фаза, където се наблюдава само потенциално накърняване на интереса на двете страни.

Тук е мястото да се изясни по принцип разликата между понятията конфликтна ситуация и конфликт. Макар и двете понятия да се използват като синоними, те не са тъждествени. Конфликтната ситуация е елемент на конфликта и така се съдържа (вмества) в конфликта, като тя е само обособен епизод (част) от конфликта в отделен и определен момент от неговото развитие.

Случва се понякога така, че предконфликтният етап е свързан с много силно социално напрежение между страните, но не прераства в открито противоборство, т.е. в явен конфликт. Това състояние може да продължи неопределено дълго време. Това е т.нар. потенциален (скрит) конфликт. Потенциалният конфликт се характеризира с реално съществуващо противоречие между интересите на двете взаимодействащи си страни, което противоречие обаче не прераства в открит сблъсък, вследствие на ред субективни и обективни причини.

В действителността се среща и т.нар. „неистински" („лъжлив") конфликт. Неистинският конфликт се наблюдава тогава, когато две взаимодействащи си страни възприемат субективно дадена ситуация като конфликтна, докато тя обективно не съществува като такава.

2. Открит етап на конфликта

За да се дойде до вторият етап на конфликта, а именно предконфликтната ситуация (фаза) да прерасне в открит етап на конфликта, е нужен формален повод, който да подтикне взаимодействащите си страни към предприемане на активни действия. Този формален повод е инцидентът, който е и първата фаза на откритият етап на протичането на конфликта.

Инцидентът може да възникне както случайно, но така също и да е провокиран съзнателно от едната или от двете взаимодействащи си страни. Поначало дори и най-малкият и незначителен формален повод би могъл да стане причина за инцидент, той е, така да се каже искрата, която запалва „пожара" на конфликта. Инцидентът е първото открито противопоставяне между страните, в което те се атаку-

ват, прибягвайки до различни методи, включително и силови, с които се стремят да решат конфликта в своя полза. Конфликтът, започнал с инцидент, може да прекрати своето действие заедно с него, напр. при т.нар. „случаен" конфликт. Като добро онагледяване на такъв вид конфликт би могла да се приведе ситуацията на случайния сблъсък между два субекта в масовия градски транспорт. При „естествения" си ход на развитие, обаче след инцидента настъпва втората фаза на откритията етап на конфликта - ескалацията.

Ескалацията на конфликта се характеризира с рязко усилване на взаимонасочените действия на опонентите. В тази втора фаза противоборството между взаимодействащите си страни достига своя връх. Ескалацията може да бъде непрекъсната, с постоянно нарастване на напрежението и силата на взаимодействие между страните и вълнообразна, когато напрежението и силата на взаимодействие ту се покачва, ту спада.

Ескалацията може да завърши с кулминация. Кулминацията е върхната точка на ескалацията и представлява най-силното изражение на конфликтното взаимодействие между страните. За нея обикновено са присъщи следните най-общи характеристики: субективно неадекватно възприемане на обективната конфликтна ситуация от страните, създаване на „образ на врага", ирационални и личностни нападки към опонента, загуба или размиване на конкретния обект на спора и въвличането на множество странични обекти в зоната на разногласията.

След ескалацията настъпва третата последна фаза на откритията етап на конфликта - завършването на конфликта. **Завършването на конфликта** може да се опише като преход от активното и интензивно противопоставяне между взаимодействащите си страни към търсене на пътища за разрешаване на проблемите от зоната на разногласията и преустановяването на конфликта.

При описанието на тази заключителна фаза се използват два възлови термина: регулиране на конфликта и разрешаване на конфликта - често в качеството им на синоними. Макар и близки в семантичен смисъл, тези термини носят различна нюансировка в разглеждания контекст. Основната разлика между регулирането на конфликта и разрешаването на конфликта е следната: при регулирането на конфликта се постига частична нормализация на отношенията между страните, докато при разрешаването на конфликта е налице пълна нормализация на отношенията между взаимодействащите си страни.

3. Завършващ етап.

Последният, завършващ етап на конфликта, е следконфликтният. Конфликтът оставя винаги след себе си субективни (преди всичко в съзнанието на конфликтуващите страни) и обективни (промяна в зоната на разногласията) следи и след отшумяването му. В преобладаващата част от случаите след-конфликтният етап (ситуация) се отличава в по-голяма или по-малка степен от предконфликтния етап (ситуация) и особено от откритията конфликтен етап (ситуация).

Първата фаза на следконфликтния етап е фазата на значително намаляване напражението и конфликтното противопоставяне.

Поначало оценката на резултатите, в зависимост от нормализацията на отношенията между конфликтуващите страни, може да бъде три вида: **частична нормализация, пълна нормализация, липса на нормализация.**

Частична нормализация е налице тогава, когато взаимодействащите си страни са удовлетворили отчасти собствените си интереси, лежащи в зоната на разног-

ласията.

Пълна нормализация имаме в случая, когато двете взаимодействащи си страни са намерили взаимоприемливи решения на конфликта, удовлетворяващи интересите и на двете страни.

Липсата на нормализация (в оценките на взаимодействащите си страни) по същество е предпоставка за избухване на нов конфликт, тъй като нито една от страните не е получила дори частично удовлетворяване на своя интерес.

Литература:

1. Анцупов А.Я, Шипилов А.И., Конфликтология, Изд. Дом „Питер“, 2006.
2. Георгиев Н., Конфликтът в бизнесорганизацията, Стопанска академия „Д. А. Ценов”, 2005.
3. Громова О.Н., Конфликтология, Москва, 2000.
4. Дарендорф Ралф, Модерният социален конфликт. Есе за политиката и свободата, София, 1998.
5. Емельянов С.М. Практикум по конфликтология, изд. „Питер”, Санкт-Петербург, 2000.
6. Паунов М., Организационно поведение, Изд.„Сиела” София, 2006.
7. Тодоров А., Кръстева.А., Конфликти. Доверие. Демокрация, София, 2005.

УПРАВЛЕНИЕ НА КОНФЛИКТ. БАЗОВ МОДЕЛ.

Генчо Б. Сандев

ШУ „Епископ Константин Преславски” Технически факултет. Катедра „Управление на системи за сигурност”

CONFLICT MANAGEMENT. BASIC MODEL

Gencho B. Sandev

K. Preslavski University of Shumen Faculty of Technical Science, Department “Management of security systems”

Abstract: *A model of conflict management is suggested in the paper. Diagnostics of the environment and organization (periodic scan, scan during changes). Planning. Organization and coordination. Influence on the pre – conflict situation (conflict). Control of results (consequences) of conflict management.*

Key words: *conflict, management, diagnostics, planning, organization, coordination, stop, permission, control*

I. Същност и структура на управлението на конфликт

Управлението на конфликта е целенасочена дейност на субекта на управление, която се извършва за предотвратяване, както и на всички етапи от възникване-

то и развитието на конфликта, до неговото завършване.

Този процес не бива да пречи на функционалните взаимоотношения между елементите на организацията, между опонентите, както и на изпълнението на целите и задачите.

Управлението на конфликта включва следните процеси:

1. Диагностика на средата и на организацията (периодично сканиране; сканиране при промени). Разкриване на отделни елементи (симптоми) на предконфликтна ситуация.

2. Планиране

▪ Диагностика на предконфликтната ситуация (конфликта):

- определяне на симптомите за възникване на предконфликтната ситуация (конфликта);
- определяне параметрите на предконфликтната ситуация (конфликта).

▪ Прогнозиране.

▪ Целеполагане.

▪ Вземане на решение.

3. Организиране и координиране

4. Въздействия върху предконфликтната ситуация (конфликта)

▪ Предотвратяване.

▪ Регулиране.

▪ Разрешаване.

▪ Стимулиране.

5. Контрол на резултатите (последствията) от управлението на конфликта и изводи за последващи въздействия

Подходът при управлението на конфликта следва да се избере в зависимост от целите на организацията, като ръководството се съобразява с етапа на развитие на същата, големината и динамиката на промяната (ако се извършва такава), от организационната култура, от степента на взаимно доверие и вътрешногрупово съгласие, както и от силата и параметрите на конфликта.

II. Базов модел на цикъла на управление

1. Диагностика на средата и организацията

Диагностика - съвкупност от познавателни и организационни методи и процедури за обозначаване състоянието на една система (организация) чрез измерване на конкретни, моментни стойности на определени пара-метри, разкриване на източниците на смущения (в средата и в организацията) и очертаване насоките за отстраняването им.

Цел на диагностиката - установяване на отклоненията на реално функционираща организация от изискванията и параметрите на нейния идеален (планиран) модел.

Периодичността на сканирането на средата и организацията се извършва в зависимост от сложността и динамиката на средата и развитието на организацията.

2. Планиране

Планиране - процес, свързан с определянето на цели, които трябва да бъдат постигнати в бъдеще с изясняването и определянето на необходимите за постигането на тези цели мероприятия и ресурси, с координирането по място и време на

тези мероприятия и ресурси.

Процесът на планиране, независимо от модела, винаги е системен, интегриран и се базира на договарянето на справедливо разпределение на ресурси и съвместяването на различни интереси между страните в конфликта с малко загуби за оптимално време.

2.1. Определяне на причините (симптомите) за възникване на предконфликтна ситуация (конфликт).

А. Обективни организационни причини:

▪ Организационна сложност (конфликтът може да се разрасне съобразно броя на йерархичните равнища и нарастването на функциите и специалните задачи).

▪ Неразумни или неясни политики, стандарти или правила.

▪ Чести промени в организацията.

▪ Неумение да се делегира властта, затруднения при нейното упражняване.

▪ Неяснота във функциите (задълженията). Претовареност на работното място.

▪ Противоречия между формални и неформални групи.

▪ Големите различия в образователното и квалификационното равнище, в доходите, в манталитета и престижа на отделните членове на организацията.

▪ Колективно вземане на решение (колкото е по-голям броя на хората, участващи при вземането на решението, толкова е по-голяма вероятността от конфликт).

▪ Вземане на решение чрез консенсус - да се осигури 100% съгласие е много по-трудно.

▪ Неадекватни комуникации.

▪ Взаимозависими задачи (напр. един човек не може да изпълни своята задача, докато другите не са я изпълнили).

▪ Нереалистични срокове или натиск за съкращаване на тези срокове.

▪ Конкуренция за ограничени ресурси.

▪ Угнетяващо въздействие на ръководството върху индивида - напрегната атмосфера, автократичен стил на управление, ограничения върху поведението, липса на перспективи за израстване в кариерата, липса на информация и съпричастност.

▪ Несъвършенства в заплащането и разпределянето на премиите.

▪ Лоши трудови условия.

▪ Неразрешени или подтиснати конфликти.

Б. Субективни причини за възникване на конфликтите.

Субективните причини са свързани с наличието във всеки конфликт на различни личности (управленски и изпълнителски персонал). За да се развие един вътрешноличностен конфликт хората трябва да притежават определени личностни характеристики и да е създадена специфична ситуация.

Личностни причини (условия):

- богат вътрешен свят с противоречиви черти на характера;
- сложна йерархия на потребностите и мотивите;
- високо ниво на чувственост;
- склонност на индивида към самоанализ и саморефлекция;
- неадекватните оценки и възприятия;
- осъзната субективна неразрешимост на ситуацията и др.

Ситуационни причини (условия):

- аномия (липса или неадекватна нормативна база);
- заплаха за значими ценности;

- препятствия за удовлетворяване на потребностите;
- обществени забрани и др.

В. Индикатори и симптоми за възникване на конфликт.

Основните индикатори и симптоми за възникване на конфликт могат да се структурират по следния начин:

- увеличаване на дискусиите за целите на организацията, показващо разрушаване на консенсуса;
- съхраняване и увеличаване на разделеността в пространството и времето; вътрешно разделение на неформални фракции;
- опасения на ръководителите на различните нива, че процесите излизат от контрол;
- увеличена честота на използване на гласуването като метод за вземане на решение; приемане на решенията от позицията „победа – поражение";
- ниска удовлетвореност от труда на много нива и групи; растящ брой откази от работа и прехвърляне към други работни места;
- увеличаване на недоверието спрямо другите (хора, групи); възприемане на хората като врагове; увеличено използване на агресивни изрази;
- дълги разтегнати съвещания; рязко увеличена (намалена) честота на посещаемост на някои общи мероприятия;
- търсене от хората на основания за различни възражения (нефокусирани тревога и гняв);
- неадекватни реакции или действия на хората; отказ от подкрепа или съпричастни действия;
- изменяне на стандартите на комуникация; склонност на хората към търсене на конспиративни методи на общуване; разпространение на слухове и клюки.

2.2. Определяне на характеристиките (параметрите) на конфликт.

При сканиране на конфликта се анализират следните елементи:

▪ Вид на конфликта.

▪ Участници в конфликта (брой, характеристики, цели, ценности, интереси):
- основни;
- несновни (косвени) - организатори, съучастници, посредници;
- странични наблюдатели.

▪ Сила и времетраене на конфликтуването:
- вид и потенциал на групите (организациите) в конфликта;
- рационалните, волевите и афективните характеристики на личностите в конфликта;
- зависимост между страните в конфликта (степен на противоречивост);
- бързина на протичане на взаимодействията между страните.

▪ Обект на конфликта - материална или духовна ценност от заобикалящия ни свят (характеристики).

▪ Предмет на конфликта - вид и сила на противоречията; антагонизъм.

▪ Цел на конфликта.

▪ Непосредствена среда на конфликта - съвкупност от условията на взаимодействие между страните (личностите или групите).

▪ Функции на конфликта (конфликтно поведение на страните) - реализиране на стратегиите избягване, приспособяване, сътрудничество и съперничество; прилагани тактики.

▪ Последствия от конфликта.
▪ Динамика на конфликта:
- етап, в който се прави диагностиката;
- етапи и фази на конфликта - характеристики;
- тенденции в развитието на конфликта.
▪ Предложения за профилактика и разрешаване на конфликта:
- приоритетни намеси в конфликта;
- структура и време на последващите намеси.

2.3. Прогнозиране.

Прогнозиране - обосновано предвиждане на възможните варианти за развитие на конфликта и вероятността те да се реализират.

Изисквания. За да се приеме една прогноза за коректна и обоснована, трябва да отговаря на редица изисквания:

- еднозначно да бъдат формулирани очакваните събития, ситуации, резултати без да се допуска двусмислие;
- ясно да бъде определено времето (хоризонтът), когато ще бъдат постигнати предвидените резултати или ще настъпят очакваните събития;
- ако прогнозата е условна, поставеното условие да не бъде нереално, неосъществимо;
- да съществуват поне две възможности по отношение на предвидените резултати: да се постигнат (изцяло или отчасти) или да не се постигнат. Ако липсват тези две възможности, прогнозата губи своя смисъл;
- да има яснота относно вероятността за осъществяване на прогнозата;
- да са известни авторът и процедурата за съставянето на прогнозата, т.е. кой, кога, как и защо е разработил прогнозата (основни методи).

Етапи при разработване на прогноза на конфликтна ситуация (конфликт):

▪ Определя се обекта на прогнозирането - конфликтна ситуация (конфликт).
▪ Събира се и се анализира информация за конфликтната ситуация (конфликта) - информацията е за определен минал период.
▪ Анализира се информацията за сегашното състояние на конфликтната ситуация (конфликта).
▪ Избира се метод на прогнозиране.
▪ Разработват се варианти на прогнозата на конфликтната ситуация (конфликта) - обикновено вариантите са три: оптимистичен, песимистичен и осреднен от първите два. Структура:
- описателен модел на конфликтната ситуация (конфликта) - същност, структура, функции, динамика и др.;
- обяснителен модел на конфликтната ситуация (конфликта) - причини, фактори, движещи сили и др.
▪ Избира се оптималният вариант.
▪ Разработва се система за контрол и реализация на прогнозите.

2.4. Целеполагане.

Процесът на целеполагане включва:
▪ Определяне на целите при управлението на конфликта.
▪ Разработване на измерители на целите.
▪ Интегриране на измерителите в цялостна система.
▪ Практически действия по осигуряването на условия за въвеждането на целите

в действие.

Изисквания при поставянето на целите при управление на конфликт, чието спазване значително повишава ефективността на процеса на целеполагане:

▪ Ясно и точно определяне на целите при управлението на конфликта и задачите за тяхното изпълнение.

▪ Оценка на целите от гледна точка степента на трудност. Съществува зависимост между степента на трудност на целта и нейното изпълнение.

▪ Определяне приоритетите на целите (съобразно конфликта), произтичащи от важността, трудността или времевите рамки на същите.

▪ Уточняване на критериите, стандартите и процедурите по изпълнението на целите.

▪ Уточняване как ще бъде измерван успехът. Когато това измерване става само на базата на крайни резултати, то могат да се използват измерители за качество, количество, необходимо време или в стойностно изражение.

▪ Изясняване на условията (на средата и конфликта), при които ще се изпълняват целите.

▪ Определяне на мотивиращите фактори за изпълнение на целите.

2.5. Вземане на решение за управление на конфликта.

Основни дейности:

▪ Обработка на информацията от диагностиката, прогнозирането и формулиране на ограниченията при разработването на решението и неговите базови характеристики.

▪ Съсредоточаване на допълнителна информация (при необходимост).

▪ Оценка на средата и конфликта (причини, фактори които влияят, характеристики, степен на опасност, вид на проявление, очаквана продължителност, връзка с други противоречия, евентуална зона на разпространение, последствия от конфликта - положителни и отрицателни и др.).

▪ Разработване на решение:

а) разработване на алтернативи (варианти на решение);

б) приемане на критерии за оценка на алтернативите;

в) оценка на алтернативите; при оценката на разработените алтернативи се взема под внимание взаимоотношението алтернатива - резултат; то се опре-деля от три възможни условия:

- сигурност - мениджърът категорично знае какви са последиците от всяка алтернатива;

- риск - мениджърът има някаква вероятностна представа за последиците от всяка алтернатива;

- неопределеност - мениджърът няма почни никаква представа за възможните последици, до които може да доведе отделната алтернатива.

г) избор на оптимален вариант на решение; използват се три подхода: вземане в предвид на предишен опит, провеждане на експеримент, изследване и анализ.

▪ Съгласуване и утвърждаване от висшестоящото ръководство на решението за управление на конфликта.

3. Организиране и координиране.

Организиране - процес на създаване на условия за ефективно управление на конфликта.

Дейности:

- обезпечаване функционирането на системата за управление (на частта от нея, занимаваща се с конфликта);

- разработване (подобряване) на интегрирани технологии или технологии на отделни процеси, където организирането на управлението на конфликта е разписано по отделни елементи (цели, последователност и време за реализиране, права, отговорности, кадри и други ресурси);

- създаване на специфични структури (избор на медиатори) за регулиране (разрешаване) на конфликта - ако е необходимо;

- създаване на работни позиции и определяне на права и отговорности (делегиране);

- реализиране на специфична система за комуникации за преодоляване на конфликта - при необходимост;

- съгласуване на плановете на структурите участващи в управлението на конфликта;

- съгласуване на организационните мероприятия с външни организации (институции) - при целесъобразност.

Координиране - процес, който цели постигането на единство в изпълнението на взаимно зависимите дейности при управлението на конфликта.

Координация е необходима винаги, когато две или повече лица, групи или подразделения, се стремят да постигнат една обща цел.

Типът координация е свързан с характера на проблемите и със ситуациите, които се решават. Там, където проблемите са рутинни и повтарящи се, може да се прилага координация по план. В такива случаи координацията може да се провежда с помощта на предварително изготвени програми, които посочват какво и кога да се предприема. В динамично променящи се ситуации, каквито са конфликтите (в тях по правило възникват непознати проблеми), по-подходяща се явява координацията чрез обратна връзка.

4. Въздействия върху предконфликтната ситуация и конфликта

Основни въздействия:

▪ **Предотвратяване (профилактика) на конфликт** - целенасочено въздействие върху потенциалните опоненти, причините или условията за конфликт в момент, когато те не са свързани в конфликтна ситуация.

▪ **Регулиране на конфликт** - дейност на субекта на управление насочена към отслабване и ограничаване на противоборството между страните и частично нормализиране на отношенията им.

▪ **Разрешаване на конфликт** - дейност на субекта на управление, чиято цел е слагане край на конфликтното взаимодействие и пълна нормализация на отношенията им.

▪ **Стимулиране на конфликт** - въздействие върху опонентите, противоречията и условията с цел да се инициира (възбуди) конфликтен процес. Тази твърде рискована тактика се предприема в случаите, когато се очаква, че чрез конфликта ще се разрешат радикално противоречията и ще се подобри организационния климат и развитието.

Като базови техники могат да се използват:

А. Техники, които водят до промяна в организационната структура:

▪ Увеличаване на взаимозависимостите между отделните единици или инди-

види в организацията.

▪ Повишаване на стандартизацията и специализацията.

▪ Наемане, уволнение, преместване на членове на организацията.

▪ Разрастване на организациите, при което бюрократичните тенденции се увеличават. Използването на тази техника единствено само с цел повишаване на нивото на конфликтите едва ли е оправдано. Тя се свързва с висока ресурсоемкост. Тази висока цена може да бъде оправдана, само ако безразличието, незаинтересоваността, безотговорността и липсата на инициативност са стигнали до застрашаващи размери.

Б. Техники, основаващи се на манипулиране на комуникационния канал:

▪ Изпращане на двусмислена или сплашваща информация. Трябва да се има предвид, че техниката на сплашващата информация може да има непредсказуем ефект. Стимулирането на конфликта е много лесно, но развитието му се свързва с по-голяма стихийност, много бързо ескалира, но трудно затихва. Дори след премахване на заплахата хората продължават да се чувстват несигурни и враждебността остава.

▪ Отклоняване на информация:

- от традиционните канали (възможно е и да е по посока на неформалните канали);

- посредством нейното филтриране (всеки, през който преминава, я филтрира по свои собствени критерии, съобразно преследваните цели).

▪ Претоварване на комуникационните канали.

В. Техники, които променят поведението на индивидите:

▪ Промяна на персоналните (личностни) характеристики на лидера (напр. назначаването на ръководител, чийто стил не съответства на етапа на развитие на колектива и др.).

▪ Създаване на ролеви конфликт (ролева несъвместимост, ролева неяснота и др.).

5. Контрол

Контрол - съвкупност от аналитични и оценъчни дейности, чрез които се установяват резултатите и се определят алтернативите за промяна на управленското въздействие.

Чрез контрола се реализира обратната връзка и се получава информация за настъпилите изменения в организацията (конфликта), които трябва да се отстранят чрез регулиращи въздействия. Чрез контрола точно се откриват отклоненията и се търсят възможности за неутрализирането им.

Етапи:

▪ Избор на методи, средства, вид и форми за контрол на планираните про-цеси.

▪ Проверка на изпълнението на предвидените в плана мероприятия.

▪ Сравняване на фактическото състояние (изпълнените мероприятия) с планираните показатели.

▪ Определяне на настъпилите отклонения.

▪ Анализ и оценка на факторите, довели до тези отклонения.

▪ Създаване на основа за промяна на плана за управление на конфликта или за разработване на нов план.

Най-убедително свидетелство за ефективността от използването, както на об-

щите стратегически принципи, така и на конкретните тактики за управление на конфликтите, са реалните резултати.

Литература:

1. Ангелов А., Организационно поведение, София, 2002 г.
2. Галтунг Йохан, Разрешаване на конфликти, София, 2005г.
3. Георгиев Н., Конфликтът в бизнесорганизацията, Стопанска академия „Д. А. Ценов", 2005г.
4. Гладичева Р., Съвременният български модел на индустриални отношения. Сравнителни модели и анализ. Кн.3, ИРМИ, 2003г.
5. Димитров Д., Управление на конфликтите, София, 2005г.
6. Дронзина Т., Разрешаване на конфликти, София, 2001г.
7. Маркхам Урсула, Управление на конфликта. Лаков прес, София, 1999г.
8. Уолтърс, П. Г., Характеристики на успешното организационно развитие, София, 1996г.

МЕЖДУНАРОДНА И НАЦИОНАЛНА ПРАВНА РАМКА НА БОРБАТА С КИБЕРТЕРОРИЗМА

Велико П. Петров **Станчо Г. Станчев**

Национален военен университет "В. Левски", факултет "Артилерия, ПВО и КИС", Катедра "Организация и управление на тактическите подразделения от полевата артилерия" гр. Шумен

INTERNATIONAL AND NATIONAL LEGAL FRAMEWORK TO FIGHT WITH CYBER TERRORISM

Veliko P. Petrov **Stancho G. Stanchev**

Abstract: *This report considers international and national legal framework to fight with cyber terrorism. The actuality of the topic is determined by the growing threat of cyberterrorism, its aggressiveness and enrichment with new and varied forms. Highlights the significance of cooperation between states and international organizations to effectively counter the new threat to the security of the transatlantic community.*

Keywords: *cyberterrorism, legal frameworkл*

През последните години международният тероризъм премина към качествено нов етап от своето развитие и придоби глобален характер. Той вече се използва не само като инструмент за постигане на конкретни политически цели в отделна страна или регионален конфликт, а е насочен към принципна смяна на съществуващата система на международни отношения. Цели се хаос и икономическа дестабилизация в страните мишени и предизвикване на страх и психоза сред населението, като в крайна сметка се преследва глобална криза и промяна на съществуващия световен ред.[**2**].

Съвременният тероризъм е комплексно и динамично явление, което успешно се адаптира към политическата и икономическата конюнктура. Оказването на ефективно противодействие не е по силите на нито една самостоятелна специализирана институция или отделна страна. Реални резултати в борбата с тероризма могат да бъдат постигнати само чрез обединените усилия на цялата международна общност.

Тероризмът е организирана и индивидуална криминална насилствена дейност с цел удовлетворяване на конкретни политически искания. Тероризмът се дефинира като триединство от цел, средства и обекти. Целта преследвана от терористите винаги е политическа. Средствата (насилие или заплаха с насилие) са според конкретните цели на всеки терористичен акт. Под насилие (сила, както е в наказателното право) ще приемем физическа интервенция върху обект (убийство, телесна повреда, разрушаване, повреждане и пр.). Обектите са хора, превозни средства и сгради.

Кибертероризмът е преднамерена, политически мотивирана атака срещу компютърни системи, компютърни програми или данни, създаваща опасност за гибел на хора, разрушения и причиняване на имуществени загуби, той е тероризъм, при който за постигане на политическите цели се използват високи технологии, т.е. персоналните компютри и връзките между тях – различните мрежи, включително и Интернет. Кибертероризмът не трябва да бъде разглеждан като отделно явление, а като продължение на терористични актове и тактики в киберпространството.

Основни обекти на кибертерористите са информационните системи, управляващи сложни технологични процеси, както и информационните системи в държавното управление, финансите, отбраната и т. н. Способите, които кибертерористите използват, са нерегламентирано проникване в компютърните мрежи, кражба на бази от данни, на програмно осигуряване, промяна на информацията в базите от данни, унищожаване на програмно осигуряване и бази от данни и други. Като сфери на злонамерено използване на високите технологии за терористични цели могат да се посочат:

- комуникацията между терористи и терористични групи при подготовката на терористичните актове;
- набирането на средства и хора за терористичните групи;
- пропагандата на тероризъм като средство за постигане на определени цели;
- разпространението на информация относно средствата и начините за извършване на терористични актове;
- комуникацията с държавните органи и институции на страните, подложени на натиск от терористите (обявяват целите и исканията си).

Като терористични цели могат да бъдат избрани:

- физически лица, представители на политическите и дипломатическите среди;
- управлението на обекти на критичната инфраструктура (железопътен и въздушен транспорт, съобщенията, електроснабдяването);
- хидротенически съоръжения – язовири, плавателни канали;
- атомни електроцентрали;
- военни обекти;
- обществени сгради (офис сгради, хотели, кинотеатри и др.);
- финансови институции.

Днес светът е пред избор: или държавите ще забравят политическите разногласия и ще обединят усилията си в борбата срещу тероризма, или терористите ще унищожат постиженията на човешката цивилизация и светът ще се върне към

варварски отношения, основани на сила и жестокост, които пренебрегват живота и достойнството на личността. Международната общност следва да създаде нова концепция за отношенията и сътрудничеството между държавите, с цел да се избегнат опасностите на тероризма .[**15**].

Интензивното развитие на европейската интеграция допринася за обединяване на усилията на държавите членки и включване в нейния предмет на сътрудничеството между тях в борбата срещу трансграничните престъпления, което от своя страна да позволи по-тясно взаимодействие и сътрудничество извън утвърдените традиционни принципи и механизми на международното публично право. Именно това предполага и наличието на редица инструменти и механизми, които осигуряват по-бързо, по-облекчено и ефективно взаимодействие за разлика от възможностите, уредени от съвременното международно публично право.

Международното сътрудничество в борбата срещу тероризма се развива в три области: издигане ролята на международния съд; прилагане на икономически санкции срещу държавите, които поощряват терористични групи; разработване на международни договори относно борбата с тероризма.

През последните няколко години бяха приети основополагащи международни документи в сферата на противодействието на тероризма в световен мащаб, между които:

- глобална стратегия и План за действие на ООН;
- стратегия и план за действие на Европейския съюз за борба с тероризма;
- стратегия и план за действие на Европейския съюз против радикализацията и набиране на терористи;
- инициативи и директиви на Съвета на Европейския съюз и на Европейската комисия, касаещи противодействие на финансирането на тероризма, сигурността на експлозивите, защитата на европейската критична инфраструктура и др.

След терористичния акт в САЩ на 11 септември 2001 г., и особено след бомбените атентати в Мадрид на 11 март 2004 г. и Лондон на 7 юли 2005 г., се взеха редица мерки, за да се създадат условия подобни трагедии да не се случват повече. Многобройни бяха действията, предприети от редица органи в ЕС, за предотвратяване на терористични актове от всякакъв характер във всички сфери на обществено икономическия живот на страните-членки на Съюза. Съвместните усилия доведоха до приемането на 30 Ноември 2005 г., от Съвета на Европа, документ, обединяващ изискванията на всички участници, а именно, Стратегията на ЕС за борба срещу тероризма „**The European Union Counter-Terrorism Strategy" („Стратегията").** Началото на реализацията на обединените действия на страните-членки и ЕС срещу тероризма обаче, беше поставено през месец юни 2004 г. с приемането от Европейската Комисия на План за действие за борба срещу тероризма **„The Action Plan to Combat Terrorism**". [**1**]

През м. март 2004 г. Европейския Съвет приема Декларация за борба срещу тероризма, поставяйки приоритетите на Съюза в тази област. През месец юни Съвета приема План за действие срещу тероризма. На основата на заложените в Плана дейности за кратко време в значителна степен се повишава сигурността на летищата и въздухоплавателните средства.

В подкрепа на Плана през 2005 г. се приемат две ключови Директиви: третата Директива срещу прането на пари " Money Laundering Directive" и Директивата за повишаване на сигурността на пристанищата **„Directive on Enhancing Port**

Security". През същата година започва да функционира и **Европейска Агенция за границите (FRONTEX)**. Съвместно с EUROPOL и EUROJUST (European Union Judicial Cooperation Unit) FRONTEX създава мрежата от изпълнителни органи за повишаване сигурността на външните граници на ЕС.

Като естествен връх на тези усилия, на срещата на министрите на правосъдието и вътрешните работи в Нюкасъл през 2005 г. се предлага приемането на Европейска Стратегия за борба срещу тероризма „The European Union Counter-Terrorism Strategy", която полага като основа за борбата срещу тероризма четири основни направления от действия (четири основни „стълба") – **превенция, защита, преследване и отговор на заплахите**. Тя изисква от всички, на национално, Европейско и международно нива да направят всичко необходимо да намалят заплахата от тероризъм и повишат нашата способност за защита и възможностите ни адекватно да отговорим на предизвикателствата на „чумата" на 21-ви век. Стратегията поставя редица цели за предотвратяване на присъединяването нови членове към терористичните организации, за по-добра защита на потенциалните цели на терористите, за преследване и разследване на членовете на съществуващите терористични мрежи и подобряване на нашата способност за отговор и управление на последствията от терористичните атаки.

На основата на така идентифицираните четири „стълба" ЕС, в изпълнение и на своята Стратегия в областта на Сигурността „European Security Strategy", обявява своя ангажимент за поемане на отговорност при поддръжката на глобалната сигурност.

Чрез Стратегията за борба срещу тероризма ЕС се стреми да допринесе за:

- укрепване на националните способности;
- улесняване на европейското сътрудничество;
- развитие на колективните способности;
- насърчаване на международното сътрудничество.

Защитата на Европейските граници е ключовият момент в Стратегията. Докато страните-членки имат като основна задача и отговорност да подобряват защитата на ключови потенциални цели на тероризъм, взаимната зависимост на сигурността на границите, транспорта и трансграничната инфраструктура изискват обединените усилия на ЕС. Единодушно се приема, че насочеността на последните трябва да бъде обърната към външните граници на Съюза, с цел предотвратяване на евентуално проникване и действие на терористи на негова територия (именно затова Стратегията и изпълнението ѝ са от особена важност за България, от гледна точка на двете външни граници на нашата страна, които са външни и за ЕС – южна сухоземна и източна морска).

За практическото приложение на предвидените действия ЕС създава Европейска Агенция за границите (FRONTEX) и формулира и изгражда визова информационна система (Visa Information System) и втората генерация на Шенгенската информационна система (Schengen Information System). Целта на Агенцията е да извършва оценка на риска като част от усилията за повишаване на контрола и наблюдението на външните граници, а двете информационни системи дават възможност за размяна в реално време на информация за желаещите да влязат в Еврозоната и при необходимост да им бъде отказан такъв достъп.

Отчитайки необходимостта от нови технологии, които да осигурят повишаване на сигурността на летища, авто и ЖП гари, пристанища, основни пътища и инф-

раструктура, Стартегията изисква по-пълноценното използване на изследователските и развойни програми на Европейската Комисия. Тя определя и ключовите приоритети, които трябва да бъдат следвани, за да се постигне надеждна и сигурна защита на потенциално опасните за терористично въздействия обекти:

- повишаване на сигурността на паспортите на жителите на ЕС чрез включване на биометрични данни в тях за притежателите им;
- изграждане на Visa Information System и втората генерация на Schengen Information System;
- разработване чрез FRONTEX на ефективен анализ на риска за външните граници на ЕС;
- прилагане на общоприети стандарти за сигурност на авиацията, летищата, пристанищата и плавателните съдове;
- приемане на Европейска програма за защита на критична инфраструктура;
- установяване на най-доброто ниво на изследванията в тази област в ЕС.

Утвърждаването на Европейската Стратегия за отбранителни изследвания и технологии European Defence Research&Technology Strategy, от министрите на отбраната на страните-членки на ЕС през месец ноември 2008 г., е необходимост, породена от логиката, следвана от Европейската политика в областта на сигурността и отбраната. От друга страна, създаването на Стратегията позволи на Европейската Агенция по отбрана (EDA) да изпълни по най-добрия начин задълженията си в следните области:

а) разработване на отбранителни способности за управление при кризи;

б) повишаване и разширяване на Европейското сътрудничество в областта на въоръженията;

в) заздравяване на отбранително-технологичната индустриална база;

г) увеличаване на ефективността на Европейските отбранителни изследвания и технологии.

Разработването на Европейска Стратегия за отбранителни изследвания и технологии е в унисон с Плана за развитие на способности и Европейската стратегия за отбранително-технологичната и индустриална база (приета на 14 май 2007 от EDA). Синергията между тези три документа, съвместно с Европейската стратегия за въоръженията, дава възможност да бъде постигната основната цел за подобряване на Европейските отбранителни способности. Хармонизирането на военните изисквания, и в резултат на това увеличаването на сътрудничеството между страните-членки, са основните пътища за удовлетворяване на Европейските отбранителни потребности и осигуряването на така желаната автономия на Европа в жизнено важните за сигурността й области.

Стратегията създаде така необходимите условия за определяне и систематизиране на ключовите технологични области и необходимите научно-изследователски капацитети за научното осигуряване на отбранителните потребности за изграждане на способностите. Определянето на списък с 22 приоритета в областта на Defence R&T, обслужващи отбранителните потребности и индустриални способности на страните-членки, осигури сърцевината на Стратегията. Основно предимство на Стратегията е, че тя представя приоритетите в изследванията и технологиите като резултантна от приоритетите, установени с Плана за развитие на способностите (Capability Development Plan), като по този начин тясно ги свързва с постигането на планираните отбранителни способности.

От друга страна, Стратегията поставя въпроса за изследванията и технологиите като „крайъгълен камък" и свързващо звено между отбранителни способности и адекватна отбранително-технологична индустриална база, което се явява ключов момент в процеса на удовлетворяването на отбранителните потребности. Това е маркера, нивото и развитието на който показва степента на удовлетвореност на способностите. Необходимо е да се отбележи, че:

1. В рамките на ЕС е разработена стройна система за реализацията на Европейската политика за сигурност и отбрана, в частта борбата срещу тероризма, с ясно очертана йерархия и взаимна обвързаност между отделните й елементи;

2. За всеки елемент на системата са създадени писмени секторни политики, които регламентират провеждането на необходимите дейности за достигане на очакваните резултати.

3. Сърцевината на системата е определянето на:

- необходимите отбранителни способности на ЕС;

- необходимите научно - изследователски капацитети за научното осигуряване на отбранителните потребности за изграждане на способностите;

- необходимата отбранително-технологична индустриална база за обезпечаване на технологичното ниво на потребностите, създавайки превъзходство в способностите.

4. В същото време обаче, проблематиката, свързана с изследванията и технологиите за борба срещу тероризма, не е охарактеризирана с ясни изисквания по приоритетни научи направления, не са поставени акцентите за всяко едно направление и матрицата от способности, които искаме да постигнем, не е разположена във времето. Т.е., на практика не става ясно как, по какъв начин изследванията и технологиите ще допринесат за борбата срещу източника на заплахата (S-strategy) и защитата на отделния индивид и инфраструктурата (L-strategy).

По отношение на критичната инфраструктура, след 2004 г., в контекста на борбата срещу международния тероризъм, политиката на Европейския съюз по нейната защита се развива много динамично. През ноември 2005 г. Европейската Комисия прие Зелена книга за Европейска програма за защита на критичната инфраструктура. На тази основа, през 2006г., ЕС стартира Европейска програма за защита на критичната инфраструктура (European Programme for Critical Infrastructure Protection - EPCIP), като в процес на разработване е и Информационна мрежа за предупреждение за критичната инфраструктура (CIWIN–Critical Infrastructure Warning Information System). От друга страна, утвърдена е и Директива на Съвета от декември 2006 г., относно идентификацията и обезпечаването на Европейската критична инфраструктура и оценка на необходимостта за подобряване на нейната защита.

Всичко това е огромна по своя обем и съдържание работа, но не е осъществена тясна взаимовръзка между разглежданите документи (Стратегията на ЕС за борба срещу тероризма, European Defence Research&Technology Strategy и регламентациите за защитата на критичната инфраструктура), което не допринася за постигане на най-добрите резултати в изграждането на адекватни способности за противодействие на заплахите от тероризъм.

Могат да се посочат следните международни актове за противодействие на тероризма и кибертероризма:

1) Европейска конвенция за борба с тероризма;

2) Конвенция за борба с незаконното завладяване на самолети (в сила за България от 14.10.1971 г.);

3) Конвенция за забрана на разработването, производството и натрупването на запаси от бактериологично (биологично) и токсични оръжия и за тяхното унищожаване (в сила за България от 26.03.1975 г.);

4) Конвенция за забрана на разработването, производството, натрупването и употребата на запаси от бактериологично и химическо оръжие (в сила за България от 29.04.1997г.);

5) Конвенция за предотвратяване и наказание на престъпления срещу лица, ползващи се с международна защита, в това число дипломатическите агенти (в сила за България от 21.06.1977 г.);

6) Конвенция за преследване на незаконните актове, насочени против безопасността на гражданската авиация (в сила за България от 24.03.1973 г.);

7) Конвенция за преследване на незаконните действия, насочени срещу сигурността на морското корабоплаване (в сила за България от 06.10.1999 г.)

8) Конвенция за ядрената безопасност (в сила за България от 01.11.1996 г.);

9) Конвенция на Съвета на Европа за предотвратяване на тероризма (в сила за България от 01.06.2007 г.);

10) Международна конвенция за борба с бомбения тероризъм (в сила за България от 14.03.2002 г.);

11) Международна конвенция за борба с вземането на заложници (в сила за България от. май 1988 г.);

12) Международна конвенция срещу финансирането на тероризма (в сила за България от 15.05.2002г.).

13) Конвенция на Съвета на Европа за престъпления в кибернетичното пространство, от 23 ноември 2001 г., подписана от нашата страна и влязла в сила.

Овен приемането на конвенции, страните членки на ЕС на различни свои срещи приемат и пакети от мерки за борба с тероризма, където се предвиждат различни мерки за засилване на контрола по летища, ЖП и автогари, както и задълбочаване на сътрудничеството между правозащитните органи на ЕС. По отношение на европейските органи е необходимо да се посочат двата правозащитни органа (служби) – „Европол" и „Евроюст".

„Европол" (Europol) е правоохранителна организация на Европейския съюз, която разполага и се занимава с информация по криминалните въпроси. Нейната цел е да усъвършенства оперативното сътрудничество между компетентните органи на държавите-членки в предотвратяването и борбата с мащабната организирана международна престъпност и тероризма. Към нейните главни задачи, освен борбата с трафика на хора, прането на пари и други е включена и борбата с тероризма.

Другата правоохранителна организация е „Евроюст". Това е нов орган на Европейския съюз, създаден през 2002 г. за повишаване на ефективността на компетентните органи в държавите-членки в борбата им срещу тежката трансгранична и организирана престъпност. "Евроюст" стимулира и подобрява координацията на разследването и съдебното преследване, както и подкрепя държавите-членки в усилията им за повишаване на ефективността на разследването и съдебното преследване. Неговата основна задача е да укрепва общоевропейското сътрудничество в борбата с организираната престъпност.

Специалните закони срещу организираната престъпност и тероризма в различните страни съдържат предимно мерки от процесуално естество: изземване и конфискация на имущество, придобито чрез престъпление; електронно следене на

заподозрените; други мерки за персонален контрол; специфични правила за разследване и събиране на доказателства (например Европейската конвенция за мерките срещу изпирането на пари).

Могат да се посочат правните норми в националното законодателство за противодействие на тероризма и кибертероризма:

1).Наказателноправна характеристика на тероризма в Наказателен кодекс на Република България [13]:

Тероризмът е вид престъпление по българския НК и е регламентиран в глава I – Престъпления против Републиката, раздел IV, чл.108а НК.

Чл. 95. (Изм. - ДВ, бр. 50 от 1995 г., изм. - ДВ, бр. 153 от 1998 г.) Който с цел да бъде съборена, подровена или отслабена властта в републиката участва в извършването на опит за преврат за насилствено завземане на властта в центъра или по места, или в бунт, или във въоръжено въстание, се наказва с лишаване от свобода от десет до двадесет години, с доживотен затвор или с доживотен затвор без замяна.

Чл. 96. (Изм. - ДВ, бр. 41 от 1985 г.) (1) (Доп. - ДВ, бр. 50 от 1995 г., изм. - ДВ, бр. 153 от 1998 г.) Който с цел да подрови или отслаби властта в републиката или да й създаде затруднения лиши от живот държавен или обществен деятел, се наказва с лишаване от свобода двадесет години, с доживотен затвор или с доживотен затвор без замяна.

(2) Който със същата цел причини тежка телесна повреда на такова лице, се наказва с лишаване от свобода от пет до петнадесет години.

(3) (Доп. - ДВ, бр. 50 от 1995 г., изм. - ДВ, бр. 153 от 1998 г.) Който с целта по ал. 1 чрез палеж, взрив, наводнение или друго общоопасно деяние причини смърт на едно или повече лица, се наказва с лишаване от свобода от петнадесет до двадесет години, с доживотен затвор или доживотен затвор без замяна.

Чл. 97. (Доп. - ДВ, бр. 50 от 1995 г., изм. - ДВ, бр. 153 от 1998 г.) Който с посочената в предходния член цел извърши общоопасно престъпление по чл. 349 или 350, се наказва с лишаване от свобода от десет до двадесет години, с доживотен затвор или с доживотен затвор без замяна.

Чл. 97а. (Нов - ДВ, бр. 41 от 1985 г.) (1) Който с целта по чл. 96 задържи някого като заложник, чието освобождаване поставя в зависимост от изпълнението на определено условие от страна на държавата, на държавна или обществена организация или на трето лице, се наказва с лишаване от свобода от три до десет години.

(2) Когато в случаите по предходната алинея деецът заплашва, че ако поставеното от него условие не бъде изпълнено, ще причини смърт или тежка или средна телесна повреда на задържания, наказанието е лишаване

Чл. 106. (Доп. - ДВ, бр. 50 от 1995 г., изм. - ДВ, бр. 153 от 1998 г.) Който с цел да отслаби властта или да й създаде затруднения унищожи или повреди обществени сгради, строежи, инсталации, съоръжения, транспортни или съобщителни средства или друго значително обществено имущество, се наказва за диверсия с лишаване от свобода от пет до петнадесет години, а в особено тежки случаи - с лишаване от свобода двадесет години, с доживотен затвор или с доживотен затвор без замяна.

Чл. 107. Който с цел да отслаби властта или да й създаде затруднения разстройва или подравя промишлеността, транспорта, селското стопанство, паричната и кредитната система, други стопански отрасли или отделни стопански предприятия,

като използва държавни учреждения, стопански предприятия или обществени организации, като възпрепятства тяхната дейност, или като не изпълнява възложените му важни стопански задачи, се наказва за вредителство с лишаване от свобода от три до десет години, а в особено тежки случаи - с лишаване от свобода от пет до петнадесет години.

Чл. 108а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Който с цел да създаде смут и страх в населението или да заплаши, или да принуди орган на властта, представител на обществеността или представител на чужда държава или на международна организация да извърши или пропусне нещо в кръга на неговите функции, извърши престъпление по чл. 115, чл. 128, чл. 142, чл. 143, чл. 143а, чл. 216, ал. 1 и 5, чл. 326, чл. 330, чл. 333, чл. 334, чл. 337, чл. 339, чл. 340, чл. 341а, чл. 341б, чл. 344, чл. 347, ал. 1, чл. 348, чл. 349, чл. 350, чл. 352, ал. 1, 2 и 3, чл. 354, чл. 356е, чл. 356з, се наказва за тероризъм с лишаване от свобода от пет до петнадесет години, а когато е причинена смърт - с лишаване от свобода от петнадесет до тридесет години, доживотен затвор или доживотен затвор без замяна.

(2) (Изм. - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Който по какъвто и да е начин, пряко или косвено, събира или предоставя финансови или други средства за извършване на престъпление по ал. 1, като знае или предполага, че те ще бъдат използвани с такава цел, се наказва с лишаване от свобода от три до петнадесет години и глоба до тридесет хиляди лева.

(3) (Нова - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Който набира или обучава отделни лица или групи от хора с цел извършване на престъпление по ал. 1, се наказва с лишаване от свобода от две до десет години.

(4) (Предишна ал. 3 - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Предметът на престъплението по ал. 2 се отнема в полза на държавата, а ако липсва или е отчужден, присъжда се неговата равностойност.

Чл. 109. (Изм. - ДВ, бр. 99 от 1989 г.) (1) (Изм. - ДВ, бр. 92 от 2002 г., изм. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г.) Който образува или ръководи организация или група, която си поставя за цел да извършва престъпления по тази глава, се наказва с лишаване от свобода до дванадесет години, но не повече от наказанието, предвидено за съответното престъпление.

(2) (Изм. - ДВ, бр. 92 от 2002 г., доп. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г.) Който членува в такава организация или група, се наказва с лишаване от свобода до десет години, но не повече от наказанието, предвидено за съответното престъпление.

(3) (Нова - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Когато организацията или групата си поставя за цел да извършва престъпление по чл. 108а, наказанието е:

1. по ал. 1 - лишаване от свобода от десет до двадесет години;

2. по ал. 2 - лишаване от свобода от две до десет години.

(4) (Изм. - ДВ, бр. 95 от 1975 г., изм. - ДВ, бр. 92 от 2002 г., доп. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г., предишна ал. 3 - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Участник в организацията или групата, който доброволно се предаде на органите на властта, разкрие всичко, което му е известно за организацията или групата и по този начин съществено улесни разкриването и доказването на извършени от нея престъпления по тази глава, се наказва при условията на чл. 55.

(5) (Изм. - ДВ, бр. 92 от 2002 г., доп. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006

г., предишна ал. 4 - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Не се наказва участник в организацията или групата, който доброволно се предаде на властта и разкрие организацията или групата, преди да е извършено от нея или от него друго престъпление по тази глава.

Чл. 110. (Изм. - ДВ, бр. 99 от 1989 г., изм. - ДВ, бр. 92 от 2002 г.) За приготовление към престъпление по чл. 95, 96, 99, 106, 107 и чл. 108а, ал. 1 наказанието е лишаване от свобода до шест години.

Чл.108 а НК включва: Престъпления срещу личността (убийство, тежка телесна повреда, отвличане): чл. 115 НК; чл. 128 НК; чл. 142, ал. 1НК.

Престъпления срещу собствеността - чл. 216, ал. 1 НК.

Престъпления против реда и общественото спокойствие

чл. 326 НК (подаване на неверни сигнали за помощ или злополука по радио, телефон); чл. 330, ал. 1 НК; чл. 333 НК; чл. 334, ал. 1 НК; чл. 337, ал. 1 НК; чл. 339, ал. 1 НК

Престъпления по транспорта и съобщенията - чл.340, ал. 1 и 2 НК; чл. 341а, ал. 1 – 3 НК; чл. 341б, ал. 1 НК; чл. 344 НК; чл. 347, ал. 1 НК; чл. 348 НК

Престъпления против народното здраве и околната среда - чл. 349, ал. 1 и 3 НК; чл. 350, ал. 1 НК; чл. 352, ал. 1 НК; чл. 354, ал. 1 НК

Престъпления при използване на атомната енергия за мирни цели - чл.356 е, ал. 1НК; чл. 356з НК

2) Наказателноправна характеристика на компютърните престъпления (вкл. и кибертероризма) в Наказателен кодекс на Република България:

В Република България правната уредба на компютърните престъпления е създадена с измененията на Наказателния кодекс (НК) от септември 2002 г. (ДВ, бр. 92 от 2002 г.). Систематично основната част от съставите на компютърните престъпления са обособени в новосъздадената глава девета “а”, озаглавена “Компютърни престъпления”. Единствено компютърната измама (чл. 212а НК) е уредена в главата за престъпленията против собствеността, преди всичко поради близостта и с класическия състав на измамата по чл. 212 НК.

Новите състави за шест вида компютърни престъпления се съдържат в Глава девета “а” от Наказателния кодекс.

Първият от тях се отнася за нерегламентиран достъп до ресурсите на компютър, копиране и използване на компютърни данни без разрешение - чл. 319 а.

Вторият от тях се отнася за престъпни посегателства срещу компютърни програми или данни - чл. 319б и чл. 319в.

Третият от тях се отнася за компютърни вируси - чл. 319г.

Четвъртият от тях се отнася за разпространяване на компютърни или системни пароли - чл. 319д.

Петият от тях се отнася за престъпления във връзка със Закона за електронния документ и електронния подпис- чл. 319е.

Шестият от тях се отнася за компютърна измама - чл. 212а.

Върху територията на страната ни вече си взаимодействат три правни системи: националното законодателство, международното право по силата на чл. 5, ал. 4 от Конституцията на Република България и правото на Европейския съюз.

Основните фактори, определящи опасността от разрастването на кибертероризма се изразяват преди всичко с:

- проникването в глобалната информационна среда и моделирането на определе-

ни психологически и социални нагласи в интерес на терористичните организации;

- създаване на благоприятни условия за разпространение на ислямистки и радикални идеи;

- компрометиране дейността на държавните и частни информационни мрежи;

- намаляване ефективността на военните, финансови и обслужващи сектори на икономически най-развитите демократични държави.

От изложеното дотук произтичат следните изводи:

1) Кибертероризмът е реално обществено опасно явление, съпроводено с използването на не по-малко насилие, отколкото при другите видове тероризъм. Той е още по-опасен за обществото, защото невинаги кибертеристите могат да бъдат в състояние да спрат вече предизвикан от тях процес, от който биха могли да произтекат големи щети.

2) В обозримо бъдеще кибертероризма ще остане основният проблем за сигурността на трансатлантическата общност. Използването на интернет от терористичните организации и групи показват, че по същество може да се говори за възникване и развитие на ново бойно поле на борбата срещу тероризма – глобалната информационна мрежа.

3) За да се борят ефективно срещу различните терористични групи и организираната престъпност държавите - членки на Европейския съюз трябва да си сътрудничат и да синхронизират техните правни системи. Трябва да се подпомагат нашите, европейските и въобще всички международни органи в борбата им с кибертероризма, а и с другите престъпления, тъй като не е важно колко конвенции и закони ще бъдат приети, ако те не се прилагат и не бъдат приведени в действие реални механизми за ограничаване и намаляване на престъпленията.

4) Българският законодател е длъжник на антитеристичната борба с кибертероризма, което налага необходимостта да се предвидят конкретни текстове, преследващи тази нова форма на тероризъм. Сближаването на нашето законодателство с това на страните от Европа може да послужи като допълнително сериозно основание за криминализацията на посочените деяния и в България. Промените в Наказателния кодекс ще увеличат капацитета на правораздавателните органи за противодействие на посочените престъпления и ще спомогнат за ограничаване и контролиране на престъпната дейност на кибертеристите.

Литература:

1) Концептуални характеристики на национална стратегия за изследвания и технологии за борба срещу тероризма, София април 2010 г.

2) Национален план за противодействие на тероризма от 2009 г.

3) Г. Стоянов – „Тероризмът (Генезис и проявление)" – ВИ 2003 г.

4) Р. К. Стоянов – "Кибертероризмът (Ахилесовата пета на глобалното общество)" – сборник материали Тероризъм, медии, сигурност, 2007 г.

5) Атлас на „Монд дипломатик" - Кибертероризъм, Информационната война - раздел „Нови конфликтни взаимоотношения на международната сцена", 2009 г.

6) Конвенция на Съвета на Европа за предотвратяване на тероризма (в сила за България от 01.06.2007 г.);

7) Европейска конвенция за борба с тероризма (в сила за България от 18.05.1998 г.);

8) Конвенция за преследване на незаконните действия, насочени срещу сигур-

ността на морското корабоплаване (в сила за България от 06.10.1999 г.)

9) Международна конвенция за борба с бомбения тероризъм (в сила за България от 14.03.2002 г.);

10) Международна конвенция за борба с вземането на заложници (в сила за България от. май 1988 г.);

11) Международна конвенция срещу финансирането на тероризма (в сила за България от 15.05.2002г.).

12) Конвенция на Съвета на Европа за престъпления в кибернетичното пространство, от 23 ноември 2001 г., подписана от нашата страна и влязла в сила.

13) Наказателен кодекс в сила от 1.05.1968г, изм. ДВ. бр.33 от 26 Април 2011г.

14) Михаил И. Илиев – "Тероризъм - европейско сътрудничество и органи за борба с тероризма".

15) „Правни мерки за борба с тероризма" - доклад на Гл. прокурор на Р. България, изнесен на конференция в Кран Монтана – 25 – 26 юни 2004 г.

ИНФОРМАЦИОННА СИГУРНОСТ

НОВИ ФОРМИРОВАНИЯ ЗА ДЕЙСТВИЯ В КРИТИЧНИ СИТУАЦИИ И ТЯХНОТО ИНФОРМАЦИОННО ОСИГУРЯВАНЕ

Маргарита В. Филипова, Костадин Н. Костадинов

РУ"А.Кънчев", катедра "ЕООС", mfilipova.vt@mail.bg , тел.+359 82 888 418;

НВУ"В. Левски", koce_knk@abv.bg, тел.+359 62 61 611

NEW FORMIROVATIYA FOR ACTION IN CRITICAL SITUATIONS AND THEIR INFORMATION SECURITY

MARGARITA V. FILIPOVA, KOSTADIN N. KOSTADINOV

Bulgaria, University of Rousse, Departament of ecology and environmental protection, mfilipova.vt@mail.bg, phone: +359 82 888 418; NVU"V. Levski", koce_knk@abv.bg, phone: +359 62 61 611

ABSTRACT: Technogenic emergencies and disasters accompany our lives. Possible consequences of them are causing material damage and human casualties. Liquidation of the consequences of particular importance is the provision of information and support between existing units to meet the new conditions and dynamics of events.

KEY WORDS: group risk materials , accidents, toxic chemicals.

1. Въведение

Аварийни ситуации техногенен характер могат да възникнат при определени условия, каквито най-често се явяват: техническа неизправност на техническа система, нарушение на технологичния процес при реализиране на даден тип производство, небрежност на човешкият фактор при работа от различно естество, неспазване на изискванията на пожарната и аварийна безопасност и др.

За успешното управление на аварийни ситуации и опасни материали –емисии, при тяхната реализация е от изключително значение правилната и навременна оценка на текущата информацията I_t^{AS}, съдържаща данни за наличие на опасности, преценка на рисковете, както и информационното осигуряване между действащите формирования. Вземането на решение за намеса, или по-често ненамеса на основата на I_t^{AS}, е отговорна и трудна задача. Повечето командири на екипи признават необходимостта от първоначално изолиране на района и идентифицира-

не на промишлени химични токсични вещества (ПТХВ) или бойни химични токсични вещества (БТХВ), но много други все още пренебрегват необходимостта от прилагане на систематичен и аналитичен подход към разрешаването на възникнал проблем [1]. За целта се налага да се обособят специализирани формирования, които на базата на текущата информацията да прилагат аналитични методи за локализация на Аварийни ситуации от техногенен характер.

1. Дефиниране на проблема. След настъпилите обществено-икономически промени в края на 80-те и началото на 90-те години „колосите" на плановата икономика поставят сериозни предизвикателства в екологично и аварийно-превантивно отношение [2]. Започва раздържавяването на тези промишлени предприятия, което допълнително повишава аварийния риск от техногенни катастрофи от различен вид. Степента на риска се определя допълнително и от липсата на гъвкава и осъвременена нормативна база, която адекватно да регулира създалите се противоречия между опасност и безопасност в дадени региони в Република България. В същото време отпадат обектовите и общински групи - формирования, обучени за действие при възникване на потенциални тежки промишлени аварии, съпроводени с изпускане химични токсични вещества (ХТВ). Службите за действие при такива ситуации търпят постоянни метаморфози относно тяхното дислокация в държавната администрация и не само това - не се закупува ново оборудване и техника, които да се заложат на оперативно дежурство, което в значителна степен ще повиши тяхната ефективност. Разработените плановете за действие, методологията на обучение и стратегиите за използване на посочените формирования са остарели и не отговарят на съвременните изисквания. Всичко това в комплекс прави заводите и предприятията свързани особено с химическата промишленост да се превръщат в потенциални „бомби със закъснител" относно безопасността на хората в даден регион. Инсталациите и технологичните процеси в тях стават морално остарели и генерират опасности от различен вид. Вредностите, емитирани в атмосферата при реализацията на крайните продукти в такива предприятия, са в пъти над приетите норми в обединена Европа [3].

Присъединяването на България към Европейския съюз спомогна още в самото начало за хармонизиране на законодателството с европейското и за въвеждане на строги екологични правила и норми при построяването и реконструирането на предприятията от химическата промишленост, както и самото им функциониране. По тази причина много от тях бяха спрени от експлоатация, а други направо унищожени [4]. Независимо от взетите мерки в това направление тези, които продължават да поддържат производствените си мощности все още са в разрив с много норми от съвременното законодателство. Причините са различни, но като някои от основните могат да бъдат изтъкнати следните:

A. Старите технологични линии са с изтичащ ресурс и реконструкцията им според новото европейско законодателство е забавена;

B. Обезопасяването в екологично отношение струва скъпо - нужно е закупуването и изграждането на филтри, пречиствателни станции и хвостохранилища.

C. В условията на постоянна липса на финансови средства и занижен контрол от страна на компетентните институции, производството от химическия сектор се нарежда на едно от първите места по вредност и опасност. Новите предприятия се строят според наставленията, доколкото това е възможно, но старите трудно се сдобиват с ISO.

Формированията, свързани с националната сигурност и отбрана в Р. България, които отговарят за аварийната безопасност, все още нямат единни оперативни процедури за действие при аварии, свързани с изтичане на ПХТВ и БТХВ. Всяко министерство в нашата страна има вътрешноведомствени инструкции, служещи като една макрорамка за реакция при инциденти. Това е негативно явление, което при често променяща се законодателна уредба и постоянно преструктуриране на службите се проявява главно с липсата на координация в действията на всички екипи за незабавна намеса. И още - разнородното оборудване за провеждане на спасителни операции най-често е остаряло или с изтекъл ресурс. Наличното съвременно оборудване за детектиране при инциденти от такъв тип не е пригодено за действие в сложна обстановка, като тежка авария, съпроводена с имитиране на ХТВ, поради несъвместимост и липсата на единна информационна система. Масово апаратурата при локализация на аварии е специализирана за откриване и измерване на имитирани вредности с познат или вероятностен произход, но тя не позволява комплектност на измерванията. Проблемите от подобен характер се открояват при инциденти като този от 03.07.2008 г. в поделение за съхранение, разснаредяване и утилизация на бойни припаси в квартал Челопечене, гр. София.

Това налага необходимостта от нови мерки и способи, за създаване на формирования и информационното им осигуряване за незабавен отговор при аварии и инциденти с токсични вещества или „Рискови материали".

2. Примерна организация и действия на формированието „Рискови материали"

В България няма единен адекватен модел за действие и управление на подобни инциденти свързани с технологични аварии. Например в Българската армия и Главна дирекция "Пожарна безопасност и защита на населението" нямат регламентиран единен „изчистен" от дублиране механизъм за съгласуване на действията и информационно осигуряване, по проблемите, свързани с авариите и начините за тяхното ликвидиране. В различните закони и подзаконови нормативни актове се срещат различни наименования на специалистите и длъжностите, участващи в ликвидирането на определен тип инциденти. Няма също така точно определен алгоритъм за действие и оперативни разчети за нужните сили и средства при ликвидирането на даден инцидент. В този процес трябва да се включат активно представители на Центровете за спешна медицинска помощ и да се възстанови професията парамедик.

Следователно България има остра нужда от хармонизиране и уеднаквяване на оперативните процедури при гражданско-аварийното и военно планиране, неотложна нужда от модернизиране на материалната база и уеднаквяване, кодифициране на оперативно-тактическите процедури за действие в такива ситуации, чрез използване на най-добрите световни практики в тази област.

Целта на хармонизиране е преди всичко в оценяване на риска е създаването на план на действие за ликвидиране на инцидента. Той трябва да включва стратегически и тактически цели за неговото ликвидиране. На тези цели са подчинени операциите по незабавна намеса - да се намали нивото на риска за служителите от единната спасителна система - аварийни екипи, обществото и околната среда. При това задачата на службите за защита на населението трябва да бъде преценка на риска, своевременното информиране на всички заинтересовани страни, а не неговото поемане.

Аварийните екипи трябва да е в състояние да прогнозира поведението на тех-

никата, технологиите и инсталациите, участващи в инцидента. Основният принцип при развитие на такива инциденти предизвикващи аварии е: Съществуват само две опасности за аварийните екипи и те произтичат от освободената енергия и свойствата на веществата и тяхното взаимодействие. За целта своевременно трябва да бъдат определени обектите, които вероятно ще бъдат засегнати от замърсяването. След като установят типа и естеството на потенциалните опасности, аварийните екипи могат да започнат оценката на риска и набелязването на защитните мероприятия, следващи от него.

В зависимост от обхвата и сложността на аварията, специалните екипи – обединени като формирования, в които обикновено се привличат сапьори, пожарникари, технически спасители като химици, дозиметристи, алпинисти и други специалисти се управляват, като *екип или група в рамките на системата за управление на инцидента*. Те могат да бъдат обединени в група, отряд или екип „Рискови материали" чиято структура е демонстрирана на фиг. 1.

Фиг. 1. Организация на група „Рискови материали"

Основните задачи и дейности на групата „Рискови материали" Фиг.1 се свеждат до следното: екипът, занимаващ се с опасни материали, е под командването на командир, който на свой ред е подчинен на командващия операциите. Отговорностите на групата са пряко свързани с всички операции по издирване на опасни материали в горещата и топлата зони на инцидента. Тактическите операции, извън тези контролирани зони с рискови материали (например действия по защита на населението) не са в компетенциите на групата. Ръководните длъжности в групата за рискови материали и основните им задачи могат да се обобщят така:

1. Служител по безопасността – той е ръководителят на групата за рискови материали. Отговаря за използването на безопасни процедури и спазването им по време на овладяване на инцидента. Правомощията и задълженията му са свързани със спиране на всички опасни действия и коригиране при необходимост на прилаганите методи и способи;

2. *Служител, контролиращ влизането/излизането в горещата зона* – отговоря за всички операции в горещата зона, включително разузнаване, наблюдение, вземане на проби и намаляване на риска. Отговаря за служителите влизащи и излизащи от зоната, а така също и за резервните екипи;

3. *Служител по деконтаминация* - отговаря за изпълнението на плана и дейностите по деконтаминацията, изграждането и функционирането на площадката или пункта за деконтаминация. Ръководи и контролира качеството и степента на обработка на персонал, пострадали, както и оборудването в зависимост от експозициите. Също така той *отговаря и за координацията по евакуацията в безопасната зона;*

4. Служител по контрол разпространението на рисковите материали - определя контролираните зоните. Под негово ръководство се извършва наблюдението за неразпространението на рисковите материали, отговаря за извършване на мероприятия по неразпространение на замърсителите. Освен това той наблюдава движението на целия личен състав и оборудването между контролираните, опасни зони. При нужда координира евакуационните мероприятия;

5. Служител по информацията - отговаря за събиране, анализиране, координиране и разпространение на всички данни и информация по отношение на възникналия инцидент. Тези данни и информация се използват от групата за рискови материали при определяне на опасностите и оценка на риска, адекватните мерки по защита на населението, изборът на ЛПС, както и разработването на плана за действие.

Освен посоченото в (1-5) всяка такава група трябва да включва и следните експертни длъжности :

А. Медицинско лице - отговоря за медицинското наблюдение и контрол на персонала преди и след влизането в опасната зона и осигурява медицинското ръководство на Групата за рискови материали, според изискванията;

В.*Служител по материално-техническото осигуряване* - отговоря за контрола и движението на всички доставки и оборудване, използвано от Групата за рискови материали по време на инцидента/аварията, включително документиране на доставките и разходваните материали. Подчинен е на лицето от кризисния щаб, отговарящо за ресурсното осигуряване.

Посочената примерна структура и длъжностите лица Фиг.1. позволява формирането на две паралелно работещи подструктури, които обединяват „командира на инцидента" и „комуникационно - информационен пункт" в една обща схема за работа, което в значителна степен издига ролята на информационното осигуряване при локализиране разнообразните аварийни ситуации от техногенен характер.

3. Информационно осигуряване локализирането аварийни ситуации от техногенен характер

Известно е, че информационното осигуряване е основополагаща дейност за успеха при **локализирането аварийни ситуации от техногенен характер** от дейността за органите за управление Аварийните екипи. Обикновено в информационното осигуряване се включва: събирането, обработването на информацията за инцидента, нейното обобщаване, подготовката на тази основа на данни за доклад на съответния ръководител, във и „комуникационно - информационен пункт" Фиг.1.; обмяната на информация за обстановката между органите за управление и разработването и представянето на отчетно-информационни документи; разработването на справочните документи.

Основните изисквания, които се предявяват към информационното осигуряване при обработка на текущата информацията I_t^{AS}, се явяват:

I. целеустременост S_t^{inf}, определяне на приоритетите на събирането, обработ-

ването и докладването (свеждането) на тази информация, която в създадената обстановка се явява най-важна в „комуникационно - информационен пункт";

II. непрекъснатост C_t^{inf} , се заключава в нейното водене по всяко време , при появяването на инцидента от всички източници на информация ;

III. активност A_t^{inf} , се постига в постоянния стремеж на органите за управление на информационните потоци;

IV. оперативност O_t^{inf} , се постига в събирането на определен срок на необходимата информация, нейното бързо и качествено обработване и незабавното докладване на ръководството.

V. достоверност D_t^{inf} се заключава в точното представяне на ситуацията във определено време.

VI. обективност O_t^{inf} се заключава в адекватното представяне на информацията с истинското състояние на обективната реалност

Редът на обработване на текущата информацията I_t^{AS} при отчитане посочените изисквания във всеки конкретен случай се определят от условията на обстановката при локализирането аварийни ситуации от техногенен характер. При това се отчита и критичното време T_{krit}^{Rea} за реакция на формированията. Последното определя качествата на представената информация K_{AS}^{inf} , която може да се представи от вида във функция от времето T_{krit}^{Rea} :

$$K_{AS}^{inf} = f(S_t^{inf}, C_t^{inf}, A_t^{inf}, D_t^{inf}, O_t^{inf}) \le T_{krit}^{Rea} \quad (1)$$

Представянето на необходимата информация в необходимото време (1) е комплексна задача, която налага развитието на интегрирана информационна среда за управление на ситуацията. Последното изисква и реализацията на единна информационна и комуникационна инфраструктура за управление на процесите при локализирането аварийни ситуации от техногенен характер.

За целта е необходимо изграждането на Информационна стратегия за задълбочено разбиране за облика на информационната среда и използването на перспективни информационни технологии и методи за вземане на решения при локализирането аварийни ситуации от техногенен характер. За целта се предлага използването на осемстъпков процес за управлението на силите и средствата при ликвидирането на крупни аварии с рискови материали. Този процес се използва от американските служби при отговор на терористични актове и инциденти и аварии, свързани с рискови материали.

Успешното начало за управлението на аварията през първия час се основава на следните умения:

a) да се открият индикатори, които сочат, че по своя характер инцидентът може да е терористичен акт или престъпление;
b) бързо да се овладее ситуацията;
c) да се установи обединено командване.

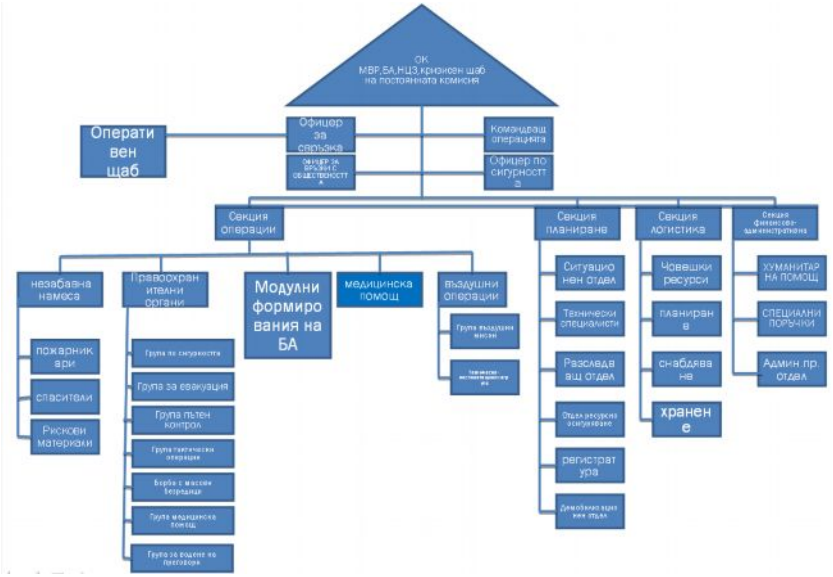
Главните фактори, служещи за индикатори, са:

a. Дали целта на атаката е определен обект или събитие?
b. Има ли данни за предишни заплахи?
c. Известни ли са причините?
d. Има ли много пострадали?
e. Има ли пострадали сред спасителните екипи?
f. Настъпили ли са вторични събития?

При работа на формированията алгоритъма на Осемстъпковият процес включва:

Управление и контрол на мястото на инцидента → Откриване на проблема →Оценка на опасността и риска →Избор на защитно облекло и оборудване →Управление на информацията и координация на ресурсите → Прилагане на стратегии за ответни действия → Операции по обеззаразяване и разчистване → Приключване на инцидента**.**

Посоченият алгоритъм може да се използва при структура на обединено командване при локализирането аварийни ситуации от техногенен характер (вариант) представена на фиг. 2.



Фиг. 2. Структура на обединено командване при локализирането аварийни ситуации от техногенен характер (вариант)

Структура на обединено командване при локализиране аварийни ситуации от техногенен характер съвместно с Групата за рискови материали може да се използва и като звено от Обединеното командване в борбата срещу терористични актове.

Изводи:

1. Предложено е създаването на модулни формирования „Рискови материали”, подчинени на обединено командване. Модулите се състоят от формирования на БА и ГД "Пожарна безопасност и защита на населението", а също и от представители на Центровете за спешна медицинска помощ.

2. Предложен е осемстъпков процес за управлението на силите и средствата при ликвидирането на крупни аварии с рискови материали или терористични актове, границата между които е все по-необозрима.

3. За извършване на първоначална експресна оценка на риска при конкретна авария или инцидент трябва да се създаде и използва единен софтуерен продукт, обезпечаващ вземането на решение от обединеното командване.

4. Описаните мероприятия, както и предложението за създаване на формирования „Рискови материали" ще гарантира успешното ликвидиране на аварии, свързани с рискови материали или терористични актове. Това ще спомогне за недопускане на излишна паника, намаляване до минимум на загубите на силите, средствата и негативното въздействие върху околната среда.

Литература:

1. Зюзин А. В. Защита производственного персонала и населения от силюодействувющих ядовитых веществ на химически опасных обектах,М., Мединор, 2008

2.Йонов К., Ванев Б., Експертни оценки, С., Техника, 1997

3. Садовникова Л., Экология и охрана окружающей среды при химическом загрязении, М., Высшая школа, 2006

4. www.mes.government.bg/ 04.2011

ИЗПОЛЗВАНЕ НА МРЕЖОВИ АНАЛИЗАТОРИ ЗА ПРИХВАЩАНЕ НА ТЕЛЕФОННИ РАЗГОВОРИ В IP МРЕЖИ

Веселина А. Гагъмова, Николай В. Пенев, Цветелин И. Цонев

София – 1504, Бул."Е. и Хр. Георгиеви" № 82, Военна академия "Г. С. Раковски", Факултет "Командно-щабен", катедра "КИС", сл.тел. (+3592)9226660, alexandv@yahoo.com; alexandv@md.government.bg; (+3592) 9226596, penevnv@abv.bg; alko@vlez.be

USING NETWORK ANALYZERS FOR INTERCEPTING AND RECORDING A VOIP TELEPHONY IN THE IP NETWORKS

Veselina A. Gagamova , Nikolay V. Penev, Tsvetelin I. Tsonev

ABSTRACT *The authors present information technologies, as so called network analyzer or "packet sniffer" software that can be used to support monitoring, control and troubleshooting networks. The Wireshark protocol analyzer's features and options such as capturing each protocol data unit (PDU) and displaying filtering of SIP and RTP protocols of VoIP are also presented.*

KEY WORDS *information security, computer networks and systems, packet sniffer, network analyzer, Wireshark, VoIP telephony, SIP and RTP protocols*

С все по-широкото използване на Internet във военната област, нарастват заплахите от кибератаки, които при определени условия могат да прераснат в кибервой-

ни [1]. Методите и практиките за водене на кибервойни са разнообразни и са свързани с архитектурата на киберпространството, в което централно място заемат IP мрежите. Основен метод за водене на офанзивни кибервойни са кибератаките срещу мрежите. Те повреда на системно и приложно програмно осигуряване, кражба на критична информация, фалшификация на информацията, злоупотреба с ресурси на организацията, кражба на услуги, записване и използване на мрежовия трафик на организацията от външни лица, разрушение на информация, инсталиране на вредни програми и др.

Целта на авторите е да се представят възможностите на анализатора Wireshark за прихващане и запис на телефонен трафик в IP мрежа (известен още като „услуга VoIP"). Откриване на опити за проникване в мрежата могат да бъдат установени, като се улавят пакетите в мрежата и се анализира съдържанието им. Wireshark е един от добре познатите ***мрежови анализатори (сниферы)*** и е инструмент за решаване на такъв вид задачи.

Представени са два основни протокола, използвани в VoIP телефонията - SIP и RTP. Показваме как DTMF сигнали се предават в VoIP средата и как да се генерира от RTP пакети аудио файл (подслушване на разговори).

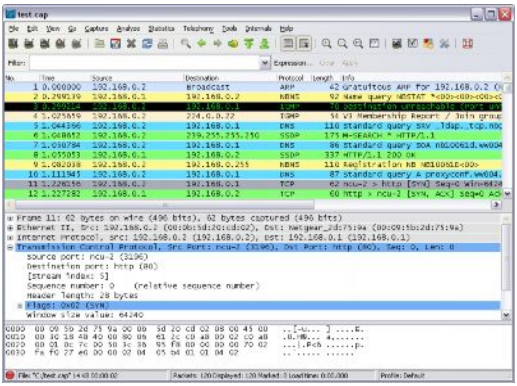
Wireshark представлява програмен продукт, чрез който може да се установят някои проблеми, възникващи в мрежата, като се уловят пакетите в мрежата и се разгледа съдържанието, посредством възможност за визуализиране на всички данни в детайли.

Wireshark може да бъде успешно използван при: отстраняване на проблеми в мрежата; проучване на проблемите в сигурността на мрежата; отстраняване на грешки по реализацията на протоколите от страна на разработчиците; научаване на повече детайли за различните мрежови протоколи.

Във функциите на Wireshark се включват: работа както под UNIX, така и под Windows; улавяне на пакети данни в реално време от даден мрежов интерфейс; визуализиране на уловените пакети с много подробна информация; осигуряване на запис и зареждане на уловени пакети, с цел по късен анализ; съвместимост с голяма част от останалите мрежови анализатори; филтриране и търсене на пакети по богат избор от критерии; оцветяване на пакети при визуализацията им, базирано на филтри; създаване на различни статистики и др. Освен това Wireshark може да записва трафика от много различни видове мрежови интерфейси, независимо от името им (включително и на безжичните LAN). Кои видове интерфейси се поддържат, зависи от много фактори като например вида и версията на операционната система, която се използва. Wireshark представлява софтуер с отворен код, и се разпространява под GNU General Public License (GPL). Може да се използва свободно на произволен брой компютри, без необходимост от лицензни ключове или такси. Освен това, целият изходен код е свободно достъпен под GPL, което позволява добавянето на нови протоколи за Wireshark като добавки (plugins), или вградени в програмата.

Трябва да се има пред вид, че Wireshark не е система за откриване на проникване (Intrusion detection system - IDS). Не се появява предупреждение, когато даден потребител извършва дейности в мрежата, които не са му позволени да извърши. Въпреки това, ако възникват особености, Wireshark може да помогне за определяне на това какво наистина се случва. Wireshark не манипулира процесите в мрежата, а единствено ги визуализира. Wireshark не изпраща пакети в мрежата, не извършва и

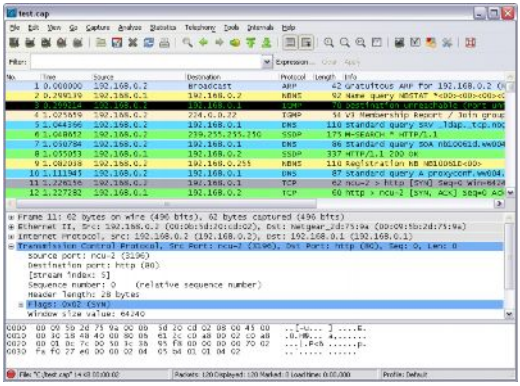
други активни дейности (с изключение на name resolution, но дори и това може да бъде изключено).



Фиг. 1. Разглеждане на съдържанието на уловените пакети.

Потребителски интерфейс

Главния прозорец на Wireshark (Фиг. 2), показва състояние, при което някои пакети са уловени или заредени от файл. Главния прозорец се състои от стандартни графични елементи – меню и лента с инструменти. Филтърът е отделна лента с инструменти, предлагаща технология за пряко манипулиране на използваните в момента филтри за визуализация.



Фиг. 2. Главен прозорец

Панелът, съдържащ списъка с уловени пакети, показва резюме на всеки от тях. С кликване върху пакетите в този панел може да се контролира показваното в другите два панела.

Панела с подробни данни показва детайли за избрания пакет от списъка.

Панелът с данните показва данните от пакета, избран в списъка, едновременно в шестнадесетичен код и в текстов вид.

Лентата за състояние показва подробна информация за текущото състояние програмата и уловените пакети.

Фиг. 3. Списъчни менюта на Wireshark

Менюто на Wireshark се намира в горната част на главния прозорец и съдържа следните *списъчни менюта* (*Фиг. 3.*): **File -** дава достъп до функции за да зареждане, записване, сливане, улавяне на пакети; **Edit** - съдържа елементи, за намиране на пакети, съответни данни за един или повече пакети. Позволява достъп до общите настройки на програмата. Изрязване, копиране и поставяне не са достъпни към този момент; **View** - използва се за контрол на визуализацията на уловените пакети, включително оцветяване, мащабиране на шрифта, разгъване и свиване на детайлите в пакети данни; **Go** –за лесна навигация и придвижване от пакет на пакет; **Capture** - възможност за пускане и спиране на процеса по прихващане и редактиране на филтрите; **Analyze** - съдържа функции, за управление на филтри за визуализация, разрешаване или забраняване на анализа на протоколи, конфигуриране на потребителски разширения за декодиране на TCP потока; **Statistics** - съдържа обекти за показване на различни прозорци със статистики, включващо и резюме на прихванатите пакети. Показват се статистически данни за вложени протоколи и други; **Telephony** – съдържа команди за показване на разнообразни прозорци със статистики свързани с телефонията, включително и анализ на медията - използвани протоколи и кодеци, диаграми на потоците, показват се статистически данни за вложени протоколи и други; **Tools** - съдържа разнообразие от инструменти в Wireshark, като например създаване на защитната стена (на базата на Access Control List правила); **Internals** - съдържа елементи, показващи информация за системни параметри на Wireshark; **Help** - съдържа елементи за достъп до описание на програмата. Достъп до ръководство за различни инструменти от командния ред, онлайн достъп до някои от уеб страниците на разработчиците, както и стандартни описания на графичния интерфейс.

Предназначение на протоколите SIP и RTP

SIP и RTP, са в основата на VoIP услугата. RTP е отговорен за правилното и равномерно предаване на потоците речеви пакети в реално време между кореспондентите в телефонните повиквания. SIP е отговорен за сигнализацията, маршрутизацията, намиране на виканите абонати, установяване и прекратяване на разговорите.

RTP (Real-Time Transport Protocol) протокол

Транспортен протокол, който използва UDP портове да предава гласови данни между абонатите. За първи път е изграден по модел на традиционните аналогови комуникации, което означава, че викащия, следва да знае IP адреса и порта на викания. Реално, в рамките на съвременната интернет архитектура, източникът не може да знае IP адреса, нито номера на порта на адресата. Това прави RTP неудобен за самостоятелно използване. По тази причина е създаден и протоколът SIP.

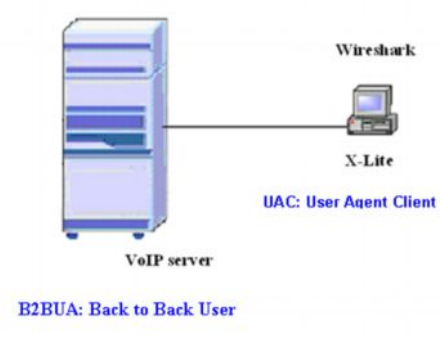
SIP (Session Initiation Protocol) протокол

Неговата цел е да помогне на RTP от началото на преговорите по видове и формати между търсещия и търсената страна. SIP предава IP адреса и порта, който ще бъде използван по време на разговора, нужен на RTP да работи правилно. Така SIP установява сесия за провеждане на разговор.

Опитна постановка

При възникнали проблеми с потребителски настройки, NAT настройки и маршрути в мрежата, един от начините е улавяне и анализ на пакетите. Wireshark може

да се използва за отстраняване на много други проблеми, възникващи в мрежата, но ние се фокусираме само на VoIP пакети.

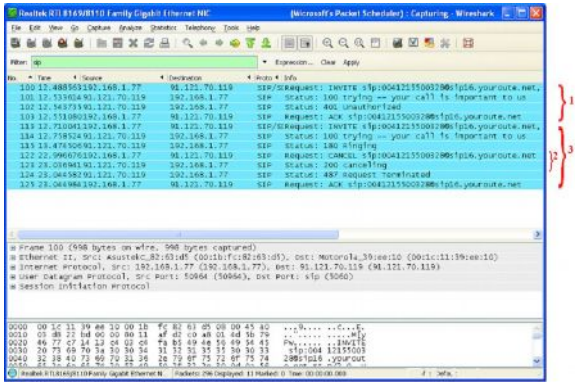


Фиг. 4. Опитна постановка

SIP филтър

След като сме избрали Ethernet интерфейса Wireshark показва всички пакети, минаващи през избраната Ethernet карта. Въвеждаме "sip" в полето за филтриране и чукваме на бутона Apply, след което улавянето започва да работи само за пакети от SIP протокола.

Примера на Фигура 5 показва опит за изходящо повикване, който е отменен след 10 секунди. Обменът показва три SIP транзакции: 1) Първата транзакция се състои от неудостоверен INVITE пакет, изпратена от клиента към сървъра. Получен е предварителния отговор на сървъра "100 trying " и последващ пакет с отговор "401 unauthorized ". След което клиента се „съгласява", изпраща "ACK" пакет към сървъра, и транзакцията прилючва; 2) При вторият INVITE пакет имаме оторизиран и приет опит за разговор. Отговора от сървъра е " 100" , последван от " 180 ringing "; 3) Третата транзакция е извършена във времевия интервал на втората. Потребителя е отказал набирането, и сървъра е отговрил с "200" (OK) .



Фиг. 5. Филтрирани SIP пакети от целия мрежов трафик

За по ясно разбиране и анализ на протокола в WireShark е резлизирана функци-

ята „FlowGraph”, или графика на потока. Избираме “Statistics” -> “Flow Graph”. От междинния диалог избираме „Displayed packets”, “General flow” и “Standart source/destinantion addresses”. Разултатът е доста по-разбираем и се вижда на фигура 6.

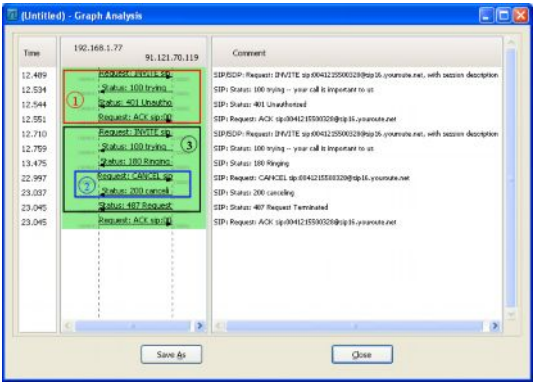
Показаната на фигура 6 диаграма дава добър изглед на съобщенията, разменяни между клиента и сървъра. Другият край на настоящия разговор (наречен страна) не може да се разглежда от страна на клиента.

Всички транзакции между викащия и викания (адресата) може да се наблюдават локално на сървъра с инструменти като ngrep, лог файлове, както и Wireshark.

192.168.1.77 = X-Lite (Client)

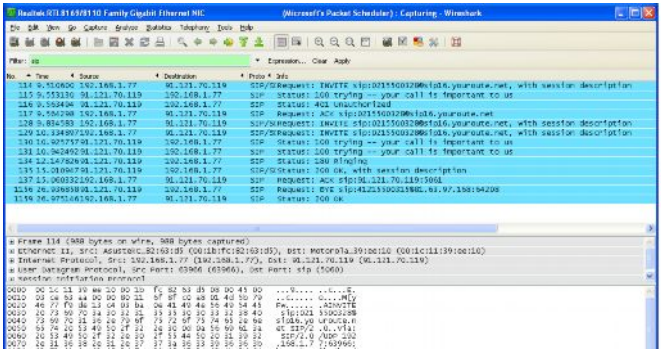
91.121.70.119 = SIP server

Процесът е разделен на 4 части: 1) клиентът изпраща "INVITE " на сървъра с молба да разговаря с друг клиент (0041215500328@sip16.youroute.net); 2) сървърът отговаря чрез изпращане на съобщение "STATUS " с код "100". Това е знак за приемането на поканата и възникване на друго действие, което трябва да се изпълни, преди да се осъществи разговор с адресата. Обикновено, това друго действие се състои в контакт с RADIUS-сървър за оторизиране на клиента; 3) сървърът изпраща съобщение "STATUS" на обаждащия се с код "401". Това уведомява клиента, че трябва да изпрати информацията за оторизация (регистрация); 4) клиентът отговаря със заявка "ACK" към полученото от сървъра оторизационно съобщение, след което SIP транзакцията се осъществява.



Фиг. 6. Графика на уловените SIP сесии

На Фигура 7 е показана SIP сесия, с проведен разговор, който по-късно ще възстановим от записаните RTP пакети и ще запишем в стандартен аудио файл. Код за състояние "200 OK", изпратен от сървъра, означава, че има отговор на повикването. След това повикващия изпраща отговор "ACK" (съгласен) на съобщението, получено сървъра. Сървърът изпраща съобщение "BYE" на викащия, когато виканият абонат е прекратил разговора (“затворил” е). На това, викащият отговаря с код "200 OK", за да приключи сесията правилно.

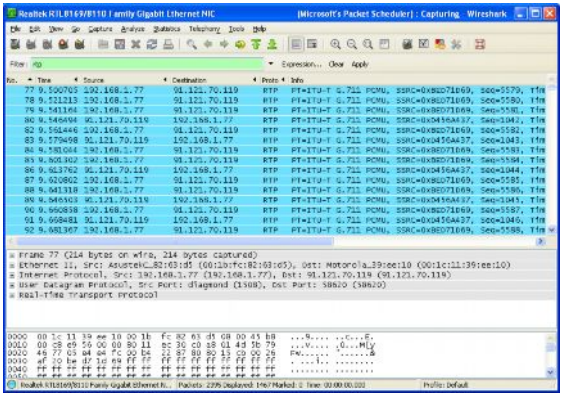


Фиг. 7. Графика на SIP сесия с проведен гласов разговор

RTP филтър

Протоколът RTP е отговорен за последователното и равномерно предаване на гласовите пакети от единия край до другия. Избираме "RTP" в менюто "Filter", за да улавяме само RTP пакети, след което кликваме бутона "Apply".

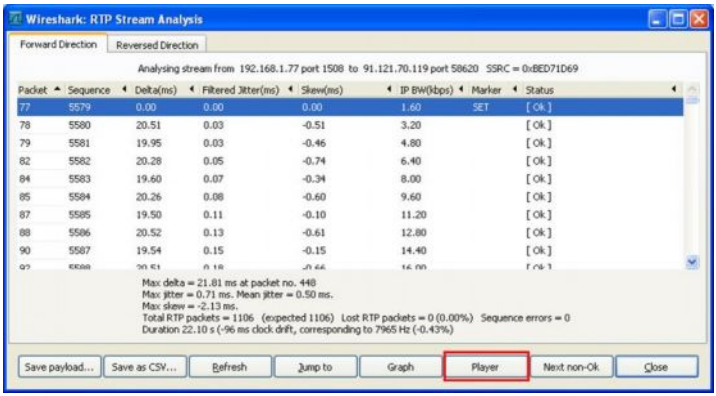
Фигура 8 показва уловените RTP пакети, както и кой кодек се използва по време на предаването. За разлика от предишните примери, тук има доста повече уловени пакети. Това се дължи на предаването на глас. Пренасянето на гласовите пакети се осъществява от протокола RTP. Затова се следят пакетите на RTP, а SIP се използва само за сигнализация - сесия и июбор на кодек.



Фиг. 8. Графика на SIP сесия с проведен гласов разговор

RTP анализ

За извършване на RTP-анализ избираме от менюто „Telephony” → „RTP” → “Stream analysis…”, както е показано на Фигура 9.



Фиг. 9. Анализ на уловени RTP пакети с проведен гласов разговор

В последния прозорец, се вижда нагоре и надолу по веригата цялата комуникация. Освен това се показва броят на загубените RTP пакети и общия брой на предадените пакети. В долната част на прозореца има списък от бутони, които представят различни функции на Wireshark.

Прослушване на RTP звуци

Wireshark може да сглоби гласовите данни, съдържащи се в уловените RTP пакети и да възстанови гласовата комуникация в едната или в двете посоки. За целта използваме бутона “Player”. След декодирането на сглобения RTP поток, можем да прослушваме разговора в едната посока, в другата посока или в двете посоки едновременно.

В заключение може да се обобщи, че използването на технологии за кодиране на трето ниво, такива като IPSec, решава до голяма степен проблема с прихващането на телефонния трафик (снифинг). Мащабируемостта, разпространеността и достъпността на IPSec го правят подходящо решение на проблема с прихващането на мрежовия трафик.

Литература

1. K. Saalbach, Cyber war. Methods and practice, version 3,0 – 12 Jan 2011, UNIVERSITAT OSNABRUCK
2. http://www.wireshark.org/
3. Калчев К., “Requirements for Modern CIS in Security and Defense”, сп. CIO, Communication & Information Technologies for the Defense, Special issue,2009.
4. Денчев С., Паргов Д., Средства информационной безопасности TCP/IP-сети, Специалний выпуск, Сборник научных трудов “Моделювання в информационый технологий“, Крым, 2008
5. Целков В., Н. Стоянов, О. Исмаилов, Международни стандарти и добри практики за защита на информацията, Поредица „Защита на информацията”, София, „За буквите – О писменехъ”, 2010, ISBN 978-954-8887-67-0

АНЕСИГУРНОСТ НА ИНФОРМАЦИОННОТО ОСИГУРЯВАНЕ ПРИ ОЦЕНКА НА РИСКА ОТ ЕКСПЛОАТАЦИЯ НА ПРЕЧИСТВАТЕЛНИ СЪОРЪЖЕНИЯ

Пламен М. Мънев[1], Любомир В. Владимиров[2]

[1]Град Русе; ул. „Студентска" № 8; Русенски университет „Ангел Кънчев"; Катедра „Екология и опазване на околната среда"; E-mail: pmanev@uni-ruse.bg

[2]Град Русе; ул. „Студентска" № 8; Русенски университет „Ангел Кънчев"; Катедра „Екология и опазване на околната среда"; E-mail: lvvladimirov@uni-ruse.bg

UNCERTAINTY OF INFORMATION SECURITY IN THE RISK ASSESSMENT OF OPERATION OF TREATMENT FACILITIES

Plamen M. Manev, Ljubomir V. Vladimirov

ABSTRACT: *The uncertainty of information security in the risk assessment from the operation of waste water treatment equipment was highlighted in this paper. The uncertainty with regard to information area and the vagueness (n-sapidity) arising from the use of specific terminology was discussed.*

KEY WORDS: *uncertainty, indefiniteness, vagueness, ambiguity, risk analysis, risk assessment*

Понятието „несигурност" намира все по-широко приложение във всички сфери от бита и живота на хората и най-често е натоварено със значенията неопределеност, неяснота и дори неадекватност.

В информационен аспект несигурността се разглежда като двусмисленост, съмнителност, проблематичност, използване на размит и/или променящ се понятиен апарат и др. Така дефинираната информационна среда носи в себе си неопределен, непроверен, размит и случаен характер - все елементи на несигурността. Използването на такава информация в процеса на изграждане на различни модели (вкл. и риск модели за анализ) води до предпоставки за груби грешки, неточни резултати и неправилни решения.

Цел на настоящата работа е да се направи анализ на несигурността по отношение на информационното осигуряване, разглеждана като компонент от комплексен алгоритъм за оценка на риска, генериран от експлоатацията на пречиствателни системи и съоръжения.

За изпълнението й е необходимо да се решат следните задачи:

- Изследване на неопределеността на информационната среда;
- Изследване на неяснотите, възникващи при употребата на специфичен понятиен апарат;
- Изследване на пропуските в стандарта БДС EN ISO 14 121-1:2007 (Безопасност на машините. Оценяване на риска. Част 1. Принципи). [6]

Оценката на риска е сложен и многокомпонентен процес, включващ в себе си

определянето и дефинирането на елементите на риска. [2] Той е съставна част от процеса на управление на риска и от своя страна включва в състава си компонентите от алгоритъма за анализ на риска.

Критично звено в тази верига е моментът на идентифициране на опасностите и дефинирането на вероятните сценарии на опасните явления и събития. Това е така поради факта, че на него са базирани преценките за тежестта на опасните явления и събития и вероятността за възникването им. Въз основа на различните им възможни комбинации (напр. нежелано събитие, водещо до вреда с висока тежест, но с минимална вероятност за възникване и реализация) се прави и преценка на риска.

За подробно идентифициране на рисковите фактори, генериращи опасностите, е необходим широк набор от информация. Тя от своя страна е във функция от характера на съставящите я данни, които носят различна степен на несигурност (в голям процент от случаите и висока).

За анализ на несигурността на информационното осигуряване при оценката на риска от експлоатацията на пречиствателни устройства и системи е използвана предложената в [4] Таблица за дефиниране и тълкуване на основните таксономични класове, категории, групи и единици на несигурността при измерване на риска. В нея са представени определенията и тълкуванията на основните таксонометрични единици на несигурността - класове, категории, групи и елементи.

Използвани са двата основни вида несигурност, дефинирани в [1], на базата на които е създадена йерархична структура. Формулирани са следните области: Област I. Неопределеност и Област II. Неяснота (*n*-смисленост). Тези области са многокомпонентни. За нуждите на настоящото изследване изграждащите ги компоненти са адаптирани към проблемите на информационното осигуряване при оценка на риска от експлоатация на съоръжения за пречистване на отпадъчни води.

Принципно неопределеностите възникват на най-ниското йерархично ниво Структурни единици. Възникват при пряко измерване на променливи величини - явления, действия и процеси, ефекти. В областта на пречистване на отпадъчни водни потоци такива са конструктивните параметри на отделните съоръжения, дебита на потока, денонощната и сезонната му неравномерност, параметрите по отношение на замърсяващите вещества, необходимата степен на пречистване и др. Паралелно с това възникват и вариации от режима на работа на производственото оборудване - помпи, хидроциклони, шнекове, гребла, мостови чистачи, въздуходувки, аерационни системи и др.

Променливостта във времето и пространството е друг елемент от ниско йерархично ниво, който генерира неясноти от информационно естество. Представя се чрез количествените промени във времевите и пространствените хоризонти. Има отношение към времепрестоя на водата във всяко съоръжение от технологичната схема на пречистване, към извеждане от съоръженията на задържаните вещества и утайки, към степента и фазата на развитие на микроорганизмите в съоръженията от биологичното стъпало, към рециркулация на част от активната утайка и др.

Информационен елемент, който не може да бъде обвързан с резултати от измервания, данни от анализи и др. са случайните събития. Те възникват без да се очакват или предвиждат и без да могат да бъдат управлявани по начин, по който да се редуцира или минимизира стойността на рисковият им потенциал. Пример за такива ситуации е съвместното третиране на водния поток с големи количества дъждовни води от интензивни валежи и/или интензивно снеготопене, различни

форсмажорни ситуации, налагащи експлоатация на съоръженията в авариен режим или в режим на критични натоварвания (залпови изпускания на големи водни количества) и др.

Висока степен на неяснота носят и лингвистичните грешки. Те, заедно с несъответствията в методологията на изследванията са със субективен характер. Дължат се на различия в понятийния апарат и използваната терминология и имат пряко влияние върху разбирането и описанието на елементите на риска. Такива възникват на всички нива от жизнения цикъл - от предпроектни проучвания, проект, избор на площадка, изграждане и доставка на оборудване за нуждите на пречиствателната станция до експлоатацията и поддръжката й, при комуникация между персонала на станцията и ВиК дружествата, при комуникация между операторите на отделните пречиствателни съоръжения и представители на обслужващи фирми-подизпълнители и др.

Субективен елемент има и при различия в схващанията на квалифицирани лица (оператори) за елементите на риска и методологията за измерването им. Към тази структурна единица са причислени съвместното третиране на битови и промишлени (съдържащи определени вещества [5]) отпадъчни води, определянето на оптималните дози на коагуланти и/или флокуланти, в случай че се използват реагентни средства, степен на квалификация на лицата, пряко свързаните с определяне на параметрите на потока на изхода на станцията и др.

Друга субективна причина, характеризираща неопределеността са променливите решения на лицата, отговорни за контрола и управлението на елементите на риска. Необходимата степен на пречистване на отпадъчни води до голяма степен зависи от стабилността на пречиствателните процеси. Решения за промяна на някои от работните параметри на производственото оборудване могат да доведат до нарушаване на тази стабилност и рязко намаляване на производителността на станцията (и по отношение на обема, и по отношение на следените показатели на изхода й). Същевременно възстановяването на оптималните условия е дълъг, комплексен и трудно осъществим процес (например възстановяване на отмрели микробиологични съобщества в биологичното стъпало на пречиствателната станция).

Субективното приоритизиране при представяне на информацията води до грешна преценка на определящите параметри - възможност за възникване, честота и степен на тежест на вредите. Приоритетността трябва да е базирана на аргументирано ранжиране на риска и неговите компоненти. Пример за това е включване на допълнителни водни количества за съвместно третиране с основния поток. На определен етап от пречиствателния цикъл допълнителните водни количества са предпоставка за нарушаване на стабилността на процесите, но при определени обстоятелства могат да окажат и положителни въздействия (например внасяне да допълнителни количества органика - хранителен за микроорганизмите субстрат).

Гореописаните причини детайлизират количествените компоненти на неопределеността. Освен тях се дефинира и неопределеност в риск моделите, тъй като моделирането е широко използван, а понякога и единствен метод за анализ и оценка на риска. Неадекватността на модела по отношение на информационното осигуряване води до редица неточности в получените на изхода параметри.

Вариативността на изследваните системи е предпоставка за натрупване на информационни несъответствия. Често в практиката еднотипни и/или еднакви пречиствателни съоръжения са ситуирани на различни места в технологичната схема

на пречистване (първични и вторични утаители). При моделиране неточности възникват, когато се използват данни, които са актуални за определено съоръжение в една ситуация, но не отговарят на действителността в друга.

Незнанието и недоброто познаване на изследваните елементи сами по себе си генерират неопределеност. Условията на средата, динамиката на процесите, обстоятелствата, причините и следствията в появяването и развитието на рисковите фактори кореспондират с широк набор от информация. Пример за незнание са възможните вреди. При пускане в експлоатация на принципно нови технологични разработки няма информация за възможните рискове и за тежестта на възможните вреди (загуби). Аналогична е ситуацията при пречистване на отпадъчни води, когато липсват необходимите знания за комбинирано (каталитично) въздействие на различните замърсители в състава на отпадъчния воден поток.

До висока степен на несигурност при моделирането води и непълната базова информация. Неточностите възникват поради неясна формулировка на изследваните ситуации и събития и водят до неадекватност на моделите. Такива модели не отразяват обективно действителността и игнорират реално възможните ситуации, а в някои случаи при моделиране се получават напълно или частично нелогични и противоречащи си данни.

Често в практиката при измерване на определени параметри се допускат грешки от различно естество, включително и по отношение на анализа и оценката на риска от експлоатация на съоръженията за пречистване на отпадъчни води. Биват абсолютни, относителни и приведени грешки на измерванията, систематизирани грешки, стандартни и вероятни грешки, груби грешки.

Освен гореописаните грешки, които са установими, е възможно да възникнат и такива, които се описват и подчиняват единствено на законите на случайността - неустановяеми и неидентифицируеми случайни грешки.

Грешки и от двата типа се допускат предимно в лабораториите на пречиствателните станции при измерване на параметрите на потока по време на движението му през съоръженията и на изхода на станцията. Дължат се на неправилно пробовземане и неподходящи съдове за него, на несъответствие на акредитираните методи с възможностите на използваните уредите за анализ, на неправилна калибровка на тези уреди, на различно представяне на дименсиите (mg/l; mg/dm^3, m^3/s, m^3/h), на несъответствие в нормалностите (N) на използваните буферни разтвори, на неточно процентно съотношение на компонентите, необходими за приготвяне на тези разтвори, на неправилно закръгляване на междинни и крайни резултати от анализи и др.

С висока степен на неопределеност и съпътстващата я несигурност се характеризират и природните феномени. Дължи се на невъзможността за моделиране на някои явления и процеси от физично, химично или биологично естество. Допълнителни затруднения възникват и от разликите в лабораторните и реалните теренни условия поради бавна реакция при промяна на един или няколко параметъра на контактната среда. В пречиствателните станции много трудно се установява оптималното количество на подавания чрез аерационните системи в биобасейните кислород. Трябва да се вземат в предвид фазата на развитие на микроорганизмите, степента на замърсеност на потока, стадия на времепрестой на водата, необходимостта от рециркулация на активна утайка, време, място и начин на подаване на коагуланти и/или флокуланти, оптимални дози на тези реагенти и др.

По аналогия с неопределеността и неяснотата (*n*- смисленост) е предпоставка за информационна несигурност при анализа и оценката на риска от пречиствателни съоръжения. Субективният й компонент е свързан с усещането, възприятието и представата за риска. Неточности възникват при комуникацията на субекти с различни темперамент и характер. Възприеманата от едни ситуация като опасна може да изглежда за други напълно в реда на нормалното. Приоритетно ранжираните задачи за изпълнение могат субективно да бъдат преподредени, а времевите им диапазони да се нарушат. Причини за това са нивото на квалификация на операторите, аналогичен опит в предишни и/или подобни ситуации, адекватност и време за вземане на управленски решения, наличието на системи за ранно оповестяване на аварийни събития, наличието на защитни механизми, блокировки и системи за активна и пасивна сигурност, възможност за комуникация, взаимодействие и работа в екип на звената в кризисни ситуации, нива на възможни емисии и имисии, стремеж за ограничаване на периметъра на опасните зони и др.

Всички тези понятия трябва да се възпроизведат по ясен и разбираем за участниците в процесите начин, т.е. в лингвистично отношение. За детайлното представяне на информационния поток трябва да се използва езиковото разнообразие. Трябва да се използват думи с точно определено значение, по възможност български. При наличието на чуждици - те да са общоприети и/или нарицателни в съответната област. По този начин се изгражда максимално опростен и общодостъпен лингвистичен модел на рисковите ситуации и събития, включително и в областта на анализа и оценката на риска от работата на пречиствателните системи за отпадъчни води.

Вторият компонент на неяснотата е рисклингвистиката и съставящата я рисклексика. Причините за възникване на неясноти в информационното осигуряване са свързани с използването на размит понятиен апарат и на думи, които не съответстват на общоприетата и специализирана терминология, използвана при идентификация, анализ, оценка, управление и редукция риска.

Начините и средствата за формализация на причинно-следствените връзки и семиотиката на риска са другите две състявящи на рисклингвистиката. Незнанието или неизпълнението на правилата за фразеологично описание на причините и следствията в появата и развитието на рисковите фактори при първата и неспазване на възприетите, доказаните и апробираните базови рискови елементи, синтактични правила, аксиоматика и семантични правила при втората са причини за възникване на неясноти от лингвистично естество.

В последствията от гореописаните причини може да се вникне при анализ на документация, описваща възникнали и реализирани критични събития. В документите (протоколи, декларациии, заключения) за трудови злополуки, техногенни и природни бедствия и аварии са използвани словосъчетания, изрази, фрази и определения, които правят информацията непригодна и неизползваема. За описание на такива събития трябва да се използват понятия, които дори и извадени от контекста трябва да са ясни и точни и да не допускат проява на многосмисленост.

Съгласно стандарта БДС EN ISO 14 121-1:2007 (Безопасност на машините. Оценяване на риска. Част 1. Принципи) [6] оценяването на риска е поредица от логически стъпки, които позволяват систематичен анализ и оценка на рисковете, свързани с машините. Където е необходимо, от оценяването на риска следва намаляване на риска, съгласно точка 5 на ISO 12100-1:2003. Повтарянето на този процес

може да е необходимо, за да се отстранят опасностите, доколкото е възможно, и адекватно да се намалят рисковете, като се приложат предпазни мерки. [6]

Стандартът установява общите признаци, които могат да бъдат използвани, за да се постигнат определените в точка 5 на ISO 12100-1:2003 цели за намаляване на риска. Тези принципи за оценяване на риска събират знанията и опита за проектиране/разработване, за използване, за инциденти и злополуки, както и за вреди, свързани с машини, за да може да се оценят представените рискове в съответните фази от жизнения цикъл на машината.

В сравнение с предходния стандарт EN 1050 примерната класификация на опасностите, опасните ситуации и опасните събития, дадена в Таблица А.1 на Приложение А е допълнена с още един вид опасности - опасности, свързани с работната среда на машината.

Въпреки допълнената в сравнение с предходния стандарт примерна класификация на опасностите, представените примери за опасности, вероятните им източници и възможните последствия, налице са и някои слабости. Тяхното коригиране би довело до усъвършенстване на предложената в предишна разработка [3] система за таксономия на опасностите, създавани от машини.

Като пропуски от информационно естество по отношение на възможните опасности в стандарта БДС EN ISO 14 121-1:2007 могат да се посочат следните:

- недостатъчна информация за вида, броя и параметрите на генерираните рискови фактори. Въпреки, че част от тях се конкретизират, не е отчетена възможността за появата на нерегистрирани до момента или принципно нови рискови фактори;
- недостатъчно обективно отразяване на естеството на генерираните рискови фактори. Не се конкретизира естеството на определен фактор, а то може да бъде от физично, химично, биологично или психофизиологично естество;
- недостатъчна информация за емитиране на рискови фактори и нивата на емисиите им. Липсва информация за начина и формата на емитиране на определен рисков фактор. Не се отчита евентуално паралелно генериране на друг стресор/и, действащ/и каталитично на анализирания;
- недостатъчна информация по отношение на продължителността на действие на рисковите фактори. Липсва информация за времетраенето на даден стресор, а също така и за евентуалната му цикличност и амплитуда. Не са разгледани възможните варианти, при които рисков фактор с ниска честота на възникване да е същевременно с ниска, средна или висока продължителност във времето и обратното – стресор с ниска продължителност на действие във времето да се проявява с ниска, средна или висока честота на възникване;
- недостатъчна информация относно обекта на въздействието на рисковите фактори. В различни ситуации рисковите фактори могат да въздействат върху редица предмети и обекти, а така също и върху хора, намиращи се в близост до източника, който ги генерира.;
- недостатъчно точна преценка относно нивата и характера на имисиите и продължителността им на действие върху обектите на въздействие. Имисиите на опасни фактори са следствие от процесите на емитиране на тези фактори. Под влиянието на определени причини те могат да се наблюдават в различни пространствени точки. В случая не са дефинирани пространствената и времева съвместимост на имисиите с обектите на въздействие;

• неточно отчитане на типа, вида, тежестта и размера на вредата и времето и разходите за възстановяване. Неточното отчитане на тежестта и размера на вредата (дава представа за нанесените материални щети, причинените икономически загуби, сведения за загинали и/или интоксикирани хора, унищожени материали, суровини, продукция и др.) води до неточно определяне на времето и разходите за възстановяване. От своя страна тези показатели са косвени, но значими и в много от случаите е възможно в определена степен да конкретизират размера на вредата.

В настоящата работа е изтъкната несигурността на информационното осигуряване при оценка на риска от експлоатацията на пречиствателни системи и съоръжения за отпадъчни води.

Разгледани са неопределеността по отношение на информационната среда и неяснотата (*n*-смислеността), възникващи при употреба на специфичен понятиен апарат. Анализирани са критичните възли и нивата от йерархичната структура за дефиниране и тълкуване на основните таксономични класове, категории, групи и единици на несигурността при измерване на риска от пречиствателни системи.

След анализ на класификацията на опасностите в стандарта БДС EN ISO 14 121-1:2007са открити някои пропуски по отношение на информационното осигуряване, необходимо за точното и пълно дефиниране на опасностите.

Литература:

1. Денчев, С., Д. Христозов. Несигурност, сложност и информация: Анализ и развитие на несигурна информационна среда. Книга 2. София, Издателство „Захари Стоянов”, 2004.

2. Мънев, П., Проблеми на преценяването на риска. Международна научна конференция “UNITECH’ 08” на ТУ Габрово, Габрово, 21 – 22. 11. 2008.

3. Мънев, П. Относно обективността на таксономията на опасностите в стандарта EN 1050. Международна научна конференция “UNITECH’ 08” на ТУ Габрово, Габрово, 21 – 22. 11. 2008.

4. Томов, В., Д. Бухов, Л. Владимиров. Несигурност на биоиндикаторните измервания при мониторинг на замърсяването на атмосферния въздух. Втора международна черноморска конференция по морско търсене и спасяване, Варна, 29 - 30.11.2008.

5. Томов, В., А. Христов. Изследване характеристиките на отпадъчните води в химическото производство. Русе, Научни трудове на ВТУ „Ангел Кънчев”, Том XXXV, Серия 7, 61 - 66 с., 1994.

6. БДС EN ISO 14 121-1:2007 (Безопасност на машините. Оценяване на риска. Част 1. Принципи)

ИНФОРМАЦИОННА НЕСИГУРНОСТ В ОЦЕНКАТА НА РИСКА ОТ ЕКОЛОГИЧНО ОПАСНИ ОБЕКТИ

Владимир В. Томов[1], Любомир В. Владимиров[2], Мариана С. Тодорова[3]

[1,2] Русе 7017, ул. „Студентска" № 8, Русенски университет „Ангел Кънчев, E-mail: vtomov@uni-ruse.bg , lvvladimirov@uni-ruse.bg

[3]Шумен 8712, ул. „Университетска" №115, Шуменски университет „Епископ Константин Преславски", E-mail: stilianova70@abv.bg

INFORMATION INSECURITY OF RISK ASSESSMENT OF ENVIRONMENTAL DANGER OBJECTS

Vladimir V. Tomov[1], Lyubomir Vladimirov[2], Mariana S. Todorova[3]

[1,2] Ruse 7017, 8 Studentska street, Angel Kanchev University of Rousse", E-mail: vtomov@uni-ruse.bg , lvvladimirov@uni-ruse.bg

[3]Shumen 8712, Universitetska 115 street, Konstantin Preslavski University of Shumen, E-mail: stilianova70@abv.bg

***ABSTRACT**: The insrcurity in the measuring is a problem which the researchers of the risk avoid. A taxonomy which includes categories, classes, groups and sub-groups is proposed in order to be revealed the reasons for the occurrence of the insecurity in the present work. They are defined and interpreted. Expert and mathematical methods for assessment are available. The possibilities for establishment, limitation and reduction of the insecurity are brought out.*

***KEYWORDS**: information, insecurity, assessment, risk.*

Съществена слабост на изследванията на риска от екологично-опасни обекти е, че се игнорира информационната несигурност в моделирането, анализ а и оценката му. Това влияе пряко върху обективността и е причина за неаргументирани защитни решения. Ето защо е необходимо проблемът с несигурността в оценката на риска да се разработи методологично, което ще бъде основание за съставяне на система правила и препоръки за редуциране. Те могат да са част изложената в [1] идея за определяне на трансграничните екологични критичности.

Цел на настоящата работа е дефиниране на несигурността в оценката на риска от екологично-опасни обекти. Основни задачи са: 1) Съставяне на структура и дефиниране на дескриптори на информационната несигурност; 2) Предлагане на метод за количествен анализ и оценка на несигурността.

За решаване на първата задача, като методологична основа за анализ, се приема формулировката за несигурност на информационната среда на С. Денчев и Д. Христозов [3]. Тази формулировка се развива в настоящата работа чрез нова структура. В нея се формулират определенията и тълкуванията на основните дескриптори на несигурността при оценка на риска-класове, категории, групи и елементи.

Използват се двата основни вида несигурност, дефинирани от С. Денчев и Д. Христозов [3] – неопределеност (клас Uncertainty) и неяснота (клас Unclarity).

Опитът ни [1,2,6] показва, че неопределеността може да се опише количествено чрез следните две категории дескриптори:

I категория. Дескриптори на информационно разнообразие Narrow restricted, които отразяват спектъра от значения на информацията за риска. Дефинира се чрез:

1) Случайност Fortuity/детерминираност Constantly на значенията на признаците на формализиране на риска,

2) Променливост Mutability на значенията,

3) Разсейване Dispersing на значенията на признаците, определящи нивото на риска;

4) Допускания Permissible при структуриране на опасностите;

5) Приблизителност Approximation при обработка на информацията за риска;

6) Методи Methods за обработване на информацията;

7) Обем Capacity на извадката данни;

8) Софтуер Software;

9) Избиране Select Distribution на статистическите закони на разпределение;

10) Грешки Error Measuring при измервания на елементите на опасностите.

II категория. Дескриптори на формализацията Risk Punctilious на риска:

1) Структуриране на опасностите Danger Structure;

2) Пространственост на ситуацията Space Situation;

3) Хронологичност на събитията Evens Chronology ;

4) Ординарност на събитията и действията Events/Actions orderly;

5) Метричност на ситуациите Situations Metric;

6) Фиксираност на ситуациите Situations Fixing;

7) Причинно-следствена зависимост Cause/Effect Relation;

8) Уязвимост Vulnerability;

9) Обстановка Context;

10) Вредност Injury;

11) Сценарийна логика Scenarios Logic;

12) Сценарийна структура Scenarios Structure;

13) Сценарийни функции Scenarios Function;

14) Критичност Criticality;

15) Екологична несигурност Environmental Insecurity;

16) Екологична сигурност Environmental Security;

17) Сценарийна селекция Scenarios Selection;

18) Каскадни ефекти Cascade Effect.

Неяснотата (клас Unclarity) се дефинира чрез две категории дескриптори:

I категория. Дескриптори на субективната неяснота Subject Unclarity:

1) Усещане на риска Risk sensation;

2) Установяване на риска Risk establishment;

3) Различаване на риска Risk Differing;

4) Идентификация Risk Identification;

5) Оценка на риска Risk Assessment;

6) Преценяване на риска Risk Estimation;

7) Заключения за риска Risk Conclusion;

II категория. Дескриптори на рисклингвистиката Risk Linguistics:

1) Лексическа неяснота Linguistics Unclarity, изразяваща се в използване на речник, който не съответства на специализираната терминология;

2) Формализационна неяснота Finical Unclarity, или незнание или неизпълнение на правилата за фразеологично описание на риск ситуациите и риск сценариите;

3) Семиотична неяснота Semiotic Unclarity, представляваща неспазване на възприети, доказани множества на структура на риска и опасностите, синтактични и семантични правила, и аксиоматика.

Дескриптори на рисклингвистиката Risk Linguistics са основание за езиково-логическата памет, чрез която се възпроизвеждат понятия, мисли, правят се разсъждения, умозаключения и оценки за риска, комуникира с други лица, формират се решения. Всичко това, обаче, се възпроизвежда лингвистично, използва се богатството на езика, за да се опише риска. С други думи се формира лингвистичен модел на риск ситуациите и събитията.

Рисклингвистиката не е следствие от субективната неопределеност, а съпътстваща и необходима област. Тя е израз на процесите на усещане, възприятие и представа за риска, форма за представянето и осмислянето им. На този проблем изследователите на риска от екологично-опасни обекти не обръщат внимание. Пропуска се факта, че всичко за което се мисли и съзнава има езиково изражение. Включително и риск сценариите на които се базират голяма част от изследванията [6]. Когато те не са правилно формулирани в езиково отношение, те са негодни и неизползваеми, въпреки че в структурно отношение moge да са обективни. Неопределеността в лингвистичен аспект се дължи на три причини: 1) непознаване на специализираните лексически елементи; 2) незнание на начините и средствата за описание на причинно-следствените отношения; 3) пренебрегване и игнориране на рисксемиотиката.

Последствията от тези причини могат да се установят при анализиране на документи за възникнали критични събития. Това доказва и нашийj опит в изследване причините за появяване на критичности в някои икономически дейности [4,5]. В документите за злополуки, замърсявания, пожари и други подобни събития се използват такива определения, изрази и фрази, сравнения и описания, които правят информацията неизползваема. Следователно, за да се ограничи неопределеността на лингвистичните модели, които описват риска на естествен език, е необходимо горепосочените причини за лингвистична неопределеност да се ограничат и по възможност да се отстранят.

Изложените дескриптори позволяват да бъдат систематизирани причините и характера на несигурността в оценката на риска. Освен въведените класове, категории, групи и елементи се прави систематизиране по три допълнителни признака- установяемост, оценка и управляемост.

Целта е, освен дефинирането на несигурността във възможните й разновидности, да се формулира идентифицируемостта, да се установи нивото и да се преценят възможностите и пътищата за предотвратяване, ограничаване или намаляване. По този начин се следва логически доказана последователност.

Установяемостта отразява способността да бъдат разкрити категориите, групите и елементите на двата класа несигурност-неопределеност и неяснота. Предварителните хипотези за нея се проверяват логически и методологично, а след това се преценява несигурността. В случай, че даден елемент на несигурността

може да се определи, то това означава, че е установяема.

Оценката е количествен израз на вида, същността и степента на несигурност. Чрез нея трябва може числено да се определи степента на значимост на елементите на несигурност от една страна, а от друга, по тях да се анализира несигурността в конкретни лингвистични и съответстващите им поли- и моноситуационни риск-модели. Следователно оценката е индикатор за достоверност на моделите.

Управляемостта показва възможностите за въздействие върху причините и намаляване влиянието им върху обективността на оценката на риска. Тя е основание за разработване на система методични указания за ограничаване на несигурността.

Значенията на тези три допълнителни признака са дадени аксиоматично. Те са резултат от опита, който е натрупан и публикуван [1,2,3,4,5,6]. Анализът показва няколко основни тенденции:

I. Може да се твърди, че всички дескриптори на несигурността са установими. Някои от тях могат да се определят чрез преки методи; други чрез непреки методи, а за голяма част се налага да се използват комбинирани методи.

II. Дескрипторите на несигурността могат да бъдат оценени предимно чрез комбинирани методи-експертни и математически, както и само чрез експертни методи. Математическите методи са приложими за елементите, свързани с ентропийността на явленията, действията и ефектите, вариативността и случайностите.

III. Основна част от дескрипторите на неопределеността и неяснотата са управляеми. Неуправляемите са свързани с природни явления и процеси, със променливост и случайност, включително и от субективен характер. Тук има един много съществен момент, че субективните неуправляеми дескриптори могат да се трансформират в управляеми чрез обучение, изисквания към поведението на субектите, контролиране на знанията за риска, специфичнителичностни качества за склонност към риск, отношение към сигурността и т.н.

Оценката на несигурността може да бъде извършена чрез два основни метода-експертна оценка и математическа оценка. Разделянето им е условно, тъй като обработката на резултатите от анализа по експертния метод се извършва математически. Целта на експертната оценка е да се установи неопределеността и неяснотата в лингвистично и графично описан модел на риска. Задачите на оценката на риска са две: 1) Установяване значимостта на елементите на неопределеността и неяснотата и графичните му интерпретации чрез поли- и моноситуационни графи; 2) Определяне на степента на неопределеност на елементите на несигурност за конкретен модел и граф на риска. Организацията и провеждането на експертизите в методично отношение се извършват съгласно опита, препоръките и указанията, посочени в [6].

Отчитайки спецификата на оценката, целта и задачите на изследването се въвеждат два критерия за оценка-рангов критерий $Rank$ на дескрипторите на несигурността и балов критерий $Rait$ на несигурността. Въведени са четири значения на критериите:

А) за ранговия критерий $Rank$: значимост (ранг 1); разбираемост (ранг 2); достъпност (ранг 3); определяемост (ранг 4);

Б) за баловия критерий $Rait$: много голяма (бал 4); голяма (бал 3); средна (бал 2); малка (бал 1). В таблица 1 е дадена извадка на форма за оценка на

несигурността.

Таблица 1

Извадка от форма-образец за оценка на информационната несигурност

Обозначения на дескрипторите	Наименование на дескрипторите	Рангов критерий *Rank* на дескрипторите				Балов критерий *Rait* на дескрипторите				Коефициент на тежест на ранговия критерий *Rank*	Коефициент на тежест на баловия критерий *Rait*
		значимост (j_1=1)	разбираемост (j_2=2)	достъпност (j_3=3)	определяемост (j=4)	много голяма (j_1=4)	голяма (j_2=3)	средна (j_3=2)	малка (j_4=1)		
D1	Fortuity	*c1.1*	*c1.2*	*c1.3*	*c1.4*	*d1.1*	*d1.2*	*d1.3*	*d1.4*	*Rank 1,k*	*Rait 1,k*
D2	Mutability	*c1.2*	*c2.2*	*c2.3*	*c2.4*	*d2.1*	*d2.2*	*d2.3*	*d2.4*	*Rank 2,k*	*Rait 2,k*
D3	Dispersing	*c1.3*	*c3.2*	*c3.3*	*c3.4*	*d3.1*	*d3.2*	*d3.3*	*d3.4*	*Rank 3,k*	*Rait 3,k*
D4	Permissible	*c1.4*	*c4.2*	*c4.3*	*c4.4*	*d4.1*	*d4.2*	*d4.3*	*d4.4*	*Rank 4,k*	*Rait 4,k*
D5	Approxima tion	*c1.5*	*c5.2*	*c5.3*	*c5.4*	*d5.1*	*d5.2*	*d5.3*	*d5.4*	*Rank 5,k*	*Rait 5,k*
D6	Methods	*c1.6*	*c6.2*	*c6.3*	*c6.4*	*d6.1*	*d6.2*	*d6.3*	*d6.4*	*Rank 6,k*	*Rait 6,k*
D7	Capacity	*c1.7*	*c7.2*	*c7.3*	*c7.4*	*d7.1*	*d7.2*	*d7.3*	*d7.4*	*Rank 7,k*	*Rait 7,k*
D8	Software	*c1.8*	*c8.2*	*c8.3*	*c8.4*	*d8.1*	*d8.2*	*d8.3*	*d8.4*	*Rank 8,k*	*Rait 8,k*
D9	Select Distribu-tion	*c1.9*	*c9.2*	*c9.3*	*c9.4*	*d9.1*	*d9.2*	*d9.3*	*d9.4*	*Rank 9,k*	*Rait 9,k*
D10	Error Measuring	*c1.10*	*c10.2*	*c10.3*	*c10.4*	*d10.1*	*d10.2*	*d10.3*	*d10.4*	*Rank 10,k*	*Rait 10,k*
D11	...	*c1.11*	*c11.2*	*c11.3*	*c11.4*	*d11.1*	*d11.2*	*d11.3*	*d11.4*	*Rank 11,k*	*Rait 11,k*
D12	...	*c1.12*	*c12.2*	*c12.3*	*c12.4*	*d12.1*	*d12.2*	*d12.3*	*d12.4*	*Rank 12,k*	*Rait 12,k*
D13	...	*c1.13*	*c13.2*	*c13.3*	*c13.4*	*d13.1*	*d13.2*	*d13.3*	*d13.4*	*Rank 13,k*	*Rait 13,k*

Отговорите на k -тия експерт по ранговия критерий $Rank_k$ образуват вектора $c_{i,j}$ ($c_{1.1}$, $c_{1.2}$, ...$c_{4.20}$). За определяне на значението на $Rank_k$ се прилага методът на ранжирането и се използва зависимостта

(1) $$Rank_{ik} = \frac{\min_k \sum_k c_{i,j_k}}{\sum_k c_{i,j_k}},$$

където c_{ij_k} е рангът на i –тия дескриптор по j –то значение на ранга, оценено от k –тия експерт. Посочените от k -тия експерт значения на баловия критерий $Rait_k$ формират вектора $d_{i,j}$ ($d_{1.1}$, $d_{1.2}$, ...$d_{4.20}$). За определяне на стойността му се прилага методът на числените оценки и зависимостта

(2) $$Rait_{ik} = \frac{\sum_k P_{ij_k}}{\sum_i \sum_j P_{ij_k}},$$

където $P_{ij_k} = d_{ij_k} / \sum_j d_{ij_k}$; а d_{ij_k} е оценката на k –тия експерт по i –тия дескриптор и j –тото значение. Значенията на критериите $Rank_{ik}$ се използват за определяне на значимостта на изведените дескриптори на несигурността, която разкрива степента им на важност при установяване общата несигурност в еколо-гично-опасни обекти. Критериите $Rait_{ik}$ се прилагат, за да се определи степента на неопределеност на моделите на риска по дескриптори. И двата критерия следва да бъдат определяне за всяка разновидност или клон на моделите. Точността на оценката по двата критерия зависи от броя на значенията им. Горепосочените подразделения на критериите са приети въз основа на препоръките, дадени в [6]. Скалите могат да се разширят, като се въведат междинни значения, но те увеличават многократно вектора на отговорите, което усложнява използването им.

Целта на математическата оценка е да се установи значението на несигурността за рисковите явления, действия и ефекти, описвани чрез количествено формулирани признаци. Тя се свързва главно с вариативността, която отразява измененията на информацията, свързана с природната и индивидуална субективна хетерогенност, времето, пространството, процесите и условията.

Игнорирането на неопределеността и неяснотата, като основни характеристики на несигурността, води до грешки, неточности, неиздържани твърдения, неправилни оценки и измервания. За да бъде решен проблемът е необходимо да се решат следните задачи: 1) Да се установи характера на променливите чрез които се моделират рисковете в екологичната сигурност. 2) Да се изберат методи и да се представи несигурността. 3) Да се установи числено степента на несигурност при измерване на конкретно моделиран риск.

За решаване на първата задача е необходимо да се анализира наличната или експериментално установима информация и да се прецени променливите величини със случаен характер ли са. Те трябва да приемат една и само една от възможните си стойности, която не може да се предскаже до провеждане на експеримента. В този смисъл е необходимо точно да се установи и характерът на случайните величини-дискретен или индискретен, тъй като влияе върху избора на формата и

начина на представяне на несигурността.

При решаване на втората и третата задача несигурността може да се анализира и представи чрез:

1) Реда на разпределение и функцията на разпределение при дискретни или индискретни случайни величини [6];
2) Анализ на границите на вероятността за появяване [3,6];
3) Ентропия на Шенон [3,6];
4) Информация на Хартли[3];
5) Ентропия на Болзман [3];
6) Аналитични методи: разлагане в ред на Тейлор [6] и апроксимация [6];
7) Моделиране чрез метод "Монте Карло" и латински хиперквадрати [3,6]
8) Интервална аритметика [6];
9) Мерки за размитост [3,6].

Първите три метода са използвани в наши изследвания [1,2,4,5] и са предпочитани, тъй като се базират на законите на разпределение на случайните величини. За оценка на несигурността се използват средната стойност, $\overline{X}$, дисперсията $\sigma^2[X]$, средноквадратичното отклонение $\sigma[X]$ или коефициентът на вариация $V[X]$. Допълнително тези величини се анализират като случайни и се установяват законите на разпределение на неопределеността. В настоящия анализ на неопределеността се предлага да се установяват числените характеристики на 6 закона за разпределение на дискретни величини и на 18 закона за индискретни величини. Проверката на хипотезите става чрез критерия χ^2, критерият на Андерсон - Дарлинг *A-D* и критерият на Колмогоров – Смирнов *K-S*. Използва се програмният продукт Risk 4.5 на Palisade Corporation.

Изхождайки от същността на метода за оценка на риска [1] следва да се отбележи значимото значение на границите на определяне на вероятността за появяване на случайните величини, а от там и на неопределеността. Диапазонът трябва да се аргументира точно, тъй като значително влияе върху резултатите за нивото на риска. Аргументите зависят от целта, задачите, обхвата и ограниченията на изследването и спецификата на оценявания обект.

Ентропията на Шенон се прилага успешно в изследвания на С.Денчев, Д. Христозов, В. Томов [3,6]. Определя се по зависимостта

(3) $$H(P(x)) = -\sum_{x \in X} p(x) \log_2(x),$$

където $p(x)$ е вероятностното разпределение върху крайното множество X, като $x \in X$.

За сравнителен анализ на две множества X и Y могат да бъдат използвани простата ентропия; обединената ентропия; условната ентропия и информационната трансмисия [3].

Изложеното ни дава основание да направим следните изводи:

Несигурността се разглежда като съвкупност от неопределеност и неяснота. Съставена е структура от дескриптори на несигурността. Структурата представя същността и определенията на съставящите класове, категории, групи и елементи. Извършен е анализ на дескрипторите.

Въведени са експертни и математически оценки. Чрез тях може да се определи

нивото на несигурността и значимостта на базовите компоненти. По този начин се допълват моделите на риска, те придобиват завършен и пълен вид и позволяват поточна оценка на риска от екологично-опасни обекти.

Литература

1. Владимиров, Л. Рискметрия в екологичната сигурност. Монография. Варна, Варненски свободен университет "Черноризец Храбър", 2009. 279 с.
2. Владимиров, Л. Теория на риска. Част I. Опасности и заплахи, рискове и критичности. Русе, Русенски университет, 2011. 270 с.
3. Денчев, С., Д. Христозов. Несигурност, сложност и информация: Анализ и развитие на несигурна информационна среда. Книга 2. София, Издателство "Захари Стоянов", Университетско издателство "Св. Климент Охридски", 2004, 179 с.
4. Томов, В., Л. Владимиров. Риск таксономия. Габрово, Технически университет, Международна научна конференция "Унитех 07", част II, 2007. II302-II 307.
5. Томов В., Л. Владимиров. Изследване на критични ситуации от запалване на материали и замърсяване на въздуха. Част I. Методика на изследването.Русе, Известия на Съюза на учените, серия "Технически науки", 2007, №6. 87-94.
6. Томов, В. Теория на риска. Монография. Русе, Русенски университет, 2003. 440 с.

ИНФОРМАЦИОННАТА НЕСИГУРНОСТ НА ИНДИСКРЕТНО ИЗМЕРВАНИ ШУМОВИ ИМИСИИ. ЧАСТ I. ИЗМЕРВАНЕ И МЕТОД ЗА ОЦЕНКА НА НЕСИГУРНОСТТА

Любомир В. Владимиров, Николай Й. Ковачев

Русе 7017, ул. "Студентска" №8, Русенски университет "Ангел Кънчев", E-mail: lvvladimirov@uni-ruse.bg, nkovachev@uni-ruse.bg

INFORMATION INSECURITY OF RISK OF INDISCRET MEASURING OF NOISE IMMISIONS. PART I. MEASURING AND METHOD OF INSECURITY ASSESSMENT

Lyubomir V. Vladimirov, Nikolai I. Kovachev

Ruse 7017, 8 Studentska street, Angel Kanchev University of Rousse, E-mail: lvvladimirov@uni-ruse.bg, nkovachev@uni-ruse.bg

ABSTRACT: A new approach for indiscreet noise imissions measurements is described in the presented paper. A new probabilistic method for informative uncertainty's assessment is proposed. New criteria are introduced – informative risks based on the mathematical expectation, standard deviation and dispersion. Their usage is argued.

KEY WORDS: uncertainty, measurement, noise, imission.

Неопределеността е характерна за изследванията на риска [1]. Дължи се на ре-

дица причини и източници - ентропийност, йерархичност, комплектност, променливост и незнание, лингвистична неяснота, информационни различия и нормативност.

Цел на настоящата работа е да се предложи метод за определяне на информационната несигурност при измерване на имисии на шум чрез индискретен метод.

За постигането й се решават следните задачи:

1.Създаване на виртуален уред за индискретно измерване на шум.

2.Дефиниране на критерии за анализ и оценка на информационната несигурност.

3.Аргументиране на начина на определяне на критериите на информационна несигурност.

При решаване на първата задача е използвано устройство за събиране на данни - *DAQ 6210* [3]. То се адаптирано към програмата *LabView 8.5*. Устройството *DAQ 6210* се свързва към компютърна система. Създава се виртуален уред за измерване на шум, който се комплектова с аналогов шумомер *SL 401*, свързан към вход *a1* на устройството.

От старт меню в *Windows* се избира *All programs/National Instruments LabView 8.5*. Отваря се диалогов прозорец. В него се стартира *Blank VI*, представляващ работната област, в която се включват измервателните модули.

В блокова диаграма на прозореца се разполагат елементи, които са необходими за програмиране. Активира се падащо меню с програмни функции. Избират се входящите инструменти и програмата *DAQ assistant* за управление на устройството. Настройват се параметрите на устройството, броя на измерванията и честотата на регистриране на резултатите от измерването.

Избират се каналите, към които са свързани отделните уреди. Скалата се настройва, за да се установят реалните значения на измерваните величини. Системата се тарира. За удобство се добавя плъзгач. Чрез него бързо се регулира броя на получените данни. Това става чрез падащо меню. *DAQ* устройството позволява работа при 250 *kS/s*. На практика се налага да се използва значително по-ниска честота.

Изгражда се блок, който превръща резултатите от измерването от волтове (*V)* в децибели *(dB)*. Прави се чрез математическия модул *Formula*. За целта DAQ устройството се настройва на честота 250 *kS/s*. Така се получава максимален брой данни за един период на трептене на мембраната на акустичния калибратор *Robotron 05 000*. Чрез него се генерира еталонен сигнал с честота 1000 *Hz* и амплитуда 94 *dB*. Тъй като дължината на периода е 0,001 *s*, то при избраната честота, броят на измерванията може да бъде произволен, но повече от 250. С модул за регистриране измерваните стойности се записват в текстов файл. За да се определи напрежението, което се получава при опорното звуково налягане се приема линейна зависимост между налягането в паскали (*Pa)* и напрежението във волтове (*V)*. За напрежението, отговарящо на праговото налягане е получена стойност 0,000000527 *V*. В модула *Formula* на блоковата диаграма върху диалоговия прозорец се въвежда зависимостта $L_p = 20*\log(((X_1 * X_1)**0.5)/0.000000527)$. Служи за определяне големината на нивото на звуковото налягане в *dB*. От падащото меню и групата с инструменти *Signal analysis* се активира модулът *Filter*. Избира се широколентов филтър. Задава се долната и горната гранична честота. При долна честота 500 *Hz* и горна – от 5000 до 10000 Hz се имитира корекционният филтър *A*, който се

вгражда в шумомерите, отговарящи на стандарт IEC 651. Избира се *FIR filter mun Chebyshev* със степенен показател 1. Входът на филтъра се свързва към изхода на модул *Filter*, а изходът на филтъра към модулите за регистриране и визуализация на получените данни.

LabView 8.5 предлага широки възможности за наблюдаване и анализ на данните на всеки етап от изследване на шумови имисии. В предния панел се намират графични индикатори. Избира се *Graph*. В блоковата диаграма се прави връзка на монитора с изхода на филтъра. По този начин в реално време могат да се наблюдават стойностите на нивото на звуковото налягане. Обхватът на скалата може да се настройва, да се въвеждат допълнителни линии, да се задава точността на показанията, да се избера логаритмична или линейна скала и да се извършват редица други помощни операции. За запис на данните се използва модулът *Write to measurement file*. Той записва данните директно в ".lmv" файл, който се поддържа от програмата *Excell*. Могат да се настроят параметрите на файла и поведението на програмата при дублиране на файлове. В проведеното изследване е избран запис в текстов файл, формат ".lmv" с една колона, а при повече от един файл програмата избира в зависимост от нуждите на изследването следващото по ред име на файла и брой на файлове. На предния панел се избира палетът *Buttons*, в който се намира *Push* бутонът. Той се свързва с вход *Enable* на модула за запис. Могат да се въвеждат стойности на различни величини. С модула *Amplitude and level measurements*, свързан към изхода на корекционния филтър, програмата изчислява в реално време средната стойност, общото ниво на шума, ефективната стойност, максимална стойност на текущото измерване. При свързване на изходите на модула към съответните текстови индикатори тези измервателни величини могат да бъдат визуализирани и записани в текстови файл.

Блокът за измерване на общото ниво на шума се допълва с модул *Spectral measurements*. Той извършва *FFT* преобразования на сигнала. Избира се този модул. Неговият вход се свързва с устройството за събиране на данни. Стойностите, които се получават са във волтове.

Сигналът към модулите за запис и визуализация се обработва математически. Извиква се модулът *Formula* и се въвежда отношението $(\log(X1*1000000))/0.045$. Чрез него стойностите на сигнала се представят в *dB*. Избрана е референтна стойност 1000000, по която се умножава получения сигнал след преобразуване. Делителят 0.045 служи, за да се постигне еталонна стойност на използване на акустичния калибратор.

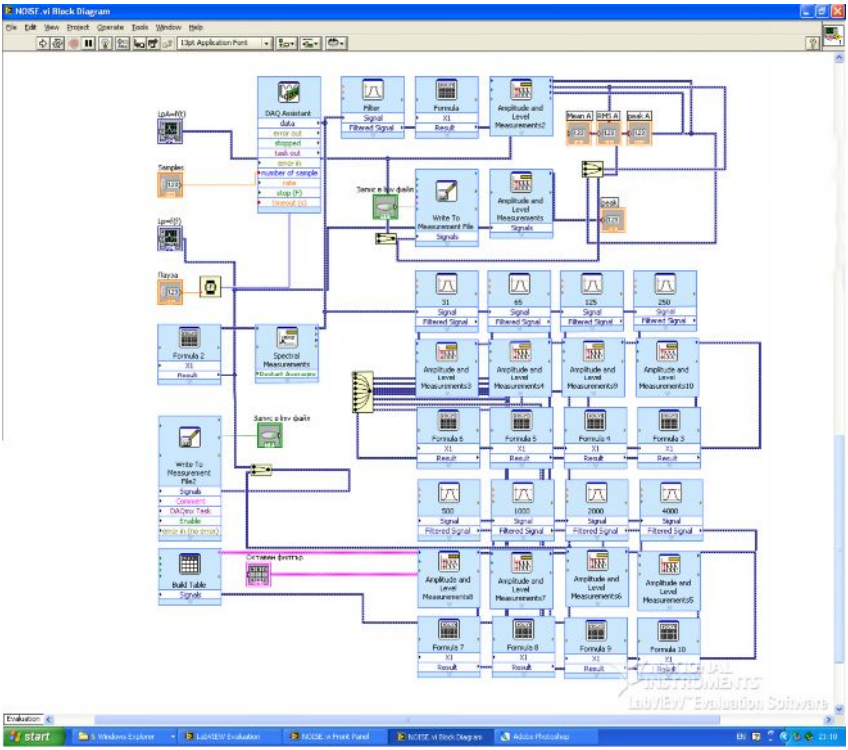
Възможностите на виртуалния инструмент са разширени чрез създаване на октавен филтър. Настройките на филтъра са *IRR* филтър тип *Butterworth*, който има степенен показател 40. Долната гранична честота е избрана да съвпада с теоретичната долна честота на съответната октава. Горната честота съответства на горната гранична честота на октавата.

Филтрираният сигнал се подава към изчислителен модул *Amplitude and level measurements*, който пресмята *RMS* на сигнала след филтрация. Този модул се свързва към *Formula*. В диалоговото поле на блока е въведено горепосоченото отношение. Получава се ефективната средна стойност на нивото на звуковото налягане в една октава. За да се обхванат всички октави описаната схема се мултиплицира 8 пъти.

За визуализиране на резултатите сигналите се обединяват в блок *Merge signals*.

Той има 8 входа. Изходът се свързва с модул *Table*. Върху предния панел се появява таблица, която чрез падащото меню е настроена на 9 колони и 2 реда. Могат да се задава точността на резултатите, големината на таблицата, шрифтът и др. За запис на данните от октавните измервания блокът е свързан към модулът за запис на данните.След като приключи измерването блоковата схема е от вида на показаната на фиг. 1.

Описаният виртуален инструмент се прилага за измерване и изследване на имисиите на шум. Отделните измервания се провеждат съгласно частните стандарти. След като са определят точките на измерване, съгласно тези стандарти, дефиниращи също изискванията към измерванията, изходът на шумомера, инсталиран в точките на измерване се свързва към устройството *DAQ 6210*. Следвайки директории *Start>All programs>National instruments LabView 8.5* и *File>Open>име на файла* с разширение ".vi", се стартира на виртуалният инструмент. Извършва се настройка на параметрите на измерване-честота на дискретизация и брой на получените стойности. Правят се чрез модулът *DAQ assistant*. Честотата на дискретизация определя броя на стойностите, който се отчитат за 1 *s*. При избиране на повисока стойност се генерира повече данни.



Фиг. 1. Блок-схема на *LabVIew 8.5* със зареден виртуален инструмент за измерване на общото ниво на шума, измерване на честотния спектър и октавен филтър

В проведените изследвания на имисиите на шум е избрана честота на дискретизация 10 kHz, която определя горната гранична честота на честотния спектър – 5 kHz. При зададена стойност 20000 за броя на измерванията на общото ниво на шума, програмата създава измервателен цикъл от 2 *s*, през който се генерират стойностите на нивата.

Стойностите, които определят честотния спектър, са 10000. Преди започване на измерването се включват бутоните, разположени под мониторите на блок-схемата, съответстващи на измерване на нивото на общото ниво на шума по корекционна крива *A* и на измерване на нивото на звуковото налягане в отделните честоти, и в отделните октави. Индикаторните светодиоди променят цвета си. Това означава, че може да се прави непрекъснат запис на данните в текстов файл с разширение „.lmv". Записват се два файла за двата вида измервани величини. Чрез включване на модул *Write to measurement file* се посочва мястото, където ще се съхраняват файловете и името на първия файл. Следващите файлове ще се записват в същата папка, със същото име, като към него се добавя следващото означение. Прави се отметка - *Use next available filename*. В лентата с бутони се активира *Run*, който графично е отбелязан като единична стрелка. Системата провежда едно измерване по зададените параметри и записва общо два файла-един с данните от измерване на общото ниво на шума, където са записани и стойностите - *RMS, Mean* и *Peak* на диаграмата, визуализирана на дисплея, и един с отделните честоти и октави.

При стартиране на *Run continuously* системата провежда непрекъснато измервания и записи на нови и нови файлове до активиране на *Stop*. Когато е необходимо може да бъде зададен броят на циклите. След като завърши измерването се прави обработка на получените данни. Те се записват във файлове, които позволяват редакция в *Excell*.

Информационната несигурност *Ifunsec* разглеждаме като обобщен признак на две съставящи [1]:

- информационна неопределеност *Ifexactness*,
- информационна неяснота *Ifclarity*.

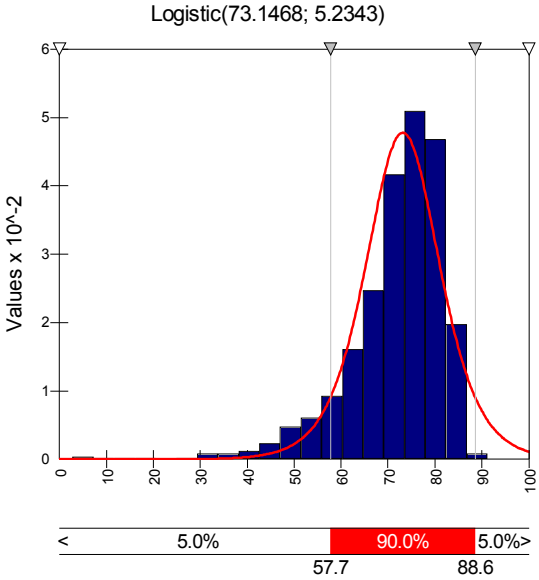
Информационната неопределеност се отразява чрез закона на разпределение *Noise Distribution* на общото ниво на шума L_{pA}. Чрез програмата Risk 4.5 се проверяват 18 закона за индискретно разпределения, съответстващи на същността и метода на измерване на шумовите имисии:

1) закон на равната вероятност - *Uniform*;
2) нормално разпределение - *Normal*;
3) логаритмично-нормално разпределение - *Lognormal*;
4) логистично разпределение - *Logistic*;
5) логоратмично-логистично разпределение - *Loglogistic*,
6) триъгълно разпределение - *Triang*,
7) експоненциално разпределение - *Exponent*,
8) екстремално разпределение - *ExtValue*;
9) гама разпределение - *Gama*;
10) бета разпределение - *Beta*,
11) разпределение на Вейбул - *Weibul*,
12) разпределение на Релей - *Rayleigh*;
13) разпределение на Пирсон - *Pearson*,

14) разпределение на Гъмбел - *Gumbel*,
15) разпределение на Ерланг - *Erlang*,
16) разпределение на Валд - *Wald*.

Анализират се графичните илюстрации на посочените закони, които са от вида на представената на фиг.2. Установяват се числените характеристики разпределенията, извадка от които са дадени в таблица 1.

Използват се следните числени характеристики: *Left X* - лява граница на случайната величина, *Left P* – лява граница на доверителния интервал, *Right X* – дясна граница на случайната величина, *Right P* – дясна граница на доверителния интервал, *Diff. X* – интервал на значенията на случайната величина, *Diff. P* – доверителен интервал, *Minimum* – минимална стойност, *Maximum* – максимална стойност, *Mean* – математическо очакване *m*, *Mode* – мода, *Median* – медиана, *Std. Deviation* – средноквадратично отклонение σ, *Variance* – дисперсия σ^2, *Skewness* – асиметрия, *Kurtosis* – Ексцес.



Фиг.2. Логистичен закон на разпределение

Неопределеността се оценява по значенията на математическото очакване $\overline{L}_{pA}=m \equiv Mean$ на измереното общо ниво на шума; средноквадратичното отклонение $\sigma_{LpA} \equiv \sigma \equiv Stan\,Dev$ и дисперсията $\sigma_{LpA}{}^2 \equiv \sigma^2 \equiv Variance$.

Таблица 1

Параметри на закона на разпределение

Parameters	Theoretical Model	Experiment
Function	Logistic	
a	73.1467	
b	5.2343	
Left X	57.7	57.7
Left P	5.00%	8.70%
Right X	88.6	88.6
Right P	95.00%	99.98%
Diff. X	30.8243	30.8243
Diff. P	90.00%	91.28%
Minimum	$-\infty$	2.8637
Maximum	$+\infty$	91.215
Mean	73.1468	71.930
Mode	73.1468	76.951
Median	73.1468	74.088
Std. Deviation	9.4940	10.130
Variance	90.1366	102.590
Skewness	0.0000	-1.7257
Kurtosis	4.2000	8.3145

Рискът за информационна неопределеност $R_{Ifexact}$ на измерванията се определя чрез вероятността P за изменение на математическото очакване, средноквадратичното отклонение и дисперсията в зададени граници на изменение на общото ниво на шума L_{pA}. Поради това се използват три негови разновидности:

1) среден информационен риск

$$R_{Ifexact}[m] = P[Mean1 < Mean < Mean2],$$

2) средноквадратичен информационен риск

$$R_{Ifexact}[\sigma] = P[S\,tan\,Dev1 < S\,tan\,Dev < S\,tan\,Dev2],$$

3) дисперсен информационен риск

$$R_{Ifexact}[\sigma^2] = P[Variance1 < Variance < Variance2].$$

Прави се проверка на хипотезата на законите на разпределение на вероятностите, както бе посочено по-горе. След това се изчисляват вероятностите математическото очакване, средноквадратичното отклонение и дисперсията да се променят в зададени интервали - $P[Mean\ 1 < Mean < Mean\ 2]$, $P[S\,tan\ Dev\ 1 < S\,tan\ Dev < S\,tan\ Dev\ 2]$ и $P[Variance\ 1 < Variance < Variance\ 2]$. За тази цел се интерират функциите на разпределение на горепосочените закони и се извеждат аналитични зависимости за изчисляването им. За част от тях използва програмата *Calc .exe* .

Границите на изменение на случайните величини, каквито при тези операции

се разглеждат математическото очакване, средноквадратичното отклонение и дисперсията, зависят от целите на изследването. Могат да варират в интервали на зададени значения на $m \equiv Mean$, $\sigma \equiv S\,tan\,Dev$ и $\sigma^2 \equiv Variance$ и чрез интервалите, определени от средноквадратичното отклонение $\pm\sigma$, $\pm 2\sigma$ и т.н.

Информационна неяснота *Ifclarity* при задаване на следните дескриптори:

I. Критерии за тестване на хипотезите за законите на разпределение:

а) критерият на Пирсон χ^2,

б) критерият на Андерсон-Дарлинг $A-D$,

в) критерият на Колмогоров-Смирнов $K-S$.

II. Брой на тестваните чрез програмата *RISK 4.5* закони на разпределение. Предимството на тази програма е, че класира установените закони на разпределение по степен на съответствие на теоретичните модели и експерименталните данни.

III. Използвани програми за обработка на експерименталните данни- *Risk 4.5; Statistica 8.0; SPSS 15.0; Statgraphics 7.0.*

IV. Обем на извадката *Capacity*.

V. Продължителност на действие на шума T_{noise}.

VI.Акустичен фон в пространството на измерване $L_{pA(\,ground\,)}$.

VII. Схема на измерванията и разположение на измервателните точки.

VIII.Среда на разпространение на шума $Middle$.

IX. Конфигурация на източниците на шум-симетричност или асиметричност, габаритни размери, насоченост на шума.

X. Показатели на пространството на разпространение на шума-затворено, открито, размери, звукопоглъщане, звукоизолация и други акустични характеристики.

XI. Ред за формиране на извадките-последователно, комбинирано, случайно.

Изложеното ни дава основание да направим следните обобщения:

Създаденият индискретен метод за измерване на шумовите имисии в околната среда се характеризира с висока разделителна способност, информационен капацитет и точност.

Предлага се вероятностен метод за оценка на информационната неопределеност при измерване на шумовите имисии.

Въвеждат се нови критерии-информационни рискове по математическото очакване, средноквадратичното отклонение и дисперсията. Те позволяват да бъдат разглеждани във вероятностен аспект и по този начин да се отчита действителния характер на величините. Определя се начинът на установяването им.

Литература

1. Владимиров, Л. Рискметрия в екологичната сигурност. Монография. Варна, Варненски свободен университет “Черноризец Храбър”, 2009. 279 с.

2. Владимиров, Л. Н. Ковачев. Динамика на неопределеността при измерване на шум в помещения. Част II. Времеви модели. Русе, Сборник доклади на научна конференция. Русенски университет “Ангел Кънчев”. 2007, с. 90-95.

3. Ковачев, Н. Методично усъвършенстване на измерването на шумови емисии.

Част I. Методика за измерване на шума с виртуален инструмент, разработен в LabView 8.5, продължителност и ред на измерванията. Русе, Научни трудове на Русенски университет "Ангел Кънчев", том 47, серия 1.2, 2008, 181-185 с.

4. Ковачев, Н., Л. Владимиров. Динамика на неопределеността при измерване на шума в помещения. Част I. Закони на разпределение и числени характеристики. Русе, Русенски университет "Ангел Кънчев", Сборник доклади на Научна конференция 2007. 9-10. 11. 2007. с. 84-89.

ИНФОРМАЦИОННАТА НЕСИГУРНОСТ НА ИНДИСКРЕТНО ИЗМЕРВАНИ ШУМОВИ ИМИСИИ. ЧАСТ II. ОЦЕНКА НА НЕСИГУРНОСТТА

Любомир В. Владимиров, Николай Й. Ковачев

Русе 7017, ул. "Студентска" №8, Русенски университет "Ангел Кънчев", E-mail: lvvladimirov@uni-ruse.bg, nkovachev@uni-ruse.bg

INFORMATION INSECURITY OF RISK OF INDISCRET MEASURING OF NOISE IMMISIONS. PART II. ASSESSMENT OF UNCERTAITY

Lyubomir V. Vladimirov, Nikolai I. Kovachev

Ruse 7017, 8 Studentska street, Angel Kanchev University of Rousse, E-mail: lvvladimirov@uni-ruse.bg, nkovachev@uni-ruse.bg

ABSTRACT: Some results from informative insecurity assessment method's approbation are presented. Results from measurements, statistical distribution laws establishment and received values of mean, standard deviation and dispersion informative risks are proposed.

KEY WORDS: insecurity, risk, assessment, noise, immision.

Цел на настоящата работа е да се апробира методът за оценка на информационната несигурност [1] при индискретно измерване на шумови имисии.

За постигането й се решават следните задачи:

1. Измерване на шумови имисии.

2. Определяне на статистическите закони на разпределение на значенията на общото ниво на шума и числените им характеристики;

3. Установяване на статистическите закони на разпределение на математическото очакване, средноквадратичното отклонение и дисперсията на имисиите и съответстващите им числени характеристики;

4. Определяне на средните, средноквадратичните и дисперсните информационни рискове.

В изпълнение на първата задача е проведен по един опит, в който е измерен шумът на три източника - битова прахосмукачка, сешоар и колесен трактор МТЗ 5ЛС. Направени са извадки от 4000 значения на шума. Възприета е честота на

дискретизация 10 *Hz*.

В таблица 1 са представени част от измерените стойности, за да се прецени чувствителността на измерването. Интервалът на измерване е 0,0001 *s*.

Таблица 1

Извадка на резултати от измерване на общото ниво на шума във функция от времето

Прахосмукачка		Сешоар		Трактор-пусков двигател	
Време, *s*	LpA, *dBA*	Време, *s*	LpA, *dBA*	Време, *s*	LpA, *dBA*
0	72,0662	0	77,3927	0	99,2781
0,0001	81,1987	0,0001	83,9922	0,0001	105,9633
0,0002	69,8038	0,0002	72,8513	0,0002	105,4467
0,0003	69,6401	0,0003	67,2896	0,0003	101,5105
0,0004	78,5547	0,0004	79,1044	0,0004	78,4711
0,0005	76,7945	0,0005	78,2541	0,0005	107,0192
0,0006	81,5101	0,0006	58,8477	0,0006	112,3511
0,0007	84,8043	0,0007	67,8153	0,0007	106,0741
0,0008	85,4396	0,0008	75,4769	0,0008	103,3392
0,0009	81,9285	0,0009	83,3625	0,0009	102,2215
0,001	78,1229	0,001	61,4433	0,001	97,37122

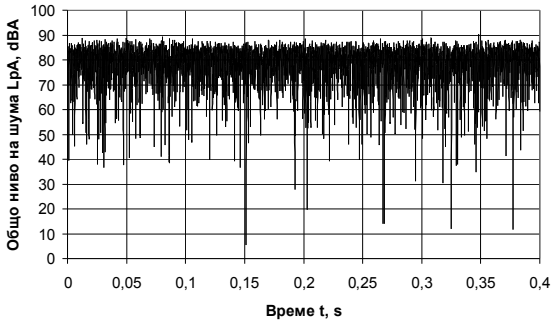
Анализът на резултатите показва, че се регистрират много големи разлики в различните моменти на дискретизация, които достигат до 12-13 dBA за трите изследвани източника. За интервал 0,0001 *s* се възникват изменения от 12 до 16 dBA. Това е илюстрация за селективността на метода за измерване и за интензивно променливия характер на шума.

Може да се твърди, че шумът от първите два източника е с идентични закони на разпределение и числени характеристики. Ето защо по-нататък ще бъде разглеждана имисията само на прахосмукачка. Съществени различия има в спектъра на шума от пусковия двигател на колесен трактор ЮМЗ 6ЛС.

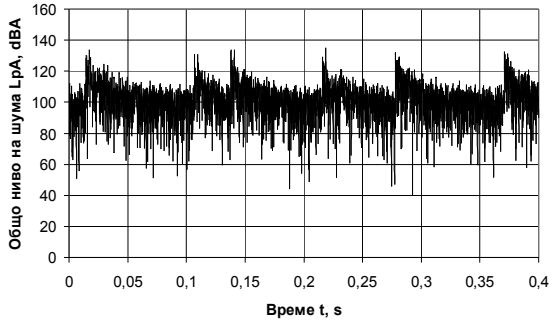
Графична илюстрация на изменението на имисиите на общото ниво на шума във функция на времето е представена на фиг. 1. Тя потвърждава съществената разделителна способност на метода на измерване и възможността за формиране на извадки от данни с голям обем.

Фиг.1 отразява динамиката изменение на общото ниво на шума, която е дескриптор на несигурността при измерванията. Чрез нея и числените значения на шума се доказват направените изводи в предишни наши изследвания [2,3].

Законите на разпределение се ранжират от програмата Risk 4.5 на основание на съотношението на съответния критерий спрямо граничната стойност за приемане или отхвърляне на статистическата хипотеза. Извадка от резултатите от проверката на статистическите хипотези са представени в таблица 2. Анализът и графичната интерпретация на законите на разпределение на шума от прахосмукачка, показани на фиг.2, доказват, че има съществена разлика между трите закона.



а)



б)

Фиг.1. Динамика на имисиите на шум от: а) прахосмукачка, б) пусков двигател на колесен трактор ЮМЗ 6ЛС

Най-голяма е средната стойност на шума при логистичното разпределение, което е на I позиция в ранжирането чрез използваната програма. След това е средната стойност по нормалното разпределение и накрая по триъгълното разпределение. Разликата между логистичното и триъгълното разпределение е близо 19 dBA. Това потвърждава важността на избиране на моделиращия експерименталните резултати закон на разпределение.

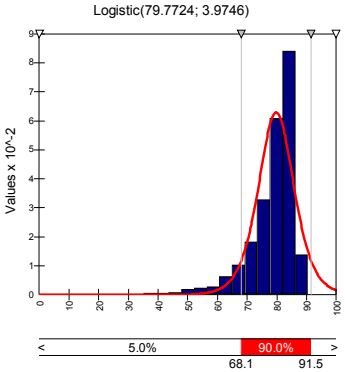
Аналогично се получава и за характеристиките на разсейването. При тях разликата между средноквадратичното отклонение σ и дисперсията σ^2 е още по-значителна, приблизително 12 dBA за σ и 332 dBA за σ^2. Тези резултати също потвърждават степента на важност на избора на закона на разпределение. В случая и трите закона не се отхвърлят, но изборът на един от тях определя по-голяма или по-малка информационна несигурност.

За изпълнение на втората задача резултатите от измерванията са обработени чрез програмата *Risk 4.5*. Проверката на статистическите хипотези се извършва чрез критерия χ^2 на Пирсон, критерия $A-D$ на Андерсон – Дарлинг и критерия $K-S$ на Колмогоров – Смирнов.

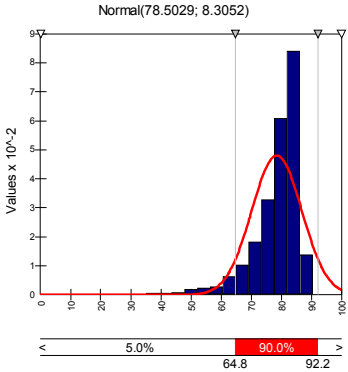
Таблица 2

Закони на разпределение на шумови имисии от прахосмукачка при проверка на хипотезата чрез критерия на Пирсон

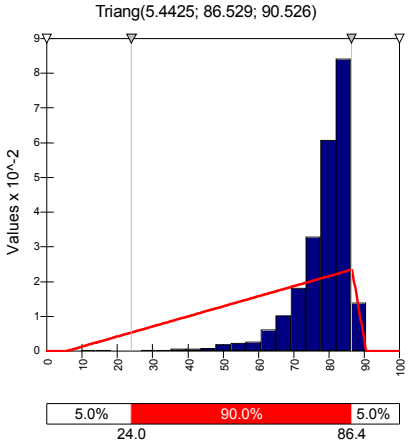
I позиция в ранжирането			II позиция в ранжирането			III позиция в ранжирането		
Parameters	Theoretical Model	Experiment	Parameters	Theoretical Model	Experiment	Parameters	Theoretical Model	Experiment
Function	Logistic		Function	Normal		Function	Triang	
a	79,77		m	78,50		min	5,44	
b	3,97		s	8,30		m. likely	86,52	
Left X	68,1	68,1	Left X	64,8	64,8	Left X	24	24
Left P	5,0%	9,48%	Left P	5,0%	6,48%	Left P	5,0%	0,15%
Right X	91,5	91,5	Right X	92,2	92,2	Right X	86,4	86,4
Right P	95,0%	100,0%	Right P	95,0%	100,0%	Right P	95,0%	94,73%
Diff. X	23,40	23,40	Diff. X	27,32	27,32	Diff. X	62,38	62,38
Diff. P	90,00%	90,53%	Diff. P	90,00%	93,53%	Diff. P	90,0%	94,58%
Minimum	$-\infty$	5,46	Minimum	$-\infty$	5,46	Minimum	5,44	5,46
Maximum	$+\infty$	90,49	Maximum	$+\infty$	90,49	Maximum	90,52	90,49
Mean	79,77	78,50	Mean	78,50	78,50	Mean	60,83	78,50
Mode	79,77	85.14	Mode	78,50	85.14	Mode	86,52	85.14
Median	79,77	80,90	Median	78,50	80,90	Median	64,17	80,90
Std.Dev.	7,20	8,30	Std.Dev.	8,30	8,30	Std.Dev.	19,6	8,30
Variance	51,97	68,95	Variance	68,97	68,95	Variance	384,17	68,95
Skewness	0	-2,44	Skewness	0	-2,44	Skewness	-0,56	-2,44
Kurtosis	4,2	12,89	Kurtosis	3	12,89	Kurtosis	2,4	12,89



а)



б)



в)

Фиг.2. Закони на разпределение на имисиите от прахосмукачка, проверени чрез критерия на Пирсон: а-I позиция, б-II позиция, в-III позиция в ранжиране чрез програма *Risk 4.5*

Таблица 3

Резултати за математическото очакване, средноквадратичното отклонение и дисперсията на ранжираните чрез програмата *Risk 4.5* закони на разпределение от 1 опит с 4000 измерени стойности на общото ниво на шума

Прахосмукачка				Пусков двигател на трактор			
Критерий на Пирсон							
Fit	Mean	St.dev	*K,%*	Fit	Mean	St.dev	*K,%*
Logistic	79,772	7,209	9,037	Weibul	100,606	11,766	11,695
Normal	78,502	8,305	10,579	Logistic	101,471	11,408	11,242
Triangular	60,833	19,600	32,219	Normal	100,734	11,632	11,547
ExtValue	81,999	18,523	22,589	ExtValue	102,875	18,508	17,990
Uniform	47,982	24,558	51,181	Triangular	93,877	19,863	21,158
Expon	78,485	73,035	93,056				

Идентични резултати за законите на разпределение и числените характеристики се получават за имисиите на другите два източника на шум.

За шумовите имисии от пусковия двигател на колесния трактор на първа позиция при ранжирането е нормално разпределение с параметри a=73,274 и b=17,604, на втора позиция инвариантно разпределение на Гаус с параметри a=767,90 и b=14622,32 и на трета позиция логаритмично нормално разпределение с параметри a=744,35 и b=17,597. Средните стойности варират съответно от 100,606 до 102,875 dBA, средноквадратичното отклонение от 11,766 до 18,508, а дисперсията от

138,444 до 342,548 dBA. В случая се установява много по-голямо разсейване на имисиите на шум.

Таблица 4

Сходство на ранжиране на законите на разпределение на шума от прахосмукачка при 1 опит с 4000 измерени стойности

Критерии на:		
Пирсон	Андерсон - Дарлинг	Колмогоров-Смирнов
Logistic	Logistic	Logistic
Normal	Normal	Normal
Triangular	ExtValue	ExtValue
ExtValue	Expon	Triangular
Uniform	Triangular	Expon
Expon	Uniform	Uniform

Таблица 5

Сходство на ранжиране на законите на разпределение на шума от пусков двигател на колесен трактор при 1 опит с 4000 измерени стойности

Критерии на:		
Пирсон	Андерсон - Дарлинг	Колмогоров-Смирнов
Weibul	Weibul	Logistic
Logistic	Logistic	Weibul
Normal	Normal	Normal
ExtValue	ExtValue	ExtValue
Triangular	Triangular	Triangular

Таблица 6

Извадка от резултати за математическото очакване, средноквадратичното отклонение и дисперсията по първи позициониран закон на разпределение при ранжиране чрез програмата Risk 4.5 и проверка на хипотезата чрез критерия на Пирсон за 30 опита и 4000 измерени стойности на всеки опит

Прахосмукачка			Сешоар			Пусков двигател на трактор		
Mean	Stand. dev.	$K,\%$	Mean	Stand. dev.	$K,\%$	Mean	Stand. dev.	$K,\%$
70,523	10,049	14,249	70,527	10,187	14,444	96,861	11,965	12,352
70,633	9,833	13,921	70,494	10,326	14,648	96,79	11,497	11,878
70,432	10,231	14,526	70,768	10,034	14,178	97,872	11,267	11,511
70,232	9,847	14,020	71,411	9,860	13,807	97,469	11,247	11,539

70,677	10,072	14,250	70,811	10,108	14,274	97,929	11,588	11,833
70,599	9,894	14,014	70,424	9,909	14,070	98,926	11,251	11,373
70,565	9,937	14,082	71,085	10,065	14,159	99,306	11,343	11,422
70,768	9,627	13,603	70,877	10,303	14,536	99,073	11,358	11,464
70,757	9,788	13,833	70,475	9,857	13,986	100,734	11,632	11,547
70,579	9,941	14,084	70,721	10,478	14,815	99,904	11,244	11,254

Анализът на числените характеристики на разсейването на резултатите в таблица 2 показва, че представянето на средноквадратичното отклонение $\sigma \equiv$ *Stand. dev.* и едновременно с него дисперсията $\sigma^2 \equiv$ *Variance* не дава особено различна информация. Твърдението се обяснява с факта, че $\sigma[X] = \sqrt{\sigma^2[X]}$.

За отстраняване на този недостатък в информацията на разсейването, съответно неопределеността, бе възприето представяне на коефициента на вариация, който се изчислява по зависимостта $K[X] = (\sigma[X] / m[X]).100$ в % - таблица 3 и 6, и по-нататък за 30 опита – таблица 7.

Таблица 7

Резултати за математическото очакване, средноквадратичното отклонение и дисперсията на ранжираните чрез програмата Risk 4.5 закони на разпределение от 30 опита и 4000 измерени стойности на всеки опит

Прахосмукачка				Пусков двигател на трактор			
Критерий на Пирсон							
Fit	Mean	St.dev	K,%	Fit	Mean	St.dev	K,%
ExtValue	70,76892	0,30236	0,427	InvGauss	128,05	12,63	9,863
Uniform	70,7315	0,30828	0,435	Lognorm	128,05	12,63	9,863
LogLogistic	70,77093	0,31369	0,443	Logistic	128,4281	12,2206	9,515
Lognorm	70,7628	0,2703	0,381	Weibul	127,943	12,801	10,005
Pearson5	70,763	0,27003	0,381	Normal	128,054	12,846	10,031
Triangular	70,7264	0,25641	0,362	Triangular	130,162	14,334	11,012
Weibul	70,76347	0,26539	0,375	Uniform	132,76	18,787	14,151
Normal	70,76267	0,27201	0,384	ExtValue	129,052	16,374	12,687
Logistic	70,74913	0,2913	0,411	Expon	127,197	25,734	20,231

Таблица 8

Сходство на ранжиране на законите на разпределение на шума от прахосмукачка при 30 опита и 4000 измерени стойности на всеки опит

Критерии на:		
Пирсон	Андерсон - Дарлинг	Колмогоров-Смирнов
InvGauss	Logistic	Logistic
Lognorm	InvGauss	InvGauss
Logistic	Lognorm	Normal
Weibul	Normal	Lognorm
Normal	Weibul	Weibul
Triangular	Triangular	Triangular
Uniform	ExtValue	ExtValue
ExtValue	Uniform	Uniform
Expon	Expon	Pareto

Таблица 9

Сходство на ранжиране на законите на разпределение на шума от пусков двигател на колесен трактор при 30 опита и 4000 измерени стойности на всеки опит

Критерии на:		
Пирсон	Андерсон - Дарлинг	Колмогоров-Смирнов
InvGauss	Logistic	Logistic
Lognorm	InvGauss	InvGauss
Logistic	Lognorm	Normal
Weibul	Normal	Lognorm
Normal	Weibul	Weibul
Triangular	Triangular	Triangular
Uniform	ExtValue	ExtValue
ExtValue	Uniform	Uniform
Expon	Expon	Pareto

Установява се, че критерият за проверка на статистическата хипотеза не влияе върху законите на разпределение и върху ранжирането им. Отхвърля се нашето първоначално предположение за влияние на критерият за проверка на статистическите хипотези. При проверка и с трите критерия се получават еднакви закони и съответно числени характеристики. В някои случаи има промяна в последователността на ранжиране, но в III или IV позиция за прахосмукачка и сешоар. Тези твърдения се доказват от данните, които са посочени в таблица 3, 4 и 5. Следователно, не може да се очаква значителна информационна неопределеност от този дескриптор на несигурност.

Таблица10

Средни, средноквадратични и дисперсни информационни рискове

Експеримент от 1 опит и 4000 стойности на имисиите							
Прахосмукачка				Пусков двигател на трактор			
Интервал $\pm\sigma$							
Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$	Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$
Logistic	0,5877	0,6239	0,6322	Weibul	0,6322	0,6537	0,6579
Normal	0,6827	0,6639	0,6538	Logistic	0,6428	0,6953	0,6889
Triangular	0,6437	0,6918	0,6759	Normal	0,6839	0,6933	0,7003
ExtValue	0,7103	0,7722	0,7684	ExtValue	0,7819	0,7972	0,8128
Uniform	0,7922	0,7827	0,7902	Triangular	0,8622	0,8438	0,8548
Интервал $\pm 2\sigma$							
Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$	Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$
Logistic	0,9137	0,9366	0,9473	Weibul	0,9468	0,9548	0,9495
Normal	0,9545	0,9728	0,9737	Logistic	0,9548	0,9647	0,9502
Triangular	0,9637	0,9803	0,9836	Normal	0,9677	0,9657	0,9600
ExtValue	0,9788	0,9888	0,9812	ExtValue	0,9679	0,9571	0,9628
Uniform	0,9811	0,9893	0,9638	Triangular	0,9982	0,9947	0,9673
Експеримент от 30 опита и 4000 стойности на имисиите във всеки опит							
Интервал $\pm\sigma$							
Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$	Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$
ExtValue	0,3822	0,3735	0,3846	InvGauss	0,4327	0,4817	0,4748
Uniform	0,4361	0,4368	0,4477	Lognorm	0,4404	0,4358	0,4728
LogLogist	0,4289	0,4437	0,4402	Logistic	0,4573	0,4834	0,4788
Lognorm	0,4482	0,4326	0,4436	Weibul	0,4733	0,4892	0,4872
Pearson5	0,4812	0,4724	0,4683	Normal	0,4926	0,4973	0,4922
Интервал $\pm 2\sigma$							
Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$	Fit	$R_{Ifexact}\ [\ m\ ]$	$R_{Ifexact}\ [\ \sigma\ ]$	$R_{Ifexact}\ [\ \sigma^2\ ]$
ExtValue	0,7291	0,7348	0,7572	InvGauss	0,8227	0,8347	0,8342
Uniform	0,8102	0,7382	0,7631	Lognorm	0,8459	0,8675	0,8475
LogLogist	0,7683	0,6937	0,7284	Logistic	0,8122	0,8702	0,8437
Lognorm	0,7381	0,7683	0,7703	Weibul	0,8711	0,8806	0,8793
Pearson5	0,7836	0,7921	0,7934	Normal	0,8726	0,8931	0,8894

По-голямо изменение в критерия за проверка на статистическите хипотези се установява при резултатите от 30 опита и 4000 стойности на имисиите на шум-таблица 7, 8 и 9.

Въз основа на резултатите от измерването са определени средните $R_{Ifexact}[m]$, средноквадратичните $R_{Ifexact}[\sigma]$ и дисперсни $R_{Ifexact}[\sigma^2]$ информационни рискове, които са систематизирани в таблица 10.

На основание на изложеното могат да се направят следните изводи:

Информационните рискове се увеличават в зависимост от позицията на ранжиране на законите на разпределение. В по-горните позиции рисковете са по-големи.

По-големи информационни рискове имат имисиите от пусковия двигател на трактор.

Средните информационни рискове са най-малки, което се дължи на малката разлика в математическото очакване при 30 опита на измерване на шумовите имисии.

Средноквадратичните и дисперсни рискове са приблизително еднакви.

По-подходящо е да се въведат рискове за появяване на неопределеност на коефициента на вариация, отколкото дисперсиите. Коефициентът е по-достъпен и разбираем.

Използването на индискретни измервания позволява създаване на големи извадки от данни при малки интервали на дискретизация на записите.

Въведените критерии за информационни рискове са достатъчно чувствителни и отразяват обективно изменението на неопределеността при измервания на имисии на общо ниво на шума.

Литература

1. Владимиров, Л. Рискметрия в екологичната сигурност. Монография. Варна, Варненски свободен университет "Черноризец Храбър", 2009. 279 с.

2. Ковачев, Н., Л. Владимиров. Динамика на неопределеността при измерване на шума в помещения. Част I. Закони на разпределение и числени характеристики. Русе, Русенски университет "Ангел Кънчев", Сборник доклади на Научна конференция 2007. 9-10. 11. 2007. с. 84-89.

ИНФОРМАЦИОННАТА СИГУРНОСТ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Асен Й. Захариев

Asen Y. Zahariev

***ABSTRACT**: The article justifies the relevance of the security information, related problems and the needs to protect information. In common lines derived actions, that ensure security information in their respective fields.*

***KEYWORDS:** security information, danger, action*

В началото на XXI век геополитиката претърпя сериозна трансформация като

относителната тежест на географския фактор постепенно намалява. Глобализацията все повече лишава географската територия и земята от тяхната някогашна стойност. В миналото геополитиката се възприемаше преди всичко като силова външна политика, отчитаща значението на географските фактори. В наши дни обаче, тя все повече се свързва с транснационалните коридори за пренос на нефт и газ, с инфраструктурните и енергийни коридори, както и с развитието на информационните мрежи.

Нарастващата роля на информацията във всички сфери на човешката дейност изменя облика на съвременното общество и го превръща в "информационно общество".

Основната тенденция, която характеризира това общество е високият относителен дял и постоянното нарастване на заетите в информационната сфера.

Информацията все по-ясно се възприема като универсален и ключов ресурс за развитие на обществото.

Събирането, натрупването и достъпът до информация в съвременните организации е основа за иновациите, които от своя страна създават условия за положителна обратна връзка в цикъла на развитието. Скоростта и точността в протичане на информационните процеси определят скоростта на развитие и степента на сигурност. Сигурността и защитата на информацията са фундаментални понятия, около които се изгражда цялата концепция за постигане на конкурентно предимство.

Посредник в общуването на хората станаха компютрите и средствата за мобилна връзка (Интернет, мобилни телефони, факсове и т.н.). Комуникацията с този вид общуване е по-гъвкава, по-динамична, по-бърза, с по-малко ограничения във времето, пространството и начина на изразяване. Промяната в механизмите на обмен на информация трансформира традиционния тип общество в общество от нов тип, с по-голямо разнообразие от взаимоотношения и нов начин на създаване и натрупване на богатство.

Като резултат от увеличения брой връзки нараства необходимостта от повече и по-точни критерии при персонификацията на лицата, които установяват контакт. В резултат на обвързването на човешките дейности с тези технологии се получиха много допълнителни предимства, но едновременно с това се появиха много непознати и неизследвани до този момент рискове и заплахи. Всичко това формира нова уязвимост на социалните организации, която превръща гарантирането на сигурността и защитата на информацията в тяхна ключова компетенция.

На въпросите, свързани с информационната сигурност, се обръща все по-сериозно внимание, но реалните действия по управление на информационните рискове много често са непоследователни и недостатъчни.

Информационната сигурност се гарантира с методи, които могат да се класифицират като правни, организационно- технически и икономически.

Правните методи включват създаването и въвеждането в практиката на юридически нормативни актове (законови и подзаконови), регламентиращи отношенията в информационната сфера и ненормативни методически документи. Най- важните направления в тази дейност са внасяне на изменения и допълнения в законодателството, регулиращо отношенията в областта на гарантирането на информационната сигурност с цел да се изгради и усъвършенства системата в тази област; да се конкретизират правните норми, формиращи правния режим на отговорността за пра-

вонарушения в областта на информационната сигурност на държавата.

Организационно-техническите методи за гарантиране на информационна сигурност са създаване и усъвършенстване на организацията в тази област.

За целта е необходимо да се разработят, използват и усъвършенстват средствата за защита на информацията и на методите за контролиране на ефективността им; да се развива надеждността на специалното програмно осигуряване. Следва да се използват криптографски средства за защита на информацията при нейното съхраняване, обработване и предаване по каналите за връзка, да се сертифицират средствата за защита на информацията, да се лицензира дейността в областта на защита на държавната тайна, да се стандартизират способите и средствата за защита на информацията.

Икономическите методи за гарантиране на информационната сигурност включват разработване на целеви програми в тази област и определяне на реда за финансирането им.

Главните области, подлежащи на гарантиране на информационната сигурност са основна съставяща на националната сигурност и влияят върху защитеността на държавните интереси в различните области на обществената активност. Заплахите за информационната сигурност и методите за гарантирането й са общи за тези области, като във всяка от тях има особености, свързани със спецификата на обектите и степента им на информационна уязвимост. В обществото на държавата, наред с общите методи на гарантиране на информационната сигурност, могат да се използват специфични методи и форми.

В икономическата област на опасности са подложени информационните системи на органите на изпълнителната власт, осигуряващи дейността на обществото и държавата в тази сфера; информационната система за мениджмънт на националната сигурност и стратегическото ръководство на въоръжените сили и отбраната; системата на държавната статистическа кредитно- финансова система; системата на Главно управление “Митници”; системата на Главно данъчно управление; системата за събиране, обработване, съхраняване и предаване на финансова, борсова, данъчна и външноикономическа информация, както и сведения за предприятията, учреждения и организации независимо от формата на собственост.

Сериозна заплаха за нормалното функциониране на икономиката като цяло представляват компютърните престъпления, свързани с проникване на криминални елементи в компютърните системи и мрежи на банки и други кредитни организации.

Основните мерки за гарантиране на информационната сигурност в икономическата област са усъвършенстване на нормативната правна база, регулираща информационните отношения в икономическата област; реорганизиране и осъществяване на държавен контрол над създаването, развитието и защитата на системите и средствата за събиране, обработване и предаване на статистическа, финансова, борсова, данъчна и митническа информация; подобряване на системата на държавната статистическа отчетност за осигуряване на по- висока достоверност, пълнота и защитеност на информацията чрез въвеждане на строга юридическа отговорност на длъжностните лица за подготовката на първичната информация, за организирането на контрол над дейността на тези лица и службите за обработване и анализиране на статистическата информация, както и чрез ограничаване на комерсиализацията на тази информация. За целта е необходимо да се внедрят сертифицирани

средства за защита на информацията в системите и средствата за събиране, обработване, съхраняване и предаване на статистическа, финансова, борсова, данъчна и митническа информация; да се разработват и внедряват стандартизирани национални защитени системи за електронно плащане на базата на интелектуални карти, системи за електронни пари и електронна търговия, както и да се развива нормативната правна база, регламентираща използването им; да се усъвършенстват методите за подбиране и подготвяне на персонал за работа в системите за събиране, обработване, съхраняване и предаване на икономическа информация.

В областта на вътрешната политика има редица заплахи за информационната сигурност: нарушаване на конституционните права и свободи на гражданите в информационната сфера; недостатъчно правно регулиране на обществените отношения в областта на използване на средствата за масово осведомяване от различните политически сили за пропагандиране на собствените идеи; разпространяване на дезинформация за държавната политика, дейността на органите на държавната власт, както и за събитията в страната и чужбина; дейност на обществени обединения, насочена към насилствена смяна на конституционния строй и нарушаване целостта на държавата, разпалване на социална, расова, национална и религиозна вражда, към разпространяване на тези идеи в средствата за масово осведомяване.

В областта на външната политика има много обекти, нуждаещи се от гарантиране на информационната сигурност. Към тях спадат информационни ресурси на органите на изпълнителната власт, осъществяващи външната политика на страната, националните правителства и организации в чужбина и международните организации; дейността на националните средства за масово осведомяване, разясняващи пред чужда аудитория целите и основните направления на държавната политика и официалното мнение по социално значими събития във вътрешния и международния живот.

Главните заплахи за информационната сигурност във външната политика са опитите за несанкциониран достъп до информационната инфраструктура, информационните ресурси и органите на изпълнителната власт, осъществяващи външната политика и ръководещи дейността на националните представителства и организации; информационно въздействие на чуждестранни политически, икономически и военни структури върху разработването и осъществяването на външнополитическата стратегия на страната; разпространяване в чужбина на дезинформация за външната политика на страната; нарушаване на правата на граждани и юридически лица в информационното пространство.

В областта на науката и технологиите има редица важни обекти, нуждаещи се от гарантиране на информационната сигурност: резултати от фундаментални теоретични и приложни научни изследвания, които са потенциално важни за научно-техническото, технологичното и социално- икономическото развитие, включително сведения, чиято загуба може да донесе щети на националните интереси и престижа на страната; непубликувани открития, непатентовани технологии, промишлени образци, полезни модели и експериментално оборудване; научно- технически кадри и системата им на подготовка; системи за управление на сложни изследователски комплекси (ядрени реактори, ускорители на елементарни частици и др.)

В областта на държавните информационни и телекомуникационни системи обекти за гарантиране на информационната сигурност са информационни ресурси, които съдържат класифицирана информация, средства и системи за информатиза-

ция, програмни средства, автоматизирани системи за управление, системи за връзка с пренос на данни, осъществяващи приемане, обработване, съхраняване и предаване на информация с ограничен достъп, техните информационни и технически полета; технически средства и системи за открита информация, но разположени в помещения, в които се обработва информация с ограничен достъп.

Заплахите за информационна сигурност в областта на общодържавните информационни и телекомуникационни системи са дейност на специални служби на чужди държави, престъпни общности, организации и групи, противозаконна дейност на отделни лица, насочени към получаване на несанкциониран достъп до информация и към осъществяването на контрол над функционирането на информационните и телекомуникационни системи.

Организационно- техническите мероприятия за защита на информацията са лицензиране на дейността на организациите в областта на защита на информация, атестиране на обектите за информация за изпълнение на изискванията за защита на информацията при дейности, свързани с използване на съдържащи държавна тайна сведения, сертифициране на средствата за защита на информацията и за контрол на тяхното използване , както и защитеност на информацията от изтичането й по техническите канали на телекомуникационните системи; въвеждане на териториални, честотни, енергийни, пространствени и времеви ограничения в режима на използване на техническите средства, подлежащи на защита; създаване и използване на защитени информационни и автоматизирани системи за управление.

Днес новите виждания за бъдещото развитие на човешката цивилизация обещават да подобрят средата на нашето съществуване. Тези виждания имат потенциала да предизвикат глобални промени. Именно те трябва да се анализират и прогнозират, тъй като предизвикват редица тревожни явления и процеси. Особена актуалност сред тях придобиха проблемите на информационната сигурност, превърнала се в един от основните проблеми на нашето време. Макар да има множество предложения, няма единна общоприета дефиниция за информационна сигурност. Съгласно традиционно прилаганият подход, за сега тя се характеризира само с развитата от нея система от понятия. Сред най-важните от тях са дефинираните в информационното пространство определения за стратегия, политика, превъзходство, мощ, инфраструктура, ресурс, конфликти, сражения, операции, отбрана, сигурност. Чрез тези понятия днес се разкриват основните аспекти на информационната сигурност, нейната същност и съдържание.

Литература

1. Закон за защита на класифицираната информация, Обн. ДВ бр. 45/2002.
2. Правилник за прилагане на закона за защита на класифицираната информация. Обн. ДВ, бр. 115/2002.
3. Стратегия за националната сигурност на Република България
4. Семерджиев, Ц. Стратегическо ръководство (лидерство), Софттрейд, С., 2000.
5. Семерджиев, Ц. Системи за стратегическо ръководство (C4I), Софттрейд, С., 2000.
6. Семерджиев, Ц. Информационна война, Софттрейд, С., 2000.

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

КОРУПЦИЯТА В МАКРОУПРАВЛЕНИЕТО НА ДЪРЖАВАТА НА ГРАЖДАНСКО ОБЩЕСТВО

Димитър Л. Александров

Университет по библиотекознание и информационни технологии
m_allexandrov@yahoo.com

THE CORRUPTION IN STATE MACROGOVERNANCE AT CIVIL SOCIETY

Dimitar L. Alexandrov
State University of Library Studies and Information Technologies
m_allexandrov@yahoo.com

Abstract. *The corruption phenomenon is broadly explored from many points of view as political, economical and psychological and etc. The author proposes multidisciplinary scientific approach and methodologies toad research of the corruption in the state of civil society. He analyzes the macrogovernance corruption stressing on the countries in transition to the democracy.*

KEY WORDS*: corruption, macrogovernance, state of civil society.*

Настоящата статия е посветена на проблемите на корупцията в макроуправлението на държавата на гражданското общество. Чрез прилагане научния инструментариум и методите на многодисциплинарния подход се разкриват същността на корупцията в държавата на гражданското общество. Анализират се условията за корупция в макроуправлението на такава държава. Основно внимание е отделено на причините, свързани със състоянието на демокрацията. Разкрито е различието в остротата на проблема и спецификата на корупционните условия между държавите с утвърдени демократични традиции и т.нар. държави в преход.

Корупцията е исторически феномен. Тя е постоянен спътник на гражданското общество и държавата на всички етапи от тяхното историческо развитие. Корупцията е социално явление, присъщо за гражданското общество и породената от него държава. Тя произтича от нерешените проблеми и противоречията на гражданското общество. Феноменът корупция е резултат на разложителните процеси в гражданското общество, проявяващи се като дисфункция на социалното управление и деградация на властта във формата на нарушаване на закона, обусловено от користна мотивация и цели. Така стигаме до извода, че корупцията е болест не само на държавата, но и на цялото гражданско общество. Следователно корупцията има две страни.

От гледна точка на държавата корупцията е противоправно използване от лица

със служебно положение от субектите на властта и управлението против интересите на службата и с користни цели, както и противоправно предоставяне от такива лица на материални или други предимства на други лица за действия или бездействия, извършвани в тяхна полза с използването на тяхното служебно положение. Както се вижда, корупцията е нещо повече от подкуп и продажност на държавните или фирмените служители. Към корупцията се отнасят користната злоупотреба с власт в държавни, общински, неправителствени и др. организации и частния сектори, различни форми на подкупна продажност на длъжностни лица. В съдържанието на корупцията се включват не само корупционните престъпления, но и други правонарушения, като административни, дисциплинарни, гражданскоправни. В това определение могат да се включат още и "неформални" действия на служители по поръчка на овластени спрямо тях лица с користни цели в интерес на "поръчителите".

От гледна точка на гражданското общество корупцията е противоправно забогатяване, чрез домогване и користно използване на механизмите на политическата власт или на възможностите на съсловни касти като магистрати, нотариуси, лекари, митничари, общинари и др., до чиито услуги често прибягва населението.

Следователно в стремежа да разкрием социалните корени на феномена корупция следва да изясним някои особености на държавата на гражданското общество. Теоретиците на гражданското общество и най-вече Хегел[1] не противопоставят гражданското общество и държавата, а ги приемат като две страни на едно диалектично единство. Гражданското общество е съдържанието, а държавата – формата на битието на един народ. Докато в гражданското общество се реализират частни индивидуални и групови интереси, държавата е предназначена да отстоява общите интереси на всички, на гражданското общество като цяло. Държавата е общият знаменател на интересите на гражданското общество. Ако в гражданското общество отношенията са предимно хоризонтални, то в държавата, състояща се от властови институции, те са вертикални, йерархично подчинени отношения. Основен регулатор на политическите отношения в държавата е правото.

Гражданското общество е съвкупността от доброволни граждански и социални организации и институции, които са в основата на функциониращия социум, пространство на изявява на частния интерес. Тук, обединени в семейни, родови и професионални общности, необезпокоявани от държавата, гражданите разгръщат своите творчески способности и реализират своите индивидуални цели. В тези отношения на обмяна на резултатите на своето материално и духовно творчество те образуват на принципа на доброволността множество формални и неформални групи, като по този начин проявяват своята свобода. Основен социален регулатор на взаимоотношенията в гражданското общество е моралът. Следователно държавата на гражданското общество е държава на моралния императив. Това е държава, чието право почива върху морала, а правоохранителната система, призвана да опазва тези регламентирани от правото морални ценности, почтено възпроизвежда социална справедливост. Самата идея за държава на гражданското общество се очертава като морален ангажимент, като дължимо поведение в интерес на обществеността благо.

Чисто етичната интерпретация се допълва от идеята за социална солидарност. Основоположникът на тази теза Емил Дюркхайм разглежда правото като „съвкупност от обективни условия на социалната солидарност”[2]. Тя е развита от Римския клуб в теорията за „новия хуманизъм“, като глобална солидарност в общата съдба

на човечеството. Ж. Атали обаче подчертава, че "съчетаването на икономическия растеж със социалната справедливост е основният нерешен и почти неразрешим проблем на съвременната цивилизация"[3]. Това е и основният източник на противоречия и конфликти в съвременния свят. Затова в рамките на ЕС, с решение 1672/2006 на Европейския парламент е създадена специална програма за заетост и социална солидарност (ПРОГРЕС) с период на действие 2007-2013 г.

Можем да обобщим, че гражданското общество е съвкупност от икономически и духовни отношения, които извират от сферата на частния интерес, но чието функциониране осигурява социална солидарност и справедливост. Висша ценност в такова общество са правата и свободите на гражданите, равенството на възможностите и социалната справедливост. Социалната справедливост се основава върху концепцията за правата на човека и равен достъп до възможности за обществена реализация, основан върху икономическия егалитаризъм, чрез прогресивно данъчно облагане и при необходимост преразпределение на доход и даже на собственост от богатите в полза на бедните. Следователно държавата на гражданското общество е държава на социалната солидарност, в която членовете на гражданското общество социално се сближават, въз основа на зависимостта на хората един от друг. Когато частният интерес е изроден в състезание за завоюване на властнически позиции, предоставящи възможност за облагодетелстване чрез корупция, тогава обществото е обречено да има корумпирана държава. Ако собствеността, стопанският живот и търговията, междуличностните, груповите и духовните отношения са пропити от корупционни мрежи, съставени от носители на политическия и държавно-властния фактор, тогава гражданското общество стремително деградира.

В структурен план гражданското общество се самоорганизира чрез пазара, медиите и Интернет пространството в различни организации и движения: вероизповедания, икономически групировки, банки, медии, синдикати, учебни заведения, културни сдружения, благотворителни и неправителствени организации и др. Ако частната собственост е материалната субстанция на гражданското общество, то свободата и произтичащите от нея принципи на демократично управление са нейната духовна съставляваща. Следователно на свободното гражданско общество съответства легитимна демократичната държавна власт. Гражданското общество е мрежа от колективни извънполитически образувания, където не само се формира общественото мнение, но и се осъществява публичен контрол върху държавата.

В условията на зряло гражданско общество властта не може да търси легитимността си само в закона. Тази легитимност следва органично да се допълва и с признаване върховенството на принципа за правата и свободите на личността, което предполага и правата на етническите и други малцинства. В условията на демокрация добре работеща държава е само допълнение към гражданското общество. Проблемите на държавата се решават от гражданското общество по еволюционен начин, свързан с активността на гражданите, отстояващи своите права в договора с държавата. Тоталитарната държава може да бъде променена само по революционен път, чрез методите на площадната демокрация. В този смисъл можем да се твърди, че всяко гражданско общество има такава държава, каквато заслужава, което означава, че зрелостта на гражданското общество е жизнено важна за състоянието на демокрацията. Това е така, защото "гражданското общество изгражда социален капитал от доверие и споделени ценности, които се прехвърлят и в политическата сфера и подпомагат държавата да запазва целостта на общността като

цяло, като улеснява разбирателството и взаимосвързаността на обществото и на интересите в него“[4]. Поради това демократичните принципи трябва да се приложат изцяло и върху всички страни на триъгълника "личност – гражданско общество – държава". Следователно държавата на гражданското общество е демократична държава с по-висок морал.

Държава, в която всички гласове имат еднаква тежест, не ограничава възможността на гражданите да станат представители във властта, а правото се осигурява чрез законово утвърдени права и свободи. Демократичните системи обикновено съдържат вътрешни механизми, като разделение на властите, които предотвратяват неравномерното разпределение на властта и потенциалното нарушаване на демократичните принципи от отделни институции.

„Тъй като понятието за гражданско общество е тясно свързано с демокрацията и представителството – отбелязва Гр. Полак – то на свой ред следва да бъде свързано и с идеята за гражданство в рамките на международно гражданско общество”[5]. Неговото начало е положено от инициативите на международни неправителствени организации и активната им намеса в дипломатическите отношения и международния законодателен процес. Постепенно дейността им се превръща в нов източник на легитимност на международното право и полага началото на международни организации на гражданското общество. Европейският съюз е пример за такова международно гражданско общество в началната му фаза на развитие. В него се прави опит да се реализират класически елементи на гражданското общество: свободен (единен) пазар; свободно движение на стоки, услуги, пари и хора върху териториите на много държави. И в съответствие с логиката на гражданското общество се формира и неговата държавна и наддържавна структура.

Следователно държавата на зряло гражданското общество винаги е и държава член на международно гражданско общество. Международно гражданско общество е общество, което полага грижи за свободното движение на хора и стоки, за повишаването на гражданската култура и доброволното сдружаване в социални мрежи, осъществява мониторинг върху състоянието на свободата на печата в света, контролира спазването на гражданските права и свободи, предотвратява изтезанията. Същевременно международното гражданско общество осигурява наднационално правосъдие в международни магистратури, какъвто е Международният наказателен съд в Хага и Европейският съд по правата на човека в Страсбург.

Макроуправлението на държавата включва съвкупността от отношенията между държавното ръководството, между висшите държавни органи на власт и управлението. Макроуправление на държавата също така определя структурата, чрез която се задават целите на държавата, средствата за постигане на тези цели и формите за контрол върху тяхната реализация. Разликата между макроуправлението и управлението се състои в обема, обхвата и времевия хоризонт. Управлението на държавата се ограничава до упражняването на политическата власт и присъщите ù институционални ресурси. Политическата власт предоставя средствата, с които макроуправлението работи. Закономерно възниква въпросът какви са условията, които генерират корупция в макроуправлението на държавата. Ситуацията е коренно различна в държава на зряло гражданско общество, държава с деградирало гражданско общество и държава без гражданско общество.

В държавите без гражданско общество, каквито са диктаторските държави, условията за възникване на корупция фактически са сведени до ниски нива, защото

всеки проблем се решава или еднолично от диктатора, или от негови доверени представители. Присъдите за корупция са изключително строги и често са свързани с физическа ликвидация в резултат на смъртни присъди или инквизиции по време на следствието. Това е така, защото всяко нарушение на закона се възприема като акт, насочен лично срещу диктатора, и води до квалификации от рода „враг на народа" с последващи строги санкции не само срещу извършителя, но и срещу неговото семейство.

По-подробно ще се спрем на условията за корупция в макроуправлението на държавите с гражданско общество, като първо ще разгледаме причините, свързани със законодателството и правоохранителните органи. В своите "Сатири" Ювенал поставя енигматичния въпрос: "Кой ще пази самите пазачи?"[6] В днешния свят този въпрос има решаващо значение за функционирането на националните юрисдикции. В държавите със зряло гражданско общество механизмите за обществен контрол са тези, които, образно казано, пазят пазачите. Така, на свой ред, правосъдието се превръща в ефективна форма на контрол за законност в макроуправлението на държавата. В държавите в преход, които се характеризират с още неформирано и вече деградирало гражданско общество, правосъдната система е обхваната от многобройни корупционни мрежи. Корупционната мрежа е „структурирана прикрита мобилизация на многобройни "ресурси", например: финансови интереси, подчинение на йерархичния ред, солидарност, семейство, приятели, насилие, което би могло да бъде етническо или племенно, религиозно, политическо, регионално, секторно, корпоративно и т.н. Нейните цели, не по-малко на брой от ресурсите, варират от прикриване на незаконни дейности – дребни или мащабни – до пресъздаването на конкуренция, практикувана на законния пазар. Сред тях е и финансирането на политически партии"[7].

В условията на корумпирано гражданско общество широките възможности за протакане на преписките и делата, мудните и архаични правни формалности, ниската ефективност и тромавостта на институциите, съставляващи правосъдната власт, благоприятстват възникването на правосъдна корупция. Тези фактори предизвикват даването на подкупи с цел ускоряване на съдебния процес и решаване в полза на една или друга подкупваща страна. В рамките на съдебната власт отлаганията на делата, разпространението на детайлизирани и архаични правни формалности допринасят за корупцията, като предизвикват даването на подкупи с цел ускоряване на процеса. Всичко това активно се използва, подхранва и поощрява от участващите в корупционните мрежи длъжностни лица по високите етажи на властта. Тяхна основна цел е да корумпират правосъдието, за да осигурят своята безнаказаност чрез превръщане на правилата и съдебните производства в практика ad hoc, основана на желанието и възможността да се плати или да се окажат взаимни услуги. За тази цел те разполагат с необходимата власт и влияние, които успешно използват като лостове за въздействие върху правосъдната власт. По този начин правосъдието се поставя над закона и се подчинява на системата на "клиентелизъм" вместо на конституцията и на действащото законодателство. Така макроуправлението на държавата се лишава от своя най-ефективен контролен механизъм.

На следващо място ще разгледаме причините, свързани с дефицита на социална солидарност. За разкриване причините за корупцията не можем да се ограничим само с взаимоотношенията между личностните характеристики и нормативната база поради факта, че личността пребивава в социална среда, която има свое спе-

цифично развитие във времето. Всеки от елементите на триадата личност – среда – поведение въздейства върху останалите и реверсивно получава тяхното реципрочно въздействие върху себе си. Следователно обкръжаващата среда може да "излъчва" както позитивни, така и "негативни" корупционни сигнали към личността, която е мотивирана да реагира на това с адекватно поведение. Ето защо важен се явява въпросът как личността се интегрира с обкръжаващата я страна.

В държави със зряло гражданско общество социалната солидарност обединява индивидите във взаимно подпомагаща мрежа от трудови, обществени и социални услуги. Активната гражданска позиция на обществото като цяло е действащ възпиращ фактор за корупцията. Обратно, държавите в преход, с още неформирано и вече деградирало гражданско общество, се характеризират с дефицит на гражданска позиция. Основание и мотив за изява на гражданска позиция е собствеността. За съжаление в повечето от страните в преход процесът на преразпределение на националното богатство облагодетелства само много малка част от населението. Така например българският капитализъм е капитализъм с блокирана регулаторна роля на пазара и тържествуващи картелни споразумения, капитализъм на беззаконието, без перспективи за можещите, а само за тези, които принадлежат към класата на олигарсите по рождение.

Разбойническата приватизация не превърна българските граждани от наемници в частни собственици, чиято собственост би ги мотивирала да формират въздействаща за властите гражданска позиция на социална солидарност. Те са изключително зависими от своите работодатели, а при подобна силна зависимост активната гражданска позиция е невъзможна. Процесите на девалвация на гражданската позиция са фактор, елиминиращ социалната солидарност и благоприятстващ възникването на корупционните мрежи. Възпиращата корупцията роля на социалния капитал от доверие и споделени ценности на социалната солидарност практически се свежда до нула. Така тяхната функция на ефективен контролен механизъм в макроуправлението на държавата деградира в демагогия. Мястото им се заема от корупционни мрежи, в които на преден план излизат изгодата от корупцията и незначителният риск за извършителите.

Като правило изгодата от корупцията е взаимна за участниците в корупционната сделка. Често нейните размери са огромни и несравними с никоя друга човешка дейност, което я превръща в един от най-съществените рискови фактори. Корумпирани длъжностни лица присвояват неправомерно несравнимо повече, отколкото ако са почтени. Най-често споменаваната причина за разпространение на корупцията в страните в преход продължава да бъде стремежът към бързо забогатяване на хората или за решаване на техни тежки проблеми, практически нерешими по друг начин. За корумпираните фирми подкупите на длъжностни лица са ефективен начин да печелят поръчки, да изиграят конкуренцията, която предлага по-добри технологии или по-ниски цени. Разходите за подкупи безпроблемно се калкулират в цените на стоките или се третират като приспадащи се от данъците разходи на компанията. Тази изключителна ефикасност на корупцията е мощен фактор, мотивиращ интереса на гражданите за участие в нея и разпространението ù във всички сфери на живота.

Корупционните сделки винаги се сключват тайно, подкупите се плащат на четири очи и обикновено се предават чрез посредници. Единичните случаи, стигащи до правоохранителните органи, лесно могат да бъдат решени със съдействието на

корумпирани полицаи, следователи, прокурори и съдии. Всеки последващ в тази верига може да елиминира почтения труд на предходния. Затова си казва: „По-добре аз да взема парите, отколкото този след мен". Подкупите често се депозират в държави със закони за стриктно укриване на банковата тайна. Правителства на страни, където корупцията е масова практика, рядко преследват даващите подкупи. Родните страни на компаниите, даващи подкупи на длъжностни лица, като правило пренебрегват това, което техните фирми правят в чужбина.

На трето място ще разгледаме причини, произлизащи от степента на зрелост на демокрацията. В държава със зряло гражданско общество демократичните институции осигуряват не само участието на гражданите в управлението на държавата, но и осъществяват действен обществен контрол върху държавните институции. Този контрол е мощен възпиращ фактор за корупционните практики и ги свежда до приемливи за обществото нива. Интерес във връзка с това представляват някои разсъждения на Антонио Грамши, който отбелязва: „На Запад между държавата и гражданското общество взаимоотношенията са били уредени (има се предвид Новото време) и ако държавата започнеше да се дестабилизира, на преден план излизаше здравата структура на гражданското общество. На Изток държавата беше всичко и гражданското общество се намираше в първично, аморфно състояние. Когато държавата се дестабилизира в условията на дълго и болезнено преразпределение на власт и богатство, мястото на обществото заемат корупционни мрежи"[8].

В демократичното гражданско общество отношенията между индивидите са отношения между свободни и равни субекти. В страните в преход те са заменени с корупционни мрежи, за които е характерна йерархичната субординация. Самите структури на гражданското общество са аморфни, пазарните регулатори са блокирани от корупционни мрежи на мафиотски групи и картелни споразумения, обхващащи стопанската област и държавния апарат, медиите са подчинени на конюнктурата на политически фактори и не са станали "рупор" на гражданското общество. В държавите в преход, които се характеризират с още неформирано и вече деградирало гражданско общество, гражданите на практика не разполагат с никакви лостове за контрол върху държавната власт. Тези взаимоотношенията между държава и гражданско общество имат следните отличителни черти:

- Държавата е силната страна във взаимоотношенията държава – гражданско общество.
- Активността на повечето граждани е блокирана. Гражданското общество няма връзка с решения на политически и законодателни проблеми. Единствената възможност на гражданските сдружения е лобирането, което не е законодателно регулирано.
- Гражданските сдружения не решават обществени проблеми, а гравитират около определени частни интереси на ограничен кръг хора и имат право да работят само в тесните рамки, които държавата им е отредила.

Споделяме мнението, че: „Българската политическа система функционира като карикатура на демокрацията, като гротеска на народовластието. Движеща сила на прехода не е волята за свобода и достойнство, а похотта за собственост и поглъщане. Тепърва ще ни става ясно каква част от българското население е избрала престъплението в борбата за „насъщния" и в опита за справяне с индивидуалните кризи"[9]. Институтите на държавността са силно разстроени и отслабнали, държавните структури са обвързали своите интереси с тези на икономическите групировки и

организираната престъпност, които функционират в устойчиви корупционни мрежи.

Така възниква проблемът с „чуваемостта", т.е. обратната връзка от управляваните към управляващите. В повечето от страните в преход отвъд псевдодемократичните привидности, т.нар. „народ" въобще няма думата. Държавата обслужва една обществена група – тази на богатите, като дискриминира всички останали. От управляваните не зависи кой знае колко, така че „чуваемостта" нищо не значи. Всичко това води до сериозна ерозия на политическото представителство. Не е ясно напълно кой кои социални интереси представлява в политическия живот на страната. Наред с традиционните партии се появяват и изчезват партии-фантоми, съществуват противоконституционни етнически партии. На практика над 60% от гражданите нямат свое политическо представителство.

Основни причини за корупцията, свързани със състоянието на демокрацията в макроуправлението на държавата, са неефективната администрация и ограничаване свободата на словото. Корупцията сред публичната администрация е свързана с ползването на властовите ресурси, предоставени от обществото на държавните служители за задоволяване на техни лични или групови интереси. Пребиваването в системата на държавния апарат се схваща като възможност да се употреби потенциалът на съответната длъжност за задоволяване на лични, семейни, родови, партийни и др. интереси. Правителствата продават и купуват стоки и услуги, разпределят субсидии, осъществяват приватизационни сделки, предоставят концесии и др. Държавните служители често имат монополен достъп до ценна информация, налагат санкции, осъществяват контролни функции. Всички тези възможности създават предпоставки за корупция по високите етажи на властта, чиито възможности в това отношение са най-значителни. Поради тези причини те представляват съществен рисков фактор за появата на корупцията. Неефективната бюрокрация поражда у гражданите и предприемачите недоверие към публичната администрация и съмнения в ефективното упражняване на законните права. Резултатът е търсене на привилегировани канали на достъп до процеса на вземане на публични решения чрез корупционни сделки. По този начин се поощрява навлизането на организираната престъпност и на сенчести икономически групировки в макроуправлението на държавата.

Друг основен фактор, който допринася за разпространение на корупцията по високите етажи на властта, е ограничената публичност и ограничението на словото. Колкото повече действията на отговорните институции във високите етажи на властта са обгърнати със секретност, поверителност и други форми на ограничаване на публичността, толкова повече намалява шансът за обществен контрол над тях, което неизбежно води до разширяване на корупцията. Зависимостта на пресата от източници на финансиране често я поставя под контрола на политиците или организираната престъпност. Произволът и липсата на прозрачност в процеса на вземане на публични решения нарастват с течение на времето, защото корумпираните длъжностни лица имат интерес да запазят привилегированите си отношения с фирмите, които им дават подкупи. Журналистиката обслужва доминиращите в гражданското общество долни страсти, направлявани от политико-икономическата олигархия. Защото журналистическата изгода е в клюкарските слухове за един или друг „политик", а не в разкриването на потайните механизми на корумпираната власт. Все още съхранените островчета на обществена градивност и инициативност не се отразяват от медиите, защото не разпалват долнопробни страсти и затова не

са интересни за собствениците на медиите.

За държавите с развито гражданско общество приобщаването към структури на международното гражданско общество, като ЕС, води до засилен граждански контрол върху властта, а с това и до формирането на още по-действени антикорупционни механизми. Трудността за страните в преход, като България, идва от това, че те още не са узрели като национални граждански общества, за да се включат по един естествен начин в общността и да не бъдат нейни "чужди тела". Така стигаме до историческата обусловеност като причина за корупцията.

В исторически аспект, в управлението на страната бедните и административно неефективни държавни администрации винаги са разчитали на "регионални брокери" на местно ниво. В Европа тези "регионални брокери" са mafiosi в Италия, caciques в Испания, comatarhis в Гърция. Те ефективно осъществяват посреднически функции между центъра и периферията в осигуряващи протекции корупционни мрежи. Тези мрежи имат функцията на важен механизъм в поддържането на социалния ред, който води до девалвация на държавността. Така възникват отношения от типа "патрон-клиент", пораждащи корупционни мрежи, естествено подхранвани от слабостите и неефективността в макроуправлението на държавата. Подобни регионални брокери са исторически възниквали в голяма част от страните в преход и разкриват връзката между разрастването на пазарите и нарастването на корупцията, която е особено силна в периодите на преход: "Бързите промени пораждат непознати нови отношения между богатството и властта, а хората се сблъскват с нови ценности и проблеми, възможности и изкушения "[10].

В страните в преход регионалните брокери започват като класически mafiosi. Впоследствие се обвързват с управляващите политически партии – толкова повече, колкото по-дълго време са управлявали. Заедно с тях те изграждат устойчиви корупционни мрежи, с чиято помощ успешно легализират своята престъпна дейност. Веднъж завладели лостовете на макроуправлението на държавата, те успешно се включват в международната организирана престъпност. Затова българската политическа класа и свързаната с нея организирана престъпност възприемат членството в ЕС като възможност към корупционно разграбване на огромните европейски фондове.

От направените дотук разсъждения може да се обобщи, че условията за корупция в макроуправлението на държавата произлизат от нерешените проблеми на гражданското общество. Те са толкова по-благоприятни за корупционни практики, колкото по-незряло е едно гражданско общество. Корупцията вилнее там, където гражданското общество е деморализирано и обзето от духа на печалбата и стремежа към бързо забогатяване на всяка цена. Обхванато от задушаващите прегръдки на многобройните корупционни мрежи, българското гражданско общество е на ръба на своето оцеляване. Днес българите са хора, лишени от ясна перспектива извън стремежа за собственото си оцеляване. Те не са в състояние задружно да произведат каквото и да било, освен поредната корупционна мрежа. Българските политици са „с поведение и мислене на компрадорска колониална администрация и с манталитета на търговски пътници, овреме пратили децата си на топли места в чужбина, където прочее са и техните пари. Когато паянтовата конструкция, наречена българско общество, се срути съвсем, те ще са първите, които ще се изнесат оттук."[11].

Общоевропейският обществен имунитет срещу корупцията отхвърля и ще продължи да отхвърля страни като България като чуждо тяло. Никакви демагогски заклеймявания на европейското „бездушие и егоизъм" не могат да замаскират

простата истина – за да се възроди нашето разложено от корупционни мрежи гражданско общество и неговата корумпирана държава, те тепърва трябва да извървят дълъг и мъчителен път на духовно възраждане. Ако изобщо има сили, които са в състояние да сторят това.

Литература:

1. Хегел, Георг. Философия на правото. С., 1982.
2. Cotterrell, Roger Emile Durkheim: Law in A Moral Domain. 1999.
3. Атали, Ж., Хилядолетие. С., 1992.
4. Robert, D. Putnam, Robert Leonardi, Raffaella Y. Nanetti: Making Democracy Work: Civic Traditions in Modern Italy. 1994.
5. Pollock, Graham. 'Civil Society Theory and Euro-Nationalism'. Studies In Social & Political Thought, Issue 4, March, 2001.
6. Iuvenalis, "Saturae. VI". Лат: "Seelquis custodiet ipsoscustodes...".
7. J. Cartier-Bresson. "Les reseauz de corruption et la strategie des "3S, Sleep, Silence, Smile",, в редактираната от M. Borghi и P. Meyer-Birsch. La Corruption, l'envers des drous de l'homme (Editions Universitaires de Fribourg (Suisse), 1995.
8. Germino, L. Dante. *Gramsci, Antonio: Architect of a New Politics*. Louisiana Press University, 1990.
9. Михайлов, Николай. Наблюдения в огледалото на отчаяните. http://www.librev.com/prospects-bulgaria/804-2010-01-15-13-38-41, 2010.
10. Johnston, Michael. Corruption Markets and Reform. Paper presented at the Seventh IACC. Beijing, China, October, 1995.
11. Христов, Иво, Икономическият живот е в долна мъртва точка. http://www.obshtestvo.net/content/view/1931/4/, 2010.

СЪВРЕМЕННИ ПРИНЦИПИ ЗА УПРАВЛЕНИЕ

Атанас Н. Митев

УНИБИТ, Адрес: София 1784, бул. "Цариградско шосе" № 119;
E-mail: atanas.nik@abv.bg

MODERN MANAGEMENT PRINCIPLES

Atanas N. Mitev

ABSTRACT: *Effective management of an organization is achieved by understanding the changes. Modern manager or director of an organization must deal with the changing environment and to understand the processes in it. For this purpose, they may use some typically "business" principles of management.*

KEY WORDS: *Management, Management principles.*

Гъвкавостта е в основано качество на успешните ръководители. Те трябва да се съобразяват с променящите се изисквания на средата, за да могат да ръководят

една организация успешно. За тази цел при управлението в сектора за сигурност могат да се използват някои основни принципи на управление, употребявани успешно в други сфери.

Управлението (мениджмънта) е реализация на ръководни функции. То е сложен процес на реализация на функциите – планиране, организиране, координиране, командване и контролиране. Те са свързани в единно цяло чрез реализацията на спомагателните функции – комуникация и вземане на решения. Управлението е особен вид комплексна дейност, превръщаща неорганизираната тълпа в ефективна целеустремена, производителна група. То стимулира социалните промени и генерира примери за успешно или неуспешно поведение на ръководителите (т.н. добри практики). [2] Процесът на управление е целесъобразно въздействие на един обект, устройство или система върху друг обект или система, насочено към параметрични или структурно-функционални изменения в последните с цел преместване по зададена траектория в пространството на състоянията, при което се осигурява устойчивостта на управлявания обект в обкръжаващата среда и се съхранява или намалява неопределеността в триадата среда – система – управление.

Целта е ефективното управление на човешките, финансовите и материалните ресурси, за изграждане и поддържане на необходимите способности в международен и съюзен контекст, като част от националния сектор, при определени законови и административни процедури.

Функциите на управлението не са изолирани и отделни, винаги приложими последователно, или предназначени да се реализират самостоятелно. Те са взаимнозависими и препокриващи се, прилагат се в неуточнен ред и са предназначени да се реализират съгласувано.

В тази традиционно утвърдила се интерпретация командването и управлението се схващат като две страни на общ циклично-реверсивен процес, в който командването е упражняване на власт („отгоре надолу"), а управлението – въздействие по линията на обратната връзка за оказване на коригиращи въздействия при реализация на предприетите действия („отдолу нагоре"). В нея командването се адресира към работата по разгръщане, развитие и експлоатиране на възможностите за въздействие върху околната среда, а контрола се възприема като налагане на ограничения чрез мониторинг, ограничаване и направляване в желано направление.

Тук се възприема схващането, че контрола е част от управлението, в която се извършва проверка (чрез сравнение за подобие, или чрез експеримент, или чрез събиране на доказателствен материал). [1]

Насоченост към клиента – Организациите зависят от своите клиенти и, следователно, трябва да разбират техните текущи и бъдещи потребности, да се готвят да ги посрещнат и да се стремят да превишат очакванията на клиента. Основните ползи са повишаване на ефективността на използваните организационни ресурси, за повишаване на лоялността и удовлетвореността на клиента, което води до регулярен бизнес. Прилагането на този принцип обикновено води до по-добрата комуникация на нуждите на клиента към цялата организация и осигуряване на съответствие между организационните цели и потребностите и очакванията на клиента. Резултатите от това са възможността за измерване на удовлетвореността на клиента и предприемане на действия в съответствие с резултатите и систематично менажиране на отношенията с клиентите. Този принцип осигурява баланс между удовлетворяване на клиентите и интересите на други заинтересовани (собственици,

служители, доставчици, финансиращи организации, местната общност и обществото като цяло).

Лидерство – Лидерите изграждат единство на целите и насоките за развитие на организацията. Те трябва да създават и поддържат вътрешна среда, в която хората са напълно приобщени в постигането на организационните цели. Основните ползи от това са разбирането на хората и тяхната мотивация за постигането на организационните цели. Дейностите се оценяват, координират и прилагат по единен начин и неразбирателството и лошата комуникация между организационните нива е минимизирано. Прилагането на този принцип обикновено води до съобразяване с потребностите на всички заинтересовани страни (клиенти, собственици, служители, доставчици, финансиращи организации, местната общност и обществото като цяло), ясна визия за бъдещето на организацията и създаване и поддържане на споделени ценности, справедливост и морални лидери на всички нива в организацията. Резултатите от това са изграждане на доверие и елиминиране на страха и осигуряване на хората с необходимите ресурси, подготовка и свобода на действие, съчетани с отговорност и отчетност. Този принцип вдъхновява, поощрява и дава признание за приноса на всеки отделен човек в организацията.

Приобщаване на хората – Хората на всички нива са същността на една организация. Тяхното пълно приобщаване дава възможност да се използват пълните им способности в полза на организацията. Основните ползи са мотивираните, посветени и приобщени хора в организацията и възможността за иновативност и творчество в постигане и развитие на целите на организацията. Всеки отговаря за собствените си резултати и хората желаят и се стремят да участват и да допринасят за непрекъснатото усъвършенстване на организацията. Прилагането на този принцип обикновено води до разбирането на хората за важността на техния принос и роля в организацията, ограниченията за своята полезност и резултатност. Хората приемат проблемите като свои и своята отговорност за разрешаването им. Те оценяват постиженията си спрямо своите индивидуални цели. Резултатът от това е, че хората активно търсят възможности да повишат своята компетентност, знания и опит, споделят ги свободно с останалите и открито дискутират проблемите.

Процесен подход – Желаният резултат се постига много по-ефективно, когато дейностите и свързаните с тях ресурси се управляват като процес. Основните ползи са по-ниски разходи и съкращаване на цикъла, чрез ефективно използване на ресурси и постигането на подобрени, постоянни и прогнозируеми резултати. Това допринася за фокусиране и приоритизиране на възможностите за усъвършенстване. Прилагането на този принцип обикновено води до възможността за систематично дефиниране на дейностите, необходими за постигане на желан резултат и установяване на ясна отговорност и отчетност, за управлението на ключовите дейности. Резултатът е фокусиране върху фактори като ресурси, методи и материали, които ще усъвършенстват ключови дейности в организацията и възможността за оценка на риска, последствията и въздействието на дейностите върху клиенти, доставчици и други заинтересовани.

Системен подход към мениджмънта – Идентифицирането, разбирането и управлението на взаимно свързани процеси като система допринася за ефективността и ефикасността на една организация за постигане на нейните цели. Основните ползи са интеграцията и съгласуването на процесите, за най-добро постигане на желаните резултати, възможността да се фокусират усилията върху ключовите

процеси и създаването на увереност в заинтересованите страни в последователността, ефективността и ефикасността на организацията. Прилагането на този принцип обикновено води до структурирането на система за постигане на организационните цели, по най-ефективния и ефикасен начин и до разбиране на взаимозависимостите между процесите в нея. Структурират се подходи за хармонизиране и интегриране на процеси и се осигурява по-добро разбиране за ролите и отговорностите, необходими за постигане на общите цели, като по този начин се намаляват междуфункционалните бариери. Резултатите от това са разбиране на организационните способности и възможността за определяне на ресурсните ограничения, преди предприемане на действия. Специално се разглеждат и се дефинират начините за изпълнение на определени дейности в системата и нейното непрекъснато усъвършенстване, чрез измервания и оценка.

Непрекъснато усъвършенстване – Непрекъснатото усъвършенстване на цялостното функциониране на организацията трябва да бъде постоянна нейна цел. Основните ползи са предимство на резултатите, чрез повишаване на организационните способности, съгласувано усъвършенстване на дейностите на всички нива в единен стратегически замисъл и гъвкавост за бърза реакция на появяващи се възможности. Прилагането на този принцип обикновено води до използването на цялостен и последователен подход за непрекъснато усъвършенстване на функционирането на организацията и се осигурява подготовка по методи и средства за тази цел. Непрекъснатото усъвършенстване на продукти, процеси и системи се превръща в цел за всеки отделен човек в организацията. Резултатът е поставянето на цели, които да насочват, и мерки за проследяване на непрекъснатото усъвършенстване.

Базиране на фактите при вземане на решения – Ефективните решения се базират на данни и информация. Основните ползи са информирани решения, повишена способност да се демонстрира ефективността на взети решения, чрез позоваване на записани фактически резултати и повишена способност за преглед, оспорване и промяна на мнения и решения. Прилагането на този принцип обикновено води до осигуряване на достатъчна точност и надеждност на данните и информацията, осигуряване на достъп до данните на тези, които се нуждаят от тях, анализ на данни и информация с прилагане на валидни методи и вземане на решения и предприемане на действия на основата на анализ на факти, балансиран с опита и интуицията. [1]

Ефективното управление на дадена организация се постига, чрез разбирането на промените. Те са неизбежни и не могат да се управляват. В днешния бързо развиващ се свят промяната е нормално явление. Обикновено промените са свързани с неприятни процеси, изискват много работа и крият много рискове. [3] Съвременния мениджър или ръководител на дадена организация (независимо от нейната сфера на дейност) трябва да се справя с променящата се среда и да разбира процесите в нея. За тази цел могат да се използват някои от тези „бизнес" принципи на управление. Тяхната реализация зависи предимно от спецификата на организацията, но като цяло те са общоприложими в почти всяка организация, включително в тези от сектора за сигурност.

Използвана литература

1. Семерджиев, Ц., Теория и практика на мениджмънта, 2005
2. Drucker, Peter F., A New Discipline, Success!, January – February, 1987

3. Drucker, Peter F., Management Challenges for the 21st Century, 1999, ISBN 109780887309984

УПРАВЛЕНИЕ НА РИСКА ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ

Атанас Н. Митев

УНИБИТ, Адрес: София 1784, бул. "Цариградско шосе" № 119;
E-mail: atanas.nik@abv.bg

RISK MANAGEMENT OF INFORMATION SECURITY

Atanas N. Mitev

ABSTRACT: *The risk will always exist and the leadership of an organization must try to manage it and minimize it. The modern world provides many new technological means through which important and valuable information can be protected, but also allow easy access to such information. Therefore these new technological means must be applied and the process of risk management understood to achieve a good level of protection.*

KEY WORDS: *Risk Management, Informational Security, Controls, Access Control.*

Процесът на управление на риска за информационната сигурност е непрекъснат и повтарящ се процес. Средата се променя непрекъснато и нови заплахи и уязвимости се появяват всеки ден. От друга страна, изборът на противодействие (компютърни системи и контрол) за управление на риска, трябва да намери баланса между производителност, цена и ефективност на противодействие и стойността на информационните активи, които ще се защитават. Не е възможно да се оправдае съществуването на системи за защита, чиято цена е по-голяма от защитаваната информация.

В общи линии, процесът на управление на риска се състои от шест основни компонента:

1. Идентификация на активи и оценка за тяхната стойност. Включва: хора, сгради, хардуер, софтуер, данни (електронни, печатни и други) и консумативи.

2. Провеждане на оценката на заплахата. Включва: природни бедствия, военни действия, аварии, злоумишлени действия с произход от, или извън организацията.

3. Провеждане на оценка на уязвимостта, като за всяка уязвимост се изчислява вероятността, че ще бъде използвана. Оценка на политики, процедури, стандарти, обучение, физическа охрана, контрол на качеството, техническа обезпеченост.

4. Изчислява се въздействието на всяка заплаха върху всеки актив. Използва се качествен или количествен анализ.

5. Идентифициране, избиране и изпълнение на подходящ контрол. Осигуряване на пропорционален отговор.

6. Оценка на ефективността на мерките за контрол. Осигурява се, че контрола предоставя необходимата ефективна защита без високи разходи или забележима загуба на производителност.

Рискът е вероятността, че нещо лошо ще се случи, причиняващо вреда на информационен актив, или загуба на такъв. Уязвимостта е слабост, която може да се използва, за да се застраши или увреди информационен актив. Заплахата е нещо, което има потенциал да причини вреда.

Вероятността, че дадена опасност ще използва уязвимост в системата, за да причини вреда, създава риск. Когато заплахата използва уязвимостта, за да нанесе вреда, тя има въздействие. В контекста на информационната сигурност, въздействието е загуба на достъпност, надеждност, конфиденциалност и други загуби (пропуснати ползи, загуба на човешки живот, загуба на недвижими имоти). Трябва да се отбележи, че е невъзможно да се идентифицират всички рискове, нито пък е възможно да се премахнат всички рискове.

Оценката на риска се извършва от екип от хора, които имат познания за специфичната област. Тя може да използва субективен качествен анализ на базата на информирано мнение или, когато има надеждни финансови данни и историческа информация, анализът може да бъде количествен.

Системата за информационна сигурност трябва да защитава информацията през целия й жизнен цикъл, от първоначалното създаване на информацията до окончателното й унищожаване. Информацията трябва да бъде защитена по времето на нейния пренос и съхранение. За времето на своето съществуване, информацията може да премине през много различни системи за обработка и чрез много различни части на тези системи. Има много различни начини, по които информацията и информационните системи могат да бъдат застрашени. За да може напълно да се защити информацията по време на нейното съществуване, всеки от компонентите на системата за обработка на информация трябва да има собствени механизми за защита. Изграждането, наслояването и припокриването на мерките за сигурност се нарича защита в дълбочина. Силата на всяка система е голяма, колкото най-слабия й компонент. С помощта на стратегията за защита в дълбочина, ако една защитна мярка не успее да проработи има и друга такава, която да продължи да осигурява защита. Това е един от най-добрите начини за управление на риска за информацията. Допълнително към тази система, за да се намали риска се включват и различни видове контрол.

Когато се избира как да се управлява и намалява риска, това се постига, чрез прилагане на един или повече от следните три различни вида контрол:

Административен контрол – състои се от одобрени писмени политики, процедури, стандарти и насоки. Те информират хората за това, как се управлява дейността на организацията и как се провеждат ежедневните им дейности. Законите и наредбите, създадени от държавните органи, също са вид административен контрол. Някои сектори на промишлеността имат политики, процедури, стандарти и насоки, които трябва да се спазват. Други примери за административен контрол включват корпоративна политика за сигурност (използването на „сигурни" пароли за достъп и т.н.), политики за наемане на персонал, както и различни дисциплинарни правила. Административните проверки са в основата на избора и изпълнението на технически и физически контрол, като те всъщност са проява на административен контрол.

Технически контрол – използване на софтуер и данни за наблюдение и контрол на достъпа до информация и компютърни системи. Например: пароли, мрежови и хост базирани защитни стени и мрежови системи за откриване на неоторизиран достъп, списъци за контрол на достъп и криптиране на данните са технически контрол. Важен технически контрол, който често се пренебрегва, е принципът на най-малки привилегии. При принципа на най-малките привилегии се изисква човек, програма или системен процес, да имат само толкова привилегии за достъп, колкото са необходими за изпълнение на задачата. Нарушението на този принцип може да се появи, когато дадено лице получава допълнителни привилегии за достъп с течение на времето. Това става, когато работните задължения на служителите се променят, те са прехвърлени на нова длъжност, или те се прехвърлят в друг отдел. Привилегиите за достъп, които се изискват от новите задължения, често се добавят към вече съществуващите им привилегии за достъп, които вече може да не са необходими или подходящи.

Физически контрол – наблюдение и контрол на околната среда на работното място и компютърните съоръжения, също така наблюдение и контрол на достъпа до и от такива съоръжения. Например: врати, ключалки, централно отопление и климатизация, алармени системи, противопожарни системи, камери, бариери, огради, физическа охрана и т.н. Разделянето на информационната мрежа и работното място във функционални области също е физически контрол. Важен физически контрол, който често се пренебрегва е разделянето на функциите. Отделянето на функциите гарантира, че дадено лице не може да завърши важна задача само. То трябва да изиска, например, подпис или упълномощаване от друго лице, за да нареди плащане или да извърши друга дейност.

Важен аспект на управлението на риска за информационната сигурност е оценяването на стойността на информацията и определянето на подходящи процедури и изисквания за нейната защита. Не цялата информация е еднаква и не цялата информация изисква еднаква степен на защита. За това се налага да се определят различни класификации за сигурност.

Първата стъпка за класификация на информацията е да се определи член на висшето ръководство като собственик на определената информация, която ще бъде класифицирана. След това се разработва методиката за класификация, като тя трябва да описва различните етикети за класификация, които се дават на всеки вид информация, определя критериите за даването на конкретен етикет на дадена информация и описва изисквания контрол на сигурността за всяка класификация. Различните видове етикети зависят от стойността на тази информация за организацията, на колко години е информацията и дали тя все още е актуална. Законите и други нормативни изисквания също са важни съображения при класифицирането на информацията.

Всички служители в организацията трябва да бъдат обучени относно методите за класифицирането на информацията, да са запознати с изисквания контрол на сигурността и процедурите за работа за всеки вид класификация. Класификацията на даден актив информация е необходимо да се преразглежда периодично, за да се гарантира, че тя все още е подходяща за тази информация и за да се осигури дали се упражнява необходимия контрол на сигурността, изискван от вида на информацията.

Достъпът до защитена информация трябва да бъде ограничено до хората, които

са получили разрешение за достъп до нея. Компютърни програми отделни компютри, които обработват информацията, трябва също да бъдат с ограничен достъп. Това изисква наличието на механизми, които да контролират достъпа до защитена информация. Силата и сложността на механизмите за контрол на достъпа, трябва да бъдат в паритет със стойността на информацията, която се защитава – колкото по-чувствителна или ценна информация, толкова по-силен трябва да бъде механизмът за контрол. Базата, на която са изградени механизмите за контрол на достъпа започват с идентификация и удостоверяване (автентикация).

Идентификацията е твърдението, за това кой е някой или какво е нещо. Ако дадено лицето се идентифицира с името си, то потвърждава самоличността си, но това твърдение може да бъде истина или лъжа. Преди лицето да може да получи достъп до защитена информация, е необходимо да се провери дали то е този, за когото претендира да бъде. Удостоверяването е действието за проверката на заявената идентичност (визуална проверка на снимка в документ, сравнение на подпис, използване на код или ключ за достъп и т.н.).

Основните начини за удостоверяване на самоличността на дадено лице са три различни вида информация: нещо, което знае (ПИН код, парола, моминско име и т.н.), нещо, което има (лична карта, магнитна карта, ключ и т.н.) или нещо, което е (отнася се за биометричните данни: отпечатъци от длани и пръсти, гласово разпознаване, сканиране на ретината и т.н.). Силния механизъм за контрол изисква идентификация, чрез предоставяне на информация за поне две от трите. В днешно време, най-разпространената форма на идентификация, се използва основно при компютърните системи: потребителско име (Username) и парола за достъп (Password). Те вършат работа, но в нашия модерен свят те вече не са адекватни. Потребителските имена и пароли бавно се заменят с по-сложни механизми за проверка на автентичността.

След като човек, програма или компютър са идентифицирани успешно, трябва да се определи, до какви информационни ресурси ще имат достъп и какви действия ще им бъдат разрешени да извършват (стартиране на програма, преглеждане, създаване, изтриване или промяна на файл). Това е упълномощаване (авторизация).

Упълномощаването за достъп до информация и други компютърни услуги, започва с административни политики и процедури. Политиките предписват, каква информация и компютърни услуги могат да бъдат достъпни, от кого и при какви условия. Механизмите за контрол на достъпа след това се конфигурират за прилагане на тези политики.

Различните компютърни системи са оборудвани с различни видове механизми за контрол на достъпа, но основно механизмите за контрол на достъпа до дадена система, се основават на един от три подхода за контрол на достъпа или комбинация тях: **Неселективният** подход обединява всички видове контрол на достъпа в централизирана администрация. Достъпът до информацията и другите ресурси, обикновено се основава на функциите на физическите лица в организацията и задачите, които те трябва да изпълняват. **Селективният** подход дава на автора или собственика на информационния ресурс, възможността да контролира достъпа до тези ресурси. При подхода за **задължителен контрол на достъпа**, достъп се предоставя или отказва на базата на класификацията за сигурност, дадена на информационния ресурс.

За да бъдат ефективни, политиката и другите видове контрол за сигурност,

трябва да бъдат приложими и налагани. Ефективната политики гарантира, че хората се бъдат държани отговорни за действията си. Всички неуспешни и успешни опити за удостоверяване трябва да се записват и всеки достъп до информация трябва да има някакъв вид отчитане, за да може да се проследяват при бъдещи проверки на сигурността.

Друг ефективен начин за управление на риска за информационната сигурност е криптирането на информацията. Това е процеса на превръщане на използваема информация във форма, която я прави неизползваема от лица, различни от упълномощеното. Информацията, която е криптирана (направена е неизползваема), може да се върне отново в оригиналната си използваема форма от упълномощен потребител, който притежава криптографския ключ, чрез процеса на декриптиране. Криптирането се използва в информационната сигурност за защита на информацията от неразрешено или случайно разкриване, докато тя се съхранява или прехвърля някъде (по електронен или физически път).

Криптографията дава на информационната сигурност и други полезни приложения, като подобрени методи за удостоверяване, цифрови подписи, цифрови сертификати и криптирани електронни комуникации. Но криптографията може да донесе допълнителни проблеми със сигурността, ако не се използва правилно. Трябва да се използват утвърдени решения, които са били подложени на строга потребителска проверка от независими експерти в областта на криптографията. Дължината и силата на криптиращия ключ е също важен фактор. Ключ, който е слаб или прекалено кратък, ще произведе слабо криптиране. Ключовете, използвани за криптиране и декриптиране на информацията, трябва да бъдат защитени със същата степен на взискателност, както всяка друга класифицирана информация. Те трябва да бъдат защитени от неразрешено разкриване и унищожаване, но те трябва и да бъдат на разположение, когато са необходими.

Рискът винаги ще съществува и неговото управление и минимизиране е основна част от задълженията на ръководството на една организация, особено ако тя разполага с информация с ограничен достъп. Съвременната епоха предоставя множество нови технологични средства, чрез които тази важна и ценна информация може да се защитава, но също така и дават възможност за лесен достъп до такава. За това средства трябва да бъдат прилагани и процесът на управление на риска разбиран, за да може да се постигне добро ниво на защита на информацията.

Използвана литература

1. Office of Government Commerce, Management of Risk. Guidance for Practitioners, 2007, ISBN 0113310382
2. Kiountouzis, E. A.; Kokolakis, S. A., Information systems security: facing the information society of the 21st century, 1996, ISBN 0412781204
3. NIST SP 800-30, Risk Management Guide for Information Technology Systems
4. http://en.wikipedia.org/wiki/Information_security

СТАНДАРТИ, СЕРТИФИЦИРАНЕ И ОДИТ НА СИСТЕМИ ЗА СИГУРНОСТ В АСПЕКТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Георги К. Баев

STANDARTS, SERTIFICIONS AND ODIT OF SECURITY SYSTEMS IN SECURITY INFORMATION FIELD.

Georgi K. Baev

Abstract: Standart in information secuity gives possibilities to organized inside order and security. The organizing people have competed advance by using the information standart.

In this paper are developed some kind of standarts, posiotion of controling officials andstages of sertification

Key words: standards, security, sertification, information.

Стандартите в информационната сигурност допринасят за вътрешния ред, сигурност и конкурентно предимство на организациите. Системите за управление сигурността на информацията помагат на организациите да бъдат по-печеливши, да работят и да управляват себе си по-добре.

Информацията, с която боравят, трябва да бъде защитена и затова за компаниите става все по-важно демонстрирането на ангажимента им към такава защита. Благодарение на стандартите в информационната сигурност, компаниите са наясно със съществуващите рискове, с възможностите да подобрят инфраструктурата си и да заявят на партньори и заинтересовани страни, че са поели ангажимент за спазване на изискванията.

Видовете стандарти се характеризират като: оценъчни стандарти, насочени към класификация на информационните системи и средствата за защита по изискванията за сигурност на информацията и технически спецификации, регламентиращи различни аспекти по реализация на средствата за защита.

Тези два вида нормативни документи са взаимосвързани. „Оценъчните стандарти определят най-важните от гледна точка на информационната сигурност характеристики на информационната система, играейки роля на архитектурна спецификация, а техническите спецификации указват начините и средствата за достигане на тези характеристики“ [2].

Сред стандартите са ISO/IEC 15408 – оценъчен стандарт, издаден на 1 декември 1999 г. Явява се метастандарт, определящ инструментите за оценка на сигурността на информационните системи и порядъка на тяхното използване.

BS 7799 - английски стандарт за управление на информационната сигурност, на който са базирани съвременните международни стандарти в тази област. В годините претърпява актуализация и развитие до три части. Първата му част е издадена през февруари 1995г.

ISO/IEC 17799 - първият международен стандарт, определящ общ модел за създаване на система за информационна сигурност. Базиран е на стандарта BS 7799

част 1 и 2. За пръв път е публикуван през 2000г.

ISO/IEC 2700x - серия международни стандарти, която днес се използва за оценяване и създаване на системи за информационна сигурност. Първият стандарт от серията ISO/IEC 27001 е публикуван през 2005 г.

ISO/IEC 27001 - стандарт, по който организациите могат да бъдат сертифицирани.

ISO/IEC 27002 - преименуван ISO/IEC 17799

ISO/IEC 27006 - ръководство по акредитация на сертифицирани организации и т.н.

У нас след приемането на Закона за електронното управление през 2008 г. и Наредбата за общи изисквания за оперативна съвместимост и информационна сигурност, на държавната администрация се налага внедряване на система за управление на сигурността на информацията (СУСИ) и сертифицирането ѝ съгласно регламента на стандарта ISO/IEC 27 001:2005. [6]

Стандартът ISO/IEC 20 000 обхваща качеството на предлаганите ИТ услуги. Когато се говори за обхвата на стандарта ISO 20 000 в администрациите, например за една община, сертификацията обхваща само ИТ услугите, които се предоставят от общината за ползвателите в нея. Що се отнася до ИТ компаниите, ISO 20 000 е много по-полезен и пълноценен, отколкото стандарта ISO 9001, категорично е и мнението на специалисти от сектора. Изразява се увереност, че след време наличието на сертификат ISO 20 000 ще бъде сред изискванията на държавната администрация за кандидатстване по обществени поръчки.

От изключителна важност е регулаторните органи да въвеждат тези стандарти с регулация, какъвто е примерът с Печатницата на БНБ, Народната банка на Македония, която няколко поредни години въвежда регулации в тази посока и ефектът е положителен. Освен в Македония, такива регулации има и в Хърватска, подобни има и в Унгария и Полша. В тези държави нормативната основа е много по-добра и това е причината нещата да се случват правилно, спазвайки изискванията на международните стандарти там, където държавата е преценила да направи задължително изискването за сертифицирани системи.

„Днес в световен мащаб има много сериозни заплахи, което предопределя отделяне на особено внимание на сигурността“ [3]. От тук се поражда и острата нужда за обучение и развитие на нови кадри в сектора. Обучението започва още със самото решение за внедряване – например това е добра фирмена позиция на компанията G4S Security Services България. Обещаващото начало започва с обучението на мениджмънта, вземащ стратегически решения. Тъй като няма представа за проблематиката на внедряването на системата, в хода на самото внедряване обучението трябва да премине през етапите на управлението на риска. Следващият етап е обучение за внедряването на механизмите за контрол, което трябва да е паралелно с процеса на внедряване на системата. Обучение при вече внедрена система е закъсняло по отношение на откриването на логиката на контрол.

Естествено това действие ще бъде безсмислено, ако системата не бъде сертифицирана. Когато една компания трябва да вземе решение кой ще е сертификаторът, няколко са основните направления, на които трябва да се спре. Обикновено се смята, че процедурата е разделена в три основни момента - проверка на акредитацията на сертификатора, цена и провеждане на консултации с контрагентите.

Според специалисти от мобилни компании в България водещ е опитът на сертифициращата организация с положително завършили внедрявания на система за

управление на ИС. Точните консултанти с необходимия опит и подходящо сертифицирани теоретична подготовка и практически приложени знания също са изключително важни в този избор. Акредитацията е формата, с която се гарантира качеството на предлаганата услуга от страна на сертифициращата организация и когато сертификатът е с акредитация, той може да бъде проследен международно, като се гарантира напълно, че проблеми с признаването му където и да е по света няма да има.

„Хората, които сертифицират системата изключително точно трябва да дефинират обхвата, защото в противен случай успешната сертификация е невъзможна“[4]. Когато се прави частична сертификация и стандартът се спазва стриктно, няма проблем да бъде сертифициран само един процес или част от дейностите. Сертифицирането само на един процес според някои обаче понякога е лош имидж за самата организация.

Една е информационната сигурност на организация, нямаща достатъчно средства и друга на организация, която има финансовите възможности и може да си позволи закупуване и въвеждане на добри и модерни технологични мерки за сигурност. Сигурността на организацията, направила по-голяма разход, е много повисока.

Най-често подценяваният разход са времето и хората. Това, с което трябва да се бори организацията като разход, освен финансовата страна, която може да бъде планирана, разсрочвана във времето и достатъчно добре намествана спрямо бизнес плановете и целите на една организация, е човешкият ресурс. Важно е планирането, предвиждането на разходи, свързани с консултантска дейност, обучение, внедряване на решението, реализиращо СУСИ, сертифицирането и поддържането на сертификацията във времето.

След успешното преминаване на всички етапи на сертификация следва одит. Той се извършва от сертификационна организация. Представлява предварително синхронизирана проверка, независима и обективна оценка, целяща да се отговори както на изискванията на клиента, така и на акредитиращата организация.

Времето се планира предварително, договаря се според изискванията на няколко стандарта и се определя спрямо сложността на областта, която ще се одитира. Едновременно с това, ангажимент на сертифициращата организация е да подбере правилната компетентност на хората си. „Подходът, насочен към управлението на риска е правилен и при извършване на одита, защото точно тогава се виждат проблемите свързани с прилагането на механизми за контрол“ [1].

Опитът показва, че първият голям одит продължава около една седмица, след което има един годишен, с продължителност около три дни. В зависимост от дейността на организацията е различна и продължителността на одита.

Има и мнения, че одиторите от съответната сертификационна организация не би следвало да са консултанти. Правилният подход на одита е процесният подход, подходът за изпълнение на план за намаляване на риска и съответно ефективността на механизмите за контрол. Често одиторите се опитват да дадат привнесена стойност, споделяне на добра практика, без да задължават някого да прави нещо.

Изводи:

Необходимостта от изграждане на Система за управление на информационната сигурност /СУСИ/ е породена от все по-нарастващата тенденция за използване на информационните технологии за електронен документооборот вътре в организаци-

ята и между различни организации и извършване на други бизнес дейности по електронен път. Това изисква висока степен на доверие между заинтересованите страни. „Необходимо е ефективно управление на технологиите и процесите, които са свързани с обмена и съхранението на данни и информация“ [5]. Внедряването на СУСИ е стратегическо решение за организацията, което зависи от бизнес нуждите и целите, изискванията по отношение на сигурността, протичащите в организацията процеси и размера и структурата на организацията. Повишаването на информационната сигурност допринася за поддържането и подобряването на конкурентоспособността, паричния поток, доходността, съобразяването със законовите разпоредби и търговския имидж.

Организацията е жив организъм – тя постоянно се развива и има външни фактори, които й влияят. Системата за управление на сигурността на информацията има стойност и сертификацията носи доказателство, че тя функционира нормално, правомерно, чрез одитите през годината. Рисковете могат да бъдат овладени, част от тях могат да бъдат елиминирани, системите за управление на сигурността на информацията и на качеството на услугите помагат на организациите да се преборят с реалната ситуация и да продължат напред бизнеса си, извличайки максимална полза от него.

Литература:

1. Цветан Семерджиев, Сигурност и защита на информацията, издателство „Класика и стил“, София 2007 год.

2. Христо Тужаров, Стандартизация на информационната сигурност, издателство „Просвета“ София 2009 г.

3. Цветан Семерджиев, Управление на информационната сигурност, ИК "Софттрейд" 2007 г.

4. Доц. д-р Георги Павлов Защита на информацията

5. Закон за електронното управление, В сила от 13.06.2008 г., Обн. ДВ. бр.46 от 12 Юни 2007г., изм. ДВ. бр.82 от 16 Октомври 2009 г.

6. Наредба за общи изисквания за оперативна съвместимост и информационна сигурност, Министерски съвет, 25.11.2008 г.

Иванов Галин Р.,

ПРЕДИЗВИКАТЕЛСТВА КЪМ МОДЕЛА ЗА КАРИЕРНО РАЗВИТИЕ НА ВОЕННОСЛУЖЕЩИТЕ ОТ БЪЛГАРСКАТА АРМИЯ*

Галин Р. Иванов

Военна академия „Г. С. Раковски" факултет „Национална сигурност и отбрана" катедра „Мениджмънт на сигурността и отбраната"
1504 София, бул. "Евлоги и Христо Георгиеви" № 82, тел. 92 26 670
E-mail: iwanow_off@abv.bg

CHALLENGES TO THE MODEL FOR CAREER DEVELOPMENT SOLDIERS OF THE BULGARIAN ARMY

Galin R. Ivanov

Annotation: *Model for career development of soldiers from the Bulgarian Army is an integral part of the development of the Armed Forces of Bulgaria. Through the model is looking for new ways and approaches to build a new army structure, numerical staff and dislocation. Through the assembly of human resources management is implemented personnel policy of the Ministry of Defence of Bulgaria.*

Key words: *Human Resource Management, model for career development, management system and development of armed forces, staffing model, subsystem for Human Resource Management, career building and development.*

Демократичните промени в Република България, започнали през 1989 г., поставят началото на реформите в цялостния обществено-политически живот и създават условия за трансформиране на Българската армия. Търсят се нови пътища и подходи за изграждане на нова армия по структура, числен състав и дислокация.

Необходимостта от качествено нови отбранителни способности в контекста на новата среда на сигурност налага провеждането на Стратегическия преглед на отбраната. Въз основа на постигнатото той подлага на преоценка съществуващите и дефинира нови връзки, параметри и норми в националната система за сигурност и отбрана, формира визията за развитие и преформулира ролята, мисията, задачите и способностите на войските и силите, както и на другите отбранителни компоненти.

Разработени бяха и се изпълниха План 2010 (впоследствие План 2004), актуализиран в План 2002. Приет е нов План за организационното изграждане и модернизацията на въоръжените сили до 2015 година, но през 2006 г. отново се налага да се търсят форми и средства за неговата актуализация. Народното събрание приема решение за ускоряване на професионализацията на Българската армия, която да

* *Авторът не претендира за пълно изследване на проблема поради неговата обширност и многовариантност, но с готовност ще приеме всички мнения и препоръки.*

завърши до 31 декември 2007 г. На 29.12.2010г. с постановление № 333 на Министерски съвет е приет „План за развитие на Въоръжените сили на Република България", който дава основната визия за развитие на Въоръжените ни сили за в бъдеще.

След периода на най-тежка оптимизация за Българската армия днес очакванията са насочени към стабилност и качествено израстване на нейните способности. Отбранителните потребности изискват качествено нова политика за реализация на човешкия потенциал, което налага промяна на сегашната философия на управление на кадрите.

Кадровият потенциал на Българската армия, определен към 31 декември 2010 г. в състав от 34 500 души, който след реорганизирането на щабовете и военните формирования ще бъде не по-малко от 26 100 души, следва да се управлява разумно и изисква да се създават условия за пълноценната му реализация чрез **Подсистемата за управление на човешките ресурси,** която да функционира в непрекъснат годишен цикъл и в синхрон с подсистемите на **Системата за управление и развитие на Въоръжените сили.**

Посредством подсистемата за управление на човешките ресурси се осъществява кадровата политика на Министерството на отбраната за комплектуване на въоръжените сили с личен състав, способен ефективно и ефикасно да изпълнява задачите по отбраната на страната и на съюзническите задължения в НАТО и в Европейските сили за сигурност. Това се постига чрез подбор на личен състав с необходимата квалификация и опит, готовност и мотивираност. **Намирането на най-подходящия човек, в най-подходящото време и за най-подходящото място е в основата на цялостния кадрови модел**.

Целта на този доклад е да се жалонират предизвикателствата към системата и модела за кариерното развитие на военнослужещите. Да се поставят проблемните въпроси, а за в бъдеще да се предложат целесъобразни насоки за изграждане на ясна и ефективна система за цялостно **кариерно изграждане и развитие** на военнослужещите, за тяхното привличане, приемане, професионално развитие, стимулиране и обучение.

С пълноправното членство на Република България в НАТО и Европейския съюз на Българската армия са определени **мисии и задачи** за изпълнение на целия спектър задачи по отбраната на страната; участие в коалиционни действия извън територията на страната за подкрепата на международния мир и сигурност; принос към националната сигурност в мирно време; участие за поддържане на мира; защита на националната територия, въздушното и морските пространства; участие в хуманитарни операции; действия за предотвратяване и неутрализиране на терористични заплахи; подпомагане на гражданските власти и население при бедствия, аварии, кризи и др. Посочените мисии и задачи са изпълними не от масова армия с тромаво управление посредством реализиране на възможности в масови настъпателни и отбранителни операции, а от **малка, мобилна, модулна и модерно въоръжена армия**.

Постигнала близките си цели, стремежът на Република България е да се превърне в просперираща държава, която да дава своя принос за утвърждаването на мира и сигурността на Балканите, в Европа и света.

Днес изпълнението на „Плана за развитие на Въоръжените сили на Република България" изисква нов подход при комплектуването на поделенията от Българската армия с офицери, сержанти и войници.

• В съвременните условия българското общество проявява болезнена критич-

ност и извършва строг отчет за изразходваните средства за отбрана и за Българската армия. То иска стоката „сигурност", иска общественото благо „отбрана", но на приемлива цена, и не приема неразумните разходи и неясните обяснения за тях. Отмина времето, в което проблемите на отбраната на страната бяха забулени в тайна, и днес прозрачността е изключително полезна и здравословна както за армията, така и за обществото.

• Службата на личния състав на Българската армия протича при силна информационна зависимост от средствата за масова информация и често това влияе отрицателно при изпълнението на всекидневните задачи от военнослужещите.

• Военнослужещите изпълняват поставените им задачи при крайни времеви ограничения, които изискват значително физическо и психическо натоварване на офицерите, сержантите и войниците, особено при подготовката на подразделенията, определени за участие в мисии зад граница.

• От военнослужещите се изисква висок морал при изпълнение на всекидневните задачи. Без него в обстановка на недостиг на финансови и материални средства част от военнослужещите лесно биха се поддали на ниски страсти и жалки действия.

• Над 10 000 военнослужещи вече са изпълнявали задачи в многонационална среда и притежават значителен професионален и боен опит. Те сравняват условията на служба, характеристиките на въоръжението и техниката, на екипировката и условията на живот с тези в съюзническите армии, бързо усвояват новото в армейския живот и полагат усилия за ускоряване на процесите в развитието на Българската армия.

• Военната наука следва да анализира, обобщава и предава натрупания опит от военнослужещите, участвали в мисии, като за това е необходимо Министерството на отбраната да отдели достатъчно финансови и материални средства.

• Постигането на оперативна съвместимост чрез въвеждането на нова комуникационна и информационна техника, ново въоръжение и бойни средства изисква от военнослужещите постоянно да се обучават и да повишават своята квалификация.

Защо е необходим нов модел за кадрово развитие?

1. Днес управлението на кариерата на военнослужещите не се възприема като постъпателно развиващ се процес, който обхваща целия път на военнослужещия от приемането му на кадрова военна служба до освобождаването му от нея.

2. Лоялността към прекия началник е водеща и често за осигуряване на служебното си развитие военнослужещият пренебрегва изискванията на системата.

3. Новият модел за кариерно развитие следва да представя вярна и обективна оценка на положените усилия и постигнатите резултати от военнослужещия. Старият модел на атестиране е нереалистичен, демобилизиращ и с явно изразен формален характер.

4. Новият модел за кариерно развитие следва да се развива и коригира от нови координиращи и консултативни органи.

5. С новия модел следва да се преодолее тясната зависимост между военноотчетната специалност (ВОС) и кариерното развитие. Той трябва да осигури условия за творчески подход в развитието на специалистите и да преодолее консервативното мислене при прогнозиране на бъдещето развитие на офицерите, сержантите и войниците. Намаляването на броя на ВОС следва да осигурява

на военнослужещите чрез кратка квалификация съответните възможности за професионалната им реализация в друг род и вид въоръжена сила.

6. Ще бъдат създадени условия за цялостно кариерното развитие, което ще започва от войника, ще преминава през службата на сержанта и ще завършва като офицер, а защо не и като генерал от Българската армия.

7. Новата визия за кариерно развитие изисква разработването на нови длъжностни разписания и нови длъжностни характеристики, съвместими както по хоризонтала, така и по вертикала на служебното развитие.

8. Кариерното развитие изисква сключването на нови по съдържание договори, в които да са определени възможностите за пълноценна реализация в Българската армия. Необходими са ясни права и отговорности за всяка от страните. Опитът показва, че настоящите договори лишават страните от увереност при изпълнение на поетите отговорности, защото са плод на законов бюрократизъм в армейски условия.

9. Новият модел на кариерно развитие ще подобри възможностите на военнообразователната система и ще спомогне за нейната поетапна реализация. Постоянното обучение и повишаването на професионалната квалификация на военнослужещите ще се превърне в задължително условие за кариерното им развитие.

10. Посредством реализирането на новия модел за кариерно развитие ще се дава предварителна оценка на влиянието на средата и службата върху здравето на военнослужещите и механизмите за превенция на риска.

В заключение ще акцентирам вниманието на следните **изводи**:

- Необходимо е в кратки срокове да се промени или се създаде нова законова и нормативна уредба в интерес на армията и личния й състав с отчитане на новите ангажименти и отговорности на страната като член на НАТО и на Европейския съюз.
- Външните и вътрешните условия са благоприятни за реализиране на новия кадрови модел.
- Ръководството на Министерството на отбраната и Щаба на отбраната на Българската армия имат волята да реализират на практика новият модел за кадрово развитие.

И на последно място, но не и по важност, трябва да си зададем въпроса, **военнослужещите готови ли са да приемат промяната и има ли обществена нагласа за това**. Въпросът е труден, но бъдещето ще покаже какъв ще е неговият отговор.

Литература

Карабельова, С. Управление на човешките ресурси. Христоматия. С., Издателство „Лик", 2000.

Карабельова, С. Управление и развитие на човешкия потенциал. С., Издателство "Класика стил" ООД, 2004.

Арабаджийски, Н. Администрация на сигурността и отбраната, С., Военно издателство, 2007.

Ангелов, П. Външна среда на мениджмънта на човешките ресурси. С., Военна академия „Г. С. Раковски", 2009.

Ангелов, П. Теоретични основи на мениджмънта на човешките ресурси. С., Военна академия „Г. С. Раковски", 2008.

Закон за отбраната на Въоръжените сили на Република България. (http://www.md.government.bg/bg/).

Правилник за прилагане на Закона за отбраната и Въоръжените сили на Република България. (http://www.md.government.bg/bg/)

Бяла книга за отбраната и Въоръжените сили на Република България, приета с решение на Народното събрание от 28 октомври 2010.

План за развитие на Въоръжените сили на Република България, приет с ПМС № 333 от 29 декември 2010.

Инструкция № 3 от 15 април 2010 г. за реда и организацията на работа на комисиите за кариерно развитие на военнослужещите в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия. (http://www.md.government.bg/bg/)

Наредба № Н-28 от 5 ноември 2010 г. за критериите, условията и реда за атестиране на военнослужещите от Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия.(http://www.md.government.bg/bg/)

МЕТОДОЛОГИИ ЗА ИЗМЕРВАНЕ НА ИНФОРМАЦИОННИЯ РИСК

Станчо М. Кайков

METHODOLOGY FOR MEASURING INFORMATION RISK

Stancho M. Kaykov

Annotation. *Risk Management and Risk Assessment are major components of Information Security Management (ISM). Risk Management, in general, is a process aiming at an efficient balance between realizing opportunities for gains while minimizing vulnerabilities and losses.*

Keywords*: risk management**, information security, risk assessment, information security systems*

Разработването, внедряването и използването на информационна система в структурата на една организация в наши дни се явява задължително условие за повишаване на нейната конкурентоспособност, както и възможност за оцеляване и развитие в съвременното бизнес общество. Успоредно с това нараства и рискът, свързан с огромното количество обработвана корпоративна информация. Отношението на организация към въпросите на информационната сигурност се превърна в основен критерий за оценка степента и на зрялост и доброто корпоративно управление. Това се потвърждава и от международния стандарт ISO31000 [1], според който „управлението на риска е основна част от всяко стратегическо управление на организацията“, а Европейската агенция за мрежова и информационна сигурност [2] препоръчва „управление на риска да се установи като постоянен процес, в рамките на организацията“.

Ясно пролича необходимостта от наличие на система за управление на риско-

вете, базирана на международни стандарти и механизми за управление на риска в корпоративните системи. Това доведе до разработването на редица национални и международни стандарти [1÷7] за управление на риска. Предлаганите в [1,5] методи, определения и цели се различават значително в зависимост от сферата на прилагането им (корпоративни проекти, инженерни, промишлени или финансови процеси, обществено здраве и сигурност).

В теорията на риска съществуват множество дефиниции за управление на риска .В общ план те разглеждат управлението на риска като „повтаряща се дейност, която се занимава с анализ, планиране, изпълнение, контрол и мониторинг на извършените измервания и прилагана политика за сигурност“.

Според [8] „управлението на рисковете е процес на приемане и реализация на управленски решения, които минимизират неблагоприятното влияние от случайно възникнали събития“. Това определение е доразвито в [9], според които „управлението на риска е процес по идентификация, оценка и класиране според приоритета на рисковете, водещо до координирано и икономически обосновано прилагане на средства, за свеждане до минимум, наблюдение и контрол на вероятността и/или въздействието на нежеланите събития, или за максимизиране реализацията на възможностите“.

Управление на риска се разглежда от [2], като „процес, с цел ефективно реализиране на баланс между възможностите за печалби и намаляване на загубите“. Подобно е и становището на [10], според който “управлението на риска запазва и добавя стойност към организацията и участниците в нейната дейност, подпомагайки постигането на организационните цели“. Пак там се посочва, че желаните резултати от управлението на риска, могат да се постигнат чрез:

- предоставяне на рамка за извършване на контролирана, последователна и ориентирана към бъдещето дейност;
- подобряване процеса на взимане на решения, планиране и определяне на приоритети чрез предоставянето на структурирано и изчерпателно разбиране на бизнес дейността, променливите движения и тенденциите, както и възможностите пред отделни проекти (или заплахите за тях);
- по-ефективната употреба и разпределение на капитала и ресурсите в организацията;
- редуциране на колебанията във второстепенните дейности;
- защита на активите и подобрение корпоративния имидж;
- развиване и подкрепяне на служителите, управление на познава-телния ресурс на компанията;
- оптимизиране на оперативната ефективност.

За изпълнението на тези процеси, пред управлението на риска в ИТ системите се поставят следните основни задачи:

- минимизиране последствията от негативни въздействия на риска свързани с използването на информационните технологии;
- създаване на солидна основа на процеса по взимане на решения;
- осигуряване възможност за изпълнение на основните бизнес цели на организацията.

Ефективното управление на риска е итеративен процес състоящ се от фази, правилно прилагане на които позволява непрекъснатото подобряване на постиженията от вземаните управленски решения. За целта е необходимо същия да бъде

интегриран в целия жизнен цикъл на информационната система, като се започне още от етапа „Планиране“, където се явява негов задължителен компонент.

Управлението на риска в областта на информационна сигурност (ИС), може да се разглежда като част от общата стратегия за сигурност на дадена организация, или може да се извършва отделно. При съществени промени в информационните процеси или активи, управлението на риска не трябва да се прилага поотделно за всеки процес, а глобално върху цялата информационна система в зависимост от избраната корпоративна стратегия за управление.

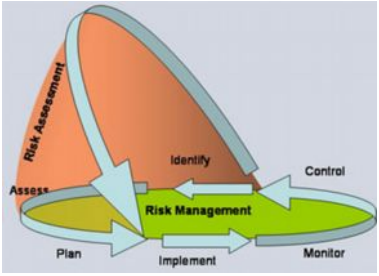
Стратегията по управление на риска е интегриран бизнес процес, който включва всички процеси, дейности, методологии и приетите политики изпълнявани в една организация. Стратегията може да включва избягване на риска чрез прехвърлянето му на трета страна, намаляване на отрицателното въздействие на риска чрез неговото управление, или да приеме всички или част от последиците от даден риск.

За изпълнение на тази задача от особена важност е способността на организацията да определи своите изисквания за сигурност. Според [2] те могат да бъдат определени от:

- оценката на рисковете за организацията, вземайки предвид нейните общи цели и бизнес стратегия. Чрез оценка на рисковете се набелязват заплахите за активите, оценява се вероятността от поява и уязвимостта и се преценява потенциалното въздействие;
- законовите, нормативните, регулаторните и договорните изисквания, на които трябва да отговарят организацията, нейните търговски партньори, доставчици и страни по договор и тяхното социо-културно обкръжение;
- конкретен набор от принципи, цели и бизнес изисквания за обработка на информацията, които организацията е разработила, за да поддържа своите дейности.

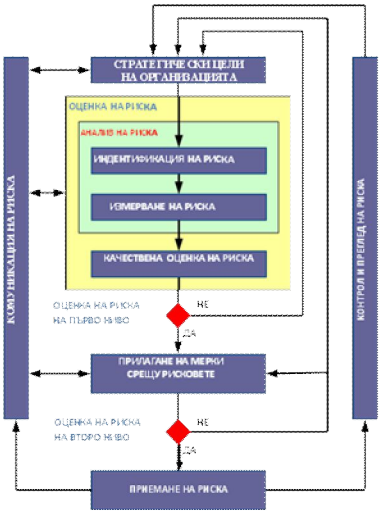
Според експерти по информационна сигурност, потвърдено в последствие в международните стандарти [1,5,6,7] управлението на риска се състои от два основни елемента: оценка и третиране на риска.

Взаимната връзка между управление на риска и оценката на риска като последователност от процеси, според [2] е отразено на фигура 1.



Фиг. 1 Взаимна връзка между процесите по управление и оценката на риска

Стандартът ISO 27005 детайлизира процеса по управление на риска за сигурността на информацията (фигура 2.2), задавайки базовите връзки на процесите, които могат да бъдат изпълнени в една корпоративна система за управление на информационна сигурност.



Фиг. 2 Процес за управление на риска в системите
за информационната сигурност според ISO 27005

Според направения анализ от експертите по информационната сигурност [2], съществуват различни методологии и софтуерни инструменти за измерване на информационния риск. Като елемент от процеса по оценка на риска, анализа на риска може да се извършва в различна степен на детайлност в зависимост от риска, целта на анализа, както и изискваната степен за защита на наличната информация, данни и ресурси. Методологиите използвани по време на анализа на риск от малък, среден или голям мащаб на положителен или отрицателен риск, включват количествено, полуколичествено или качествено измерване на риска в зависимост от вероятността му за настъпване и възможните последствия. Нивото на сложност и необходимите разходи за тези анализи, във възходящ ред, е качествен, полуколичествен и количествен.

Качественото измерване се използва за идентификация на рисковете, изследване на техните особености, разкриване на последиците от тяхната реализация (икономическа загуба), разкриване на източниците на информация за всеки риск. На по-късен етап се преминава към по-конкретни или количествени измерения на големите рискове. Количественото измерване предполага пълна и точна информация за честотата (вероятността) на реализация на риска и размера на загубите, както и вида на тяхното статистическо разпределение, също и други характеристики, които са необходими за по-нататъшен анализ.

А) Качествено измерване

Качественото измерване на риска използва косвени (изразни) скали за измерване размера на потенциалните последици и вероятността от сбъдването на риска. Резултатът от качественото измерване на риска се използва:

- като първоначална проучвателна дейност за идентифициране на рискове изискващи по-подробен анализ;
- където този вид анализ е подходящ за вземане на управленски решения;

- при липса на материални аспекти на риска (напр. репутация, култура, изображение и т.н.);

- когато цифрови данни или ресурси са недостатъчни за количествена оценка.

Качественият анализ следва да използва фактическа информация и данни, където има такива.

(Б) Полуколичествено измерване

Полуколичественото измерване на риска цели, чрез използването на формули, да се дефинират по-конкретни разширени нива на рисковете измерени чрез цифрови стойности. Тези стойности обикновено са примерни и не са реални, но изразяват по реалистични стойности на измерения риск в сравнение със стойностите получени от качественото измерване.което е предпоставка за количествен подход. Мерните единици могат да бъдат линейни, логаритмични или други. Независимо от този факт е необходимо да се отчете, че получените резултати от полуколичественото измерване не отразяват с абсолютна точност действителния размер на риска към вероятността и/или последиците от неговото сбъдване особено при екстремни ситуации. Това може да доведе до противоречие, аномални или неподходящи резултати от управлението на риска.

(В) Количествено измерване

Количественото измерване използва техники за достигане до количествени данни от различни източници. Качеството на измерването зависи от точността и пълнотата на цифровите стойности и правилното прилагане на избраните методи за измерване на риска. Количествена оценка в повечето случаи е резултат от екстраполацията на експериментални проучвания или исторически данни за инциденти, статистики, таблици и графики.

Изборът на методология за измерването на риска зависи в голяма степен от способностите на специалистите да анализират рисковете, дефинираните корпоративни стратегическите цели и решенията на ръководството на организацията. Елементите на процеса по измерване на риска по избрана методология са: оценка(остойностяване) на активите, измерване на заплахите и уязвимостите в корпоративната система, както и въздействието на риска върху процеса по непрекъснатост на бизнеса.

Оценката на активите и въздействието

Оценката на активите започва с класификацията на активите по приоритет, въз основа на значението им за постигане на бизнес целите на организацията и се извършва чрез количествени (стойностни) или качествени скали. В зависимост от информацията с която се разполага за всеки актив и характеристиките на организацията, определени активи с предварително известна стойност се оценявани чрез местна парична единица, а други се оценяват от "много ниска "до" много висока" стойност. Използването на количествен или качествени мащаб се определя от ръководството на организацията, като той се прилага върху всички активи подлежащи на остойностяване. Възможно е използването и на двата вида оценка за едни и същи активи.

Типични термини, използвани за качествено оценяване на активите предложени от [7] включват определения като: нищожен, много малък, малък, среден, висок, много висок и критичен. Изборът и обхватът на термините, подходящи за дадена организация зависи в голяма степен от размера на организацията, необходимата степен на информационна сигурност, както и други организации и специфични фактори.

Критериите, използвани като основа за определянето на стойност на всеки актив не трябва да дават възможност за тълкуване. Това често е един от най-трудните аспекти при оценката на активите, тъй като остойностяването се явява субективен фактор. Критерии по които може да се извърши определяне стойността на даден актив включват: първоначална стойност, стойност при неговата подмяна или повторно създаване или абстрактна стойност (например репутацията на организацията).

Друга основа за оценка на активите са разходите, направени в резултат на: загуба на поверителност, цялостност, наличност, отговорност, автентичност и надеждност в резултат на инцидент.

Някои активи в процеса на остойностяване, могат да получат различни целеви стойности. Например: бизнес плана може да бъде оценяван на базата на изразходвания за разработване му труд или по оценка на труда за въвеждане на данни. Определените стойности най-вероятно ще се различават значително. Крайната стойност от оценката на актива, може да бъде:

- най-голямата от всички изчислени стойности;
- сума от определени стойност;
- сума от всички изчислени стойности за актива.

Необходимо е да се извърши внимателен анализ и избор на крайната стойност за актива, т.к. тя ще бъде заложена и използвана в плана за третиране на риска асоцииран с актива. Това налага всички изчислени стойности на активите да бъдат съобразени с общата рамка и стратегия на организацията за управление на риска. За целта [1] предлага критерии, чрез които може да се оценят възможните последствия от загуба на поверителност, цялост, наличност, отговорност, автентичност или надеждността на активи, и те са:

- нарушение на законодателството и/или подзаконов акт;
- влошаване на икономическите резултати;
- загуба на репутация/отрицателен ефект върху репутацията;
- нарушение, свързани с личната информация;
- застрашаване на личната безопасност;
- неблагоприятно въздействие върху правоприлагането;
- нарушаване на поверителността;
- нарушение на обществения ред;
- финансови загуби;
- прекъсване на дейността си;
- застрашаване на безопасността за околната среда.

Предложените критерии не са задължителни, като избора кои да се използват зависи от сферата или типа на дейност на самата организация.

Установяване на общи критерии е базата на която се определя и мащаба за качествената оценка на активите, който ще се прилага в цялата организация. Няма правила по отношение на броя на нива за оценка, като [1] препоръчва, те да варират от 3 (напр. ниска, средна и висока) до 10.

Целесъобразно е всяка организация самостоятелно да дефинира граници си за стойностите на активите, които ще се оценяват съответно с "ниска", "средна" или "висока". Последиците, които могат да бъдат катастрофални за малка организация, могат да бъдат оценени като слаби или дори безвредни за много голяма организация. Това определя и основните показатели за оценка на активите - разходи за тяхната подмяна и последиците за бизнеса. Списъка с активите се анализира и

оценява от органите ангажирани с бизнес планирането, финансите, управлението на информационни системи и други свързани дейности, с цел да се идентифицират допустимите стойности за всеки един от тези активи. Определените стойности следва да са свързани с разходите за придобиване, внедряване и поддържане на активите, както и евентуалните неблагоприятни последици за бизнеса от загуба на: поверителност, цялост, наличност, недопускане на отхвърляне, отговорност, автентичност, или надеждност.

Почти невъзможно е да се определи количествена оценка за всеки актив в организацията. За целта е необходимо да се установи стойността или степента на важност в нефинансови, т.е. качествени измерения. В противен случай ще бъде трудно да се определи нивото на защита, и размера на ресурсите, които организацията трябва да отдели за защита на активите си.

От особено значение при оценка на активите е анализиране и определяне влиянието на актива, което той оказва върху непрекъсваемостта на бизнес процеса в организацията. Броят на бизнес процесите свързани с даден актив влияе върху базовата му оценъчна стойност. При този анализ е необходимо да се отчете и зависимостта на актива от другите активи в организацията. Зависимостта може да промени крайната му оценъчна стойност според [7] по следния начин:

- ако стойностите на зависимите активи са по-ниски или равни на стойността на базовия актив, определената базова стойността не се променя;

- ако стойностите на зависимите активи са по-високи, то стойността на базовия актив се преизчислява, като крайната му оценъчна стойност зависи от степента му на зависимост и стойностите на другите активи.

Измерване (оценка) на заплахите

След идентифицирането на източника на заплахата (кой и каква е причината за заплахата) и заплашената цел (кои елементи на системата могат да бъдат засегнати), е необходимо да се измери (прецени) вероятността от сбъдването на заплахата. При това се отчитат:

- честота на заплахата (колко често може да се случи, в съответствие с опита, приложими статистика и т.н.);

- мотивацията, способностите и ресурсите на киберпрестъпниците за извършване на атака към информационната система, отчитайки ценността на информацията в системата и възможните уязвимости;

- географски фактори като близост до химически или петролни инсталации, възможността за екстремни метеорологични условия и фактори, които могат да повлияят за допускане на човешка грешка и неизправност в оборудването, както и случайни източници на заплаха.

За достигане на по-високо ниво на точност при измерване на заплахите, е необходимо да се разделят активите на съставните им компоненти и да се асоциират съответните заплахи за всеки от тях.

Крайният резултат от измерването на заплахите е изработването на отчет съдържащ списък на заплахите, асоциираните с тях активи, вероятността от сбъдването на заплахата и качествена или полуколичествена скала за измерване.

Измерване на уязвимостта

Измерването на уязвимостите в информационната система и нейните активи е от особена важност за организацията, т.к. то определя възможностите на заплахите да използват дадена уязвимост в определена ситуация. При управлението на риска

в организацията е необходимо да се отчетат съществуващите контроли и способа за измерване на уязвимостите. Липсата на контроли за управление на даден актив в системата води до възникване на непосредствена уязвимост.

Резултатът от тази стъпка в процеса по управление на риска е списък на уязвимите места/активи, идентифицираните с тях заплахи, и качествена или полуколичествена скала за измерване.

Измерване на въздействието

Въздействието на риска върху бизнеса може да се определи чрез моделиране на резултатите от дадено събитие(инцидент) или поредица от събития (инциденти), или чрез екстраполация на данни от експериментални проучвания. Последствията могат да бъдат изразени по отношение на паричната политика, технически или човешки критерии за въздействие, или другите критерии приети от организацията за управлението на риска. В определени случаи е необходимо да се определят повече от една цифрова стойност за измерване на въздействието на риска върху информационната система за различно време, места, активи или ситуации. Въздействието се измерва чрез същия количествения или качествения подход използван за измерване на заплахите и уязвимостите

Заключение:

Измерването на риска се явява основен елемент за оценка на последиците от реализирането на инциденти и определяне нивата на рисковете в информационната система. Избора на методика за идентифициране и измерване на активите, заплахите, уязвимостите, въздействията и прилаганите и планирани контроли за управление на риска се явява базов показател за осигуряване изпълнението на стратегическите цели на организацията.

Използвана литература:

1. ISO 31000:2009 „*Risk management - Principles and guidelines"* (Управление на риска - принципи и указания)
2. http://www.enisa.europa.eu
3. ISO/IEC 17799:2000 - „*Information technology – Code of practice for* information *security management"* (Информационни технологии - Кодекс за добра практика за управление сигурността на информацията)
4. ISO 27002 - Code of practice for ISMS describing a information security control objectives and best-practice security controls – Практически код на системи за управление на информационната сигурност
5. ISO Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards
6. ISO/IEC 13335-1:2004 Информационни технологии. Ръководство за управление сигурността на информационните технологии (ИТ);
7. ISO 27005 Информационни технологии. Мето-ди за сигурност. Управление на риска за сигурност на информацията;
8. Николова Н. И. – Концепция за приемливия риск в управлението на фирмата, Технически университет, г. Варна, 2004.
9. Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46;
10. www.ferma.eu, Federation of European risk management associations, Стандарт по управление на качеството ISO 31000.

ПРЕГЛЕД НА НОВОПРИЕТАТА СТРАТЕГИЯ ЗА НАЦИОНАЛНА СИГУРНОСТ: ИДЕНТИФИЦИРАНЕ НА ВЪЗМОЖНОСТИ ЗА ВЗАИМОДЕЙСТВИЕ С НЕПРАВИТЕЛСТВЕНИЯ СЕКТОР И ИЗПЪЛНЕНИЕ НА ПРОЕКТИ В ТАЗИ ОБЛАСТ

Мария Г. Кантарджиева

***Abstract**: The document represents a brief review of the Strategy for National Security of the Republic of Bulgaria adopted in February 2011. It outlines the new elements incorporated in the existing concept namely placing the citizens as central point of the security policy thus searching for synergy to response the new challenges in the changed global security environment.*

***Key words**: Strategy for National Security of the Republic of Bulgaria, non-governmental organisations (NGO) in security sector, cooperation in the field of national security.*

I. Общ преглед на Стратегията: мотиви, структура, цели.

На 10.12.2010 г. Министерски съвет на РБългария, със свое Решение № 872 одобрява проект на Стратегия за национална сигурност на Република България и предлага на Народното събрание да разгледа и приеме проекта на стратегия. Това става на 25.02.2011 г. на основание чл. 86, ал. 1 от Конституцията на Република България[8] и чл. 16, т. 5 от Закона за отбраната и въоръжените сили на Република България.[9]

Сред мотивите за приемане на нов стратегически документ, правителството изтъква настъпилите промени във вътрешната и международната среда за сигурност след приемането през 1998 г. на предишния стратегически документ - Концепция за национална сигурност. Стратегията „дава ново разбиране на политиката за национална сигурност, което съответства на новите условия, изисквания и виждания за функционирането на системата за национална сигурност и нейното значение за сигурността на гражданите, обществото и държавата"[10].

Същевременно качествено нов момент в документа е *поставянето на гражданина в центъра на политиката за сигурност и изтъкване на възможностите за взаимодействие с неправителствения сектор,* при запазване от страна на държавата на водеща роля в областта на националната сигурност, като в документа тя се разбира като взаимна обвързаност между сигурността на гражданина, обществото и държавата. В проекта са очертани институционалната рамка и основните дейности на системата за национална сигурност, като е изведена ролята на междуинституционалното сътрудничество и *партньорството между гражданите, техните*

[8] Чл. 86. (1) Народното събрание приема закони, решения, декларации и обръщения.

[9] Чл. 16. Народното събрание приема т. 5 Стратегия за национална сигурност на Република България по предложение на Министерския съвет;

[10] Мотиви за приемане на Стратегия за национална сигурност на РБългария, Министерски съвет, Решение No 872, 2010 г.

организации и държавата[11]. В стратегията са включени и нови аспекти на понятието „национална сигурност", а именно: икономически, финансов, екологичен, социален, правосъден аспект - разгледани и развити като секторни политики, а традиционните - отбрана, външна политика, вътрешна сигурност и разузнаване, са актуализирани.

Стратегията за национална сигурност представлява обширен и подробен документ, състоящ се от 175 параграфа, структурирани в шест части, както следва: I. Увод, II. Общи положения, III. Среда за сигурност, IV. Политика за сигурност V. Система за национална сигурност и VI. Заключение.

В *Увода* и *Част II. Общи положения* са изведени основните принципи на политиката за национална сигурност, а именно: законосъобразност и равенство пред закона на всички граждани; обвързаност и зависимост между сигурността, основните права и свободи на гражданите; диалог и разширено партниране между гражданите, обществото и държавата (вече цитираният чл. 18, т. 3); доверие между държавните институции и сътрудничество с частния сектор, неправителствените организации и гражданите, със съюзниците в НАТО и ЕС; национален консенсус по политиката за национална сигурност; неделимост на националната сигурност от сигурността на НАТО и ЕС; проактивност и координация в дейността на държавните институции и организации; прилагане на комплексен междуинституционален подход при изграждане на системата за национална сигурност; откритост, прозрачност и отговорност при формирането и провеждането на политиките за сигурност; ефективност и ефикасност на управленските и изпълнителските дейности; демократичен контрол над системата за национална сигурност. Изредени са и националните интереси на страната, групирани като: *1. Жизненоважни интереси* (запазване на суверенитета, националната цялост и интегритета на българското общество, защита на населението при аварии и други) и *2. Други интереси* (ефективно функциониране на българските институции заедно с тези на ЕС и НАТО, добросъседски отношения и други). В *Част III. Среда за сигурност* са разгледани външната и вътрешна среда за сигурност, рискове и заплахи. *Част IV. Политика за сигурност* разглежда освен общите положения и приоритетите, така и секторните политики, както и новите компоненти в тях. Това са и най-обширните текстове в документа, като секторните политики са подредени в следния ред:

- Политика за финансова и икономическа сигурност
- Политика за социална сигурност
- Политика за енергийна сигурност
- Политика за сигурност в отношенията човек - природа
- Политика за правосъдие и вътрешен ред
- Външна политика за сигурност
- Отбранителна политика

Това подреждане не е по приоритети, а има изчерпателен характер, отразявайки взаимодействието между средата за сигурност, националните интереси, съществуващите ресурси и възможностите за постигане на задоволително състояние на

[11] Чл. 14 Стратегията за национална сигурност на Република България е основополагащ документ за единно формиране, планиране, осъществяване, координиране и контрол на политиката за национална сигурност, провеждана от държавните институции в сътрудничество с гражданите и техните организации (във връзка с чл. 18 т.3 и 4, 149, 151, 156, 171).

нивото на сигурност на гражданите, обществото и държавата. *Част V. Система за национална сигурност* разглежда основните насоки за действие, както и контрол и отчетност на органите с преки отговорности към системата за национална сигурност и *Част VI. Заключение*. Следва да се отбележи, че в процеса на изработване, стратегията е съобразена със Стратегия 2020 на Европейския съюз, както и със Стратегическата концепция на НАТО, приета на срещата в Лисабон на 18 и 19 ноември 2010 г.

Важна цел и главен приоритет на стратегията, е „повишаване нивото на управляемост на системата и търсенето на синергия".[12] Този нов подход в разбирането на идеята за национална сигурност се налага предвид новите реалности, новите рискове и заплахи в средата за сигурност, особено след събитията в САЩ от 11 септември 2011 г, развитието на информационните технологии, глобализацията и възможностите за все по-свободно придвижване на хора във все по-голям мащаб. Именно обединението на усилията на различните институции и граждански субекти, заедно е ново разбиране на проблематиката в сферата на националната сигурност се разглежда, възприема и налага като успешен подход за отговор на новите предизвикателства.

Опити за възприемане на подобен подход има и преди изработването и приемането на разглежданата стратегия и по-точно опити за привличане на гражданския сектор към работата на някои институции от сектора на сигурността и решаването на проблеми, свързани с работата им. Такива примери можем да намерим сред документи, утвърдени от Министерство на отбраната и Министерство на вътрешните работи. Ето някои от тях:

а. / Министерство на вътрешните работи.

• *Стратегически насоки за развитие на интегрирания модел "Полицията в близост до обществото" 2006–2010 година.* Основна цел на тези насоки са „подобряване на партньорството между полицията и структурите на гражданското общество, чрез продуктивно и полезно сътрудничество по превенцията, противодействието на престъпността и осигуряване на обществения ред и сигурност в условията на прозрачност и зачитане правата и достойнството на гражданите".

• Наредба *№ 13-1457 от 28 август 2007 г. за условията и реда за привличане на граждани и неправителствени организации, които на доброволни начала да помагат за изпълнение на законово определените функции на национална служба "Полиция"*. Издадена от Министерството на вътрешните работи, Обн. ДВ. бр.75 от 18 септември 2007 г. Целите на партньорството между органите на Национална служба "Полиция", гражданите и неправителствените организации са: „изучаването на проблемите на вътрешната сигурност и обществения ред и удовлетвореността от дейността на полицията; разработване и реализация на програми и дейности по превенция на престъпността; разработване и реализация на конкретни проекти за решаване на проблеми на вътрешната сигурност и обществения ред; подпомагане на лица, застрашени или пострадали от престъпление; реализиране на обучителни, медийни и други кампании".

б. / Министерство на отбраната.

• *Отчет за дейността на Министерството на отбраната през първите 100 дни на правителството (2009 г.).* В този документ намираме следния текст: „При

[12] Чл. 11

осъществяване на програмата вече се използва потенциала на публично-частното партньорство против корупцията с участие на български неправителствени организации, учени, медии и партньорите на Министерството на отбраната от Прозрачност без граници - Великобритания".

II. Възможности за участие на неправителствения сектор

Както вече бе посочено, събитията от края на XX и началото на XXI век доведоха до коренно изменение в световната среда за сигурност. Това налага промяна и на отношенията в рамките на сектора за сигурност и отбрана, разбирани като реформа, насочена към отваряне към гражданите и техните организации, прозрачност и предвидимост. Съществена характеристика на този процес на качествена промяна е нарастването на ролята на гражданското общество, разбирана като участие на неправителствени структури, които активно и под най-различни форми могат да се включват във функционирането на сектора.[13] Дейностите, осъществявани от тях досега включват:

- Граждански контрол на сектора за сигурност;
- Обучение на политици, журналисти, млади изследователи и други по проблемите на доброто управление и свързаната с него реформа на сектора за сигурност;
- Участие с експерти в дискусии по съществени въпроси, засягащи сигурността и отбраната;
- Изготвяне на независими предложения за решения под формата на доклади и други документи.[14]

Константин Пудин пише: „У нас има около 30 такива организации [15], между които: Център за изследване на демокрацията, Атлантически клуб, Сдружение „Джордж Маршал" – България, Център за югоизточноевропейски изследвания, Фондация „Демокрация и сигурност", Институт за изследване на сигурност та и международните отношения, Сдружение „Българска отбранителна индустрия", Център за либерални стратегии, Институт за регионални и международни изследвания, Европейски институт, Съюз на офицерите от резерва „Атлантик" и др. Поголямата част от неправителствените организации у нас, към които се отнасят и изброените по-горе фондации и сдружения, са ангажирани с разработването на изследователски проекти. Финансирането на тези проекти е различно: най-често това са пари по програми на ЕС, НАТО, ООН или са отпуснати от отделни европейски правителства – Кралство Норвегия, Кралство Холандия, Кралство Швеция, ФРГ и др. Освен с аналитична дейност тези организации се занимават и с обучение." [16].

Също така в България функционират (макар и не добре ресурсно обезпечени) студентски организации, имащи отношение към сектора на сигурност. Те функционират в рамките на висшите учебни заведения, представляват определена група

[13] Водеща все пак остава ролята на държавата и на експертите от сектора. (виж Стратегия за национална сигурност, чл. 14).

[14] Пудин, Константин. Структурите на гражданското общество в националния сектор за сигурност и отбрана. В. сп. Икономически алтернативи, брой 3, 2010.

[15] Неправителствени организации с интерес в сектора на сигурност (бел. авт)

[16] Пудин, К. Пак там.

студенти от съответните висши учебни заведения и са част от академичната общност в тях. В България има няколко десетки такива организации, например Студентска асоциация за изследване на международните отношения (САИМО), Младежка асоциация за изследване на сигурността и отбраната (МАИСО), Студентски дипломатически клуб, Его Политико и др. Сред основните цели на тези сдружения са свободната изява на студентите и техните възгледи, участие в изследвания на актуални обществени процеси.

Същевременно поставянето на гражданина в центъра на политиката за сигурност и изтъкване на възможностите за взаимодействие с неправителствения сектор, както и въвеждането на нови секторни политики, предлага разширяване на възможностите за сътрудничество между институциите, ангажирани в областта на националната сигурност и неправителствени организации (НПО) с интерес в същата област. Тук имат място за изява организации, както следва:

- екологични сдружения, работещи за чиста околна среда и организации в сферата на опазване на културно-историческото наследство на страната;
- организации, насочени към защита на човешките права, срещу полицейския произвол и дискриминация на български граждани;
- организации, насочени към защита на интегритета на нацията; към насърчаване на мирното съжителство, културното взаимодействие и взаимното опознаване на етносите в страната;
- организации с интерес към кампании за осведомяване (public awareness campaigns) по отношение на действия, свързани с измами на граждани, разпространение на наркотици сред подрастващите, примамване на девойки и млади жени към проституиране и трафик на хора;
- организации, работещи за насърчаване на мирни добросъседски отношения, включително краеведски организации;
- организации, предлагащи образователен компонент в средното образование по теми, свързани с европейска интеграция, гражданско образование, права на човека.

До момента такова участие на НПО няма или е изключително слабо застъпено (има представени примери в т. III). Именно затова новоприетата Стратегия за национална сигурност може и трябва да бъде разглеждана като възможност за навлизане на НПО в тази област чрез активно подпомагане на експертните и институционални усилия за отваряне към обществото и прозрачност в тази област.

III. Някои примери за изпълнение на проекти от неправителствени организации или такива с външно финансиране, съвместно със структури от сектора на националната сигурност.

Програма Phare

- Phare BG 2004/IB/JH/09 "Модернизиране на българската полиция и повишаване на нейната ефективност - укрепване на изградените специални структури за полицейско разследване в МВР";
- Phare BG 2005/IB/JH/05 "Мениджмънт и усъвършенстване на полицейската дейност на местно ниво в РПУ, ориентирана към близост до обществото";
- "Подобряване на положението и интеграция на лица в неравностойно положение, принадлежащи към уязвими етнически малцинства със специален фокус върху ромите" - проект, реализиран от Национален съвет по етнически и демог-

рафски въпроси към Министерски съвет;

• Изграждане на мрежа по проект "Граждански наблюдатели в полицията", със съдействието на Институт "Отворено общество" в гр. София, Пловдив, Плевен, Бургас и Варна.

Програма Еркюл II на Европейската комисия

Еркюл II (2007-2013) обхваща период от 1 януари 2007 г. до 31 декември 2013 година. Финансовият пакет за този период е 98,5 милиона евро. Програмата предвижда финансиране от Общността посредством предоставяне на грантова помощ, но се предлагат и възможности за обществени поръчки. Правилата за финансиране от Общността са определени в Регламент (ЕО, Евратом) № 1605/2002 на Съвета. Основните цели на програма Еркюл II са както следва:

• Засилване на сътрудничеството между участниците в борбата срещу измамите в ущърб на финансовите интереси на Общността, т.е. - Комисията и Европейската служба за борба с измамите (OLAF);

• Укрепване на мрежите за обмен на информация между държавите-членки и страните-кандидатки;

• Предоставяне на оперативна и техническа помощ на правоприла-гащите органи в държавите-членки, по-специално на митническите органи.

• След проучване сред българските НПО бе открита само една инициатива, реализирана с финансовата подкрепа на Програма Еркюл II на Европейската комисия, а именно:

• Регионален семинар за Югоизточна Европа "Предизвикателства пред превенцията и наказателното преследване на измамите с ДДС в разширяващия се европейски пазар", София, 27-28 Ноември 2008 г. Този семинар е проведен с финансовото съдействие на Европейската служба за борба с измамите (OLAF) по програма Еркюл II на Европейската Комисия "Обучение в областта на борбата с измамите", на Регионалната антикорупционна инициатива, Сараево, както и с програмното съдействие на Националната агенция по приходите. Целта на форума е била да подготви ръководни служители от институциите, отговорни за противодействие на измамите от десет страни от югоизточна Европа по управление на риска, превенция и наказателно преследване на трансграничните измами с ДДС.

За съжаление възможностите на тази програма не се познават или не се прилагат в България, като причините може да се търсят сред фактори като слаба популяризация или трудно удовлетворими изисквания за участие. Също така дългите срокове за разглеждане, одобрение и изпълнение се оказват демотивиращ фактор за институциите, ангажирани с изпълнението на проекти в тази област.

IV. Заключение.

Стратегията на национална сигурност, приета от Народното събрание през м. февруари 2011 г. следва да се разглежда като отправна точка при формулирането и впоследствие реализирането на вторични (последващи) политики с цел развитие на системата за национална сигурност. Съгласно идеята, заложена в разглежданата стратегия, системата за национална сигурност следва да се изгражда и да функционира като генератор на политики, адекватни на средата за сигурност, националните интереси и наличните ресурси. Тази система е инструмент за реализиране на стратегията, за контрол върху функционирането на подсистемите за сигурност и за осигуряване ефективност на реагиране при конкретни ситуации. Предвид новите

моменти в нея, стратегията предлага много форми за сътрудничество с неправителствения сектор и организациите с интерес в областта на националната сигурност. Съществуват също така възможности за финансиране на дейности със средства извън бюджета на ангажираните в сектора министерства.

Използвана литература:

1. Стратегия за национална сигурност на Република България. Информационна система за правна информация на Министерски съвет. www.government.bg.

2. Решение № 872 от 10 декември 2010 г.; Мотиви. Информационна система за правна информация на Министерски съвет. www.government.bg.

3. Отчет за дейността на Министерството на отбраната през първите 100 дни на правителството, 2009. Електронна страница на Министерство на отбраната. www.mod.bg.

4. Закон за отбраната и въоръжените сили на Република България Електронна страница на Министерство на отбраната. www.mod.bg.

5. Пудин, Константин. Структурите на гражданското общество в националния сектор за сигурност и отбрана. В: сп. Икономически алтернативи, брой 3, 2010.

6. Стратегически насоки за развитие на интегрирания модел "Полицията в близост до обществото" 2006 – 2010 година. Електронна страница на Министерство на вътрешните работи. www.mvr.bg.

7. Наредба № 13-1457 от 28 август 2007 г. за условията и реда за привличане на граждани и неправителствени организации, които на доброволни начала да помагат за изпълнение на законово определените функции на национална служба "Полиция". Издадена от Министерството на вътрешните работи, Обн. ДВ. бр. 75 от 18 септември 2007 г. Електронна страница на Министерство на вътрешните работи. www.mvr.bg.

8. Конституция на РБългария. Информационна система за правна информация на Министерски съвет. www.government.bg.

9. Информационни материали от електронната страница на Асоциация за мониторинг на управлението (АМУ) www.gma-bg.org.

10. Информационни материали от електронната страница на Сдружение "Джордж Маршал" – България. http://www.gcmarshall.bg

ЗАЩИТА НА ПАМЕТНИЦИТЕ НА КУЛТУРАТА. ПРОУЧВАНЕ НА РЕГИОНАЛНИЯ ИСТОРИЧЕСКИ МУЗЕЙ, ГРАД ПЛЕВЕН. РАЗВИТИЕ НА МУЗЕЙНОТО ДЕЛО. ПОЖАРОИЗВЕСТИТЕЛНА СИСТЕМА И ОХРАНА

Мартин Люб. Кръстев

Варненски свободен университет „Черноризец Храбър”, Юридически факултет, Специалност „Защита от бедствия и аварии“ (ЗАБ), к.к. „Чайка”, 9007 Варна

PROTECTION OF CULTURAL MONUMENTS. RESEARCH OF THE REGIONAL HISTORICAL MUSEUM, TOWN PLEVEN. DEVELOPMENT OF THE MUSEUM WORK. FIRE ALARM SYSTEM AND SECURITY

Martin Lyub. Krastev

Varna Free University “Chernorizets Hrabar”, Faculty of Legal,Department of Security and Safety; Major Protection from emergencies and disasters (PED)

ABSTRACT**:** *The issue of protection of cultural monuments from fires, vandal attacks, terrorism and etc. This is a research of the Regional Historical museum, town Pleven. The research includes history of the museum, organization structure, and protection.*

KEY WORDS: *museum, fire, security, national importance, fire-extinguishers.*

СВЕДЕНИЯ

Развитие през годините:

Музейното дело в Плевен има дългогодишни традиции. По инициатива на бележития български възрожденец и революционер Стоян Заимов през периода 1903-1907 г. в Плевен и околността са изградени Военноисторическите музеи и паметниците на падналите в Освободителната война от 1877-1878 г. руски и румънски воини. През 1903 г. местни любители историци създават археологическо дружество в града. То се заема със събирателска работа и през 1911 г. открива скромна археологическа сбирка.

Истинско развитие музейното дело получава едва след Втората световна война. През 1952 г. Музеят става държавен и създава експозиция на отдел ”Археология’’. Няколко години по-късно (1959 г.) на музея е предоставена красива сграда от края на XIX в. След преустройството и ремонта й, след извършена събирателска и проучвателска работа, на 3 септември 1961 г. е открита за пръв път по-цялостна историческа експозиция с отдели: ’’Археология’’, ’’Етнография’’ и ’’Работническо революционно движение’’. По-късно са създадени и отделите ’’Възраждане’’, ’’Социалистическо строителство’’, ’’Природа’’ и Художествена галерия. Разгръща се многостранна дейност по проучване културно-историческото наследство от дълбока древност до наши дни. Едновременно с това възниква нужда от разширя-

ване на материалната база.

За нова сграда на музея са предложени няколко варианта. През септември 1978 г., само няколко месеца след обединяването на Окръжния исторически музей и Военно-историческите музеи в Дирекция ''Културно-историческо наследство'', бюрото на Окръжен комитет на БКП решава всички нейни експозиции да се реализират в построената през 1884-1888 г. по италиански проект сграда, използвана до този момент като казарма и Школа за запасни офицери. Едно от предимствата на сградата е че , дава възможност на музейните работници да разполагат с достатачно площ и с помещения за всички видове музейна дейност.

Днес:

Регионалният исторически музей, Плевен е научен и културно-просветен институт, самостоятелно юридическо лице на бюджетна издръжка към Община Плевен. Осъществява своята дейност по издирването, проучването, представянето, опазването и популяризирането на паметниците на културата, природните образци, флората и фауната на територията на Област Плевен, където са разкрити значими археологически обекти - римският град Улпия Ескус при с. Гиген, късноантичната и ранновизантийска крепост Сторгозия край Плевен, средновековната българска крепост в Никопол. По профил музеят е общоисторически с природонаучен отдел. В структурата му са включени следните основни специализирани отдели и обслужващи звена: Археология, История на България XV - XIX в., Нова и най-нова история, Етнография, Природа, Фондове и научен архив, Връзки с обществеността, ателие за реставрация и консервация, Фотолаборатория, библиотека. Музеят и музейните фондове са разположени в представителна двуетажна сграда - паметник на културата с национално значение, с обща площ от около 7000 м2 и парк с открита експозиция на площ от 37 дка. Основният фонд на музея включва над 180 000 музейни единици. Специализираната библиотека на музея разполага с над 10 000 тома научна литература и периодични издания.

Характеристика на туристите:

През 1979г. в Историческия музей се регистрират 1 346 325 посещения- число, с което може да се гордее всеки голям европейски музей. През последните години той се посещава от около 150 000 души, като чужденците са малко повече от 10%. Те са със среден към висок социален статус. Техен основен мотив за пътуването е запознаване с природните забележителности, историята, културата и обичаите на страната ни или по бизнес.

Освен от българи, музеят се посещава и от руски и румънски туристи, както и от организирани германски, израелски, испански, английски и американски групи.

Инфраструктурата е добре развита като цяло. Плевен е важен транспортен възел поради централното му местоположение в Дунавската равнина. Важна гара на ж.п. линията София - Варна, а чрез гара Ясен градът се свързва със селищата по Дунавския бряг. В Плевен гостът може да пристигне с влак от няколко посоки. Чрез автобуси той е свързан с над 300 селища в цялата страна. В самия град най-използвания транспорт е тролейбусния.

Музеят предлага следните услуги: експертни оценки на старинни предмети и оръжия, документи, монети и др.; консултации и рецензии; реставрационно-консерваторска дейност, изложби и фотоуслуги; изложби с паметници на култура-

та от всички исторически епохи, експозиционна площ за временни изложби с надеждна охрана. Като специфични туристически услуги на туристите се предлагат и различни сувенири: керамични праисторически и антични идоли, маски, лампи и други; битова и декоративна троянска керамика.

Оценка на ценовата политика на обекта:

Входните такси са следните:

- Индивидуални посетители - ученици, войници, хора с увреждания и пенсионери - 1.00 лв.
- Организирани групи - 0.50 лв.
- Всички останали посетители - 2.00 лв.
- Индивидуални посетители в четвъртък и на всички официални празници на Република България и официалния празник на Община Плевен - безплатно

Такси за беседи:

- на български език - 5.00 лв.
- на чужди езици - 10.00 лв.

Такси за прожекция на видеофилми, свързани с музейната експозиция:

- за организирани групи- на човек по 0.50 лв.
- за индивидуални посетители- на човек по 0.50 лв.

Такси за любителско видео и фотоснимане- 3.00 лв.

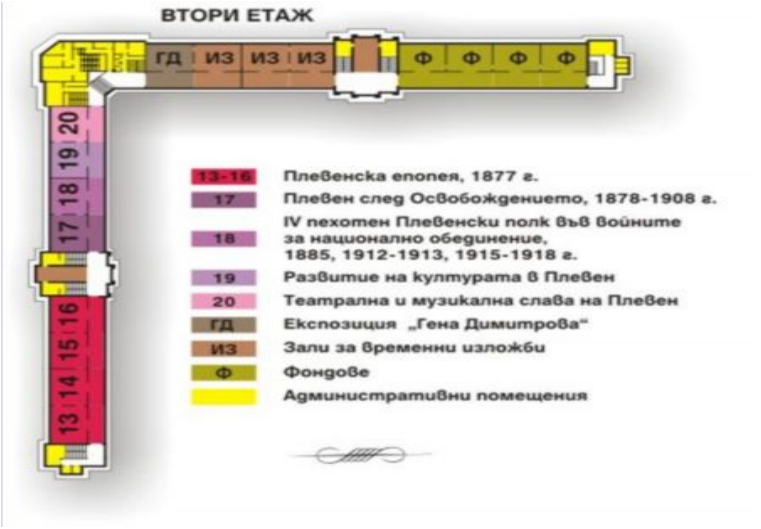
ОПИСАНИЕ НА СЪСТОЯНИЕТО

След реставрация на фасадата от преди няколко години, Регионалният исторически музей, Плевен е може би културният паметник в най-добро състояние в окръга за момента. По време на ремонта са били взети всички мерки за запазване на автентичния вид и укрепване на цялостната фасада. В процеса на работа са вложени най-добрите материали на пазара, като са спазени всички изисквания за качество и безопасност. В изложбените зали и антретата не са извършвани ремонти в последните години, което личи и на пръв поглед. Този факт обаче не прави интериора неугледен, напротив – мраморната настилка и гранитни колони на първо ниво, карат залите да изглеждат елегантни и сигурни. За поддръжката на огромната сграда се грижат служителите на музея, като следят за изрядния и вид ежедневно.

Музеят разполага с оградена външна площ, в която също са изложени редица артефакти. Оградата е смес от масивна и ажурна част, като основата е каменна, а ажурната част – метална (желязо). Има два входа – главен и второстепенен. Главния вход представлява сводеста част на сградата с ширина около шест метра, височина около десет и дължина около дванадесет метра (схема на първия и втория етаж можете да видите на фигура 1 и фигура 2). Достъпа през главния вход се ограничава посредством масивна порта от ковано желязо. Сградата е изградена от каменна и тухлена зидария, а прозорците и вратите са от дърво.

Охранява се от наета охранителна фирма, като за целта спомага видео наблюдение на външните и част от вътрешните входовете. Влизането се контролира от служител на фирмата.

Фигура 1



Фигура 2

В сградата има действащ евакуационен план, заверен от контролните органи и поставен на определените за това места (фигура 3).

Фигура 3

Паник бутоните са достатъчно на брой и са разположени на оптималните за целта места и височина (фигура 4).

Фигура 4

Във всяко обособено помещение има датчици известяващи за наличие на дим (фигури 5 и 6). Разположени са един спрямо друг по предписанията на ПБЗН.

Фигура 4

Фигура 5

Всяка зала е снабдена с два вида пожарогасители. Всички са минали периодичния преглед за техническа изправност, имат съответните талони и указателни табели (фигури 7 и 8).

Фигура 6

Фигура 7

Изградени са на удобните за целта места и определения от ПБЗН брой противопожарни кранове. Всички от тях са минали технически преглед и нужните тестове (фигура 9).

Фигура 8

ПРЕДЛОЖЕНИЯ ЗА МЕРКИ

От изложеното до тук става ясно, че разглеждаме един поддържан и спазил изискванията обект. Редовните проверки на ПБЗН не са установили нарушения за момента. От противопожарна гледна точка единствената препоръка е редовно тестване и бъдещо обновяване на пожаро – известителната система. Това е препоръчително, поради моралната амортизация на някои от уредите. В момента на пазара, благодарение на стремглавото развитие на технологиите, могат да се намерят противотожарни системи от много по-висок клас (газови и др.). Музей от национално и дори световно значение, какъвто е Регионален исторически музей, гр. Плевен се нуждае от сигурна защита на безценните богадства, с които разполага. При направеното проучване бяха разгледани всички елементи от системата за противотожарна безопасност, като за гаранция за законосъобразност послужиха представените документи.

Що се отнася до човешкия фактор свързан с противопожарната безопасност – бих препоръчал провеждането на по-чести учения и тренировки. При направената проверка се установи, че знанията и уменията на част от низшестоящия персонал не са достатъчни за справяне с евентуално възникнала криза.

За разлика от добре поддържаната противотожарна система, охранителната

система има някои слаби звена. На първо място след проверката се установи, че живата охрана не е с достатъчен капацитет, за да подсигури постоянната охрана върху целия периметър. Обиколките на служителите на охранителната фирма са на големи интервали и траят прекалено много време. През две от петте посещения не срещнахме охранител и влезнахме в обекта необезпокоявани. Препоръчва се увеличаване на персонала за жива охрана, особено през тъмните часове на нощта.

Както вече бе споменато сградата разполага с видео наблюдение, но то далеч не е оптимизирано. Охранителните камери не са достатъчно на брой, за да се покрият всички потенциално опасни зони. Препоръчва се монтиране на повече на брой камери и тяхното оптимизиране, за да се избегнат „белите петна" при наблюдение.

Слабо звено са и вътрешните входове на сградата. Вратите са от части дървени, от части стъклени, което ги прави силно уязвими при опит за проникване и вандализъм. Освен това не на всички бяха открити датчици сигнализиращи за проникване. Препоръчва се изграждането на магнитни или друг тип датчици, сигнализиращи при отваряне на врата, както и датчици сигнализиращи при счупване на стъкло.

Близостта на сградата до няколко улици я прави изключително уязвима при евентуална атака тип „кола-бомба", но за съжаление на този етап тази заплаха не може нито да бъде избегната, нито намалена, поради факта, че улиците са главни артерии на града и при назначаване на пропускателен режим би се затруднило движението до неприемливи граници.

Като цяло можем да заключим, че Регионален исторически музей, гр. Плевен не е нито рискова ценност, нито застрашена културна ценност според Закона за културното наследство. Проверките, които бяха извършени акцентират най-вече върху това дали за спазени всички изисквания на законодателството за пожарна безопасност на сгради и охрана на обект от национално значение. Въпреки няколкото слаби звена сградата остава добре защитена и охранявана и се надяваме и в бъдеще да не попада в категорията на рисковите обекти.

Използвани нормативни актове при проверката

1. Закон за културното наследство
2. Наредба №із-1971 от 29.10.2009 г. за строително-технически правила и норми за осигуряване на безопасност при пожар
3. Наредба № рд-07-2 от 16 декември 2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд
4. Наредба №із-491 /17.03.2010 г. за реда за осъществяване на пожарогасителната дейност и аварийно-спасителната дейност от органите за пожарна безопасност и спасяване на министерството на вътрешните работи
5. Наредба №із-489 от 28 март 2007 г. за реда за осъществяване на държавен противопожарен контрол
6. Инструкция за експлоатация на пожарната техника на национална служба "Пожарна безопасност и защита на населението" – МВР

ОЦЕНКА НА МАТЕРИАЛНИТЕ И МОРАЛНИ ЩЕТИ ОТ НАРУШЕНИЯТА НА ПРАВАТА ВЪРХУ ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ

Николай А. Митев

УНИБИТ, гр. София, бул. Цариградско шосе 119
GSM: 0887 394 403, E-mail: nikolay.am@abv.bg

EVALUATION OF THE MATERIAL AND MORAL DAMAGES OF INFRINGEMENTS OF INTELLECTUAL PROPERTY

Nikolay A. Mitev

Abstract: *Much of today's companies based on its business of production and exploitation of intellectual property. Piracy causing large economic losses to these companies, but legislative and technological measures taken to protect IP rights are highly controversial.*

Key words: *intellectual property; copyright; protection; infringement; piracy.*

Моделите на развитие в съвременните икономически условия показват, че за постигане на просперитет и конкурентно предимство компаниите все повече разчитат на създаване и използване на интелектуални ресурси. Традиционната икономика свързана с материалното производство на оборудване и продукти за потребление все по-бързо отстъпва своето място в развитите държави за сметка на разработването, икономическата експлоатация и трансферите на интелектуалните продукти. Преобладаващата част от най-бързо развиващите се и просперираци компании, основно високотехнологични, Интернет компании, софтуерни, консултантски, свързаните с развлекателния бизнес видео и звукозаписни компании дължат поголямата част от пазарната си стойност основно на притежаваните от тях обекти на интелектуална собственост под формата на нематериални активи. За този тип организации притежаването на правата върху търговска марка, авторски договор, патент, ноу-хау или група обекти на интелектуалната собственост (ИС) под формата на технологии е с много по-голямо значение от гледна точка на процесите на създаване на стойност, отколкото наличието на други видове активи. Употребата в производствените дейности и управлението на интелектуалните ресурси като нематериални активи, процесите на трансфер, лицензиране или продажба на тези активи са в основата на дейността на посочените компании. Затова създаването на интелектуални активи от наличното в организацията и придобитото знание, превръщането им в интелектуална собственост чрез осигуряване та правова защита и включването им във вид на нематериални активи в икономическата дейност е от жизнено важно значение както за отделните компании, така и за държавите.

При тези условия наличието на надеждна и сигурна защита на правата върху ИС и предотвратяването на тяхното нарушаване и заобикаляне е от съществено значение за функциониране на икономиката на държавите, гаранция за възвращаемост на инвестициите, вложени в разработването на интелектуални продукти и

предотвратяване на загубите от нарушаването на правата върху ИС както на компаниите, така и на отделните индивидуални собственици. Представа за мащабите на проблема дава доклад, направен по поръчка на Международната търговска палата и представен в Париж в началото на 2011 г., според който производството на фалшификати и пиратството струват над 1 трилион долара на световния бизнес, в страните от Г-20 те са причината за загубата на 2,5 милиона работни места. Фалшификатите и пиратството през 2008 година са били на стойност от 455 до 650 милиарда долара. Международната търговия с пиратски продукти представлява половината от целия й обем от 285 до 360 милиарда долара. Производството и потреблението на национално равнище се оценяват между 140 и 215 милиарда долара, а пиратските продукти,търгувани чрез интернет, са на стойност между 30 и 70 милиарда долара. Според прогнози през 2015 година общата стойност на фалшивите продукти ще бъде между 1,22 трилиона и 1,77 трилиона долара.[6]

Пиратството представлява нарушаване на правата на притежателите на ИС чрез с производството и разпространението на нерегламентирани и подправени (контрафактни) продукти. Терминът е придобил гражданственост чрез средствата за масова информация и получава широко разпространение в теоретичните разработки на различни автори и документите на организации (частни и обществени) за защита и колективно управление на правата на собствениците на ИС. Основния международен нормотворчески документ, в който е дадено определението на понятието „пиратство" е Съглашението по търговските аспекти на правата върху ИС (TRIPS) на Световната търговска организация, където в чл. 51 е посочено, че пиратска продукция представляват:

(b) „... „стоки, нарушаващи авторските права", означава всякакви стоки, които представляват копие на оригинала, изготвено без съгласието на правообладателя или лице, упълномощено от правообладателя в страната на изготвянето, и които пряко или косвено възпроизвеждат това копие, което вече се е явило нарушение на авторското право или сродните права…" [2]

Пиратството е сериозен проблем за световната икономика и предизвикателство пред международните организации и държавите, защото нанася сериозни щети на легалните производители и собственици на ИС във всички области, но най-масовите, лавинообразно нарастващи са нарушенията в областта на авторските права (АП). Според доклад от 2009 г. на Международната федерация на звукозаписната индустрия (IFPI) над 95% от всички песни, свалени от интернет през предишната година, са били пиратски. От мрежата са свалени нелегално почти 40 млрд. песни за цялата година. Само 1,4 млрд. е броят на песните, придобити легално, твърдят от IFPI. Според еврокомисаря за информационното общество и медиите Вивиан Рединг, направено през 2009 г., че според изследване, 60% от хората на възраст между 16 и 24 години в Европейския съюз са сваляли от интернет аудиовизуално съдържание, обект на АП, без да плащат. [7]

Развитието на компютърните и комуникационно-съобщителните технологии и на Интернет през последните години и тяхната все по-голяма достъпност за големи групи хората предизвиква ескалация на нарушенията на авторските права. Три са основните достижения от последно време, които правят това възможно:

- създаване на високотехнологични способи за компресиране на информацията, което прави възможно предаването на големи обеми информация с висока скорост;
- създаване на високоскоростни компютърни линии за връзка;

- създаване на сравнително евтини средства за съхраняване на големи обеми компютърна информация.

Причините за извършване на нарушенията на АП в Интернет могат да се разделят на две големи групи, в зависимост от участниците и движещите мотиви: [8]

А) Получаване на икономическа изгода от производството и разпространението на пиратска продукция. Незаконните приходи се получават директно от цената, заплащана от потребителите за получаване на незаконни продукти в материална или електронна форма, или благодарение на търговска реклама, която се явява типичен атрибут на нелегалната реализация на продукти чрез Интернет;

Б) Нарушения, които не са свързани с търговска дейност и не преследват пряко материална изгода чрез използване на пиратски копия. Това са огромната маса от нарушенията на АП, извършвани от индивидуалните потребители на интелектуални продукти в Интернет.

Малко потребители са наясно или се замислят по въпроса, че всяко пускане на компютъра ни въвежда в досег с невидимия свят на обектите на авторското право – програмното осигуряване, инсталирано на нашия компютър; сайта който посещаваме също се охранява като обект на интелектуална собственост – от една страна като съвкупност от компютърни програми и база данни, и от друга като средство за масова информация, съдържащо авторски информационни материали. Разглеждането на Web-страниците, съхраняването на част от тях в паметта на компютъра, препращане на съобщения с електронната поща – всяко поведение на ползвателите на Интернет влияе върху правото на авторите и техните правоприемници. При нарушаване на АП често потребителите извършват незаконните действия не само за икономическа изгода, а поради неинформираност и незнание на законите, защитаващи правата на собствениците. Според повечето професионалисти и автори на научни трудове, работещи в областта на защитата на АП законодателството се е усложнило много, станало е неразбираемо и неинтуитивно за средно грамотните и средно интелигентни хора. Например повечето хора не знаят и не разбират как и защо, ако са си купили например диск с филм, не могат да правят с него всичко каквото поискат, след като е тяхна собственост – например не могат да го копират, го дават за ползване и да го разменят чрез мрежата и т.н. Ако се направи аналогия с книга, която също е обект на АП се вижда разликата – всеки собственик може да я прави със своето копие каквото поиска – да я заема, копира за свои нужди, да я препродава, ако вече не му е нужна.[3].

Според някои проучвания причините за нарушенията на АП сред индивидуалните потребители се разпределят така: [8]

- свързани с цената – а) отсъствие на финансови възможности за придобиване на легални продукти (77%); б) убеденост в това, че цената на легалните продукти е завишена (66%);

- убеденост в правомерността на противоправното поведение: - значителна част от потребителите (от 25% до 50% в зависимост от контекста) възприемат производството и придобиването на контрафактна продукция като законен вид дейност.

Най-често срещаните нарушенията на правата върху интелектуалната собственост в информационната среда са:

- копиране и разпространение на компютърни програми (софтуерно пиратство) – създаване на незаконни копия на оригинален или не софтуер и тяхното разпрост-

ранение; незаконно придобиване или разпространение на софтуер чрез използване на телекомуникационните технологии; копиране на инсталационни дискове за разпространение; инсталиране на едно лицензирано копие на множество компютри; използване на академичен или друг софтуер с ограничено приложение за търговски цели и др.

- Интернет пиратство – придобиване на програмите чрез дистанционно копиране на защитени произведения (основно музикални произведения, филми, компютърни игри и др.) директно от потребителя през мрежата от интернет сайтове, които предоставят тази възможност в нарушение на авторското право върху тези програми. Технологиите за придобиване могат да бъдат разнообразни, като освен прякото копиране от сайтове с незаконно съдържание, се използват и такива, които „заобикалят" законите за авторското право, използвайки тяхното несъвършенство, като непрекъснато се развиват: мрежи с равноправен достъп (P2P) - файловете са разпръснати из цялата мрежа, позволяват потребителите да съхраняват и да разпространяват информация помежду си, без необходимостта от централен сървър; електронната поща – разпространяване на нерегламентирани копия на продукти като приложения (прикачени файлове); новинарски групи за дискусии, основани като публични електронни пощи; Usenet мрежи, позволяващ публикации и размяна на файлове между участници в тематични конференции, където информацията се обменя между голям брой променящи се сървъри, които разменят информация помежду си и др. [8]

Различните мерки, които се вземат, за засилване на контрола върху начините на употреба на интелектуалните продукти – законодателни и технологични, често предизвикват критики и негативни реакции които се изразява в във формулирането на няколко възражения:

1. Нарушаване на правото на неприкосновеност на личните данните и информация;
2. Нарушаване на правата на собственост и на идеологията за свободно ползване (fair use), залегнала във всички съвременни законодателства, регламентиращи случаите на използване на обектите на АП без необходимост от разрешение и компенсации за притежателя на правата;
3. Нарушаване на правата на гражданите за достъп до знание и информация и по този начин потискане на процеса на развитие и творчество, основаващ се на развитие на съществуващите идеи;
4. Налагане на разходите по контрол на съдържанието на Интернет трафика на компаниите-доставчици, като се облагодетелстват компаниите собственици на ИС, осъществяването на неприсъщи функции на контрол от доставчиците.

Обвиненията към големите компании от развлекателните браншове са, че те въобще не се интересуват от възнагражденията на авторите , а преследват своите корпоративни интереси и се интересуват единствено от собствените печалби. Авторите на интелектуални продукти (с някои редки изключения на някои много известни имена) получават незначителната част от генерираните приходи, като основната част от тях остават за компаниите, защото те са правоносителите на АП на основата на авторски , изпълнителски, продуцентски и т.н. договори. Най-силен натиск, осъществяван чрез различни механизми на лобиране, за засилване на законовите ограничения и търсене на отговорност от нарушителите идва от представителите на музикалния бизнес, който най-трудна се ориентира към нови модели на

бизнес поведение и където загубите от производство, разпространение и размяна на незаконни копия на обекти на АП са най-големи. В момента, например пазара на звукозаписната индустрия се владее от 6 големи международни корпорации, оперирящи с огромни средства и големи възможности за влияние. [9] Техните усилия, и тези на подобни на тях корпорации, насочени към законодателно засилване на ограниченията за ползване на обекти на АП в Интернет предизвиква редица възражения. Тенденцията за налагане на ограничения на крайните потребители на интелектуални продукти едва ли ще доведе до успех, поради две основни причини:

а) крайните потребители не са длъжни и не могат в повечето случаи да знаят дали това което купуват в Интернет е законно или не. Често даващите им достъп до дадени обекти сайтове печелят от реклама чрез отчитане броя на посещенията, а не чрез заплащане на съдържанието, което се изтегля от тях;

б) голямото количество потребители, които волно или неволно нарушават законите за защита на авторските права. Няма физическа възможност за наказателни действия срещу такава голяма група хора. От друга страна не е обществено приемливо да съществуват закони, класифициращи огромни групи хора като закононарушители. Както казва известният харвардският професор по въпросите на АП Лари Лесинг, един от най-печалните резултати от този вид законодателство, е че се създава цяло ново поколение, основно млади хора, което се научава, че законът е лобистки, несправедлив и неприложим и да възприемат като норма на поведение, че няма нищо лошо в това такъв закон да бъде нарушаван. [10].

Изводи. Съвременното развитие на информационните и комуникационни технологии и особено на Интернет, поставя системата на регулиране на отношенията между създателите и потребителите на продуктите на интелектуалната собственост пред сериозно изпитание. Свидетели сме на непрекъснато появяване на нови обекти на интелектуалната собственост и на нови способи за разпространение и популяризиране. Освен че е основно човешко право, достъпът до информация и знания е предпоставка за продължаващо развитие и прогрес. Същевременно в създаването на продуктите на интелектуалната дейност се влагат огромни материални и интелектуални ресурси, за които трябва да бъде осигурена съответна възвръщаемост. Съществуват области на ИС (издаване на вестници и списания, музикална индустрия, филмова индустрия и др.), които трудно се приспособяват към новите условия и изискват непрекъснато засилване на защитата на ИС и нарастване на ограниченията за ползване на техните продукти. Такива ограничения биха довели до запазване на статуквото, на съществуване на един остарял и консервативен модел и биха възпрепятствали развитието на новите иновативни бизнес модели изцяло базирани на Интернет (Google, Facebook, YouTube, Twiter, iPod и iTunes на Apple и др.), които трансформират света и дават по-нататъшен тласък на неговото развитие. [5] Един от примерите за промяна на този модел чрез прилагане на нови, алтернативни схеми е iTunes, които в началото на 2010 г отпразнуваха 10 милиарда продажби. Същевременно с голяма увереност може да се каже, че ще се увеличават усилията за предотвратяване на нарушаването и заобикалянето на правата върху ИС законово (международни спогодби и норми и национални законодателства) и чрез развитие на технологиите за дигитално управление на правата, като от друга страна ще се поощряват предоставянето на свободен достъп и достъпът за лично ползване до електронни библиотеки, справочници, електронни хранилища на информация и знания.

Въпросът, който стои на дневен ред е какво е бъдещето на сегашната система

за управление на взаимоотношенията в областта на интелектуалната собственост в съвременното информационно общество – каква ще е посоката й на развитие и доколко успешна ще бъде трансформацията и приспособяването й към съвременните условия.

Използвана литература

1. Петков К., сборник, Информационното общество и правата върху интелектуалната собственост, Университетско издателство „Св. Кл. Охридски", С, 2006

2. Мэггс П., Сергеев А., Интеллектуальная собственность, Юристь, М., 2000

3. Bruce A. Lehman, The Internet and Intellectual Property Protection: A U.S. Perspective, Presented in connection with the First China Internet and Intellectual Property Protection Summit Hangzhou, December 17, 2009

4. Darrell Panethiere. The persistence of piracy: the consequences for creativity, for culture, and for sustainable development. UNESCO, 2006

5. Hideyasu Sasaki, Intellectual Property Protection for Multimedia Information Technology, IGI Global, 2008

6. http://www.economynews.bg/$1-трлн-загуби-от-пиратство-и-фалшификати-news16089.html

7. http://www.vesti.bg/index.phtml?tid=40&oid=1266738

8. http://unesdoc.unesco.org/images/0018/001876/187683R.pdf

9. http://en.wikipedia.org/wiki/World_music_market:

10.http://www.ted.com/talks/lang/bul/larry_lessig_says_the_law_is_strangling_creativity.html

УПРАВЛЕНИЕ И ЗАЩИТА НА ПРАВАТА ВЪРХУ ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ В СЪВРЕМЕННОТО ОБЩЕСТВО

Николай А. Митев

УНИБИТ, гр. София, бул. Цариградско шосе 119
GSM: 0887 394 403, E-mail: nikolay.am@abv.bg

MANAGEMENT AND PROTECTION OF INTELLECTUAL PROPERTY RIGHTS IN CONTEMPORARY SOCIETY

Nikolay A. Mitev

Abstract: *Intellectual property is the basis of the dynamics of the formation of the modern world, the foundation for development and prosperity of modern society, but also a reason for controversy, disputes and conflicts. So how to regulate access to the objects of IP is in the focus of huge public interest.*

Key words: *copyright; protection; legislation; open access; digital rights management.*

Еволюцията и развитието на човешкото общество са се основавали винаги на постиженията на основата на придобиване и приложение на нови знания, на инте-

лектуалния труд. Основата на всеки следващ етап на възходящо развитие са интелектуални пробиви – изобретяване на нови начин на производство, нови материали, нови инструменти и оръжия. Всички те са продукт на интелектуалната дейност, като основният стимул за нея е възможността за индивида или социалната група да придобият предимство пред конкурентите или съперниците. Този начин на развитие непрекъснато ускорява човешкия прогрес, за да се стигне до съвременния свят, характеризиращ се със съществуването на общество на знанието, където основата на просперитета и конкурентното предимство на всяка организация и държава е във възможността да усвоява, генерира, управлява и използва нови знания. Движещите сили в обществото на знанието са глобализацията, доброто управление и иновациите, осигуряващи растежа на икономиката на знанието чрез тясното преплитане и взаимодействие на технологично развитие, пазари и култура, източник на благоденствие и същевременно на неравенство между имащи и нямащи. Иновациите променят нашия свят всеки ден, носейки промени във всички области, чрез развитие на информатиката, високите технологии, фармацевтика, биотехнологии, развлекателната индустрия – филмова, и музикална. Преди половин век Джозеф Шумпетер (Joseph Schumpeter) развива теорията за динамичната конкуренция, която описва иновациите като „непрекъснат източник на *съзидателно разрушение (creative destruction)*", което може да революционизира икономическите структури и да създаде нови пазари „чрез непрекъснато разрушаване на старите структури и непрекъснато създаване на нови". [6]

Иновациите в нашия динамичен свят са част от деструктивен процес, и същевременно от това как и колко добре създаваме иновации днес зависи и се формира нашето бъдеще, така те се явяват движеща сила на една деструктивна съзидателност. Затова голямото внимание, което се обръща в последните години на създаването и придобиването на интелектуална собственост (ИС) като движещ мотив за глобалните иновационни процеси е напълно разбираемо. Системата за защитата на ИС е начин за канализиране и регулиране на динамичните иновационни процеси, защото е инструментът, който спомага за насърчаване и практическо осъществяване на иновациите.

В зависимост от насочеността си, сферата на приложение и начина на управление и защита, правата върху обектите на ИС могат да бъдат обособени в няколко групи – авторски права, патенти, търговски и промишлени секрети, търговски и сервизни марки - на пръв поглед напълно различни помежду си, които обаче имат еднаква основа. ИС е резултат на таланта, творчеството, инициативността на хората, които създават нови знания, нови идеи. Същевременно новите идеи не възникват на празно място. Творческите, съзидателни личности надграждат своите идеи върху минало знание, след това ги развиват и споделят с другите хора от своята общност, като техните усилия се обединяват за достигане на ново по-високо ниво на знания, които от своя страна са предпоставка за бъдещи интелектуални достижения. Разпространени в обществено пространство във вид на иновации те движат развитието напред, увеличават общественото богатство и водят до нарастване на благосъстоянието на все повече хора. По този начин се ускорява цикълът на иновациите, което непрекъснато води до появяването на нови продукти на интелектуалната дейност, нови начини за разпространението им в обществено пространство, за реализацията и употребата им. Това представлява предизвикателство пред системата за управление и защита на правата върху ИС, чието предназначение

е да осигури баланс на интересите – от една страна възнаграждение за творческата дейност на създателите на интелектуални продукти и възвръщаемост на инвестициите в ресурси, необходими за създаването им; и от друга интересите на обществото за осигуряване на възможно най-широк достъп до резултатите на интелектуалната дейност.

Защитниците и опонентите на системата за защита на ИС дебатират за и против нея в продължение на много десетилетия, и особено когато иновациите и развитието поставят системата извън равновесие и се налага продължително и трудно преустройство. В продължение на повече от столетие съвременните взаимоотношенията между притежателите и потребителите на ИС се основават на приетите в края на XIX в. Парижката конвенция за закрила на индустриалната собственост (1883 г.) и на Бернската конвенция за закрила на литературните и художествените произведения (1886 г.), които постепенно се разширяват и допълват с нови съглашения и конвенции в следващите десетилетия, защото глобализацията, развитието на цифровите, съобщителните и телекомуникационни технологии в съвременното информационно общество изправят системата за управление на правата върху ИС пред непрекъснатите предизвикателства да се развива и обновява, за да може да даде адекватен отговор на тези промени.

Информационното общество и предизвикателства пред системата за защита и управление на интелектуалната собственост

Съчетанието на експоненциалният ръст на информационните технологии със залегналите в основата на съвременните демократични отворени общества права на всеки човек на изразяване, свободата на словото, свободата да създава и да обсъжда това което чува и вижда, дава основните характеристики на обществото на знанието. В него информацията тече свободно, давайки достъп на огромни групи хора до продукти и услуги в областта на знанието и културата. Същевременно се формират потребности от нови продукти на интелектуалната дейност и начини за тяхното разпространение и доставка до потребителите. Така те излизат извън рамките на съществуващите класификации и предизвикват спорове за тяхната същност и място в системата за регулиране на правата върху ИС. Разбирането за ролята на правата върху ИС в тези нови области изисква значителни нови изследвания и изучаване и са тема, разглеждана от много автори, стремящи се да определят мястото им в системата на обектите на ИС и методите за тяхното управление и защита.

Масовият достъп до обектите на ИС, обусловен от развитието на съвременните информационни технологии и създават предпоставки за ескалация на случаите на заобикаляне и нарушаване на правата на създателите на интелектуални продукти (пиратството), което предизвиква огромни загуби за притежателите на правата върху обектите на ИС. Усложнените законови регулации често водят до извършване на незаконни действия и нарушаване на АП от потребителите не само за икономическа изгода, а и поради неинформираност и незнание на законите, защитаващи правата на собствениците.[17] Това са явления застрашаващи цялата съществуваща в момента система за управление и защита на ИС и особено областта, предмет на авторското право. Противоречиви са мненията на представителите от различните

[17] „Аз изказвах много пъти недоволство в тази книга, че авторското право е сложно, мистериозно, неинтуитивно и хората не вярват че казва това, което е правилно….Законите за АП от друга страна са достигнали ниво далеч отвъд възможността за осъзнаване и разбираемост от средната личност".[4]

заинтересовани страни, на изследователите и автори на множество публикации за начините и подходите за справяне с проблема като те могат да бъдат обобщени основно до:

- засилване на законодателната защита на правата на притежателите на ИС;
- използване на технически методи за контролиране на достъпа и копиране на продуктите, обекти на ИС;
- осигуряване на свободен достъп до интелектуалните продукти чрез лицензи за отворен достъп.

Засилване на законодателната защита на правата на притежателите на ИС. Законодателното регулирането на отношенията между притежателите и потребителите продуктите на интелектуална собственост в областта на цифровите технологии и Интернет определено изостава в своето развитие поради дългия период на съгласуване и приемане на новите правила. Като стъпка в това отношение може да се смятат законодателните изменения предприети от най-големите създатели и потребители на продукти на интелектуалната собственост – Директива 2001/29/ЕО на Европейския парламент и на Съвета на ЕС относно хармонизирането на авторското право и сродните му права в информационното общество, Директива 2004/48/ЕО на Европейския парламент и на Съвета на ЕС относно упражняването на права върху интелектуалната собственост, и Закон за авторските права в цифровото хилядолетие (Digital Millennium Copyright Act – DMCA) в САЩ.

Опитите за ограничаване на нерегламентираното използване и все по-широкото разпространение на пиратска продукция чрез по-строги мерки често предизвикват критики както от страна на потребителите на интелектуални продукти, така и на професионалистите от различни области, занимаващи се с темата за правата върху ИС, в обслужване на икономическите интереси на големите мултинационални компании основно от развлекателната и софтуерната индустрии. Законодателните ограничения прехвърлят тежестта (технологична и финансова) за защита на правата на ИС от притежателите им върху разпространителите и потребителите. От разпространителите (доставчиците) се изисква въвеждане на технически възможности за следене на преминаващата информация, което освен че изисква допълнителни инвестиции, но и поради нуждата от проверка може да забави предаването на информацията от други, коректни ползватели на Интернет – размяна между потребителите на собствени материали (снимки, клипове, документи и др.), дейността на компании за електронна търговия - електронни книжарници, продажба на музикални и филмови записи, видеоигри, софтуер и др. [2] Тези дейности се разглеждат се като вид цензура и явление, което може да доведе до ограничаване и нарушаване на правата на потребителите за свободно изразяване, правото на неприкосновеност на личната информация от наблюдение и проверка, правото на достъп до информация „…законът за авторските права ограничава изразяването: той ви ограничава от писане, рисуване, публични изпълнения, или казано по друг начин, от този начин на комуникация, който харесвате и ви е най-удобен”. [5]

По този начин поставената от Директива 2001/29/ЕО цел „…за оказване на адекватна подкрепа на разпространението на културата не трябва да бъде постигната, като се жертва строгата закрила на правата или като се толерират незаконни форми на разпространение на имитирани или пиратски произведения на изкуството.” е още далече от практическо осъществяване и предстои да се види понататъшното развитие в тази област.

Използване на информационните технологии за ограничаване на нерегламентирания достъп до обектите на ИС - тези технологии позволяват да се ограничи достъпа на потребителите до продуктите чрез различни методи на кодиране (основно на мултимедийни продукти преди излъчване или при доставяне); прилагане на технологията на „водните знаци" (watermark) - представляващи невидими за потребителя програми, въведени в съдържанието получавано от потребителя и съдържащи информация за продукта и притежателя на правата върху него, които не разрешават нерегламентирано ползване или го унищожават при опит за отстраняването им; технологии за маркиране на оригиналните копия на обектите на ИС и прилагане на лицензи (напр. EULA лицензите на софтуерни продукти) с условия за ползването им и др. Регламентирането на достъпа на потребителите до интелектуалните продукти в новата информационна среда са известни като метод на цифрово управление на правата (Digital rights management - DRM). Във връзка с масовото използване на Интернет като работна среда, среда за информиране и забавление на потребителите, притежателите на права върху ИС широко използват DRM системата за контролиране на онлайн достъпа до защитените произведения в цифров вид,. Това са технически средства, налагащи рестриктивни правила за крайния потребител, които позволяват идентифицирането му и осигуряват или отказват достъпа до защитените произведения, като същевременно премахват възможността за създаването на копия и препращане на съдържанието на някой друг.

Методът DRM може да се разглежда като състоящ се от две части: техническа и правова.[1]

От техническа гледна точка методът DRM е общо понятие отнасящо се до технологиите за контрол на достъпа. Според дефиницията, използвана в становище на Федерацията на европейските издатели (FEP) към Европейския комитет за стандартизация:

„DRM може да се раздели на два ясно очертани слоя:

- идентификация и описание на интелектуалната собственост, права отнасящи се до продукта (digital rights management);
- техническо прилагане на ограничения за ползване (digital management of rights).

Следователно DRM може да се отнесе към технологиите и/или процесите, които са приложени към цифровото съдържание за неговото описване и идентифициране и/или за дефиниране, прилагане и налагане по сигурен начин на правила за ползването му."

Правовата защита обикновено предвижда отговорност за преодоляването, унищожаването или премахването на технически средства за защита. Според чл. 47 на Директива /2001/29/ЕО „Технологичното развитие ще позволи на притежателите на права да използват технически мерки, които имат за цел да предотвратят или ограничат действия, които не са разрешени от титулярите на авторско право" …. „необходимо е да се предвиди правна закрила срещу действия на заобикаляне на ефективните технически мерки и срещу предоставянето на устройства или услуги за тази цел."

В българския ЗАПСП такава закрила е предвидена в чл. 97.

Въпреки привидно удобното разрешение на проблема с нерегламентираната употреба на ИС, DRM има и своите противници. Те виждат опасност във факта, че потребителят няма достъп и контрол върху действието на системата на DRM, по-

ради което тя може да заплаши правата на индивида, навлизайки в личното му пространство чрез събиране и записване на информация за интелектуалните му интереси: „DRM разрешава върху съдържанието (на компютъра) на потребителя да се упражнява далече повече контрол над защитените материали, отколкото закона за авторското право предоставя".[2]

Методът на отворения достъп - информацията, намираща се в електронните хранилища е безплатна и достъпна за всеки желаещ. Няма нарушаване на правата върху ИС, тъй като всеки може да ползва свободно съдържанието, обикновено без условия, като на потребителите се дават правата да копират и разпространяват материалите, в някои случаи да създават нови и да редактират съществуващите материали. Към отворения достъп и свободното ползване се ориентират предимно научни организации, университети, автори на научна литература, електронни научни архиви, електронни справочници, електронни библиотеки. Осигуряването на широк и бърз достъп на потребителите позволява на авторите да увеличат в максимално възможна степен броя на читателите си и да популяризират произведенията си, да разберат мнението и да получат рецензии на свои колеги в съответната област, да бъдат цитирани. Финансовите и технически препятствия пред разпространението на научни материали забавя развитието и напредъка на науката и иновациите, разпространението на информация, знания и идеи, които са основата на развитието и нарастването на ИС в обществото. Отвореният достъп използва технологичното развитие, за да намери разрешение на проблема с непрекъснатото поскъпване на научните публикации и произтичащото от тях стесняване на читателския кръг. Демократизира се достъпа до материалите, като:

- се премахват финансовите бариери и се дават равни възможности за достъп до информацията;
- всеки може да чете и да изучава изследванията, на основата на които може да достигне ново, по-високо качество;
- спомага за разкриване на потенциала на всеки, който може да се развие чрез самообучение. [1]

Отвореният достъп не означава, че правата върху обектите на ИС не съществуват, но притежателите се отказват от част от тях в полза на потребителите, като могат да задържат друга част (най-често морални, неимуществени права). По това те се различават от свободния достъп до обектите на ИС в публичното пространство, които са обществена собственост (напр. произведения с изтекъл срок на защита на правата, фолклорни произведения и др., изброени в чл. 4 на ЗАПСП) и не са обект на авторски права. При някои от лицензите за отворен достъп притежателите на правата могат да налагат определени условия за ползване на материалите - работите, които се базират на съществуващите разработки също да бъдат за свободно ползване; за задължително цитиране на лиценза или на оригиналната разработка при ползването й; за не комерсиално ползване на материалите, обект на лиценза и на разработките на тяхна основа, и др.

Методът на отворения достъп до обектите на ИС естествено среща широката подкрепа и одобрение на потребителите, но остават открити някои проблеми пред широкото му разпространение, като например достоверността и сигурността на публикуваната информация, но най-големият е финансирането, което обикновено се извършва от обществени фондове, спонсори, от реклама.

Различните методи за управление на правата на авторите на интелектуална соб-

ственост в цифровата информационна среда са опит за адаптиране на системата на правата върху ИС към съвременните условия на създаване, разпространение и употреба на интелектуални продукти. Развитието на Интернет и информационните технологии допринесе много за демократизирането на знанието и разрастването на възможностите за достъп до културата, които остават обаче недостатъчно използвани. До голяма степен това се дължи на консервативното и рестриктивно законодателство по отношение на интелектуалната собственост и авторските права, предназначено в основата си за печатната епоха, интересите на издателската и развлекателната индустрии и на конвенционалните медии. [2] Неясните и спорни въпроси, свързани с регулиране на отношенията между притежателите и потребителите на правата върху ИС в информационната среда, съществуващите различия в законовите уредби на различните държави, са сериозно предизвикателство пред понататъшното развитие на системата за защита на правата върху ИС.

Използвана литература

1. Петков К., сборник, Информационното общество и правата върху интелектуалната собственост, Университетско издателство „Св. Кл. Охридски", С, 2006

2. Bruce A. Lehman, The Internet and Intellectual Property Protection: A U.S. Perspective, Presented in connection with the First China Internet and Intellectual Property Protection Summit Hangzhou, December 17, 2009

3. CEN/ISS, Digital Rights Management: Final Report, 30 September 2003

4. Jessica Litman, Digital copyright: Protecting Intellectual Property on the Internet, Prometheus Books, 2001

5. Hideyasu Sasaki, Intellectual Property Protection for Multimedia Information Technology, IGI Global, 2008

6. Schumpeter J., Capitalism, Socialism and Democracy, Harper, 1975.

7. Директива 2001/29/ЕО на Европейския парламент и на Съвета на ЕС относно хармонизирането на авторското право и сродните му права в информационното общество

8. Директива 2004/48/ЕО на Европейския парламент и на Съвета на ЕС относно упражняването на права върху интелектуалната собственост

9. Закон за авторското право и сродните му права (ЗАПСП), 2009 г.

КАКВО Е КИБЕРТЕРОРИЗМА И ДО КОЛКО РЕАЛЕН Е ПРОБЛЕМА

Павлина В. Николова

WHAT IS CIBERTERRORISM AND IS IT A REAL PROBLEM

Pavlina V. Nikolova

Abstract: In the age of informational community computers and informational systems are used in all spheres of human activity and state. Despite the variety of advantages concerning scientific and technological progress it is obviously that they lead to new terrorism form emerge – cyber terrorism. This dangerous phenomenon hasn't led to human victims yet, but it is not myth it is reality.

Key words: ciberterrorism, internet, terrorist, hacker, hacktivism.

През последните няколко години в света настъпиха драматични изменения. Встъпването на човечеството в новото хилядолетие е помрачено от постоянно нарастващата тенденция на разпространение на международния тероризъм. Древната китайска поговорка "Убий един – изплаши сто", дала принципа на целта и заплахата на терористичния акт, мултиплицирана през хилядолетията в съвременен вариант звучи като "убий хиляди – изплаши милиони".

В процеса на своето развитие държавите все повече зависят от високите технологии, включително компютърните, от които в голяма степен зависи управлението на жизнено важни обекти на националната инфраструктура. Глобализацията на информационните процеси доведе до появата на нова форма на тероризма - кибертероризма. За разлика от традиционния подход, при този тип тероризъм, в терористичните действия се използват най-новите постижения на науката и технологиите в областта на компютърните и информационните технологии.

Ударите на кибертеристите могат да бъдат насочени срещу банковата и търговска системи, електронното обслужване, управляваните с компютърни системи газо и нефтопроводи, електромрежите, системите за контрол на земния и въздушен транспорт, телефонните системи, сферата на здравеопазването, военните системи за комуникация и логистика. В една или друга степен всички те са уязвими за електронни атаки и подривни действия. В съвременни условия крупен терористичен акт по обекти на жизнено важна инфраструктура в единия край на света е в състояние да предизвика тежки икономически последствия в другия, което налага глобални усилия за защита на ключовите инфраструктури по целия свят в тясно взаимодействие между националните правителства и частния сектор. [1]

Освен всичко друго, компютърният саботаж не изисква кой знае какви ресурси. Така, за да бъде взривен голям язовир е необходим един тон мощен взрив, да не говорим колко е сложно да се организира доставката и поставянето на взрива в най-уязвимите места. Много по-лесно е водата от язовира да бъде изпусната като чрез Интернет се подадат съответните команди в предварително „пробитата" от хакери-терористи компютърна система за управление. [2]

Терминът "кибертероризъм" се появи в ИТ-лексикон през 1997 г., тогава специалния агент от ФБР М. Полит определя този вид тероризъм като "предумишлено, политически мотивирано нападение срещу информационни, компютърни системи, компютърни програми и данни, изразено в използването на насилие срещу граждански цели от страна на субнационални групи или тайни агенти." А добре известния експерт Дороти Деннинг (*американски изследовател в областта на информационната сигурност, професор по компютърни науки и директор на Института по информационна сигурност в Джорджтаун)* определя кибертероризма като "незаконно нападение или заплаха от нападение на компютри, мрежи или на информацията, съхранена в тях, осъществено, за да се принудят властите да помогнат за постигането на политически и социални цели.*"* [3]

В. А. Голубев *(Владимир Александрович Голубев - основател и директор на "Център за изследване на компютърната престъпност", член на Международната полицейска асоциация, също така член на Международната асоциация за борба с киберпрестъпността),* предлага следната формулировка на термина: под кибертероризъм следва да се разбира съзнателното, политически мотивирано нападение срещу информация, обработвана от компютър, компютърна система и мрежа, което създава риск за човешкия живот и здраве или възникване на други сериозни последици, ако тези действия са извършвани с цел нарушаване на обществената сигурност, сплашване на населението и органите на властта, или провокиране на военен конфликт. Той се проявява и в заплаха от насилие, поддържане на състояние на постоянен страх, за да се постигнат определени политически или други цели, принуждаване в определени действия, и привличане на вниманието към отделните кибертерористи или терористичната организация, която те представляват. Характерна особеност на кибертероризма е неговата откритост, когато условията на терористите са широко оповестени.

Откриването и неутрализирането на кибертерористите е трудно поради твърде малкото следи, оставени от тях, за разлика от реалния свят, където следите от престъпление са много повече. За разлика от обикновените терористи, използващи за постигане на целите си взривни вещества, огнестрелни оръжия, съвременните кибертерористи ползват модерните информационни технологии, компютърните системи и мрежи, както и специално програмно осигуряване, даващо им възможност да „пробиват" успешно защитата на чуждите компютърни системи и да организират дистанционна атака срещу информационните ресурси на нищо неподозиращата жертва. Главно, това са компютърни програми и вируси, осъществяващи принудително отвеждане, промяна или унищожаване на информация, така наречените "логически бомби", троянски коне, снифери (sniffers), и други форми на информационни оръжия.

Но има и скептици, които вярват, че кибертероризма е мит, че киберпространството няма да се превърне в следващото бойно поле, и кибертерористите не представляват сериозна опасност. "Вирусите са лошо оръжие за борба; те нямат насочващи системи, така че този, които ги е пратил, може също да се окаже жертва, ако не са поставени защити; освен това, появата на антидот дори и за най-сложните вируси е въпрос на няколко часа "- заявява един от противниците - Греъм Крюли, старши технологичен консултант в Sophos (антивирусна компания от Съединените щати).

Въпреки това, реалностите опровергават мнението на скептиците – доказателство за противното е, когато през февруари 2000 г. са били нападнати световно известни уеб-сайтове Yahoo.com, Amazon.com, CNN.com, eBay.com и много други. Щетите от продължилите три дни атаки на тези сайтове според официалните данни възлизат на около 1,2 милиарда долара. Разследване на тези нападения, извършено от ФБР, показва, че кибертерористите първоначално приложили злонамерени програми (наричани "зомби агенти") до "неутрални" компютри, и едва след това им дали команда за изпълнение на различни злонамерени действия. Така когато срещу търсачката Yahoo.com от 50 различни места като залп са пуснати стотици или дори хиляди искания за секунда, това за 3 часа е извело компютрите на Yahoo.com от строя.

"Особено много щети от кибертерористи понася икономиката на САЩ" – мнение, изказано от Кондолиза Райс. "Днес киберпространството е станало част от нашата икономика. Практически всички отрасли в икономиката на страната, включително енергетиката, транспорта и комуникациите, банковото дело, използват компютърни мрежи и, следователно, зависят от тяхната ефективност. Прекъсването на работата на тези мрежи, може да парализира страната", - каза Райс в реч пред форум за компютърна сигурност. [4]

Първият известен терористичен акт срещу компютърните системи на дадена страна беше през 1998 г., когато клон на Тамилските тигри в продължение на около две седмици бомбардира посолствата на Шри Ланка с по 800 писма на ден по електронната поща. Съобщенията гласяха: "Ние сме Черните Тигри на Интернет и правим това, за да разрушим комуникациите ви."

Преди време японската полиция разкри, че софтуерната система, закупена да проследява 150 полицейски коли, в това число и немаркираните, е била разработена от сектата Aum Shinryko, стояща зад газовата атака в метрото в Токио през 1995 г., при която 12 души бяха убити, а хиляди други ранени. Когато полицията направи разкритието, сектата вече беше получила секретни данни за 115 коли, освен това е действала като подизпълнител, разработващ софтуер за 10 други правителствени агенции и поне 80 частни фирми.

Но операцията, която се запечата най-силно в съзнанието през 2010 г., бе вирусът "Стъкснет" (Stuxnet). Миналата есен той порази чувствителни инфраструктури, главно в Иран. Той се разпространи чрез слабите страни на защитата на операционната система "Windows" и мишената му бяха главно софтуерни продукти на "Сименс", използвани за управление на промишлени автоматизирани системи. Един от обектите, който беше заразен, е ядрена електроцентрала в Иран. Въпреки, че тогава нямаше никакви животозастрашаващи последствия, подобни кибератаки имат изключително голям унищожителен потенциал. [5]

Според много експерти, сред които Татяна Тропина, *(аспирант в катедрата по наказателно право в Юридическия институт на Далекоизточния държавен университет, изследовател към Центъра за изследване на компютърните престъпления),* съществуват два вида кибертероризъм:

- извършване на терористични действия с помощта на компютри и компютърни мрежи (наречен условно тероризъм в "чист вид");
- използването на кибер-пространството от терористични групи, но не и за директни атаки.

Кибертероризмът в "чист вид" е преднамерено нападение срещу компютри,

софтуер, компютърни мрежи, или създадената и обработвана информация в тях, създаващо опасност за живота на човека, причиняващо значителни щети на имущество, или други обществено опасни последици. Това деяние се извършва с цел нарушаване на обществената сигурност, заплашване на населението, или влияние върху вземащите решения държавни органи. Към този тип тероризъм може да се отнесе и заплахата за извършване на тези действия за постигане на същите цели.

Що се отнася до втория тип кибертероризъм - въпросът за използване на киберпространството от терористични групи за осъществяване, популяризиране, и за насърчаване на тяхната дейност, но не и за направляване и непосредствено осъществяване на атаки, е спорен. Според закона тези действия не се квалифицират като тероризъм, но ако се ръководим от здравия разум, то причисляването им към кибертероризма изглежда разумно. [3]

В изследването на Габриел Вайман "Използването на ИНТЕРНЕТ в терористичната дейност" са посочени осем различни, макар и понякога да се застъпват, начина за използване на Интернет от терористите:

- психологическа война и психологическо въздействие;
- реклама и пропаганда на терористичните организации;
- събиране на информация;
- събиране на финансови средства;
- вербовка и мобилизация;
- създаване и поддържане на мрежи от терористични групи;
- разпределение и разпространение на информация за самоподготовка и обучение на терористи;
- планиране и координация. [6]

Внимание трябва да се обърне на т.нар. „**стеганография**", т.е. вмъкване на тайни съобщения в други текстове, така че обикновените посетители на съответния сайт да не могат да заподозрат нищо. Американските специални служби многократно са посочвали, че Ал Кайда крие карти и фотографии на целите на бъдещите терористични атаки, както и указанията си за тяхното осъществяване на различни спортни, или дори порнографски сайтове. Скритите послания могат да бъдат въведени в аудио, видео или фотографски файлове, като при това скритата информация обикновено се съдържа в най-малко значимите части на цифровия файл. Както е известно, стандартната шифровка, напротив, се основава на определени шифри или кодове. [2]

Много от медиите използват термина кибертероризъм некоректно, създавайки объркване в понятията, и поставят равенство между термините "хакер" и "кибертерорист".

Преобладаващата част от хакерите нямат за цел да извършват актове на тероризъм или гражданско неподчинение. Те влизат в компютърните системи по-скоро за нещо като интелектуално упражнение, отколкото по политически или идеологически причини. Много организации, включително правителствени агенции, канят и наемат хакери, за да посочат слабите места в мрежите им, така че администраторите да запълнят дупките.

"Повечето активисти, независимо дали са участващи в Похода на милионите майки, или в уеб-протест, не са терористи. Това е важно разграничение" — казва Дороти Денинг [5]

През последните години все по популярно става едно ново понятие – "хакти-

висти", което идва от съчетанието на думите хакер и активист. "Техните мотиви са идеологически и политически, а не финансови", отбелязва Лоран Хело от фирмата за информационна сигурност Симантек (Symantec).

Според Катя Долмаджан от Франс прес "хактивисти" и "кибервоини" са новото лице на престъпността в Интернет.

Като пример може да се посочи нашумелия случай с Уикилийкс. Опитите да се запуши устата на "Уикилийкс" породиха нещо като народен бунт в редиците на стотици или хиляди технологично грамотни активисти.

Ден след като Visa и MasterCard саботираха електронните разплащания към организацията, поддържаща сайта WikiLeaks, хакери активисти атакуваха и блокираха частично сайта на MasterCard. Групата хакери, нарекла се "Анонимни", пое отговорността за атаката над сайта на компанията за кредитни карти, както и този на швейцарската банка PostFinance, която замрази сметката на Джулиан Асандж. Пробита бе защитата и на сайта на шведската прокуратура, както и на адвоката, който е повдигнал обвиненията срещу Асандж за изнасилване и сексуален тормоз.

Пред репортер на "Гардиън" говорител на "Анонимните" заяви: "Поддържаме "Уикилийкс" не защото сме за или против разгласените данни, а понеже не сме съгласни с каквато и да е форма на цензура в Интернет." "Ето защо се вдигнахме срещу тези компании, защото смятаме, че ако оставим "Уикилийкс" да падне без бой, тогава правителствата ще решат, че могат да затворят всеки сайт, който пожелаят или който е против тях", допълва 22-годишен хакер, представил се като Coldblood.

Друг пример на кибератившизма е от май 2010 г. след израелския щурм срещу международната хуманитарна флотилия за Газа. Тогава палестински симпатизанти атакуваха израелски сайтове и проникнаха в профили във "Фейсбук", за да протестират срещу израелската операция.

През 2011 се очаква ръст на политически мотивираните атаки, или т.нар. хактивизъм, сочи доклад, разпространен от дистрибутора на McAfee у нас - Computer 2000 България. Хактивизмът ще се извършва от хора, които твърдят, че са независими от всички правителства или движения. Действията ще бъдат по-организирани и стратегически, като в този процес ще се включат и социалните мрежи. Очаква се хактивизмът да се превърне в нов начин за демонстриране на политически позиции през 2011 и в следващите години. [8]

Кибертероризма е сериозна заплаха за човечеството, съпоставима с ядрени, химически и бактериологични оръжия, и степента на тази заплаха, защото е нова, все още не е напълно разбрана и проучена. Опитът на световната общност в тази област ясно показва, извън всякакво съмнение, уязвимостта на всяка държава, още повече, че кибертероризма не разполага с граници, кибертеристите могат да застрашат еднакво информационни системи, разположени почти навсякъде по света. [7]

Източници:

1. Славчо Велков – *"Съвременният тероризъм и рисковете и заплахите за обектите на инфраструктурата"*
2. Емил Коприваров – *"Мрежата като инструмент на терора"*
3. Тропина, Татьяна – *"Киберпреступность и кибертерроризм"*
4. Голубев, В.А. – *"Кибертерроризм - миф или реальность?"*

5. Дъглас Холмс – *"Стратегии за електронно правителство"*
6. Габриел Вайман – *"Използването на ИНТЕРНЕТ в терористичната дейност"*
7. Андриан Георгиев – "Руски и грузински сайтове паднаха жертва на ожесточена информационна война"
8. В-к Дневник – *"Хактивисти нападнаха сайтовете на враговете на Асанджс"*

РОЛЯТА НА ЧОВЕШКИЯ ФАКТОР КАТО ИЗТОЧНИК НА ЗАПЛАХА СРЕЩУ ЕЛЕКТРОННОТО ПРАВИТЕЛСТВО

Огнян Н. Иванов

Гр. София 1510, ж.к. «Хаджи Димитър» бл. 138, вх. Б, ет. 6, ап. 37

ROLE OF HUMAN FACTOR AS A SOURCE OF THREAT AGAINST THE E-GOVERNMENT

Ognyan N. Ivanov

ABSTRACT: *People – the Human Factor, lie at the heart of cyberspace management, including the informational systems of Bulgaria's E-Government. The reliability and accuracy of the exchanged information depend on people's moral and motivation. The realization of the "Electronic Government" project and its corresponding socio-economic benefits are directly dependent on the human factor.*

KEY WORDS: *e-Government; cyberspace; the human factor; Prevention; threat; National Security; Information Security; Administration.*

Електронното правителство е синоним на нов мироглед и философия. То е средство за повишаване качеството на административните услуги при най-приемлива цена за обществото и възможност за намаляване на времето за обслужване на гражданите чрез внедряване на конкретни мерки за бързина, сигурност и надеждност при електронното управление на информация.

Основен инструмент на политиката за електронно управление в България е Закона за електронното управление /ЗЕУ/. Той регламентира обществените отношения, свързани с провеждането на **държавната политика за въвеждане на електронно управление** и създава основа за съдействие на централните и териториалните органи на изпълнителната власт и други държавни органи, на физически и юридически лица за предоставяне и ползване на електронни услуги.

Базата за създаване на Националната и Европейска политика за Електронно управление е използването на съвремени информационни и комуникационни технологии.

Дейността по изпълнение на политиката за електронно управление, реализиране на проекта „Електронно Правителство" и съответстващата им обществено -

икономическа полза са в пряка зависимост от човешкия фактор, при наличие на подсигурени финансови средства и нормативна уреденост.

Заетите лица, пряко и непряко, с подготовката, проучването, оценката, реализацията и мониторинга на дейностите, свързани с „Електронното Правителство" са разпределени условно в следните подгрупи:

а) потребители на услуги, лица желаещи да получат бързи и надеждни административни услуги по електронен път;

б) потребители на услуги, лица не желаещи, въздържащи се да получат административни услуги по електронен път;

в) лица, ангажирани с подготовката на информационната среда за предоставяне на електронни услуги – консултанти, държавни служители и др., в голямата си част специалисти в информационните технологии;

г) лица, служебно и пряко ангажирани с обработката на информацията, верификация на услугите, контролна дейност при предоставяне на услугите – категорично специалисти в своята секторна област на администрацията / данъчна администрация, здравеопазване, регистри и т.н./ област.

Голяма част от представителите на условно изброените по-горе групи нямат готовност да се включат ефективно в процеса на предоставяне административни услуги по електронен път, поради редица съществени фактори:

а) непознаване на нормативната уредба и липса на практически опит;

б) неумение за работа с компютър;

в) липса на нагласа за предоставяне и получаване на услуги по електронен път, като приоритет;

г) непознаване механизмите и правилата за работа в информационна среда;

д) непознаване на практика механизмите за ефективен технически мониторинг;

е) извършване на непонятна и непосилна дейност от неспециалисти за предоставяне на електронно услуги.

ж) липса на доверие към надеждността на електронния обмен на информацията и опазване на конфиденциалността на електронните документи;

з) предоверяване във възможностите на информационните системи и занижен контрол върху приеманата и предоставяна информация;

Връзката между участниците в процеса на предоставяне административни услуги по електронен път трябва да е прозрачна, бърза и надеждна, с цел:

- ✓ контрол;
- ✓ оценка на постиженията;
- ✓ анализ на ефекта от предоставяне на услуги и обмен на данни по електронен път;
- ✓ информация за въведени в практиката електронни услуги по сектори;
- ✓ информация за извършени нарушения при предоставяне и получаване на услуги по електронен път;
- ✓ брой открити пунктове за обществено използване на електронни услуги за населението;
- ✓ финансирани проекти за разработка на електронното управление и неговите компоненти;
- ✓ възможност за обработката на информацията с цел изготвяне на стратегически анализи за напредъка на България в рамките на iEurope и т.н..

Политиките свързани със създаването на Електронното управление на ни-

во законодателна и изпълнителна власт са многообразни и обхващат голям брой стратегически дейности. След последния Европейски доклад за напредъка на държавите-членки по инициативата iEurope, стана известно, че България е на едно от последните места по въвеждане на механизмите на електронното управление. Отчетен е сравнително малкия брой предоставяни електронни услуги, както и невъзможността на 57 процента от населението да използва Интернет.

В Доклад **свързан с осъществяването на електронното управление и предложения за спешни мерки, свързани с осъществяването на електронното управление** и приет от Министерски съвет на 27 февруари 2011 година, се потвърждава изоставането на страната ни. Основните констатации, които са направени в процеса на събиране и анализ на получената информация са, първо, че е необходимо да се актуализира правната рамка в областта на електронното управление. Имаме Закон за електронното управление, но за съжаление всички останали нормативни актове не са приведени в съответствие към този закон и това възпрепятства реализацията на тази програма. Затова е необходимо с бързи темпове да започнат промени в наредбите и свързаните със закона нормативни актове.

Според плановете на Правителството до 2015 година трябва да бъдат разкрити над 700 публични терминала за обществено ползване на интернет и електронни услуги, както да бъдат предоставяни 215 услуги за гражданите и бизнеса. Основа за използване на възможностите, които ни дава или които предстои да ни дава електронното подаване или получаване на административни документи е Интернет. Той навлиза в живота ни и ние ставаме постепенно зависими от него. Интернет ни прави зависими и от глобалното киберпространство, което е обект на националната сигурност, като потенциална опасност за държавността и гражданите. В приетата през 2011 г. Стратегия за национална сигурност на България е отбелязано: „Киберпрестъпността е глобална и анонимна заплаха за информационните системи. Деструктивните въздействия върху информационните системи и мрежи могат да доведат до криза чрез затрудняване и/или блокиране нормалното функциониране на важни за икономиката, финансовата система и държавното управление системи или отделни компоненти". В основата на управление на киберпространството в т.ч. информационните системи на Електронното правителство на България е Човекът – Човешкия фактор. От неговия морал и мотивация зависи надеждността и верността на обменяната информация.

Сигурността, защитата на личния живот, защитата на собствеността и общото управление на сектора са необходими за изграждане на доверието на гражданите в информационното общество. Това е особено важно от гледна точка на потребителите относно загубата на личен живот, непочтени и незаконни търговски практики, нежелани съобщения, както и във връзка с незаконното и вредно съдържание и защита на малолетни и непълнолетни. Много усилия се прилагат, за да се движат в Интернет в такова положение, като работата за реализация на безопасен Интернет за децата, системи за управление на риска и контрол на инциденти, действията на спам. Инфраструктурите на съвременния живот, например в банковото дело, финансите, здравеопазването, енергетиката, транспорта и други силно разчитат на ИКТ и са взаимно зависими и неуспехите могат да имат важни последици. В същото време, неприкосновеността на личния живот и защитата на данните става все по-проблем с мощни възможности за осигуряване на сравнително лесен достъп до изчерпателна информация за частни лица, така и интелектуална собственост. [1]

Принципен е въпроса за подбора на кадрите, които имат достъп до информационните бази данни на администрацията. Обикновено се обръща сериозно внимание на въпросите за кибер-сигурността. За нивото на достъп, за защита от вируси, за предотвратяване модификацията на данни, заличаването на данни и т.н.. Предвижда се компютърно обучение на административния персонал на всички нива за работа в средата на електронното управление. Но е занижен контрола върху физическите лица – административен или нает персонал през призмата на поведенческите им характеристики. Човешкия фактор – физическото лице и поведението му е също толкова важно, колкото техническите – хардуерни и софтуерни решения.

Човешкия фактор – лице или група лица в сговор са най-сериозната заплаха срещу Електронното правителство и гражданите. Нивото на заплахата е правопропорционално на съвкупността от:

1. Пробивите в правоохранителната и правораздавателната системи на страната;
2. Пробив в системата за Национална сигурност и липса на превенция срещу киберпрестърпенията;
3. Липсата на чувство за заплаха в гражданите, използващи интернет и електронни услуги;
4. Нивото на корупция и корупционните практики в страната.

Човешкият фактор, като заплаха за сигурността на електронното правителство, трябва да се разглежда и от няколко различни ролеви аспекта ситуирани по хоризонтала и вертикала спрямо нивото на отговорност и важността на информацията.

Ролевите аспекти се идентифицират с разположението на длъжностите и лицата, които ги заемат в администрацията, както и субектите имащи достъп до съответните информационни нива по силата на съответен административен или правен акт – аутсорсинг, общинска фирма, консултанти и т.н..

За служителите на различните нива в администрацията, които имат достъп до вътрешните и външни информационни системи на електронния обмен на данни е въпрос на мотивация и морал да спазват правилата за работа и съхранение на информация или да злоупотребят със служебните си задължения и да предоставят информация нерегламентирано на заинтересовани лица. За да се предотврати злоупотребата с информация, която би нанесла непоправими щети на администацията, държавата, физически и юридически лица е необходима превенция в следните направления:

1. Граждани ангажирани към службите за национална сигурност в изпълнение на Стратегията за национална сигурност, да се ангажират и насочват приоритетно за работа по превенция срещу киберпрестъпленията в т.ч. физическите лица, кандидатстващи за заемане на длъжност или вече наети, обработващи и управляващи информация в държавната и общински администрации, здравни, образователни и социални заведения и др. сектори на електронното управление;
2. Промяна на изискванията за назначаване на лица за длъжности, имащи служебен достъп и/или администриращи информация и документи от електронния обмен на вътрешните и външни информационни системи на Електронното правителство, по отношение на: задълбочена проверка на опита, представен в автобиографиите; документите за образование и професионална подготовка; поведенчески тестове с приоритетно проучване устойчивостта на кандидатите по отношение

нагласата им за надлежно опазване на станалата им известна служебна информация или документи;

3. Засилени информационни кампании, провеждани от Правителството за гражданите. Информационните кампании да обхващат изясняване правата и задълженията им, при ползване на услуги по електронен път, както предупреждения за евентуални заплахи, които биха могли да настъпят и да увредат интересите им.

Информацията, протичаща в мрежите на електронното управление на държавата, представлява интерес за различни среди – физически лица, политически партии, държави, фирми и др. Не винаги документите и информацията, която се вижда от администраторите на данни или висшите административни служители може да се оцени по същество и важност. Това е следствие обикновено от образователното ниво, социалния статус, обща култура, характерови особености на служителите. По тази причина някои от нерегламентираните изтичания на информация и документи е по причина недооценка на важността й. Превенцията в този случай трябва да обхваща действия по начина на преоценка на важността на информацията от конкретните служители, които е установено, че са предоставили нерегламентирано информация.

За целенасоченото търсене на информация от системите на Електронното правителство, която е ценна за субекти, неразполагащи с регламентиран достъп, обикновено се правят предварителни подготовки. Използват се различни оперативни методи за постигане на целта:

1. Ориентиране в административната среда и фактическата обстановка – запознаване със структурата на административната единица, което съхранява информацията и съответните уязвими звена; Набиране на неофициална информация за служителите и възможностите им за достъп до информация, запознаване с техните индивидуални наклонности, интереси, социални връзки, проблеми; анализ на характеровите особености, касаещи лоялност към работодателя и отношение към съхраняваната информация. Взаимовръзки и личностни отношения в административната единица на всички нива; Възможности за изтичане на информация по официални и неофициални канали, след подходяща «провокация» / експеримент/.

2. На база на предварителните проучвания на фактическата обстановка и оценка на уязвимите звена, планиране на мероприятия за придобиване на информацията;

3. Манипулиране на проучени предварително лица от административната единица, с цел поставяне в зависимост, за да се придобие чрез тях необходимата информация. Манипулацията най-често се осъществява, използвайки предимно техните слабости и амбиции, като: алчност; недооцененост в службата и обществото; безотговорност спрямо извършваната служебна дейност; сексуална зависимост; алкохолна, хазартна и наркотична и др. зависимости, водещи до съгласие за предоставяне на информация нерегламентирано.

4. Използване на религиозни, политически и националистически убеждения, за тяхната манипулация и достигане до степен на съгласие за издаване на информация или увреждане на информационните системи;

5. Склоняване към корупционни действия с цел поставяне в зависимост;

6. Заплаха към личностите на слежителите, техните семейства и близки – в т.ч. заплаха от загубване на службата или имуществото, заплаха със физическа разправа и др..

7. Проучване на кредитната задлъжнялост на служителите от административното звено и последващ психолоически тормоз – пряк или косвен, чрез фирми събиращи дългове, съдебни изпълнители с цел склоняване към предоставяне на информация.

Като превенция на изброените преки заплахи, оказвани от лица, работещи за субекти с интереси за придобиване на нерегламентирана информация, върху личността на административните служители, е необходимо създаването на комплекс от контраразузнавателни мерки по отделните сектори на административните единици. Засилване на мероприятията за ограничаване на достъпа до служебна и класифицирана информация на нивата изхождащи от принципа «необходимо да се знае».

Без предприемане на превантивните мерки спрямо «човешкия фактор» при управлението на Електронното правителство, може да се достигне до нежелани действия компрометиращи сигурността му и доверието на гражданите в целите му.

Използвана литература:

[1]Брюксел 19.11.2004г., COM (2004) 757 окончателен; СЪОБЩЕНИЕ НА КОМИСИЯТА ДО СЪВЕТА, ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ Предизвикателствата пред европейското информационно общество след 2005 г.

ИДЕНТИФИЦИРАНЕ НА ЗАПЛАХИТЕ СРЕЩУ СИГУРНОСТТА НА ЕЛЕКТРОННОТО ПРАВИТЕЛСТВО

Огнян Н. Иванов

Гр. София 1510, ж.к. «Хаджи Димитър» бл. 138, вх. Б, ет. 6, ап. 37

IDENTIFICATION OF THREATS AGAINST THE SECURITY OF E-GOVERNMENT

Ognyan N. Ivanov

ABSTRACT:*The security of e-government is one of the priorities of public authorities and organizations worldwide. Especially today, the information stored in state information systems with the highest degree of danger and its protection is of highest priority in the overall national security strategy globally. Protection of cyberspace is a challenge for citizens, administration and security services.*

KEY WORDS: *e-Government; cyberspace; Prevention; threat; National Security; Information Security; Administration*

Електронното правителство в България е елемент от прехода от индустриално към информационно общество и е средство за ускоряване процеса на евроинтеграция. То е процес на промяна, който позволява да се разширят възможностите на гражданите и бизнеса за участие в една нова, базирана на знанието икономика. За

да се реализира целият потенциал на електронното правителство, е необходимо реформиране на администрацията, на управлението на бизнес процесите и на информацията. Изисква се промяна и в начина, по който служителите в държавната администрация мислят и действат, в отношението им към работата и в общуването с гражданите и с бизнеса.

Основната роля на електронното правителство е да отговори на нуждите на обществото от качествени и леснодостъпни административни услуги. Изграждането на електронното правителство се обуславя и от необходимостта да се намаляват корупционните практики. Услугите ще бъдат предоставяни по начин, място и време, удобни за гражданите и за бизнеса. Освен традиционните канали за комуникация ще се използват и всички нови среди и устройства, като обслужването ще се извършва на принципа "едно гише". Клиенти на услугите на електронното правителство са гражданите и бизнесът, както и държавната администрация. Услугите ще бъдат групирани в теми и събития от живота, описани с ежедневния език на гражданите.

Визията за електронно правителство в България е определена от правителството на Република България, което ще осъществява модерно и ефикасно управление със средствата на съвременни информационни технологии, за да посреща реалните потребности на гражданите и на бизнеса по всяко време и на всяко място.

Правителството на Република България смята да развива необходимата организационна, комуникационна и информационна среда за ефективно функциониране на държавната администрация в съответствие с принципите, нормите и най-добрите световни практики.

Изграждането на електронно правителство се обуславя от необходимостта:Да се съкращават разходите и да се повишава ефективността на държавното управление.

- Да се посрещат очакванията на гражданите и да се подобряват условията за взаимодействие с тях.
- Да се подобрява бизнес климатът.

Електронното правителство обхваща четири основни направления за комуникация и услуги:

- **"**Администрация – Граждани" – съвременни Интернет и интранет WEB базирани решения, съчетани с традиционните средства за осигуряване на широк достъп, които да водят до качествени промени в условията за комуникиране и предоставяне на услуги за гражданите.
- "Администрация – Бизнес" – съвременни решения, които оптимизират процесите и деловите отношения между администрацията и различните икономически субекти.
- "Администрация – Администрация" – развитие на информационните технологии в национален и междудържавен аспект с оглед на ефективно взаимодействие между различните административни структури.
- "Вътрешноведомствена ефективност и ефикасност" - организиране и оптимизиране на бизнес процесите, на отношенията "Администрация – Служители" и на комуникацията в отделните административни структури.

Правителството на Република България си е поставило следните стратегически цели за електронно правителство:

- Предоставяне по електронен път на качествени, икономически ефективни и леснодостъпни административни услуги на гражданите и бизнеса.

• Разширяване на технологичните възможности на гражданите и бизнеса за участие в държавното управление.

• Създаване на организационна, комуникационна и информационно среда за ефективно и прозрачно функциониране на държавната администрациа в съответствие с принципите, нормите и най-добрите практики на Европейския съюз. [1]

Сигурността на Електронното Правителство е един от приоритетите на държавните органи и организации в цял свят. Особено днес, информацията акумулирана в държавните информационни системи е с най-висока степен на опасност и опазването ѝ е от най-висок приоритет в общите стратегии за национална сигурност в глобален мащаб. Защитата на киберпространството е предизвикателство за гражданите, администрацията и службите за сигурност. Държавните системи за електронно управление съхраняват и обработват от публична до специфична секретна информация и всяко едно посегателство и атака върху тях може да нанесе непоправими щети за гражданите и дестабилизация на страната като цяло в т.ч. върху банки, регистри, секретни обекти, имоти ... По тази причина информационните системи на държавата са включени в така наречената „критична инфраструктура".

Основните заплахи за сигурността на Електронното правителство са в четири направления:

1. Технически – софтуерни и хардуерни;
2. Човешкия фактор – физическите лица имащи достъп до информационните системи;
3. Политически;
4. Административни.

Защитата от киберзаплахите е глобален проблем и няма географско местоположение. Тя трябва да надхвърля обичайните мерки за противодействие като откриване на нерегламентирано влизане в информационните системи или предотвратяване, антивирусна защита и трябва да включва конкретни превантивни действия, които могат незабавно да предават информация, че се предвижда заплаха, с какви способи, кога ще се случва.

Приоритетни действия трябва да се предприемат по отношение устойчивостта на информацията срещу кибератаки. Това може да бъде постигнато единствено със създаване на независими и несвързани с вътрешните и външни административни информационни системи - „гнезда за съхраняване на информацията". Тези „гнезда за съхраняване на информацията" трябва да действат на принципа „остров" и да имат само ограничен вход на информацията без възможност за използването и преди настъпването на „срив" в съответната информационна система/и. „Гнездата" ще позволят автоматизирано дублиране на информацията с цел защита сигурността на гражданите и държавата. При създаване на подобни защити от първостепенна важност е същите така да бъдат структурирани и каталогизирани по степени на важност, секретност и сектори, че тя при състояние на загуба на информация от системите на Електронното Правителство, бързо да възстанови всяка информация, която е унищожена или увредена.

Принципа на успешните и защитени информационни системи е правилното съчетание на хора, процеси и технологии. Това се отнася с тежест за информационните системи, подложени на най-голям интерес от неправомерно злоумишлено посегателство – държавните, банковите, съдебните и тези на правоохранителните органи. Така проектирани и управлявани системите са гаранция за обществото и администрацията,

че са надеждни и могат да издържат на посегателство, като имат преимущество да се възстановят бързо от евентуален срив и да продължат да работят.

В новата Стратегия за Е-Управление на България, приета с Решение № 958 на Министерския съвет от 29.12.2010, се извеждат следните рискове за Електронното управление, които са идентифицирани през изминалите няколко години от създаване на Електронното Правителство:

1. Липса на политическа воля и положителен натиск за изпълнение на общата рамка и националната програма;
2. Националната програма остава на високо ниво, без да се декомпозира на ниво министерства и агенции;
3. Разработените програми на ниво министерства остават само пожелателни документи, без практическа реализация;
4. Висока степен на текучество и ниски нива на възнаграждения в ИТ звената на публичната администрация;
5. Липса на специфични умения и знания в публичната администрация (лидерство, управление на промяната, управление на проекти);
6. Слабо участие и незаинтересованост на гражданите и бизнеса;
7. Непознаване и незачитане нуждите на крайния потребител;
8. Липса на стимули за ползване на електронните услуги от гражданите и бизнеса;
9. Ниска информационна култура и познания сред гражданите;
10. Ясно изявена в някои администрации пасивно-защитна организационна култура;
11. Липса на интеграция и оптимизация на процесите, изпълнявани от различни звена на администрацията;
12. Невъзможност на технологичната среда да подкрепи и осигури необходимата среда за планираните електронни услуги;
13. Риск от недостатъчна сигурност на данните;
14. Съпротива на администрацията поради липса на умения.

На 28 февруари 2011 г., Българското Правителство прие Доклад с насоки за за ускореното развитие на електронното управление в страната с необходими осем допълнителни стъпки. Те са свързани с:

- актуализация на правната рамка;
- извършване на координация от надведомствен орган;
- избор, внедряване и/или развитие на ключовите централни системи на електронно управление;
- приоритетизация и внедряване на услугите на регистрите на ключови първични администратори;
- избор и реализация на приоритетни комплексни административни електронни услуги за гражданите и бизнеса;
- описание на процесите на услугите, които предлагат всички администрации и реинженеринг по приоритетност;
- поетапно внедряване на системи за вътрешен електронен документооборот в администрациите, централна документооборотна система и присъединяване към централните системи на електронното управление;
- внедряване на централизирана система за управление на държавните такси по електронен път.

Чрез изпълнението на изброените стъпки Държавата ще повишава доверието и сигурността на потребителите, като подобрява защитата правата им в електронния свят чрез:

• координирани и активни действия на компетентните органи и организации;

• популяризиране на правата на потребителите в електронния свят и средствата за защитата им.

Тези действия на Правителството са декларация за изпълнение на Препоръка Rec (2004)15 на Комитета на Министрите към страните-членки за електронно управление (е-управление),(Приета от Съвета на Министрите на 15 декември 2004 г. на 909 заседание на представителите на министрите.

От изброените рискове и съществуващата потенциална заплаха за Електронното управление, могат да се направят изводи, че в страната има множество слаби звена, касаещи сигурността на информационните системи в държавата. Наложително е да се изготви специален Анализ на заплахите, който да отчете всички влияещи на сигурността на Електронното управление фактори в т.ч. и от терористични действия.

Използвана литература:

[1] Стратегия за електронно правителство, решение на Министерски съвет N 866 от 28 декември 2002

АНАЛИТИЧНО МОДЕЛИРАНЕ НА УДАРНАТА ВЪЛНА, ПОЛУЧЕНА ОТ ТОЧКОВ ВЗРИВ – ЗАДАЧА ЗА БУТАЛОТО

Георги Хр. Петков

1463 София, бул. „Патриарх Евтимий” 81, ет.2, ап.4 Георги Христов Петков

ANALYTICAL MODELLING OF BLAST WAVE, RESULTING FROM POINT EXPLOSION – PISTOL PROBLEM

George H. Petkov

Abstract: *In the present paper is proposed a way of analytical modelling of the blast waves using self-similar solutions. The proposed way is realized, and the numerical results are commented from the point of view of blast pressure and total energy of the process. We assumed a form of the solution, and this enabled us by use of the Rankine-Hugoniot conditions to find an (approximate) closed form solution of the entire problem.*

Key words: *Mathematical modeling, Shock waves, Blast waves, Explosions, Differential equations, Hyperbolic equations, Numerical solutions, Blast pressure, Explosion energy*

Въведение

Войната в Ирак и Афганистан, зачестилите терористичните нападения, които разтърсват света през последните десет години, определят необходимостта от

изследване на един фактор, който все повече се налага като съществен за оценката на пораженията в резултат на експлозии и действието на ударната вълна върху човека. Според направени изследване около 1,5 милиона войници от американската армия получават мозъчни наранявания всяка година и около 200 000 души медицински персонал се занимава с диагностицирането на пораженията. Установено е, че освен директното въздействие на взривната вълна, което действително увреждa тъканите, има и други въздействия, дължащи се на индуцираните от взрива вътрешни стрес вълни, които по-трудно се определят и които не подлежат на директна диагностика.

За да се изучат ефективно взривните наранявания трябва едновременно да се работи в няколко направления, едното от които е математическото моделиране на взрива, не само по отношение на неговата сила и обсег, а и по отношение на отделяната във всеки момент енергия и нейната връзка с причиненото свръхналягане.

В настоящото изследване е моделиран аналитично точков взрив, като за полученото решение е изследвана зависимостта на свръхналягането и общата енергия в един специален частен случай.

Методи

Взривът е моделиран чрез задачата за буталото. Разгледали сме „малки" движения на сферично бутало, което избутва въздуха около себе си. В симетричния случай малките движения се определят от линейно вълново уравнение:

(1) $$\Phi_{tt} = c_0^2\left(\Phi_{rr} \| \frac{2\Phi_r}{r}\right)$$

Където Φ е "velocity potential" за решението u. Потенциалът на скоростта се използва в динамиката на флуидите, когато флуид заема „просто-свързана" област и извършената работа не зависи от пътя (консервативност). В такъв случай $\nabla \times u = 0$, където u е скоростта на потока флуид. Като резултат u може да бъде представена като градиент на скаларна функция $\Phi: u = \nabla\Phi$ където Φ се нарича потенциал на скоростта за u и Φ е единствено с точност до константа.

Фактът, че задачата за буталото моделира специален случай на точкова експлозия, е разгледан в светлината на енергийните характеристики на проблема. Настоящият подход е предложен от [(1)]. Той предполага, че като резултат от движението на буталото, общата енергия – сумата от кинетичната и вътрешната енергии на газа, се променя във времето съгласно следния закон:

(2) $$E = E_0 t^s$$

Където E_0 и s са константи. Случаят $s = 0$ отговаря на ударна вълна, чиято енергия зад удара е константа. В нашия случай $s \geq 0$, което означава, че общата енергия на потока се увеличава с времето (или поне остава константа). Предполагаме, че потокът е предизвикан от голямо движение на буталото и е воден от безкрайно голям по сила ударен фронт. Позицията на повърхнината на буталото ще бъде намерена чрез числено интегриране на система ОДУ, получени в резултат от предположението за самоподобие на потока, започвайки интегрирането от фронта на удара и локализирайки буталото така, че да е изпълнено кинематичното условие. При разглежданията е игнориран ефектът на разсейване.

Резултати

Разглеждаме едномерен променлив поток от идеален газ, който се описва чрез системата:

(3) $$u_t + uu_r + \frac{1}{\rho}p_r = 0$$

(4) $$\rho_t + u\rho_r + \rho u_r + \frac{ku\rho}{r} = 0$$

(5) $$\left(\frac{p}{\rho^\gamma}\right)_t + u\left(\frac{p}{\rho^\gamma}\right)_r = 0$$

Където u, ρ, p са съответно частните скорост, плътност и налягане на газа на разстояние r от центъра на взрива след време t; $при\ k = 0,1,2$ съответно за равнинна, цилиндрична и сферична симетрия.

Удобно е да заменим уравнение ***(5)*** със следната еквивалентна форма:

(6) $$\left(\frac{1}{2}\rho u^2 + \frac{p}{\gamma-1}\right)_t + \frac{1}{r^k}\left\{r^k u\left(\frac{1}{2}\rho u^2 + \frac{\gamma p}{\gamma-1}\right)\right\}_r = 0$$

Системата нелинейни ЧДУ ***(3), (4)*** и ***(6)***, заедно с ***(2)*** трябва да бъде решена при спазване на граничните условия върху буталото и върху удара, който то е произвело. Въвеждаме нова променлива:

(7) $$x = \frac{r}{R}$$

Където $R = R(t)$ е радиусът на удара (при $x = 1$ това представлява локуса на удара). Скоростта на удара се определя чрез

(8) $$V = \frac{dR}{dt}$$

Решението се търси в себеподобна форма:

(9) $$u = Vf(x)$$

(10) $$p = \frac{\rho_0 V^2}{\gamma} g(x)$$

(11) $$\rho = \rho_0 h(x)$$

Където ρ_0 е равномерната плътност на газа пред ударната повърхност (пред ударния фронт). Общата енергия на газа е:

(12) $$E = \int \frac{1}{2}\rho u^2 d\tau + \int \frac{p}{\gamma-1} d\tau$$

Където $d\tau$ е обемен елемент. Първият интеграл в ***(12)*** е общата кинетична енергия, докато вторият е общата вътрешна енергия, съдържаща се в пространството между повърхността на буталото и повърхността (фронта) на удара. Ако заместим ***(9) - (11)*** в ***(12)*** ще получим:

(13) $$E = \rho_0 \epsilon_k V^2 R^{k+1} \int_{x_0}^{1} \left(\frac{1}{2} hf^2 + \frac{g}{\gamma(\gamma-1)}\right) x^k dx$$

Където $\epsilon_k = 2^k \pi^{\frac{1}{2}k(3-k)}$ и x_0 са координатите на разширяващата се повърхност. Интегралът ***(13)*** включва параметрите γ, k, s ***(вж.*** [(2)]***).*** С γ означаваме адиабатния индекс $\gamma = \frac{c_p}{c_v} = \frac{\alpha+1}{\alpha}$, където със c_p означаваме специфичният топлинен капацитет при постоянно налягане, а със c_v означаваме специфичният топлинен капацитет при постоянен обем. α представлява броят на степените на свобода, разделен на 2 (3/2 за едноатомни газове и 5/2 за двуатомни газове). За двуатомни газове (поголямата част от състава на въздуха) $\gamma = {}^{7}/_{5} = 1.4$

От ***(2)*** и ***(13)*** получаваме:

(14) $$R^{\frac{1}{2}(k+1)} \frac{dR}{dt} = \left(\frac{E_0}{\epsilon_k \rho_0 J}\right)^{\frac{1}{2}} t^{\frac{s}{2}}$$

Където

(15) $$J = \int_{x_0}^{1} \left(\frac{1}{2} hf^2 + \frac{g}{\gamma(\gamma-1)}\right) x^k dx$$

Като интегрираме ***(14)*** получаваме:

(16) $$R = \left(\frac{k+3}{s+2}\right)^{\frac{2}{k+s}} \left(\frac{E_0}{\text{kp}_0}\right)^{\frac{1}{k+s}} t^{\frac{s+2}{k+3}}$$

Използвахме условието ($R = 0, t = 0$). От уравнение ***(16)*** могат веднага да бъдат отделени два важни случая:

- $s = 0, R \propto t^{\frac{2}{k+2}}$, получаваме радиуса на удара за точкова експлозия, отговаряща на различни геометрии при $k = 0, 1, 2$

- $s = k + 1, R \propto t$, случай на равномерно разширяване съответно на равнинно, цилиндрично или сферично бутало.

Тези два специални случая в действителност задават краищата на интервала на промяна на s . Решението ***(9) - (11)*** променя ***(3), (4)*** и ***(6)*** до:

(17) $$(x - f)f' = \frac{g'}{\gamma h} + \frac{s-k-1}{s+2} f$$

(18) $$(x - f)h' = h\left(f' + \frac{kf}{x}\right)$$

(19) $$\left(x^k f\left(\frac{1}{2} hf^2 + \frac{g}{\gamma - 1}\right)\right)' = x^{k+1} E_1'(x) + \frac{2(k+1-s)}{s+2} x^k E_1(x)$$

Където

(20) $$E_1 = \frac{1}{2} hf^2 + \frac{g}{\gamma(\gamma - 1)}$$

Сега ще разгледаме условията за силен удар (***Rankine - Hugoniot***):

(21) $$u_1 = \frac{2}{\gamma + 1} V$$

(22) $$\frac{\rho_1}{\rho_0} = \frac{\gamma + 1}{\gamma - 1}$$

(23) $$\frac{p}{\rho_0 V^2} = \frac{2}{\gamma + 1}$$

Ако горните условия бъдат представени във вида ***(9) - (11)***, то те ще изглеждат по следния начин:

(24) $$f(1) = \frac{2}{\gamma + 1}$$

(25) $$h(1) = \frac{\gamma + 1}{\gamma - 1}$$

(26) $$g(1) - \frac{2\gamma}{\gamma + 1}$$

Движението на буталото се дава при $x = x_0$, което означава $r = x_0 R(t)$. Кинематичните условия на буталото изискват скоростта на буталото да е равна на частичната скорост в тази точка. Следователно от ***(9)*** и $r = x_0 R(t)$ получаваме $f(x_0) = x_0$. Задачата се редуцира до намирането на x_0, такова, че за зададено γ, да удовлетворява системата ***(17) - (19)*** с начални условия ***(24) - (26)***, където интегрирането се извършва от единица до онази стойност на $x = x_0$, за която $f(x_0) = x_0$.

Заключения

Предположението за себеподобност означава, че общата маса на газа между фронта на удара и буталото остава постоянна през цялото време. Този факт се използва за проверка на числените решения на задачата. На фигури **Error! Refer-**

ence source not found., 1, **Error! Reference source not found.** по-долу са изчислени и представени по отношение на точката, в която се появява разширяващата се повърхнина, налягането в тази точка и интегралът на енергията, определящ общата енергия пренасяна от потока съответно за равнинна, цилиндрична и сферична геометрия.

Нека разгледаме уравнения ***(17) - (19)***, притежаващи константно решение за равнинна симетрия с $k = 0$. Това решение е просто:

(27) $$f(x) = \frac{2}{\gamma+1}$$

(28) $$g(x) = \frac{2\gamma}{\gamma+1}$$

(29) $$h(x) - \frac{\gamma+1}{\gamma-1}$$

Ясно е, че в този случай, позицията на буталото се дава с

(30) $$x_0 - f(x_0) - \frac{2}{\gamma+1}$$

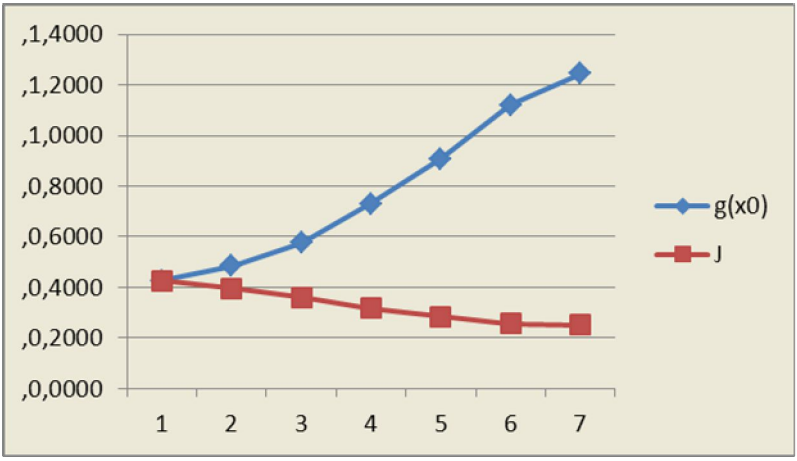
От където, в термините на физически променливи получаваме, че решението е:

(31) $$u - \frac{2}{\gamma+1}V$$

(32) $$\rho = \rho_0 \frac{\gamma+1}{\gamma-1}$$

(33) $$p = \frac{2\rho_0 V^2}{\gamma+1}$$

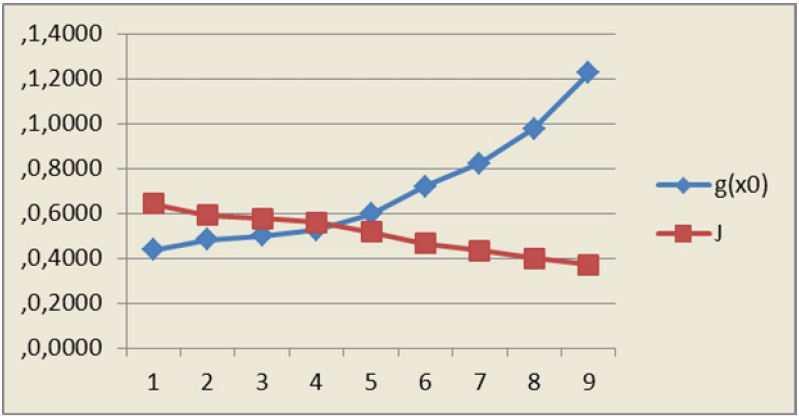
Където V е постоянната скорост на ударния фронт. В действителност, буталото напредва с постоянна скорост $\frac{2V}{\gamma+1}$, така, че обемът, оставащ след удара постоянно се увеличава с времето. Общата енергия на потока за единица площ на сечение е $\frac{4\rho_0 V^2 R}{(\gamma+1)^2}$



Фиг. 1. *Графика на разпространението на налягането и общата енергия – сферична симетрия с параметри* $\gamma = 1.4; k = 2$

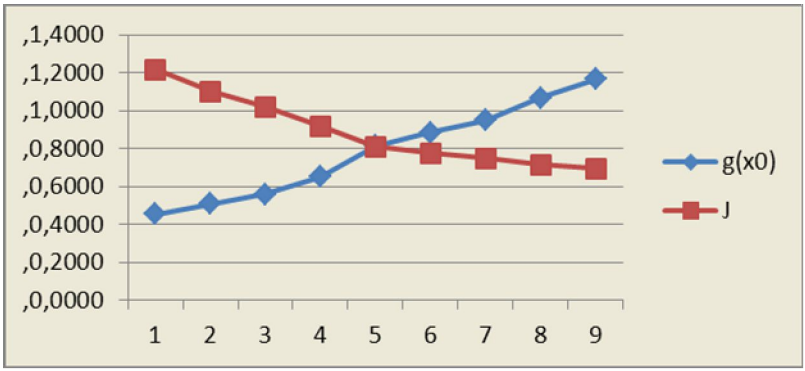
При сферичната симетрия налягането и общата енергия стартират от една и

съща точка (стойност), като от там нататък общата енергия намалява, а налягането расте. И двете величини се изменят почти линейно, като растежът на налягането е много по бърз от намаляването на общата енергия. Това означава, че увеличаването на налягането за сметка на общата енергия е много бързо в някакъв начален интервал и се компенсира по-късно с намаляване на общата енергия, когато налягането достига максимум и започва да намалява.



Фиг. 1. *Разпространение на налягането и общата енергия – цилиндрична симетрия с параметри* $\gamma = 1.4; k = 1$

При цилиндрична симетрия налягането стартира от по малка стойност, сравнено с общата енергия. До точката на пресичане, увеличаването на налягането е изцяло за сметка на намаляването на общата енергия. От там нататък общата енергия намалява, а налягането расте, като и двете величини се изменят почти линейно и следват картината при сферична симетрия, т.е. характерът се повтаря, когато цилиндърът стане достатъчно голям ни съответно неравностойната компенсация на налягане с енергия ще продължи по-кратко.



Фиг. 3. *Графика на разпространението на налягането и общата енергия – равнинна симетрия с параметри* $\gamma = 1.4; k = 0$

При равнинната симетрия налягането стартира от много по-малка стойност, сравнено с общата енергия. До точката на пресичане, увеличаването на налягането е изцяло за сметка на намаляването на общата енергия, като този характер на изменение на графиките се запазва и след пресичането. От тук можем да заключим, че увеличението на налягането при равнинна симетрия е изцяло за сметка на изменението на вътрешната енергия.

Литература

1. Similarity ows behind strong shock waves. **Rogers, M.H.** 1958 г., Quart. J. Mech. Appl. Math., 11, стр. 411.

2. The Air Wave Surrounding An Expanding Sphere. **Taylor, G. I.** 1946 г., Proc. Roy. Soc. Lond., A, 186, стр. 273-292.

МЕТОДОЛОГИЯ ЗА ЕФЕКТИВНО ПРОГНОЗИРАНЕ НА ЖЕРТВИТЕ СРЕД ЦИВИЛНОТО НАСЕЛЕНИЕ ПРИ ВЗРИВОВЕ ОТ ТЕРОРИСТИЧЕН ХАРАКТЕР

Георги Хр. Петков

1463 София, бул. „Патриарх Евтимий" 81, ет.2, ап.4 Георги Христов Петков

METHODOLOGY FOR EFFECTIVE PREDICTION OF CIVILIAN CASUALTIES IN CASE OF TERORIST BLAST

George H. Petkov

AbstractM *In the present paper is proposed a way of modelling of the blast trauma resulted in terrorist attack. The proposed model is based on mathematical modelling, medical statistics, and prediction methods and algorithms. The practical realization of the proposed way will help to the medical teams in organization of effective organization and management of the rescue process, i.e. pre-hospital, and hospital trauma live support resulting in less possible victims.*

Key wordsM *Mathematical modeling, Shock waves, Blast waves, Explosions, Differential equations, Medical statistics, Blast trauma, Pre-Hospital Trauma Live Support, Hospital Trauma Live Support*

Въведение

Международният тероризъм представлява в настоящия момент най-голямата угроза за мира в демократичните общества. Практически всички въоръжени конфликти, които възникваха в Азия, Африка, Близкия и Среден изток, на Балканите, на територията на бившите съветски републики се съпровождаха с диверсионно-терористични актове, като основните последствия бяха за мирното население. От октомври 2005 година жертвите от самоделни взривни устройства възлизат на една трета от всички американски смъртни случаи в Ирак.

Използването на големи количества ниско технологични взривни вещества с цел предизвикване на масова смърт се превърна в бързо разпространяваща се так-

тика в съвременната война и в терористичните атаки.

Стратегическата цел, чието постигане се преследва с настоящото изследване, е да се противодейства по възможно най-ефективен начин на взривовете с терористичен характер. Работата в тази насока може да бъде обобщена в следните две направления:

- Да се предотврати (минимизира) възможността за тероризъм и терористични взривове на обществени места;
- Да се конструира адекватна стратегия за минимизиране на жертвите сред цивилното население при взривове от терористичен характер.

И двете направления са изключително важни и в комбинация осигуряват надеждна защита срещу тероризма и повишават доверието на хората в държавата и институциите.

Цел, задачи и методи

Настоящото изследване представлява част от дейността, която е необходимо да се извърши по второто от двете направления, като се базира на хипотезата – „Защитата на дадено обществено място от тероризъм е преодоляна по някакъв начин и взривът е факт!". В този случай най-важна е организацията на служби като полиция, пожарна, спешна помощ и гражданска защита, които трябва да пристигнат на мястото на инцидента и максимално бързо и ефективно да ограничат последствията, водещи до възможна смърт сред поразените. Основна роля в минимизиране на последствията от инцидента играят медицинските екипи. За да могат да оптимизират организацията си и начина си на действие, те трябва да разполагат с предварителна информация за броя на поразените, типа на травмите и тяхната тежест. Следователно медицинските екипи трябва да разполагат с методи и инструменти за прогнозиране на медицинските резултати от взрива, което е и целта на представеното изследване.

Основна цел на настоящата работа е да се предвидят последствията (травмите и нараняванията) върху хора в следствие на взрив на обществено място (резултат от терористична дейност, авария или бедствие).

Конкретната цел на изследването е да се построи математически модел на взривовете, даващ като резултат възможните травми сред населението, получени в резултат на взривове от терористичен характер, в закрити и открити помещения.

Експлоатирането на този модел ще даде точна представа на медицинските екипи за броя на пострадалите.

За да постигане на поставената цел е необходимо да се решат следните две задачи:

А. **Да се моделира взривния процес и в резултат да се получи налягането на ударната вълна върху всеки един от потенциалните пострадали.**

Б. **Да се приведе налягането на ударната вълна, получено при решаване на задача А. в термините на травми и поражения върху хората, потенциални пострадали.**

Решаването на тези две основни задачи, във всеки конкретен случай е свързано с голям брой подробности (детайли), чиито стойности намират отражение в параметрите на модела. В резултат на решаването на упоменатите по-горе задачи може да се построи общ модел, който да дава възможност за корекции при прилагането му във всеки конкретен случай.

Резултати

На първо място трябва да се започне от теорията на взрива, разгледана от гледна точка на приложната математика. Трябва да се изучат явленията „експлозия" и „ударни вълни" в широкия контекст на хиперболичните системи от частни диференциални уравнения. Основната ни мотивация е свързана с явлението „експлозия", като настоящият подход към проблема е изцяло конструктивен.

За да бъде построен модел, във всяка конкретна ситуация е необходимо да се разполага със следната информация:

- Конструктивни характеристики на сградата, където е избухнал взрив;
- Материали, с които е изпълнена сградата;
- Статистическа оценка за плътността на човекопотока в момента на взрива;
- Мощността на взрива (като тротилов еквивалент);
- Местоположението на взрива в сградата;

С помощта на гореописаните начални данни и знанията за природата на взрива и разпространението на взривната вълна, може да се създаде модел на ситуацията, численото решение на който дава оценка за налягането на ударната вълна и интензивността на потока на осколки във всяка точка от сградата, респективно усреднено налягане и поток на осколките, на които е изложен човекопотокът. По този начин могат да се получат конкретни формули за изчисляването на пика на свръхналягането и профила на налягането във времето за всяка точка от интересуващото ни пространство.

Обща схема на процеса

Нека разгледаме общата схема на процеса. Началният процес за постигане на основната ни цел е представен на схема 1. Това е процесът на моделиране на взрива и уточняване на параметрите на модела в зависимост от конкретната ситуация. Резултатът от тази първа стъпка се изразява в решаване на задача А или в установяване на „Налягане на взривната вълна, поток на ударната вълна и плътност на потока осколки върху единица обем на помещението във времето".

Първо е разгледана общата теория на хиперболичните частни диференциални уравнения (1), и с тяхна помощ се моделира действието на сферично бутало. Мощността и типа на взрива, местоположението му, конструктивните характеристики на сградата, както и материалите и предметите, които потенциално могат да причинят създаването на осколки при взрива, са отчетени в параметрите на модела (7). Следва привеждането на създадения модел в система ОДУ или подходяща изчислителна схема (8) и получаване на числено й решение (9). Резултатът (10) представлява разпределение на налягането в следствие на взривната вълна, заедно с плътността и скоростта на потока осколки в пространството и времето.

Макар и свързана с множество теоретични и технически трудности, решаването на тази част от проблема е принципно ясно: Моделира се един известен процес. Това създава реална възможност моделирането да бъде извършено за множество важни обекти, където създаването на такъв модел може да се окаже близка реалност, ползвайки методологията, описана в настоящата работа. Ето защо при решаването на втората поставена задача (Б), а именно: „Да се приведе налягането на ударната вълна, получено при решаване на задача А. в термините на травми и поражения върху хората, потенциални пострадали" ще считаме, че задача (А) е решена по метода на черната кутия Схема2.

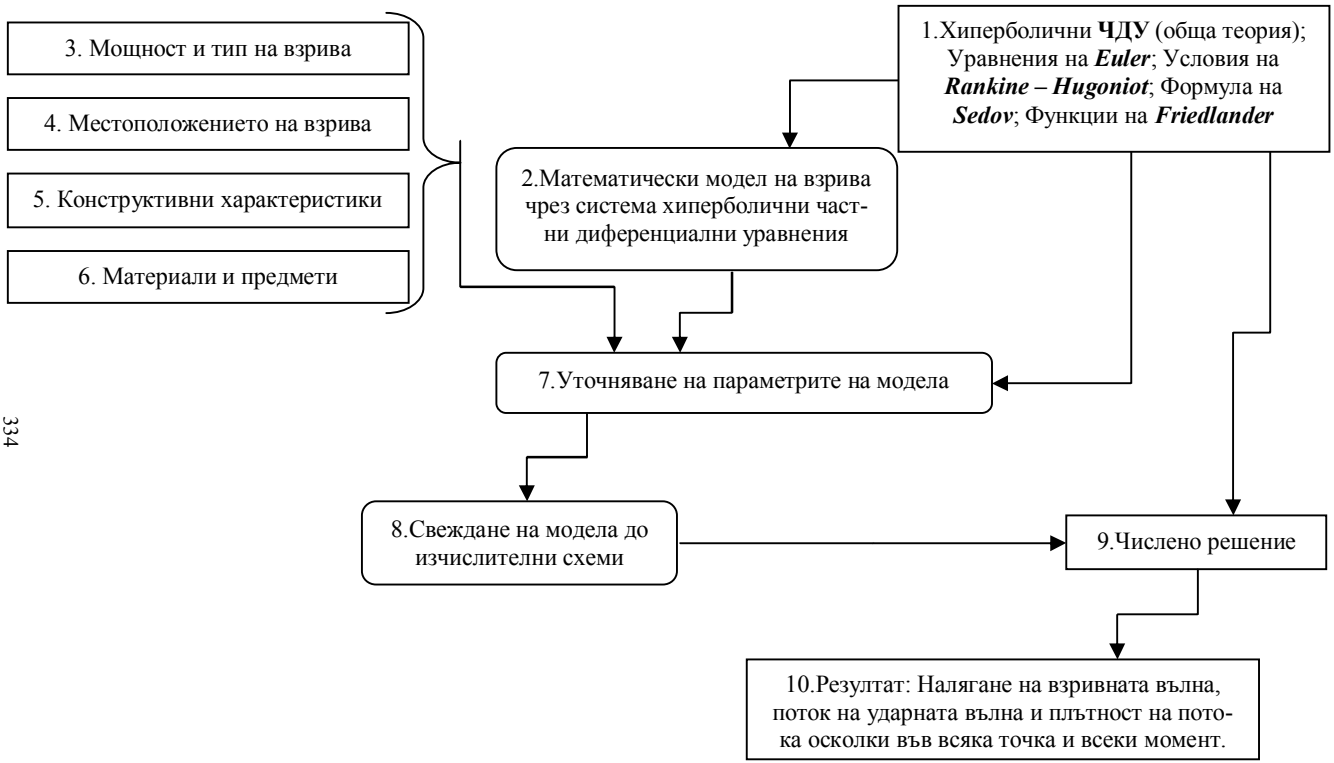

3. Мощност и тип на взрива
4. Местоположението на взрива
5. Конструктивни характеристики
6. Материали и предмети
1.Хиперболични **ЧДУ** (обща теория); Уравнения на ***Euler***; Условия на ***Rankine – Hugoniot***; Формула на ***Sedov***; Функции на ***Friedlander***
2.Математически модел на взрива чрез система хиперболични частни диференциални уравнения
7.Уточняване на параметрите на модела
8.Свеждане на модела до изчислителни схеми
9.Числено решение
10.Резултат: Налягане на взривната вълна, поток на ударната вълна и плътност на потока осколки във всяка точка и всеки момент.

Схема 1.

Синтезирана схема

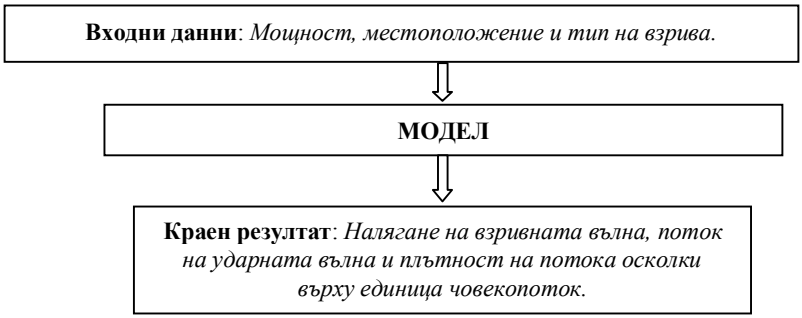


Схема 2.

Сега ще коментираме проблема с решаването на задача (Б), при положение, че разполагаме с решението на задача (А).

За да може да се извади заключение за реалните поражения и травми върху хората, е необходимо да се изучат травмите, причинени от съответен взрив. На базата на статистическо изследване на множество терористични атентати може да бъде оценена вероятността за получаване на съответното нараняване в зависимост от разстоянието до взрива и мощността на взрива. Получените вероятностни разпределения на съответните типове травми по същество решават задача (Б) и заедно с получения в резултат от решаването на задача (А) математически модел ни дават необходимият инструмент за прогнозиране.

Разбира се действието на получения модел за прогнозиране трябва да бъде валидирано, т.е. резултатите от неговото действие трябва да бъдат проверени. За целта трябва да се анализира обширна медицинска статистика, описваща подробно състоянието на всеки един поразен – мощност на взрива, разстояние до взрива, поток осколки, травми, лечение и т.н. На базата на тази статистика и компютърните модели на човешкото тяло, тъкани и органи, може да се построи модел на травмата, който заедно с модела на взривната вълна да се използва за предсказване на пораженията (нараняванията).

Изводи и обсъждане

Или за да се реши окончателно тази задача, трябва да се използва обширна медицинска статистика, т.е. статистически данни за резултатите от различни по сила и тип взривове върху хора, заедно с подробно описание на получените травми и приложените лечения. При решаването на тази задача може да бъде създаден самообучаващ се и само-коригиращ се устойчив модел, като резултат от който да се получава прогноза за съответните видове травми и поражения върху цивилното население във всеки конкретен случай, което е показано схематично на Схема3.

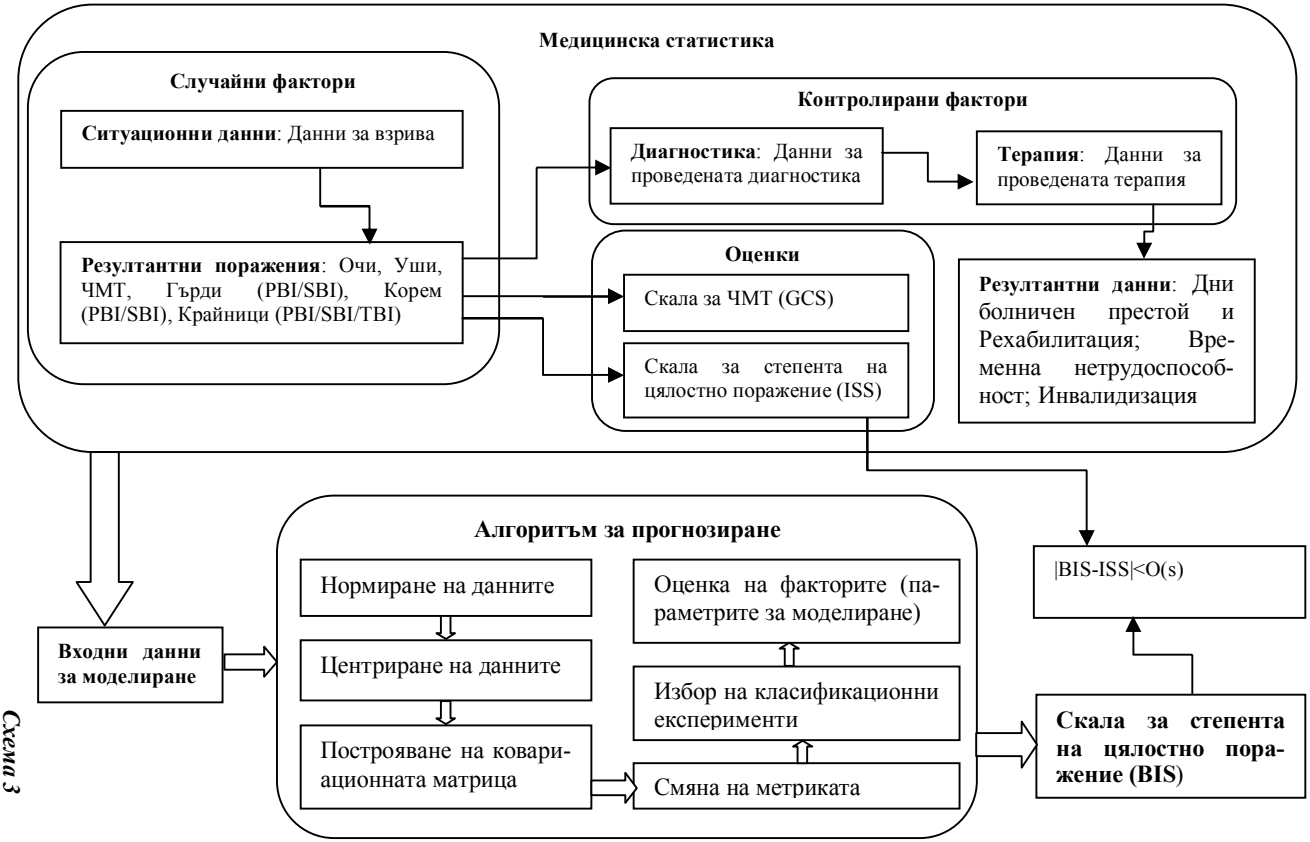

Медицинска статистика
Случайни фактори
Ситуационни данни: Данни за взрива
Резултантни поражения: Очи, Уши, ЧМТ, Гърди (PBI/SBI), Корем (PBI/SBI), Крайници (PBI/SBI/TBI)
Контролирани фактори
Диагностика: Данни за проведената диагностика
Терапия: Данни за проведената терапия
Оценки
Скала за ЧМТ (GCS)
Скала за степента на цялостно поражение (ISS)
Резултантни данни: Дни болничен престой и Рехабилитация; Временна нетрудоспособност; Инвалидизация
Входни данни за моделиране
Алгоритъм за прогнозиране
Нормиране на данните
Центриране на данните
Построяване на ковариационната матрица
Оценка на факторите (параметрите за моделиране)
Избор на класификационни експерименти
Смяна на метриката
|BIS-ISS|<O(s)
Скала за степента на цялостно поражение (BIS)

Схема 3

На схемата е показана подробната структура на медицинската статистика, която трябва да се използва при създаването на модела за прогнозиране и неговото алгоритмизиране. Първият интересен факт е, че случайните фактори от медицинската статистика почти напълно повтарят изходните данни, получени от модела на взрива (Схема 1). Реално цялата информация от статистическите данни е включена в модела за прогнозиране при неговата алгоритмизация. От тук следва, че ако са спазени направените предположения за разпределението на случайните фактори, то всяко добавяне на нов случай към модела ще води до корекция в крайния резултат и по-прецизно отразяване на действителността. Това означава, че при спазване на направените предположения можем да получим самообучаващ се и самокоригиращ се алгоритъм за прогнозиране на резултатите. Не на последно място трябва да се отбележи медицинската страна на въпроса. В статистиката са дадени много медицински данни, които заедно с построения модел и алгоритъм за прогнозиране на резултата могат да се използват за широко изследване и оптимизиране на медицинската дейност (скоростта и правилността на реакция) в подобни ситуации.

След направените описания и коментари, можем да заключим, че общата идея и схема за реализация на целия процес ще изглежда по начина описан в Схема 2 и корекция чрез Схема 3. Ако познаваме мощността, местоположението и типа на взрива, то можем да ги подадем, като начални данни на модела, конструиран за специфичната сграда. В резултат ще получим началните данни за алгоритъма за прогнозиране, в резултат от чието действие ще имаме оценка степента на поражение. Ако освен това разполагаме с оптимизирана медицинска методология за действие в такива ситуации, можем да осъществим основната цел на всички такива разработки: запазването на човешкия живот.

ПОЛИТИЧЕСКИЯТ ТЕРОРИЗЪМ - АКТУАЛЕН И ДНЕС

Николинка Стефанова **Бориславa Тинкова**

НВУ" В. Левски", Факултет „ Артилерия, ПВО и КИС" гр. Шумен, Р. България

THE POLITICAL TERRORISM – STILL IN EFFECT TODAY

Nikolinka Stefanova **Borislava Tinkova**

NATIONAL MILITARY UNIVERSITY 'V. LEVSKI" FACULTY'ARTILERY, AIR DEFENSE AND CIS" SHUMEN,BULGARIA

Acts of terrorism and detailed characteristics of political terrorism are discussed in the paper.

The goals which the political terrorists are striving to reach and the political results are summarized in the paper.

Key words: terrorism, political terrorism

Терминът тероризъм е производен от латинския термин „Terrere", което на латински означава „карам да трепери". Въведен като насилие по време на война, в

мирно време теророът остава да виси като меч над главите, които се опитват да се надигнат. В деспотичните общества, той е инструмент за раболепие и гарант за подчиненост на масите.

Актове на тероризъм са довели болка, тъга, страх и несигурност в Света. Тероризмът никога няма да се спре, той може само да бъде забавен. Предотвратяване на тероризма е от съществено значение, но какво трябва да направи всяко едно правителство, за да се опита да спре това?

Въпреки, че по своята същност **политическият тероризъм** е изключително хетерогенен феномен, неговите основни характеристики съвсем не са многообразни.

1. Основните характеристики на политическия тероризъм:

Първата важна характеристика е, че политическия теророзъм *се изразява в осъществяването на насилствени, най-вече въоръжени, действия*. Влиянието на политическия тероризъм не трябва да се свързва с чисто физическия ефект, като напр. количеството жертви, тъй като за политическия тероризъм, както в миналото, така и днес много по-съществен е емоционално-психологическият ефект, проявяващ се в изплашване на населението и ориентирането му в желаната от терористите политическа ориентация на мислене и поведение. Следователно най-негативният резултат се изразява в това, че при политическите терористични акции настойчиво се поставя под съмнение самата способност на страната да се справя със ситуацията и да обезпечава правов ред, да охранява живота, достойнството и имуществото на гражданите си.

Втората важна характеристика на политическият тероризъм *е неговият групов характер*. Социалната история познава доста примери на политически терористични бойци- самотници, но в същностната си основа политическият тероризъм е най-вече дейност, която се извършва от организирани групи.

Третата важна характеристика на политическия тероризъм е *неговото основаване върху междугруповите конфликти*. Като основно правило обектите на тероризма имат дадени групови характеристики (религиозни, национални, партийни, класови и други), присъщи на тези, по отношение, на които субектът на терористичния акт е настроен враждебно. Така, разкриването на отношението на субекта на терористичния акт към именно тези характеристики, всъщност, разкрива мотивите на дееца.

Всяко политическо терористично движение се старае да прикрие неморалния и престъпния характер на своите действия, както пред членовете си, така и пред членовете на обществото. Съществена роля в това отношение се възлага на идеологическото обосноваване, на моралното и религиозното оправдаване (доказващи целесъобразността и справедливостта на деянието, както и правомерността му).

Сред аргументационния арсенал в това отношение се използват например:

1. Една от главните версии на политическите терористични организации е, че:

- пръв е започнал обектът на техните посегателства;
- обектът интензивно поддържа конфронтацията.

Следователно *"Нашите действия са неизбежни", "те са в резултат от обективните условия, при които сме поставени", "те са достоен отговор на насоченото против нас поведение", "те са отговор на провокацията, на която сме подложени"*. При тази стратегия аргументацията се свежда до еднозначна интерпретация на чуждите и на своите действия, като причинноследствената верига е

далеч от истината;

2. Вторият съществен аргумент на политическите терористични организации е: *„Обектът на нашия терор е безумно непримирим и вредоносен, поради което по отношение на него са оправдани всякакъв вид насилствени действия"*. При тази аргументация се употребява древният психологически стереотип за изначално вражеската същност на "*другия*", "*на всички, които не са наши*";

3. Третият важен аргумент от аргументационния арсенал на политическия тероризъм е: *"Законните действия са неефикасни, единственото ефикасно средство са въоръжените акции"*. В повечето случаи аргументът е обединен с оценки и примери от дейността на правосъдната система;

4. Четвъртият аргумент в този аспект се свежда до твърдението, че *„целта оправдава средствата"*, при което на тероризма и терористите се приписват високоблагородни идеали и цели, като напр. обезпечаване на „*щастието на народа*" и на „*класовата или социалната справедливост*".

Четвъртата важна характеристика на политическия тероризъм е вземането на *заложници*. В арсенала на политическите терористични действия се съдържат множество действия, но особено силно психологическо влияние върху властта и населението оказва именно *вземането на заложници*. При тези ситуации властите често са затруднени от стремежа за постигане на две взаимноизключващи се стратегии – от една страна - да освободят заложниците, а от друга - да не допускат да правят отстъпки пред терористите.

При вземането на заложници широко се използват:

1. Похищение на отделни лица или групи, и отвеждането им на скрити места при обезпечаване на невъзможност за силовото им освобождаване, и при възможност за осъществяване на заложничество за сравнително дълъг период от време;

2. Завземане на транспортни средства заедно с пътниците – самолети, влакове, кораби, автомобили;

3. Завземане на помещения заедно със заложници – на държавни или обществени заведения, затвори, хотели и други.

Като правило за властите, поставени в ситуацията на вземане на заложници, са възможни две стратегически решения:

1. *Недопускане на никакви отстъпки на терористите* (към стратегията се придържат преди всичко САЩ);

2. *Прилагане на гъвкаво реагиране*, в арсенала на което е включено прилагането преди всичко на преговори и компромиси, наред с възможността и за употребяването на силови методи.

Петата важна характеристика на политическият тероризъм е, че той е *вид тактика*, прилагана от опозиционни групировки на властта в борбата им против политическия режим. Отделните актове на лично възмездие или израз на ненавист към съществуващия строй не са политически тероризъм, доколкото при тях липсва систематичност и организираност. В условията на съвременната масова престъпност далеч не всеки пожар, взрив или изстрел е терористичен акт, а още по-малко – политически терористичен акт, защото по своята същност политическите терористични актове винаги са идеологически мотивирани действия, които преследват специфично политически цели.

Ориентацията към политически покушения като основна форма на опозиционно противоборство отличава политическия тероризъм от масовите мирни или на-

силствени действия от типа на демонстрациите, въстанията и войсковите сражения за завземане на територии на противника. Тактиката на покушенията разграничава опозиционния тероризъм от държавния тероризъм, опиращ се върху репресивната дейност. И двете покушения са „*кръвно свързани*", но между тях има разлика.

Характерна черта на политическия тероризъм е това, че той е *оръдие за политическо опозиционно действие, което въпреки че няма истинска масова база, съвсем не е политически безпочвено*. Напротив- както политическият, така и всеки друг вид тероризъм притежава достатъчно дълбоки социални корени, формира се върху основата на противоречия и стълкновение на интересите на различни слоеве на обществото и групите в атмосферата на напрежение и нестабилност, така че в крайна сметка всеки тероризъм изхожда от същите обстоятелства, от които произтича и всяко масово движение.

Шестата важна характеристика на политическия тероризъм е, че *ирационалното начало се съчетава с употребяването на дадени политически или философски идеи като средство за политизация на емоциите, като инструмент за съзнателна трансформация на предразположеността към разрушителни действия*.

Политическият тероризъм се основава върху *максималистко-екстремистка трактовка на определени социалнополитически идеали, национални стремежи или религиозни психологически установки*, които сами по себе си, съвсем не водят до появата на терористична опасност, но тяхното обединяване с благоприятна среда рязко стимулира проявата им в най-вече тази насока.

Политическият тероризъм от края на XX и началото на XXI век има непосредствени предтечи в лицето на крайно радикалните направления в регионалното, националното, международното движение в Европа, както и на народоволското, анархистическото и социалистическото движение в Русия.

Съвременният политически тероризъм запазва родовото си единство с тези движения, наследява от тях много от принципните идеологически обосноваванията, мотиви и базови прийоми, при което се характеризира и с особеностите на конкретната историческа ситуация при новите условия. При това днес в него намират израз и някои същностни характеристики, които в предишни времена са били само загатнати като съществуващи в потенциална форма, като напр. *възможностите за мащабност*.

Предишните форми на политическия тероризъм са се основавали върху тираноборчески републикански или анархистически идеологически обосновки.

Съвременните форми на политическия тероризъм се основават преди всичко върху *различните форми на прокомунистическите и профашистките идеи и идеали*, сред които особено чести са проявите на т. нар. ***„ляв тероризъм***", който представлява най-показателния и специфичен съвременен модел на тероризма, и предявяващ претенции за освобождаване на човечеството от „*тиранията на държавата*", от „*капиталистическата експлоатация*", от „*империалистическия гнет*", с принципи и идеологически обосновки.

Седмата важна характеристика на политическия тероризъм е свързана с *избора на обектите на покушението*. В началния етап на терористическите движения, обект на терористическите покушения са били преди всичко монарсите и отговорните висши държавни чинове, които злоупотребяват със своята власт (квалифицирани като „*тирани*", „*сатрапи*" и „*палачи*"), при което самото покушение е приема характера на „*заслужено възмездие*", на „*героическо единоборство на*

доброто срещу злото", на „*съзнателно самопожертвование*". Терористите от старата „*идеалистическа генерация*" най-старателно се грижат при актовете им да не се стига до случайна гибел или раняване на невинни хора, дори на животни и предмети, а ако се стига до такова, те се отдават на искрено мъчителни разкаяния. Самото „*право на убийство на тиранина*" при терористите от старата генерация е предмет на интензивно философско и етическо обсъждане и спорове, свързани с проявата на сложна душевна борба.

Бавно по бавно се проявява тенденцията за разширяване кръга на политическите фигури, считани за „*виновни пред народа*", върху които се разпростира принципът за „*непредотвратимото възмездие*". Екстремистката насока в анархизма дори е била стигнала до идеята за правомерността на изтреблението на всякакви „*експлоататори*" и „*представители на държавата*", включително и офицери, войници, жандармеристи, висши и дори нисши държавни служители. Тази екстремистка насока е продължена от съвременния екстремизъм, а обекти на покушенията вече са „*прислужниците на държавата*", проявяващи се като „*съучастници на тиранията на потребителското общество*", при което под „*съучастници*" са разбирани абсолютно всички, които не участват в откритата борба срещу режима, с произтичащите от това последици.

Осмата важна характеристика на политическия тероризъм е, че в съвременните условия се очертава съществуването на различни видове тероризъм в зависимост от неговото местопребиваване и цели. В т. нар. „*капиталистически метрополии*" доминира *„социалният тероризъм"*, а в държавите от „*Третия свят*" – „*националният тероризъм"*. Между двата вида тероризъм е възможно взаимодействие, основано върху „*общата ненавист към световния империализъм*" и привързаността към идеята за „*световна пролетарска революция"*. В идеологията на съвременните терористически групировки влизат преди всичко редица комунистически клишета и интензивни международни контакти – обмяна на информация, опит, оръжие, убежище, обучение, често пъти и провеждането на съвместни операции. По тази причина съвременният тероризъм е съвсем нетипична насилническа форма в сравнение със скоро съществуващите заговорнически и фанатически организации.

Съвременният тероризъм е изграден върху основата на прецизното вътрешно разделение на труда в рамките на лаборатории, скривалища, складове, типографски центрове, болници, доходоносни производствени предприятия, доходоносни модерни бизнес организации, както и върху основата на използването на специфичен военен опит, ефективно въоръжение, най-съвременен транспорт и радиовръзки, ограбване на банки и дори притежаването на собствени банки, и други.

За съществуването и засилването на тероризма в съвременната обстановка спомагат редица предпоставки от социален, национален, идеологически и психологически характер. Сред тях са крахът на комунистическата система и разпадането на нейната империя, стопанско-икономическата криза, рязкото спадане на жизнения статус на населението при едновременното увеличаване на слоя на богатите, масовата безработица и неустойчивостта на обществените отношения. Освен това, в продължение на дълги години (не само по време на комунистическата власт) в някои от бившите социалистически страни като Русия и България в масовото съзнание постоянно са се закрепвали традициите на проявлението на духа, на нетърпимост и зло, на безпрекословното подчиняване на личността, на волята, на държа-

вата или на толерираните от държавата институции, на придържането към безсмислени и безпощадни бунтове, заговори, кървави преврати, граждански войни и терористични прояви.

Всъщност, едва е възможно именно и само болшевиките да са заложили в Русия вкуса към държавния терор и опозиционния тероризъм.

Непосредствената история на възраждането на опозиционния тероризъм в Русия води началото си от войната в Афганистан, която събуди в общественото съзнание малко позабравената мисъл за естествения характер на противопоставящото насилие. Постепенно в земите от бившите съветски територии тероризмът поне външно, видимо започна да се вписва в параметрите, определени от класическите прояви на феномена – социален ляв и десен тероризъм, религиозен тероризъм.

Деветата важна характеристика на политическия тероризъм е очевидното противоречие между теорията и практиката. Така, известно е, че в теорията на т. нар. „*научен комунизъм*" се сочи тезата, че комунистическата партия отхвърля тероризма и превратите като форма на борба за власт и приема единствено „*масовото въоръжено въстание*" и „*революцията*".

Днешните форми на терористична борба на комунистите са много порафинирани. Във времето на планираното отстъпление от класическите комунистически позиции при условията на предоставената им възможност да създадат „*преходно законодателство*" и „*преходен политически механизъм*" към т. нар. „*посттоталитаризъм*" *главната ударна терористична вълна на комунистите са криминалните престъпници и формиращите се мафии*. За това е създаден специален правен механизъм, при който се осъществява пълен хаос в правосъдната система и интензивно стимулиране на всички форми и средства за криминален удар върху обществените структури и ценности, разширяват се сферите на конфликтите между всички. Особено се стимулират криминогенните фактори в отделните етнически формации (ромите, изостаналите слоеве на турското население), в отделните възрастови групи (непълнолетни, младежи, пенсионери).

Извод:

Целта на политическия тероризъм в наши дни вече *не е толкова в отстраняването на най-влиятелните личности от сцената на официалния политически живот*, а е *в търсенето на обществен резонанс*.

Тероризмът днес е вид насилие, разчитащо на масово възприятие, на изплашване на обществеността. Основните търсени ефекти са заплахата и страхът– да се изгради в обществото представа за всемогъществото на терористите, за беззащитността на всеки и за безсилието на властите пред терористите. От тази гледна точка става оправдано провеждането на „*безадресни терористични актове*", целта, на които е една единствена– постигането на страх и добиване на широка самореклама чрез средствата за масова информация.

Използвана литература

1. Проф. Янков Я. Кутията на Пандора (Една калейдоскопичнията на визия върху тероризма). - София, "Янус", 2007.
2. *Стоянов, Георги Ст.*. Тероризмът. - *България, Военно издателство, 2003.*
3. http://terorizam.start.bg/

ЗАПЛАХИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА В ЕЛЕКТРОЕНЕРГИЙНИЯ СЕКТОР И ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Здравко Ю. Кузманов

THREATS TO CRITICAL INFRASTRUCTURE IN THE ELECTRICITY SECTOR AND INFORMATION AND COMMUNICATION TECHNOLOGY

Zdravko Y. Kuzmanov

ABSTRACT: *The report presents the issues related to structure and threats of critical infrastructure at the electricity sector. There are three main issues enclosed. What is the structure of the energy infrastructure of the country, its place and its ties with energy grinds of countries from the European Community? What is the electricity information and communication technology interface? What has been done by now about protection of the critical infrastructure and cyber security in the European Union?*

KEY WORDS: *Critical infrastructure, Electricity, Information and communication technology, Cyber security.*

Сигурността, икономиката и благосъстоянието на държавата и нейните граждани, зависи от управлението и работата на определени инфраструктури и услуги. Унищожаването или нарушаването на тяхната работа, би могло да доведе до загуба на човешки живот, собственост, срив на общественото доверие и морал в държавата. Такъв тип обекти се определят като критична инфраструктура (КИ) на държавата. Тяхната специфика и значение изисква непрекъснато да се изследват заплахите и последствията от възможни въздействия или манипулации за да се сведат до минимум възможните загуби, да бъдат управляеми, географски изолирани и с минимални последствия за държавата и нейните граждани. Терористични атаки в Мадрид (2004 г.), Лондон (2005 г.), кибер атаките в Естония (2007 г.) и прекъсванията на електрозахранването в Германия (2006 г.) показаха потенциалната уязвимост на обекти от инфраструктурата, както от тероризма, така и от оперативни повреди.

Законодателството на Република България определя „критичната инфраструктура", като система от съоръжения, услуги и информационни системи, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху здравето и безопасността на населението, околната среда, националното стопанство или върху ефективното функциониране на държавното управление [1]. Паралелно с това определение в българското законодателство се използват още 4 термина,[1] които частично или напълно се припокриват с понятието „критична инфраструктура".

В контекста на пълноправното членството на страната в Европейския съюз

[1] Потенциално опасен обект и потенциално опасна дейност; Стратегически обекти и дейности; Национално стопанство; Техническа инфраструктура.

(ЕС) следва да се отбележи и термина „европейска критична инфраструктура" (ЕКИ), който означава критична инфраструктура, разположена на територията на Република България, чието повреждане или разрушаване би оказало съществено негативно влияние върху поне още една държава-членка на ЕС. Значимостта на това негативно въздействие се оценява чрез взаимносвързани критерии, които включват последствия, загуби или щети, произтичащи от между секторни зависимости, свързани с безопасността и сигурността на инфраструктурата на енергетиката, на транспорта или на други видове инфраструктура.[2]

Европейската комисия (ЕК) определя „критичната инфраструктура", както актив, система или част от нея, разположена в държава-членка, която е от съществено значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на хората, чието повреждане или разрушаване би оказало съществено негативно въздействие върху дадена държава - членка в резултат на отказ на тези функции. В допълнение - „европейска критична инфраструктура", означава критични инфраструктури, разположени в държавите-членки, чието повреждане или разрушаване би оказало съществено влияние върху най-малко две държави-членки.[3]

Изхождайки от изложеното до тук целата на доклада е да се изследват въпросите свързани със структурата и заплахите на критичната инфраструктура в електроенергийния сектор.

Първият въпрос, който следва да се постави е каква е структурата на енергийната инфрастуктура на страната, какво е нейното място и какви са нейните връзки с енергийните мрежи на държавите от Европейската общност.

Държавата е силно зависима от постоянен достъп до устойчиви, конкурентни и сигурни източници на енергия. Всяко прекъсване на енергийните доставки може да окаже значително влияние върху здравето, безопасността, сигурността и икономическото благосъстояние на гражданите.

Ясно е, че от всички сектори в енергетиката, всякакви смущения в електроенергийната система[2] (ЕЕС) ще засегнат най-бързо и с широко въздействие много други сектори, като: транспорт (светофарна система, железопътни сигнализиращи системи); водоснабдяване и канализация (генериращи помпи, пречиствателни станции); финансовата и банкова системи (невъзможност за извършване на ежедневни финансови операции без съвременни комуникационни средства. Показателен пример в това отношение е колумбийската фондова борса, която прекрати дейността си по време на прекъсване на електроснабдяването през април 2007 г. Друг случай със значителни последствия са събитията в Германия през 2006 година, когато прекъсване на електроснабдяването доведе до спране на железопътния транспорт. Без електрическо захранване останаха не само влаковете, но и системите за сигнализация и комуникация. Това събитие също така илюстрира взаимозависимостта и взаимосвързания характер на националните ЕЕС. По вина на една страна, са засег-

[2] Всички електроенергийни обекти на територията на страната се свързват и функционират в единна електроенергийна система с общ режим на работа и непрекъснат процес на производство, преобразуване, пренос и разпределение и потребление на електрическа енергия. Електроенергийната система обхваща електрическите централи, преносната мрежа, отделните разпределителни мрежи и електрическите уредби на потребителите. (Виж Закон за енергетиката. Глава девета. Раздел I.)

нати 15 милиона домакинства в Европа, главно в Италия, Испания и Австрия.

Няколко са големите предизвикателства засягат ЕЕС на страната в момента:

- увеличаването на потреблението. След 2004 г. в страната се установи постоянна тенденция на нарастване на годишното потребление на електроенергия. Общо потребление на електроенергия в България възлиза на 37.4 TWh през 2009 г. Същата година, прогнозата за развитие на брутното електропотребление в страната е актуализирана предвид възникналата световна икономическа и финансова криза. Въпреки това се запазва прогнозната тенденция за увеличаване на брутното потребление – 42.1 TWh през 2020 г., макар и по-консервативно и доближаване до средните стойности на този показател за ЕС.[4]

- повишаване на изискванията към управлението на една все по-сложна система, част от ЕЕС на ЕС;

- стареенето на енергийната инфраструктура изисква съществени инвестиции. Една последица от това е, че старото оборудване е изградено на електромеханични основи, които са по-малко податливи на кибер атака. Подмяната с ново, базирано на съвременна цифрова техника за контрол, носи множество позитиви, но и нови рискове и предизвикателства произтичащи от характера на този тип техника;

- екологичните съображения;

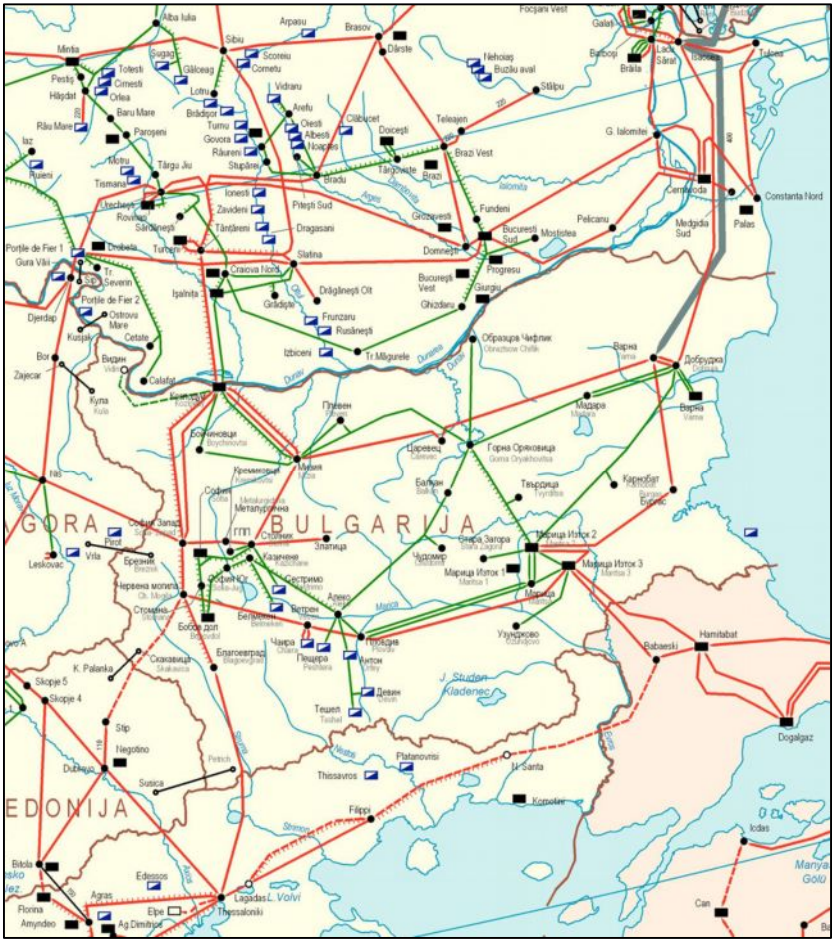
- риска от съвременния тероризъм.

Тези предизвикателства обобщава контекста, в който физически електроенергийната инфраструктура е разработена и се управлява.

Мрежата на ЕЕС, както и междусистемните връзки са илюстрирани на фигура 1 и фигура 2.

Съюзът за координация на преноса на електроенергия UCTE (сега Европейска мрежа от оператори на преносни системи за електроенергия – *European Network of Transmission System Operators for Electricity* (ENTSO-E)) координира синхронно сложна система свързваща 24 страни в континентална Европа, в това число и ЕЕС на Република България. Националните системи на операторите са свързани в паралелна работа, с еднаква честота. Това създава предпоставки, смущения в ЕЕС на една държава-членка да се отрази върху цялата европейска система по ефекта на доминото. Ето защо, е необходимо въпросите свързани с критичната инфраструктура в електроенергийния сектор да се разглеждат, както от национална гледна точка, така и в контекста на членството на страната в ЕС.

Фигура 1. Електропреносна система на Република България.
[Източник: ЕСО, http://www.eso.bg/default.aspx/mrezha-na-ees/bg]



Фигура 2. Междусистемни връзки на българската ЕЕС.
[Източник: ЕСО, http://www.eso.bg/default.aspx/mrezha-na-ees/bg]

ЕЕС е зависима от богатството на отделните мрежи и инфраструктури за генериране, пренос и разпределение на електричество. Всяка от тези мрежи и инфраструктури са от решаващо значение за поддържане доставките на електроенергия за задоволяване на нуждите на страната.

Електроенергетиката е най-критична подсистема от цялостната енергийна система на страната, защото нейното оперативно управление, контрол и координиране на режимите на ЕЕС се осъществяват в реално време. Смущенията могат да се разпространяват за секунди, а последствията от спиране на тока често са тежки.

Към електроенергийната критична инфраструктура могат да се отнесат следни-

те елементи, които да се групират в две големи групи:

а) физическа инфраструктура, която включва:

- генераторни мощнисти;
- подстанции;
- трансформатори;
- електропроводи;
- диспечерски центрове;
- офис сгради.

б) виртуална архитектура, която включва:

- SCADA системи;
- мрежа;
- бази данни;
- бизнес системи;
- телекомуникации.

Важно е да се отчете факта, че ЕЕС на страната е конфигурирана с отчитане на търговските цели на енергийните дружества. Това се отнася до физическата инфраструктура и виртуалната архитектура, както и процесите и процедурите. Възможността за прекъсване обикновено се разглежда от гледна точка на техническа неизправност, а не толкова като умишлено нападение. Възможно е еднократна повреда/авария да бъде изолирана, без да наруши нормалната работа на системата. В електроенергетиката, една преднамерена атака срещу системите за оперативен контрол, базирани на съвременните информационни и комуникационни технологии (ИКТ), може да доведе до нестабилност или срив на системно ниво.

Освен създаването на устойчива ЕЕС, която да се отчита на етап проектиране, от съществена важност е и защита на отделните критични елементи, които я съставляват. Това предполага поставянето на акцент върху въпроси като:

- планиране на стандарти;
- комуникация и обмен на данни между операторите на преносни системи;
- аварийно планиране;
- обучение – с транснационално измерение;
- координация и ръководство.

Както в много други сектори и в електроенергетиката елементи на критичната инфраструктура се притежават и експлоатират, както от държавата, така и от частни организации. Това поставя нарастващо изискване за разбиране от страна на бизнеса, с цел да се гарантира внедряването на подходящи правила и механизми, които да гарантират сигурността на критичната инфраструктура в сектора.

Вторият въпрос е какъв е електроенергийния информационно-комуникационен интерфейс.

Както електроенергетиката, така и ИКТ са идентифицирани като критична инфраструктура от страна на Европейската програма за защита на критичната инфраструктура (*European Programme for Critical Infrastructure Protection* - EPCIP). В съвременните системи е на лице корелация между ИКТ, която може да предизвика каскадни ефекти, върху две и повече системи. Заимозависимостта между физическите и виртуални структури, при липса на адекватна защита води до негативни взаимни последици.

Функционалното предназначение на ЕЕС, определят необходимостта от специализирана информационна среда за реализация и то в задължителните, за всяка една

такава система, условия на изключително високи критерии за безотказна работа.

В електроенергийния сектор, ИКТ е от решаващо значение за:

- управление на ЕЕС - всекидневно осигуряване на оперативност и гъвкавост в реално време;

- регулиране пазара на електроенергия - контрол на енергопотреблението, разпределение, управление и търговията с електроенергия;

- поддръжка на електропреносната мрежа;

- интеграция с европейската ЕЕС.

Системите за контрол и събиране на данни (*Stands for Supervisory Control and Data Acquisition* - SCADA), са ключов фактор за безопасността и сигурното функциониране както на физическата инфраструктура така и на виртуалната архитектура. SCADA е диспечерската система, която събира и натрупва данни за един процес и изпраща управляващи команди за процеса.

Към SCADA обикновено се отнасят централизирани системи следящи и управляващи изцяло състоянията на съоръженията, както и за комплекси разположени върху големи площи. Повечето управляващи действия се извършват в автоматичен режим от програмируеми логически контролери (*Programmable Logic Controllers* или *PLCs*) или от отдалечени терминали (*Remote Terminal Units* или *RTUs*), предаващи телеметрични данни към системата и/или променящи състоянието на обектите на основата на управляващи съобщения получени от системата.[5]

Тези системи са част от Системата за управление в реално време, например за пренос и разпределение на електроенергия. SCADA системите предлагат модерни решения за интелигентно управление на ЕЕС, с дълготраен положителен ефект, като възможността за контрол на множество процеси, намаляване на пътуванията на място и др. Въпреки това, ползите от една точка на контрол и широкото използване на мрежи означава също, че ако тези системи бъдат подложени на злонамерени атаки могат да причинят големи щети с бързо и широко разпространение.

Четири са основните ключови заплахи за SCADA системите, а именно:

- malware - например червеи, вируси, троянски коне и шпионски софтуер;

- вътрешна „атака" - случайно или преднамерено от служител;

- хакери - външна атака, която може да доведе до срив на системата;

- кибер тероризма - може да предизвика голям диапазон щети, които да се отразят върху голяма част от населението.

Системите базирани на съвременните ИКТ могат да функционират неправилно в следствие на няколко причини - като човешка грешка, хардуерни и софтуерни откази и преднамерена атака. Преднамерената атака може да бъде целенасочена към определен сектор или организация, или да въздейства върху сектора чрез безцелни заплахи като вируси.

За критичната инфраструктура на равнището на ЕС в електроенергийния сектор, съществуват следните тенденции:

- броят на кибер атаките значително се е увеличил през последното десетилетие;

- все по-често тези атаки произхождат от външни източници;

- има значителни различия в информираността и готовността на държавите-членки относно заплахите, а кибер атаката може да има много сериозно отражение върху електроенергийния сектор, в частност.

Третият въпрос е какви са заплахите и какво е направено до този момент по защитата на критичната инфраструктура и киберсигурността в Евро-

пейския съюз.

Европейската инициатива за надеждност (*European Dependability Initiative* - EDI) е публикувана през 1998-1999 г. и представлява серия от изследвания, чрез които Европейския съюз цели да отговори на въпросите свързани със защитата на критичната инфраструктура, като са включени планове за съвместно сътрудничество между ЕС и САЩ в тази област. EDI признава все по-нарастващата зависимост на съвременното общество от информацията чрез софтуерно базирани системи за контрол, комуникационни приложения и услуги. Също така се отбелязва, че широкоспектърния характер на новите технологии е основата на нови типове проблеми и предизвикателства за надеждност на технологиите [EDI, 1998].

След EDI, ЕС поставя началото на Инициатива за надеждност и подпомагане на развитието (*Dependability Development Support Initiative* - DDSI). Тя е проведена в периода юни 2001 г., а от ноември 2002 година. DDSI, признава нарастващата зависимост на широк кръг европейски инфраструктури, в това число производството на електроенергия, от мрежовите информационни системи. Това води до уязвимост на критичните инфраструктури и социалните процеси от случайни или злонамерени повреди на информационните системи и мрежи. Тази инициатива също признава необходимостта от разработването на общи политически инициативи на европейско ниво, за защита на гражданите, подкрепа за бизнеса и сигурност на критичните инфраструктури. [DDSI, 2007] DDSI (2002) отбелязва, че *защита на критичната инфраструктура продължава да бъде отговорност на всяка държава-членка.* Въпреки това, нарастващите компетенциите на европейските институции по отношение на сигурността и външната политика, както и разширяването на „европейското семейство" водят до разбирането, че е необходимо засиленото и широко сътрудничество при управлението на рисковете за взаимозависими инфраструктури. [DDSI, 2002]

Европейската комисия постави началото на програма за защита на критичната инфраструктура (*European Programme for Critical Infrastructure Protection* - EPCIP) през 2004 г., с публикуването на съобщение, озаглавено „Защита на критичната инфраструктура в борбата срещу тероризма". Сред работата по програмата е разработката на „Зелена книга на Европейска програма за защита на критичната инфраструктура" (COM (2005) 576 окончателен), издадена през 2005 г. и доразвита през 2006 г. Обявената цел на EPCIP е подобряване защитата на критичната инфраструктура в ЕС. За постигането на тази цел се предвижда прилагането на:

- процедура за определяне на Европейската критична инфраструктура и общ подход за оценка необходимостта от подобряване на защитата;
- мерките, предназначени да улеснят прилагането на EPCIP, включително план за действие, предупредителна информационна мрежа на критичната инфраструктура (*Critical Infrastructure Warning Information Network* - CIWIN), създаване на защита на критичната инфраструктура (*Critical Infrastructure Protection* - CIP), създаване на експертни групи на ниво ЕС, внедряване на процеси за обмен на информация, както и идентификационен анализ на зависимостите;
- подкрепа за държавите - членки по отношение защитата на националните критични инфраструктури (*National Critical Infrastructures* - NCIs), които могат по желание да бъде използвани от дадена държава-членка;
- планиране при извънредни ситуации;
- съпътстващи финансови мерки, и в частност специална програма на ЕС от-

носно „Предотвратяване, готовност и управление на последиците от тероризъм и други рискове за сигурността" за периода 2007 - 2013 г., която финансира възможности за ЗКИ и свързаните с това мерки. [Генерална дирекция „Правосъдие, свобода и сигурност", 2009 [6]

През декември 2008 г., Съветът на Европейския съюз прие Директива относно определяне и обозначаване на ЕКИ и оценка необходимостта от подобряване на тяхната защита.

Директивата установява обща процедура за определянето и обозначаването на европейските критични инфраструктури и въвежда общ подход за оценка на нуждите от подобряване на защитата им. Тази оценка подпомага подготовката на специфични мерки за защита в отделните сектори.

- критерий на *пострадалите* (оценява се потенциалният брой на загиналите или ранените);

- критерий на *икономическите последици* (оценява се значимостта на икономическите загуби и/или влошеното качество на продуктите или услугите, включително възможните последици за околната среда);

- критерий на *обществените последици* (оценяват се последиците за общественото доверие, физическото страдание и нарушаването на ежедневния живот, включително загубата на основни услуги).[3]

Оценката на изискванията за сигурносттта на подобни инфраструктури следва да се извършва в рамките на *общ минимален подход.* Защита на ЕКИ следва да се основава на двустранни механизми за сътрудничество между държавите-членки в областта на ЗКИ, която представлява утвърдено и ефикасно средство за защита на трансгранична критична инфраструктура. [Съвет на ЕС, 2008]

Като такъв по силата на директивата, всяка държава-членка е длъжна да прецени дали определената, като ЕКИ, разположена на нейната територия притежава ***Оперативен план за безопасност*** (*Operator Security Plan* - OSP), или еквивалентни мерки разглеждащи въпроса за сигурността. OSP или еквивалентните мерки съдържащи идентификация на активите, оценката на риска и установяването, подбора и приоритизирането на превантивните мерки и процедури, трябва да са налице във всички определени ЕКИ. Когато такива планове не съществуват, всяка държава-членка следва да предприеме необходимите стъпки, за да се гарантира, че необходимите мерки са въведени в действие. Всяка държава-членка, взима *самостоятелно решение* относно най-подходящата форма на действие по отношение на установяването на OSP.

В изпълнение на Директивата, Министерски съвет издаде Постановление № 18 от 1 февруари 2011 г., с което се уреждат процедурата за установяването и означаването на европейски критични инфраструктури, разположени на територията на Република България, и мерките за тяхната защита в секторите енергетика и транспорт. За установяването на потенциални ЕКИ се прилагат междусекторните и секторните критерии, определени с Директивата на Съвета.[2]

На 27 октомври 2008 г. Европейската комисия представи предложение за решение до Съвета на ЕС, относно създаване на Предупредителна информационна мрежа за критичната инфраструктура (*Critical Infrastructure Warning Information Network* - CIWIN), която има за цел да предостави на държавите-членки защитена комуникационно информационна система за бързо предупреждение и обмен на информация, свързана със ЗКИ. Системата ще улеснява сътрудничеството между

държавите-членки, чрез осигуряване обмена на информация относно заплахите и уязвимостите, както и стратегиите за подобряване на ЗКИ. CIWIN се състои в следните две функции:

- електронен форум за обмен на информация, свързана със ЗКИ;

- функция за бърза тревога, която ще предостави възможност на участващите държави-членки и на ЕК да да изпращат сигнали за тревога относно непосредствените рискове и заплахи за критичната инфраструктура.[7]

Продължава работата на комисията по разработването на Европейска политика за киберсигурност. Като признание за важността на ИКТ като цяло, Съветът на Европейския съюз прие Рамково решение 2005/222/ ПВР от 24 февруари 2005, атаки срещу информационните системи, което посочва четири вида дейности, идентифицирани от държавите-членки, като криминални до 16 март 2007 г.:

- *неправомерен достъп до информационни системи* - всеки умишлен неправомерен достъп до цялата информационна система или до части от нея;

- *неправомерна намеса в системата* - всяко умишлено спиране или възпрепятстване на функционирането на информационната система чрез неправомерно въвеждане, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни;

- *неправомерна намеса в данни* - всяко умишлено изтриване, увреждане, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни в дадена информационна система;

- *подбудителство, подпомагане, съдействие и опит за извършване на престъпление* - подбудителството, подпомагането и съдействието за извършване на престъпленията, посочени в предходните три вида дейности.[8]

Съобщението на Европейската комисията относно борбата срещу престъпленията в кибернетичното пространство (SEC 2007/641, 642, Брюксел, 22.05.2007) определи подхода на ЕС в борбата му срещу престъпленията в кибер пространство.

В съобщението се посочва, че броят на престъпленията в кибер пространство нараства и престъпните дейности стават все по-сложни излизайки извън границите, често организирани от престъпни групи. Въпреки това, броят на европейските съдебни преследвания, въз основа на трансграничното сътрудничество в правоприлагането не се увеличава. [ЕК, 2007 г.]

За да се справи със заплахите, произтичащи от престъпленията в кибер пространство, ЕК обявяви за основна политика подобряването на европейското и международно ниво на координация в борбата срещу този вид престъпления. Целта на тази политика е да се засили противодействието на национално, европейско и международно ниво. По-нататъшно развитие на конкретна политика е признато като приоритет от държавите-членки и Комисията.

Акцентът на инициативата е поставен върху правоприлагането наказателноправните аспекти на тези мерки. Политиката в крайна сметка включва следните компоненти:

- подобряване на оперативното съдебно сътрудничество;

по-добро политическо сътрудничество и координация между държавите-членки;

- политическо и правно сътрудничество с трети страни;

- повишаване на осведомеността, обучението и научните изследвания. [ЕК, 2007 г.]

През март 2009 г.[9] ЕК съобщи намерението си да защити Европа от кибер атаки и смущения (Защита на критичната информационна инфраструктура - нова инициатива, 2009 г.). Комисията призова за действия относно защитата на критичните информационни инфраструктури, което да ги направи по-подготвени и устойчиви на кибер атаки и смущения. Заедно с това се признава, че ниското ниво на подготвеност в една страна може да се отрази на останалите, а липсата на координация намалява ефективността на мерките за противодействие.

Анализът на законовата и нормативна база на страната показва, че са нужни промени насочени към подобряване на законодателството по отношение на инкриминирането на кибер престъпленията в Наказателния кодекс, полагане на повече усилия за борбата с тези *„нови"* престъпления от държавните структури и реално прилагане на конвенцията на Съвета на Европа от 2001 г. (и допълнителните протоколи), които са ратифицирани от страната.

Експлоатацията на електроенергийните системи е силно зависима от ИКТ за всекидневното производството, пренос, разпределение на електроенергия и спешната намеса в случай на прекъсване. Защитата на критичната електроенергийна инфраструктура и ИКТ, изисква разбиране на всички уязвимости и елементи, които са от значение за надеждната и непрекъсната работа. В много случаи, зависимостите и уязвимостите излизат извън държавните граници. Някои национални правителства имат въведени адекватни политики за защита на критичната си електроенергийна инфраструктура и ИКТ, но много други нямат.

Системата за защита на критичната инфраструктура на Република България се развива главно под влиянието на ЕС чрез дефинираните от съюза политики, програми и мерки. Това е така, защото опазването на критичната инфраструктура на страната и в частност електроенергийната се превръща във важен въпрос не само за нашата сигурност и енергийна стабилност, но и в рамките на общноста.

ЕС постигна значителен напредък при идентифициране на зависимостите, уязвимите места и мерките за защита, както в електроенергетиката, така и в сектора на ИКТ, чрез създаването на оперативни стандарти за сигурност, изследователски програми и мрежи за споделяне на информация.

Въпреки това, процеса засега остава на ниво *„идентифициране и определяне"*, докато ясна структура за управление липсва. Подходът към настоящия момент е в много направления и потенциално неизчерпателен. Ефективната защита зависи от комуникацията, координацията и кооперирането на национално ниво. Именно в това направление е необходимо да бъдат насочени усилията, като се отчитат следните основни изводи:

- в началото на XXI в. националната КИ, включително електропреносната мрежа, електроцентралите и другите електроенергийни инфраструктури, почти изцяло зависят от широко разпространени и функционално съвместими софтуерни системи. Повишаването на ефективността изостря чувствителността на тези инфраструктури към кибер атаки;

- електроснабдяването е в основата на всички ИКТ и предоставяните чрез тях услуги. Прекъсване на електрозахранването могат да причинят големи смушения на критичните ИКТ с каскадни ефекти в други сектори на икономиката и обществения живот;

- веригата от зависимости водят до непредвидени последици и пулсации, когато прекъсване на една инфраструктура се превръща в източник на смущения за други

инфраструктури. Прилагането на ефективни мерки за подготовка при извънредни ситуации е от решаващо значение за справяне с възможните каскадни ефекти;

- експлоатацията на съвременните информационни системи освен множеството позитиви, води и до проблеми със сигурността, които могат да имат значително въздействие върху устойчивостта и надеждността на критичните инфраструктури, независимо от това дали поддържащите системи са централизирани, самостоятелни или вградени. Уязвимостта на компютърните мрежи не води непременно до пропорционална уязвимост и на критичните инфраструктури;

- автоматичните системи за защита са предназначени да гарантират стабилността на ЕЕС, свеждайки до минимум вероятността техническа повреда или умишлена атака да доведе до нестабилност на системно ниво, но са уязвими откъм случайно или умишлено вмешателство;

- контролът на процесите и SCADA системите стават все по-зависими от съвременните ИТ технологии, което повишава уязвимостта на електроенергийната критична инфраструктура към кибер атаки, въпреки увеличаващия се брой на стандарти, добри практики и наличието на технологии за сигурност;

- броят на точките за достъп се увеличава в резултат на въвеждането на интелигентни електронни устройства, сензори, измервателни уреди, както и интеграцията между оперативните и корпоративни бизнес мрежи за обмен на данни са източници на повишена уязвимост;

- увеличаване на нивото на риска за критичната инфраструктура може да се получи от неоторизирани действия на лижа и организации, които имат за цел достъп до информация, която да бъде използвана за атаки от по-голям мащаб.

- при оценка на риска не бива да се подценява заплахата от вътрешен саботаж от служители, които имат достъп до информационно-комуникационните системи;

- за кибер атаки могат да се използват голямо разнообразие от инструменти, които се използват за атака на ИТ системите;

- съвременните дейности за ЗКИ, не бива да включват само политики и практики за защита на физическата инфраструктура, а и такива осигуряващи сигурността на информационно-комуникационните и управляващи системи в електроенергетиката, които да се предвиждат и усъвършенстват през целия жизнен цикъл на системите.

Това са някои от обобщенията по отношение на структурата на критичната инфраструктура от електроенергийния сектор на станата и основните заплахи за него. За пълното изясняване и оценка на рисковете следва да се проведат отделни изследвания.

Използвана литература

1. Закон за отбраната и въоръжените сили. Допълнителни разпоредби § 1 т. 18. Обн. ДВ. бр.16 от 26 Февруари 2010г.

2. Постановление на МС № 18 от 1 февруари 2011 г., За установяването и означаването на европейски критични инфраструктури в Република България и мерки за тяхната защита. Обн. ДВ. бр.11 от 4 Февруари 2011г.

3. Директива 2008/114/ЕО на Съвета от 8 декември 2008 г., Относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита. Текст от значение за ЕИП. Официален вестник n° L 345, 23/12/2008 стр. 0075 – 0082.

4. НЕК. (Годишен доклад, 2009), http://www.nek.bg/cgi.
5. Интелигентно диспечерско управление на енергийните мощности – съвременни тенденции, Сгурев В., Койнов Ст., Институт по информационни технологии-БАН.
6. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en..htm.
7. Законодателна резолюция на Европейския парламент от 22 април 2009 г., Относно предложението за решение на Съвета относно Предупредителна информационна мрежа за критичната инфраструктура (CIWIN) (COM (2008) 0676 – C6-0399/2008 – 2008/0200(CNS)). Официален вестник n C 184 E, 08/07/2010 стр. 0174 – 0180.
8. Рамково Решение 2005/222/ПВР на Съвета от 24 февруари 2005 година. Официален вестник n L 069, 16/03/2005 стр. 0067 – 0071.
9. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, Март 2009 г.

УПРАВЛЕНИЕ НА ПРОЕКТ ЗА ИЗГРАЖДАНЕ НА СИСТЕМА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Живко Ив. Сивов
Гр. София, ВА „Г. С. Раковски", Катедра „КИС", Тел: 029226599

PROJECT MANAGEMENT OF INFORMATION SECURITY SYSTEM DESIGN

Zhivko Iv. Sivov

ABSTRACT: The paper is aimed at presenting an option for designing an information security system, based on methods and tools needed for a successful project leading to the rational utilization of time and resources.

KEY WORDS: information, security, project management.

УВОД

„Колкото повече държавата „планира", толкова по-трудно става планирането от страна на отделния човек."
ФРИДРИХ ФОН ХАЙЕК[18]

В динамично променяща се среда за сигурност и при поети ангажименти от страна на Република България, по изпълнение на съюзни и коалиционни договори и споразумения за осигуряване на колективната отбрана, се изисква граждане на адекватни способности. В този аспект е и **целта на доклада в сбита форма да систематизира *теоретичен подход* за управление на проект, чиято същност е**

[18] Австрийски икономист и политически философ в средата на 20 век.

изграждане на системата за информационната сигурност (СИСг) и да изведе една рационална дейност, способстваща процеса за постигане на необходими възможности и способности на информационните системи, адекватни на средата, в която функционират.

България не е в състояние сама да опазва своята сигурност или да се стреми към сигурност чрез неутралитет поради недостатъчния си финансов, икономически и военен потенциал. Новите реалности предпоставят необходимостта да се приобщим към ефективните колективни системи за сигурност. Акцента се премества към надеждността на информационната среда, към сигурността и защитеността на информационните системи (ИС). Налага се трансформация на разбирането за придобиване, владеене и използване на информацията в контекста на информационния мениджмънт и развитието му като част от сектора за сигурност.

Управлението на процесите на всички нива в глобализиращия се свят все повече се основава на нови начини за обработка на информацията, на прилагането на нови информационни технологии и на внедряването на нови комуникационни канали, немислими до преди едно десетилетия.

Съвременните тенденции се изразяват в преминаването от отделни подсистеми и задачи, към обща единна система на организиране и управление.

Същевременно съсредоточаването на информацията в обща система, предоставя възможност на управленските органи да анализират същността на процесите и явленията и на тази основа да изработват и вземат обосновани решения. Допълнително, ускореното внедряване на информационните технологии води до засилваща се зависимост от тях и до разширяване на възможностите за употреба на информационните средства за нанасяна на вреда на всяка една държава, организация или фирма.

Разработване на адекватна на времето СИСг и нейното внедряване и използване от органите и организациите отговорни за националната сигурност, води до помалък разход на ресурси и съкращаване на сроковете за постигане на целите, изпълнение на задачите, ефикасност и ефективност на ИС.

Ограничаването на ресурсите за изграждане на СИСг в контекста на съвременните изисквания за сигурност, налага трансформация на разбирането за информационна сигурност от институционално базирана и фокусирана, към стратегия, насочена към сигурност чрез превенция, интеграция и съвместимост на национално ниво, както и в необходимата степен на компетентност със съюзниците в политически, икономически и военен смисъл. В този аспект се очертават основни тенденции, които следва да се отчитат при проектирането на СИСг:

- **Разширяване на обхват на СИСг;**
- **Редуциране на управленските нива за вземана на решение;**
- **Фокусиране към мениджърското ниво.**

С **разширяване на обхват на СИСг** се постулира разбирането, че политиката за сигурност се насочва освен към защита на неотменните държавни, национални, политически, икономически и персонални интереси, но и към защита на съюзническите мултиплицирани интереси като в процеса на глобализация, обхвата на тези интереси непрекъснато се разширява.

Реалността днес е, че нито един вид заплаха за националната сигурност не може да бъде отразена без надеждна ИС. Този извод предполага край на делението на традиционните сфери за изграждане на ИСг само за „политически цели", само за

„военни цели", само за „икономически цели" и т.н.

Редуциране на управленските нива за вземана на решение е породено от възможностите на информационните технологии и порасналите оперативни възможности на системите въобще като вземането на решение и последващите действия, налагат съвместимост на системите, както в и между висшите ешелони на управление, така същото и на съюзническо ниво.

Изменящата се геостратегическа среда за сигурност, обусловена от нововъзникващи центрове на нестабилност и модерни информационни средства за въздействие, методи и технологии за нанасяне на щети и вреди, определят цели и задачи на СИСг, преместващи **фокуса от висшите ръководни нива към мениджърските равнища**.

1. УПРАВЛЕНИЕ НА ПРОЕКТ

Управлението е целенасочено въздействие върху някакъв обект, съобразено с обективните условия и възможности, за постигане на определени цели.

Основни елементите на управление са:

- Анализ на ситуацията и определяне на целите (целе полагане, уточняване на целите);
- Планиране на ресурси и действия за постигане на целите;
- Създаване на организация за реализиране на плана;
- Контрол на организирания процес на управление (събиране на информация за изпълнението, анализ на постигнатото, управленско въздействие за постигане на целите).

Управлението се състои основно от две групи дейности.

Към първата група се отнасят повтарящи се дейности, свързани с функционалното предназначение на организацията. Тук имаме множество повтарящи се управленски цикли, които могат да протичат за седмица, месец, тримесечие или година. Например доставките на офис консумативи за нуждите на дадено поделение от БА. Дейността се планира за месец или година и след, като веднъж е организирана по същество, тя циклично се повтаря.

Втората група дейности са уникални по своя характер, като резултата е нов продукт или услуга. Те се извършват в точно определени период от време т.е. имат начало и край, и разчетен във времето на ресурс от хора, материали, финанси и др. Става дума за **проекти и управление на проекти**.

Формалната дефиниция за проект е уникално и ограничено във времето начинание. Проектът е временно и еднократно начинание, с цел създаване на **уникален продукт или услуга**, носещи благоприятна промяна или добавена стойност за фирмата/организацията или обществото.

Все повече дейности на фирмите и организациите се управляват като проекти. Управлението на проекти, се е доказало в области като инженеринга, строителството, развойната дейност, консултиране и др. и се е превърнало в задължителна рамка на управление и в сектори, като отбраната, където доскоро подобен подход беше несвойствен.

Възможностите на този метод осигуряват контрол върху ресурсите, финансите, информацията, задачите, качеството и риска. Неговата ефикасност и ефективност налага много държави в света да въведат законови изисквания, свързвани със спаз-

ването на стандарти и на прилагането на утвърдени методологии за управление на проекти.

Управлението на проекти е организиране и управление на ресурси, по начин, осигуряващ завършването на проекта в рамките на предварително дефинирани граници за обем, качество, време и цена.

Управление на проекти е науката за проектите. Цялостната наука за управление на проекти се развиват от различни организации по света като най-известната е Института за управление на проекти[19], базирана в САЩ и с клонове в цял свят с периодично издавана книга в сферата на управлението на проекти[20] - PMBOK Guide.

В Европа е създадена Международната асоциация по управление на проекти[21]. В Европа е популярна методологията PRINCE 2, създадена и поддържана от правителството на Великобритания. Япония - P2M, Германия - V-Modell и Швейцария - HERMES са изработили свои методологии, специфични за техните нужди.

Определено можем да кажем, че не може да има управление на ресурсите само заради самите ресурси Те винаги са съществена част от по-голяма дейност, начинание или проект. От двете групи дейности по управлението, разгледани по горе, интерес представлява реализацията на СИСг като част от проект или самостоятелен проект. Тогава определено осигуряването на дадено поделение от БА, например като рутинна и повтаряща се дейност, стои след въпроса трябва ли това поделение да съществува и ако „да" с какво, колко и как то допринася за сигурността на обществото.

Разглеждайки управлението на проектите или програмите за отбрана, винаги ще изхождаме от положението, че те подпомагат процеса за достигане на целите на отбраната и осигуряват изграждането на способности за отбрана. От тази позиция изградената СИСг като част от подготовката на обществото за отбрана и изграждането на неговите способности за противодействие на агресия, можем да приемем като проект или група от проекти – програми.

Защо именно проект и управление на проект?

Проучване на KPMG[22] проведено в САЩ и Канада показва следните данни от практиката:

- 87 % от задачите надхвърлят времето за изпълнение с 1/3 или повече;
- 56 % от задачите надхвърлят бюджета си с 1/3 или повече;
- 45 % от задачите приключват с резултат, който се отклонява значително от това, което е предвидено в заданието.

Според друга статистиката в една средно голяма европейска организация:

- Около 80% от всички проекти се провалят;
- Изпълнените проектите, излизат извън бюджет си с около 50%, а други 50% излизат извън сроковете;
- Около 90% от хората работещи по проекти работят извънредно.

[19] Project Management Institute
[20] A Guide to the Project Management Body of Knowledge, PMBOK Guide.
[21] International Project Management Association-IPMA
[22] Интернационална фирма, специализирана в извършване на одит услуги.

Това е резултат от липсата на добра система за управление на проекти. Въвеждането на такава система само за първите две години води до положителен превес средно с 30% на основните параметри на всеки един проект:

- По-добър продукт / по-доволни клиенти;
- По-бързо изпълнение на проекта;
- По-малък бюджет.
-

Въвеждането на качествена система за управление на проекти, води до чувствително увеличение на ефективността и ефикасността на организацията.

За да е успешен един проект, той трябва да бъде:

- Полезен (за всички участници и ползватели);
- Реалистичен;
- Изпълним,

което е се определя от три основни взаимосвързани параметъра:

- Обхват;
- Време;
- Цена/бюджет,

и се визуализира с „Триъгълник на проекта" (Фиг. 1).

Фиг. 1

Комбинацията от тях се асоциира с качеството на проекта.

Трите елемента са взаимосвързани. Когато увеличим обхвата на проекта (например да направим 5 самолета вместо 4), или увеличим качеството (последно поколение самолети), това води до увеличаване на времето на проекта и/или увеличаване на цената/ бюджета на проекта. За да съкратим времето за изпълнение на проект, се съкращава обхвата на проекта или се намалява качеството му, или се увеличава бюджета на проекта. Когато искаме да съкратим бюджета на проекта, това може да се постигне със съкращаване на обхвата на проекта/намаляване на качеството и/или увеличаване на срока за изпълнение.

2. УПРАВЛЕНИЕ НА ПРОЕКТ ЗА ИЗГРАЖДАНЕ НА СИСТЕМА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Проекта за изграждане на СИСг е дейност за определяне, реализиране и развитие на необходими възможности и способности на самата СИСг и на свързаните

с нея информационни, комуникационни, човешки, финансови, материални и други ресурси за постигане целите и задачите на СИСг.

Извършва се въз основа на:

- Стратегията за развитие на националната, организационната, фирмената и персоналната сигурност;
- Основните стратегии и актовете на Европейския съюз в областта на информационната сигурност и стратегическите концепции на политико-икономическите и политико-военните съюзи;
- Достигнатото ниво на развитие на информационните и комуникационни системи;
- Подготвеността на човешкия фактор за използване и внедряване на последните постижения на науката.

Цел на проекта е да конструира решение на основните проблеми при изграждането на СИСг и като се използва натрупания опита в мениджмънта на информацията, да се осигури съвместимост на СИСг на национално, коалиционно и съюзническо ниво и възможност за прилагане на добрите практики в планирането на сигурността във водещи държави.

Способност е комбинацията от *възможности, умения и ресурси*, осигуряваща постигане на *измерим резултат* при изпълнение на *определени задачи* в конкретни условия и при спазване на зададени *стандарти*.

Способностите служат като ***измерител*** при оценяване на вариантите за развитие на СИСг и са ***основен продукт*** в процеса на тяхното изграждане.

Управлението на проекта стартира със стратегия и дефиниране на СИСг, продължава с планиране и изпълнение на мероприятията от плана и завършва с готовия продукт – функционираща система за сигурност на информацията.

Проектите са по същество уникална дейност и в някаква степен са носители на неопределеност. За по-висока степен на определеност, по-добро управление и подходяща свързаност с останалите организационни дейности, те се разделят на проектни фази, известни като „Жизнен цикъл на проекта". В специализираната литература броя на фазите е различен. Пример за един стандартен жизнен цикъл е със следните **фази**:

1. Фаза „Иницииране".
2. Фаза „Планиране".
3. Фаза „Изпълнение".
4. Фаза „Контролиране".
5. Фаза „Закриване".

Друг вариант на жизнен цикъл е:

1. Фаза „Проучване".
2. Фаза „Планиране".
3. Фаза „Изпълнение".
4. Фаза „Внедряване и след проектен контрол".

Проучване/ иницииране на проекта е фазата, в която се определя дали проектът е изпълним, колко ресурса са необходими за реализирането на СИСг, дали изпълнението е оправдано, т.е. дали вложените ресурси ще са по-скъпи от постигнатия

ефект. Тук се прави оценка на рисковете и се изработват критерии за качество, съблюдавайки международните изисквания и достигнатата степен на развитие на ИТ. Всички оценки на тази фаза са груби и първоначални. Използват се експертни оценки, анализи за рентабилност, аналогии с предишни проекти и т.н. В края на тази фаза се подготвя първоначално техническо задание и се избира изпълнител. В зависимост от целите и задачите на СИСг самото проучване може да се реализира като самостоятелен, отделен проект, които да обоснове необходимостта от последващото изпълнение на останалите фази.

Планиране – тук се изработват различни сценарии за развръзка на проекта (оптимистичен, тенденциозен и песимистичен). Прави се списък на задачите и се подреждат по последователност, така че да отразят цялото протичане на проекта по изграждане на СИСг. Оформя се т.нар. „критичен път" – сбор от последователни задачи, които започват с началото на проекта и завършват с края на проекта. Всяка промяна в задачите от критичния път води до промяна в срока за разработка на проекта. Извън критичния път има задачи, които могат да бъдат изтеглени напред или назад, без това да доведе до някакви промени, особено в крайната дата за приключване на проекта. На този етап се разработва и бюджетът на проекта, прави се разбивка на разходите (преки и непреки).

Изпълнението е активната фаза на проекта. Това е същинското изпълнение на проекта. Управлението се състои в ръководене, координация на различни членове на екипа при изпълнение на отделни задачи и текущ контрол. Той се извършва под формата на регулярни срещи с участниците в проекта, на мениджърския и техническия състав и регулярни отчети към екипите на възложителя. Съставят се графици и се следи процеса спрямо изработения план.

Приключване и оценка - документират се техническите параметри на СИСг и се подготвя техническа документация.

Точния брой и наименование на проектните фази се дефинира от изпълнителя на проекта в зависимост от неговите предпочитани, специфичните характеристики на проекта и контрол от страна на възложителя.

Жизнения цикъл на проекта за изграждане на СИСг служи за определяне на неговото начало и край, а проектните фази дефинират постигането на определени резултати. Те съдържат съвкупност от работни продукти (документи), целящи изграждане на желаните условия за управление.

За успешно управление на проекти са необходими знания в девет основни **функционални области**:

1. Управление на интегрираността на проекта.
2. Управление на обхвата в проекта.
3. Управление на времето за реализация на проекта.
4. Управление на цената в проекта.
5. Управление на качеството на проекта.
6. Управление на човешките ресурси на проекта.
7. Управление на комуникацията на проекта.
8. Управление на проектния риска.
9. Управление на снабдяването на проекта.

Обучението по управление на проекти и въвеждането на система за управление

на проекти по специално при разработването и изграждането на СИСг е процес, свързан с промяна на организационната култура и съществуващият начин на работа. Организацията в която се въвежда трябва да демонстрира воля и желание за промяна, като резултата винаги си струва.

Нека разгледаме някои от функционалните области и се спре по подробно на тяхната същност.

Управление на времето за реализация на проекта

Оценяването на необходимото време за реализация е опит да се прогнозира бъдещото развитие на ИТ и свързаните с тях ИС. Съществуват методи и техники, с които се повишава вероятността за доближаване до реални времеви параметри. При управлението на времето се въздейства върху следните проектни процеси:

1. Определяне на дейности за изграждане на ИС.
2. Определяне на тяхната последователност.
3. Оценяване на продължителността на всяка една дейности.
4. План-график на проекта.
5. Контрол на изпълнението на план-график на проекта.

Управление на цената в проекта

Тук се включват дейности, насочени към осигуряването на изпълнението на проекта в рамките на зададения бюджет. Те са фокусирани най-вече върху разходите на ресурси. На този стадий се извършва оценяване на жизнения цикъл на проектния продукт. Съдържанието на тази функционална област е:

1. Планиране на ресурсите необходими за функционирането на СИСг – по типове ресурси (материални, финансови, човешки и др.), количество и качество за необходимите дейности.
2. Оценяване на разходите – изготвяне на предварителни оценки за разходите на ресурси при различни алтернативи на реализация на проекта.
3. Бюджетиране на проектните разходи – разпределяне на оценените проектни разходи между отделните проектни елементи с цел създаване на условия за измерване. Цели се минимизиране на разликата между разработения бюджет и направените действителни разходи.
4. Контролиране на разходите по проекта – наблюдение и измерване на разходите.

Управление на снабдяването на проекта

Управление на снабдяването на проекта се състои от процеси на придобиване на средства и услуги от външни за изпълнителя на проекта фирми или организации. Състои се от:

5. Планиране на доставките на ИТ софтуер и хардуер, на системи за физическа защита – идентифициране на потребностите от продукти и услуги за проекта, които ще бъдат закупени от външни организации и вземане на решение за реализация им.
6. Планиране и реализация на консултантските услуги – подготовка на необходимите документи за осигуряване на консултантските услуги в интерес на снабдяването и получаване на информация за потенциални доставчици.

7. Избор на доставчици – анализ на предложенията на потенциалните доставчици и избор на такива.

8. Административно управление на договорите – дейностите по доставките да отговарят на изискванията на договорите.

9. Финализиране на договорите за доставка – потвърждаване на изпълнението на договорите, документиране на крайния резултат и финализиране.

Управление на човешките ресурси на проекта

Човешкия ресурс се явява основен при изграждането и използването на СИСг. Това е наука за разпределяне на човешките ресурси между различните проекти или бизнес единици, за максимално използване на наличните ресурси на персонала за постигане на целите на организацията и извършване на дейности, които са необходими за поддържането на този ресурс (хората).

В контекста на управлението на проекта, човешкия ресурс се считат за най-важния ресурс във всяка една организация и включва процеси, като:

1. Организационно планиране – състои се от идентифициране и документиране на проектните роли, отговорностите и взаимоотношенията на индивидуално и колективно/ групово ниво.

2. Формиране на проектен екип – набавяне на необходимите индивидуални и групови човешки ресурси.

3. Развитие на проектния екип – индивидуално развитие на членовете на проектния екип в техническо и управленско направление.

ЗАКЛЮЧЕНИЕ

Сложната икономическа обстановка в страната след преминаването към пазарна икономика, постави нови изисквания към намирането, осигуряването и реализацията на обществените блага. Тези нови изисквания са породени от принципно новите условия на средата за сигурност, както и от изискванията за внедряването на нов коалиционен и съюзнически опит и традиции. Това повишава значително изискванията към планирането, реализацията и осигуряването на системите за управление, системите за сигурност и в частност реализацията на тези системи чрез проекти.

Проблемите за същността, съдържанието, подготовката и използването на системите за информационна сигурност в интерес на отбраната на страната са сложни и разнообразни по съдържание, мащаби и характер. Успешното им решаване е в тясна зависимост от икономическите възможности на страната, от мирновременното им планиране и разпределение, както и от ефективния контрол за тяхното използване. Това в голяма степен зависи от уменията на политическото и военно ръководство на отбраната да организира и да преследва постигането на ефективност и ефикасност в информационното осигуряване.

Разгледания модел за реализация на СИСг е неразривно свързан с националните приоритети и използването на възможностите на Евроатлантическата система за сигурност.

Източници

1. Георгиев В., Тимева Е. Управление на проекти – същност, съдържание, про-

цеси и взаимодействие, Военно издателство, 2006 г.
2. Млеченков М.П, Методика за разработване на система за информационна сигурност, НВУ, Шумен, 2010.
3. Андреев Ог. Менижмънт на проекти, Софттрейд, 2006 г.
4. Сариев Ив. Мениджмънт на информацията, Класика и стил, 2007 г.
5. Велкова Л. Административен мениджмънт, Софттрейд, 2008 г.
6. Ангелов П. Теоретични основи на мениджмънта на човешките ресурси, ВА „Г.С.Раковски", София 2009 г.
7. Български тълковен речник, Наука и изкуство, София, 2004 г.
8. http://www.nsi.bg/index.php - Национален статистически институт.
9. http://www.moby2.com/other/articles/Project%20management.pdf - Управление на проекти.
10. http://denel.dir.bg/PROMGM.pdf - Управление на проекти.
11. http://www.proekti.bg/?act=show_razdel&id=65 - Управление на проекти.
12. www.md.government.bg/bg/index.html
13. www.government.bg
14. www.gcmarshall.bg
15. www.mediapool.bg
16. http://en.wikipedia.org
17. http://bg.wikipedia.org
18. http://ru.wikipedia.org

СИСТЕМНИ РЕШЕНИЯ ЗА СИГУРНОСТ – НЕОБХОДИМОСТ ЗА СЪВРЕМЕННАТА БЕЗОПАСНА СРЕДА НА ЖИВОТ И БИЗНЕС

„Сектрон" ООД, гр. София, бул. „Д-р Г. М. Димитров" №52, сграда СЕКТРОН/СОТ, тел.: 02/ 91 982, факс: 02/ 873 25 76, e-mail: info@sectron.com, www.sectron.com

В съвременния динамичен и забързан свят като, че ли не забелязваме някои малки неща и/или системи осигуряващи безопасното ни и удобно ежедневие. Такъв тип системи са и системите за сигурност. Тези неизменн помощници помагащи ни да установим, когато някой се опита да влезе в апартамента ни или да видим кой е откраднал нещо от магазина ни.

Съвременните системи за сигурност и защита са навсякъде около нас и се грижат за сигурността и защитата на нас и нашето имущество: алармени системи в дома, системи за контрол на достъпа и отчитане на работното време в офиса, видеонаблюдение в магазина, пожароизвестителни системи алармиращи ни при опастност от пожар, пожарогасителни инсталации потушаващи възникналите пожари в сървърните помещения, системи за периметрова охрана на вилата и т.н.

Когато избираме решение за сигурност трябва да внимаваме за няколко основни черти за всички видове системи:

- надеждност – системите за сигурност и безопастност трябва да са изпитани, за да могат да осигурят спокойствието ни постоянно, а не „от време на време".
- обслужване на системата – колко лесно се обслужва и колко често се налага техник от поддръжката да се грижи за нея – планови спирания, техническа профилактика.
- стойност на системата – инвестирането на десетки хиляди за охрана на стоки на стойност 200 лева не е оправдано, нали.

Успоредно с посочените по горе характеристики, всеки вид системи има собствени специфични технически параметри – резолюция, осветеност, памет за определен брой събития, обхват и т.н., които трябва да бъдат оптимално определени за всяка една система, за да осигурят необходимата защита за Вас и вашата собственост.

За изграждането на едно съвременно пълнофункционално решение за сигурност може да се комбинират различни видове системи за сигурност. Да вземем например една система за охрана на соларен парк – при нарушаване на периметъра, системата за периметрова охрана определя точното място на нарушение и автоматично подава сигнал към системата за видеонаблюдение, която насочва някоя от управляемите камери към проблемната зона и в реално време предава видео сигнал за обстановката в мониторинговия център на охранителната фирма отговаряща за охраната на обекта или на собственика.

„Сектрон" ООД е първата частна компания в България занимаваща се с проек-

тиране и дистрибуция на системи за сигурност. През годините компанията утвърди мястото си на лидер на пазара България. Фирмата предлага широка гама от алармени системи, системи за видеонаблюдение, пожароизвестяване и пожарогасене, контрол на достъп, работно време и хотелска сигурност, системи за детекция на вода и изтичане на газ, системи за периметрова охрана, цифрови комуникационни системи, интегрирани системи за централизирана мониторинг и предаване на данни, както и цялостен инженеринг за тях.

1. АЛАРМЕНИ (СОТ) СИСТЕМИ

Алармени системи се използват за контрол и известяване за тревожно събитие, което може да бъде нежелано проникване, пожар, наводнение или природно бедствие. Алармени системи имат различни характеристики в зависимост от това къде е предназначена - за дома, офиса, търговски и промишлени комплекси.

Основните функции на алармените системи са регистриране на нежеланото действие или ситуация (пожар), навременно информиране за действието или събитието на собственика или охранителната фирма чрез подходящо оборудване; събиране на доказателствена информация, която да подпомогне идентифицирането на нарушителя, контрол на достъпа до мястото.

Digiplex EVO системи осигуряват най-високо ниво на защита за обекти, луксозни жилищни и всяко място, където максимална сигурност е от съществено значение. Тези системи са проектирани да бъдат лесни за употреба, с модулна концепция позволяваща бързо, удобно и лесно инсталиране, поддръжка и разширяване на тези системи.

PARADOX EVO 192		
	Максимален брой зони	192
	Разделения	8
	Контрол на достъп	32 врати
	Нива на достъп	16
	Памет за събития	2048
	Поддръжка на IP/GSM/GPRS комуникатори	Да IP100/PCS200
PARADOX TM 4 Клавиатура със сензорен екран		
	• Интуитивен потребителски интерфейс с икони • 4.3-инчов (10.9cm) дисплей с ярки цветове • Настройваеми етикети: на зони, групи, потребители и PGM изходи • Възможност за управление на до 8 PGM изходи • Слот за SD карта за потребителски теми и звуци, снимки и обновяване на фърмуера • Зонов/температурен вход	

PARADOX K641R 32-символна LCD клавиатура с интегриран четец за контрол на достъп	
	• 32-символна клавиатура със син LCD екран с програмируеми етикети • Интерфейс на български език • 1 адресируема зона и 1 PGM изход • Вграден четец на карти • Разрешава достъп чрез карта и/или код за достъп • Включване/изключване чрез карта за контрол на достъпа
PARADOX DG85 Външен цифров датчик за движение без регистриране на движението на домашни животни до 40 кг	
	• Двойно оптична филтрираща система • UV защитени лещи • Осигурява изключителна защита срещу засичане на домашни животни, използвайки патентована комбинация от модерни оптични елементи и цифрови обработващи технологии • Не засича животни с тегло до 40 кг. • Двойно оптика, 11m X 11m; 90° ъгъл на покритие
PARADOX PCS200 GSM/ GPRS комуникационен модул	
	• Рапортуване през GPRS • Качване/Сваляне на данни през GPRS: • Обновяване на фърмуера през GPRS • Рапортуване чрез кратки текстови съобщения(SMS) • Контрол на комуникационната връзка с контролният панел

2. СИСТЕМИ ЗА КОНТРОЛ НА ДОСТЪП И РАБОТНО ВРЕМЕ

CDV Centaur е усъвършенствана, модулна система за контрол на достъпа в реално време, оптимизирана за широк кръг от приложения от апартаментни комплекси до обекти с високи изисквания към сигурността – места за лишаване от свобода, инфраструктурни и индустриални съоръжения.

Centaur е изпитана напълно развита и стабилна технология с множество малки и големи инсталации в Канада, САЩ и по света. Системите Centaur са с повече от 10 годишна история на производство и изпитания.

Системата оптимизира вложената инвестиция чрез осигуряване на подробни справки, експертен софтуер за отчитане на работно време, реалновремеви графичен интерфейс, интеграция със система за видеонаблюдение, паркинг мениджмънт, контрол на асансьори и много други.

Всяка система за контрол на достъп се състои от:

CDVI CT-V900-A Контролер за контрол на достъпа	
	• 2 врати (разширяеми до 8 с помощта на модулите CA-A470-A) • Поддръжка на 16348 карти • 256 нива на достъп • 256 разписания (разширяеми) • буфер за 2048 събития (разширяеми) • 16 вградени зонови входа • 2 вградени релета (разширяеми до 16 с помощта на модулите CA-460A-P) • Фърмуер, който се обновява on-line • TCP/IP поддръжка • Управление на асансьори до 64 етажа
CDV Centaur 	Софтуер за управление на системата за контрол на достъп
SUPREMA BioLite Net EM IP-базиран биометричен система с пръстови отпечатъци с функция за контрол на достъп и работно време	
	• Подходяща за външен монтаж, влагоустойчива. • Графичен монохромен LCD дисплей с резолюция 128x64 pixel и клавиатура с 12+3 функционални бутона • 500dpi оптичен сензор за прочитане на пръстови отпечатъци • Възможност за идентификация със скорост 2000 отпечатъка/сек • Вътрешна памет:до 10 000 отпечатъка /5000 потребителя/

CDVI NANOPW Миниатюрен безконтактен четец, подходящ за вътрешен/външен монтаж	
	• Миниатюрните размери и изчистените линии правят този четец подходящ за монтаж в помещения със строги архитектурни изисквания към интериора. • Wiegand 26 интерфейс • Възможност за употреба навън • Залята с епоксидна смола платка • Визуална и звукова верификация на работата на четеца

3. СИСТЕМИ ЗА ВИДЕОНАБЛЮДЕНИЕ

Съвременните системи за видеонаблюдение са навсякъде около нас – в офиса, на улицата, в градския транспорт, „Големият брат" ни гледа навсякъде. Съвременното видеонаблюдение може да се раздели на: Аналогово, IP и хибридни системи за видеонаблюдение.

При Аналоговото видеонаблюдение имаме три основни компонента: камера, записващо устройство и коаксиална преносна среда.

Корпусни камери	
JVC TK-C9300E Ден/Нощ камера с висока резолюция	
	• 1/3“ CCD матрица с нов 14-bit DSP процесор • Висока резолюция от 600TV линии • Светлочувствителност: 0.003 Lux • True Day/Night функционалност с IR cut филтър • Разширен динамичен обхват (ExDR) • 3D цифров шумов филтър • Бавен затвор x2 до x128 • Вградена детекция на движение
CNB BBB37F Ден/Нощ камера с широк динамичен обхват	
	• 1/3" SONY Double Scan CCD • Светочувствителност 0.0007 Lux • Механичен ИЧ филтър • Широк динамичен обхват • Интелигентна компенсация на фонова светлина (HSBLC) • 3D цифров шумов филтър • Цифров стабилизатор на картината • Цифров zoom (18x), екранно меню (OSD), AWB

Куполни камери	
JVC TK-C2201E Вандалоустойчива камера с висока резолюция	
	• 1/3“ CCD сензор и нов 14-bit DSP Easy Day/Night функционалност • 3D цифров шумов филтър • Компактен дизайн и вандалоустойчив купол • SLL- Super LoLux • Резолюция от 600 TV линии • Варифокален обектив f=2.8~10.5 • Светлочувствителност от 0.015 Lux
Камери с Инфрачервена подсветка	
CNB LFM-21VF Вандалозащитена куполна камера с вградена ИЧ подсветка	
	• 1/3“ SONY Super HAD CCD • 600 ТВ линии • Вграден варифокален обектив с автоматична бленда f=3.8~9.5 mm • Интелигентна ИЧ технология с обхват до 15 метра (25 IR диода) • Функция Ден/Нощ с вграден инфрачервен филтър (ICR) • Светлочувствителност: 0.005 Lux / 0 Lux (IR LED On) • Влагозащитен корпус IP66
CNB BE5810PCR Влагозащитена камера ден/нощ с механичен ИЧ филтър	
	• 1/3” SONY Super HAD CCD • 550 ТВ линии • Вграден варифокален обектив 7.5~50mm/f=1.2 • 206 ИЧ диода (850nm) с обхват до 80 метра • Функция Digital Slow Shutter • Super Digital Noise Reduction • Светочувствителност 0.3lux/0.00lux • Скрито окабеляване във стойката • Вградено отопление и вентилация • Влагозащитен корпус IP65

Управляеми PTZ/ Zoom камери	
JVC TK-C686WPE Моторизирана управляема камера с 36x zoom	
 JVC The Perfect Experience	• 540 TV линии • Super LoLux: 0.5 Lux • Вграден варифокален обектив с 36X оптично увеличение • Обектив f=3.43~122 mm • Оптичен стабилизатор • Вграден инфрачервен филтър Изключително тих механизъм (Direct Drive Motor) • Скорост: 500º/секунда • Автоматично проследяване
CNB ZBN-21Z27F 23X zoom Ден/Нощ камера с висока резолюция	
 CNB TECHNOLOGY Inc.	• 1/4” SONY Super HAD CCD сензор • 580 TV Line • Автоматичен фокус и автоматична бленда • Вграден моторизиран обектив с 23x оптично увеличение • 10x цифрово увеличение (Max. 230x) • Функция Ден/Нощ с вграден инфрачервен филтър (ICR) • RS-485 интерфейс (Pelco-D) • Функция за подобряване на светочувствителността (DSS) • Захранване 12VDC
Цифрови видео рекордери	
HIKVISION DS-8116HDI-S 16-канален цифров рекордер/сървър	
 HIKVISION	• Запис в реално време с общо 400 к/с при 2CIF (704×288), 200 к/с при 4CIF (704×576) • 16 канала видео (компресия H.264) • 16 канала аудио • Поддръжка на до 8 SATA диска USB2.0 порт за архивиране на USB • BNC + VGA

IP системите за видеонаблюдение се състоят от камера, записващо устройство – NVR или сървър със софтуер за запис и TCP/IP мрежова преносна среда.

IP камери	
ARECONT VISION AV 1315 DN 1.3 мегапикселова цветна IP камера	
	• 1.3 мегапикселова цветна IP камера • 1/2.7" CMOS • Резолюция 1280x1024 @ 32fps • Компресия H.264 • Ден/Нощ с IR филтър • Светлочувствителност: 0.1 lux @ F1.4 • Изключително компактен размер • PoE/15~48Vdc
VIVOTEK FD 8161 Куполна 2 Мегапикселова IP камера с ИЧ осветление	
	• Резолюция 2.0Mpx (1600x1200) • 1/3" CMOS сензор • Ден/Нощ с IR cut филтър • Светлочувствителност: 0.1 lux • IR осветление до 15 м • Варифокален обектив 3~9 мм • Алармен вход/изход • Аудио пренос (вграден аудио вход) • Слот за SD/SDHC карта • Тройна компресия H.264/MPEG-4/MJPEG • Наблюдение от мобилен телефон • PoE (7W)/12Vdc/24Vac
ARECONT VISION AV2825IR FullHD 1080p Ден/Нощ влагозащитена IP камера	
	• 1/2.7” CMOS • Вграден 4.5-10mm варифокален обектив с IR корекция • Светочувствителност 0.1 lux @ F1.4, PoE/15~48Vdc • 48 IR LEDs, обхват от 25 метра • H.264 и MJPEG компресия • До 24 кад./сек. при 1080p • Резолюция 1920×1080 • Вградени в корпуса вентилатор и нагревател

SANYO VCC-HD5400P 2-мегапикселова моторизирана IP камера

- 1/2.5" Progressive scan CMOS сензор
- Резолюция FullHD@25кад/сек
- 10x оптичен zoom, 0.1 Lux
- MJPEG/H.264 (Quad Stream)
- Безконечно въртене
- Оптичен стабилизатор
- HDMI мониторен изход
- 4 алармени входа / 2 релейни изхода
- Двупосочно аудио
- Слот за SD карта
- Функции за автоматично проследяване
- 12Vdc/24Vac/PoE - 21W (VCC-HD5400P)

Мрежови видео рекордери (NVR)

VIVOTEK NR8301 9-канален IP видеорекордер (NVR)

- Компресия H.264, MPEG-4 и MJPEG
- Симултанен преглед и запис на 8 IP камери
- Съвместим с VAST CMS софтуер
- 4 канала PoE
- Автоматично конфигуриране и инсталиране на IP камери
- Ракмаунт дизайн
- eSATA интерфейс
- USB интерфейс за видео бекъп
- LED статус индикатори
- Вграден Firewall
- Вграден Gateway за разделяне на мрежовия интерфейс за мрежовите камери и преноса на данни
- Поддържа уведомяване по E-mail
- Поддържа всички VIVOTEK камери

IP софтуерна платформа за видео управление, анализ и запис

Milestone XProtect™ е водеща софтуерна платформа за IP видео управление. Тя действа като ядро на система за IP наблюдение, като свързва целия хардуер, който сте избрали в едно оптимално интегрирано решение. Софтуерът се предлага като пакети оразмерени

според различните нужди на бизнеса ви. Софтуерът на Milestone поддържа повече от 800 различни модели камери и видео декодери от над 35 производители. Тази поддръжка ви предоставя най-широкия избор на точното устройство за всяка ситуация. • Отворена архитектура за интеграция • Преглед на място и чрез отдалечен достъп • Разпознаване на номера на автомобили от над 60 страни в света. • Надеждна и доказана технология • С възможност за посрещане на бъдещите изисквания

4. ПОЖАРОИЗВЕСТИТЕЛНИ И ГАСИТЕЛНИ СИСТЕМИ

Пожароизвестяването е критичен фактор за безопасността на производството, дома или офиса ви. Системите за Пожароизвестяване и пожарогасене са първата пречка пред опасности от огромни човешки и имуществени щети, предизвикани от една от най-безпощадните стихии на модерния ни живот – неконтролируемият огън. Сериозният подход към проблема е от изключително важно значение за оцеляването на обитателите, както и на бизнеса в силно критични ситуации.

KENTEC Syncro Аналогово Адресируеми пожароизвестителни контролни панели серия 2-8 кръга	
 Kentec Electronics Ltd.	• Свързване в мрежа на до 64 панела • Интелигентен интерфейс за системи за сградна автоматизация (BMS) • Поддържа Hochiki ESP, Apollo и Argus протоколи • Поддържа до 127 адресируеми устройства Hochiki на всеки кръг • Варианти с 2, 4, 6 и 8 кръга • Опция за зонови LED индикатори за 16, 48 или 96 зони • 4 програмируеми конвенционални кръга за сирени • Програмируеми входове и изходи • LCD рипитери • Лесен за ползване системен софтуер за настройка • Система за управление на алармите GUIDE

HOCHIKI ACA-E Комбиниран мултисензорен детектор – димооптичен и термичен	
	• Комбиниран детектор ACA-E е подходящ за ползване както за помещения, в които един принцип на детекция не е достатъчен за ранно установяване на пожар, така и на места, където се налага промяна на метода и/или чувствителността на детекцията в рамките на деня. • Нископрофилен дизайн • Покрива площ до 112 м² • Цвят: Слонова кост и бял • Монтира се на височини до 10.5 м
HOCHIKI ALG-EN Аналогов адресируем димооптичен детектор	
	• Високотехнологичната димооптична камера • Два червени светодиода с 360° видимост за следене на активността • Покрива площ от 112 м² • Настройка на чувствителността • Електронно адресируем • Съответства на LPCB & VdS • Предлага се в три цвята: слонова кост, бял и черен
HOCHIKI ACB-E Аналогов адресируем мултисензорен термичен детектор	
	• Два термочувствителни елемента - термистор и сензор, реагиращ на бързи температурни изменения • Два червени светодиода с 360° видимост за следене на активността • Покрива площ от 56 м² • Съответства на LPCB & VdS • Предлага се в два цвята: слонова кост и бял • IP64
HOCHIKI HCP-E Аналогов адресируем ръчен пожароизвестител	
	• Нечуплив пластмасов елемент • Съответстващ на стандарт LPCB EN 54-11:2001 • Възможност за вграден или повърностен монтаж • Влагозащитена версия HCP-W

HOCHIKI YBO-BSB Аналогова адресируема основа-сирена с флаш лампа	
	• Захранва се от адресния кръг и заема един адрес • 51 тона, които са в съответствие със стандарта EN54 - част 3 • Сертифицирана от LPCB и VdS • Силата на звука може да се регулира в диапазона от 50 до 98dB(A).

Повече информация за пожароизвестителните системи може да намерите на fire.sectron.com

В почти всяка сграда съществуват зони, където използването на вода като гасителен елемент може да причини големи материални щети или да е нежелателно поради други причини. Използването на сухи/газови пожарогасителни системи е разпространено за защита на скъпо оборудване, телекомуникационни съоръжения, сървърни помещения с особено ценна информация, трансформаторни помещения, самолети, кораби и др. При тези случаи като алтернатива на конвенционалните спринклерни системи се използват газови пожарогасителни инсталации изплозващи сухи химикали, инертни или химически газове – аргон, FM200, NOVEC и др.

Гасенето с химически газове като FM200 или NOVEC е базирано на принципа на разрушаване на верижната реакция която подържа огъня и охлаждане на горящите повърхности. Тези газове са много ефективни дори при ниски концентрации и не са опасни при вдишване

Газовите пожарогасителни системи имат собствен контролен панел който е свързан и комуникира с главната пожароизвестителна централа. Гасителният елемент се освобождава автоматично след подаване на сигнал от пожароизвестителната централа, като понякога в зависимост от използвания газ освобождаване става след определен период необходим за сигнализиране и евакуация на хората от зоната на пожар.

KENTEC Sigma XT - Конвенционален пожарогасителен контролен панел Sigma XT	
 Kentec Electronics Ltd.	• 1-4 пожарогасителни зони • Дисплей за време • Индикатор за налягане • Програмируеми зони • Програмируемо закъснение на зоновия вход и сирените • Индикатор „задържане” • Режим „обходна” проверка • Релейни контакти „пожар” и „грешка”
MINIMAX MX-200 - Химически пожарогасителни системи	
 MINIMAX	Химическата пожарогасителна система MX-200 е ефективна и безопасна за околната среда. MX-200 използва гасителен агент химическото съединение HFC-227ea. Този тип пожарогасителна система се използва за защита на ценни и критични материали. Основните предимства на пожарогасителната система MX-200 • Висока ефективност на гасенето • Кратко време за изпускане на агента, безостатъчност, безопасност за хората и малки обеми за съхранение. Пожарогасителната система MX-200 се състои от стоманени бутилки с гасителен агент, които се свързват с тръбна мрежа, на която се монтират специални дюзи, които не позволяват на гасителния агент да се изпари, докато не стигне до тях.

MINIMAX MX 1230 - Пожарогасителната система с пожарогасителен агент Novec

MINIMAX

Благодарение на бързото и равномерно разпространение на гасителния агент пожарогасителната система на MINIMAX – MX 1230 с пожарогасителен агент Novec ™ на 3M ™ дава решение, което предлага много предимства при защитата на електрическо и електронно оборудване.

Тази система е екологично чиста, спестява място и гарантира високо ниво на сигурност за хората.

Характеристиките на гасителния агент Novec™1230 са уникални:

- Съхранява се на стайна температура, компактно като вода;
- Гаси като газ – с хомогенна дистрибуция в цялата зона на гасене;
- Не оставя никакви остатъци.
- Системата автоматично разпознава риск от пожар в ранна фаза, автоматично прекъсва електрическото захранване и гаси пожара, бързо и безостатъчно.

5. КОМУНИКАЦИОННИ СИСТЕМИ

Системите за комуникация са една от най-важните придобивки на съвременното общество. В този постоянно променящ се свят обмена и преноса на информация е едно изключително необходимо и ценно преимущество.

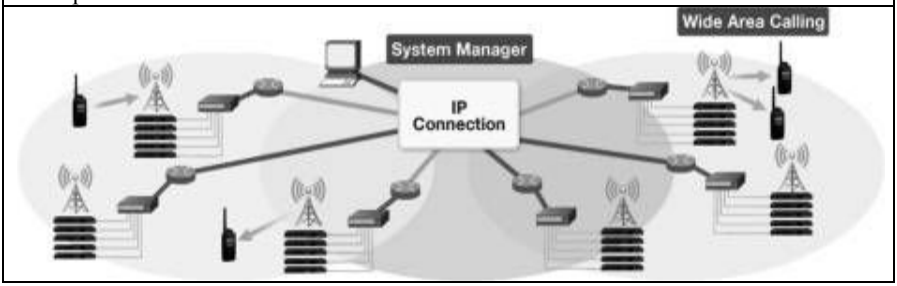
Сектрон ООД винаги се стреми да предложи на своите партньори и клиенти най-добрите и качествени решения, включително и в областта на системите за комуникация.

NEXEDGE – МНОГО РЕШЕНИЯ –ЕДНА СИСТЕМА

NEXEDGE е иновативна цифрова система на KENWOOD за радио комуникация, която отговаря на новите и все по-сериозни изисквания за сигурност и надеждност на връзката. Съвременната DSP технология за обработка на гласа дава възможност за съвместно използване и плавен преход, от съществуващите аналогови системи, към новата цифрова система – NEXEDGE. FDMA метода приложен за достъп до канал, позволява максимално ефективното използване на честотния ресурс.

NEXEDGE ви осигурява още: IP свързаност между отделните сайтове, изпращане на видео изображение, изпращане на SMS и GPS кординати, възможност за връзка с външни телефонни номера, роуминг, контрол, анализ и статистика на състоянието на системата, защита от прослушване, лесно разширяване и отдалечено конфигуриране на системата.

NEXEDGE поддържа голям капацитет на групи и абонати, което позволява разделянето на системата и използването ѝ от големи организации с национален мащаб и покритие.



Сигурността е функционалното състояние на дадена система, което осигурява спокойствието и противодействието ѝ фактори оказващи деструктивон влияние върху системата.

Съвременните системи за сигурност подсигуряват живота и здравето на лицата, държавата, дейността им, както и бизнеса от страна на потенциални и/или реални заплахи. Високата степен на сигурност осигурява увеличаване благосъстоянието на дадено лице или общество, подсигурявайки възможността усилията и защитените блага да бъдат насочени за натрупване на богатства в негова полза.

Благодарение на натрупания опит като пионер в проектирането, дистрибуцията и изграждането на съвременни решения за сигурност „Сектрон" може да предложи пълната гама от услуги и продукти за осигуряване на решения за Вашата сигурност от дома и офиса, до най-големите промишлени, търговски и институционални обекти.

Фирмата има дългогодишен опит и предлага пълната гама услуги, съпътстващи изграждането на системата за комуникация- изготвяне на проект, доставка на оборудване, изграждане, обучение за работа със системата, гаранционна и следгаранционна подръжка, както и отличен сервиз с подготвени специалисти.

СЕКТРОН
СИСТЕМИ ЗА СИГУРНОСТ И КОМУНИКАЦИИ

SECTRON
SECURITY & COMMUNICATION SYSTEMS

ЕТАПИ В РАЗРАБОТВАНЕТО НА СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ*

ВЛАДИМИР П. КРУМОВ

ПОДЕЛЕНИЕ 42910 ГРАД ШУМЕН УЛ. КАРЕЛ ШКОРПИЛ № 1
E-MAIL : VLADIMIRKR@ABV. BG

STAGE IN DEVELOP INFORMATION SEGURITY MANAGEMENT SYSTEM

VLADIMIR P. KRUMOV

ABSTRACT *:In this report examine stage in develop information secutity system.*

KEY WORDS *: Alert , Control objective ; Information security ; Risk assessment ; Risk management*

Процеса на глобализация в началото на 21век повиши изискванията за управление и комуникация в обществения живот. Това доведе и до развитието на мобилните комуникации и автоматизацията на управлението наложи разработването и въвеждането в употреба на необходимите информационни технологии което доведе и до развитието на мобилните комуникации и автоматизацията на управлението. Заедно с това се появиха много заплахи и рискове непознати досега породени от уязвимостите на тези автоматизирани информационни системи, което породи необходимостта и от разработване на системи за управлението на информационната сигурност, които чрез тяхното използване да сведат съществуващите рискове и заплахи до минимални приемливи граници.

В световен мащаб базови за разработването на такива системи за управление на информационната сигурност са стандартите ISO/IEC 27001:2005; ISO/IEC 27002-2:2005.

Стандартът ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements; Информационни технологии – Техники за сигурност – Системи за управление на информационната сигурност – Изисквания) обхваща едни от основните аспекти на сигурността като : оценка и управление на риска; контрол на достъпа.

Стандарта ISO/IEC 27002-2:2005 („Information Security Management – Part 2 – Specification Security Management Systems"). ни описва как да бъдат разработвани и утвърждавани в практиката системите за управление на информационната сигурност ISMSs (Information Security Management Systems).

Стандартът ISO/IEC 27002 също така е начална база за разработване на специфични за конкретните организационни структури ръководства, наредби, практики и процедури за управление на защитата на информацията.

Етапите при разработването на системи за управление на информационната сигурност са : [1]

* Докладът е изнесен в секция "Студентско-докторантска"

1. Дефиниране на обхвата на СУИС и определяне на информационните активи
2. Дефиниране на подхода за оценка на риска
3. Идентифициране на риска
4. Анализ и оценка на риска
5. Третиране на риска
6. Внедряване и изпълнение на Плана за третиране на риска
7. Наблюдение и преглед на СУИС
8. Документи разработвани при формирането на СУИС

При първия етап основната дейност която се извършва е да бъдат ясно определени всички важни активи, също така трябва да се определят нормативните изисквания които ще удовлетворява дадената система, както и показателите и критериите за оценка на риска.

Типовете активи които подлежат на определяне могат да се класифицират в следните групи :

- информационни активи ;
- софтуерни активи ;
- физически (хардуерни) активи ;
- услуги ;
- личния състав на организацията;
- други нематериални ценности.

При втория етап се определят какъв ще е използвания метод за оценка на риска; през какъв период от време ще се извършва и нивото на остатъчния (допустим) риск .

През третия етап се извършват следните дейности :

- описване и оценяване на активите ;
- определяне на заплахите за всеки от определените активи и уязвимите места;
- резултата от въздействието на заплахата или риска върху определените активи.

При описването на активите на информационната система всички те в някаква степен са ценни но всеки един има собствена тежест. Това, както и идентификацията на ценностите е първата стъпка към определяне на областите, на които е необходимо да се обърне внимание.

Оценка на риска се извършва на база определените граници на защита и степен на детайлизация като се подбира конкретен метод за анализ на риска, чрез който той се измерва и вероятността за реализиране на заплахи, вследствие на тези рискове.

Последната дейност в този етап е оценка на резултата от въздействието на дадената заплаха и определянето на възможните щети които може да причини дадената заплаха или риск.

Четвъртия етап при разработването на система за управление на информационната сигурност е един от основните и най – важния при разработване на СУИС. Първа стъпка в този етап е правилното дефиниране на структурата на СУИС и правилното определяне на уязвимостите и заплахите за всеки един от елементите на СУИС. Важно е също така да се определи, какви щети и вреди би довело евентуалния пробив в сигурността ако се реализират определените по – рано заплахи.

Методиките за оценка на риска са разгледани в стандарта ISO/IEC TR 13335 – 3 ("Информационни технологии – указания за управление на сигурността на инфор-

мационните технологии – техники за управление на ИТ сигурността "). Също така може да се използват математически модели чрез които на всеки риск се задава числена стойност след което се подреждат по възприета за целта скала. Това дава възможност да се определят рисковете които са неприемливи и трябва веднага да бъдат третирани, както и да се определят тези които са на приемливо ниво и спрямо на които да се предприемат мерки за контрол с цел поддържането им в това приемливо ниво.

След оценката на риска следва да се определи дали риска е приемлив и налага ли се третиране на риска ако той е неприемлив. Примерни критерии по които може да стане това са следните :

1. Нарушение на законите и/или подзаконовите актове;
2. Нарушаване на конфиденциалността на личните и служебните данни;
3. Неосигуряване на личната сигурност;
4. Финансови загуби;
5. Заплаха за околната среда.
6. Честота на проявление на дадения риск
7. Нанесени щети за организация вследствие реализиране на дадената заплаха.

През петия етап става третирането (обработката) на риска. То обхваща избора и реализацията на мерките за контрол и средствата за минимизиране на риска, Способите които се използват за обработка на риска са следните: [1]

1. Намаляване на риска – рискът се счита за неприемлив и за минимизирането му се реализират съответните средства и механизми за сигурност.
2. Прехвърляне на риска – рискът се счита за неприемлив и при определени условия се преадресира към друга организация (в рамките на застраховане или аутсорсинг).
3. Приемане на риска – рискът се счита за осъзнато допустим (организацията приема възможните последствия). В тези случай цената която трябва да се плати за неутрализирането на риска е по – висока отколкото стойността на потенциалните загуби.
4. Отказ от риска – отказване на дейностите, явяващи се причина за риска за сигурността на системата.

След като се обобщят и систематизират резултатите от извършената оценка на риска се изготвя План за третиране на риска в който се определят стойностите на остатъчните рискове. В плана се прилагат действията описани в Приложение А на стандарта ISO/IEC 27001:2005 – Цели по контрол и механизми за контрол. В това приложение са дефинирани практики за управление на риска, които вкючват 33 цели разделени в 11 области, в които от включват 133 механизма за контрол. Също така се използва и стандарта ISO/IEC 27002:2005, чрез който се препоръчват приложимите механизми за контрол за намаляване на рисковете до допустимо ниво.

Реализирането на този план зависи от финансовото осигуряване и инвестициите в закупуване на хардуер, софтуер или други информационни системи, които да спомогнат за неговото изпълнение. Неразделна част от плана за третиране на риска са механизмите за наблюдение , преглед и контрол на СУИС.

При внедряването и изпълнението на плана за третиране на риска последователността на действията е следната:

- осигуряване на ресурси за осъществяване на плана;
- разработването на съответните правила и документация, регламентирани от

стандарта ISO/IEC 27001:2005;

- разпределят се отговорностите на ръководния състав на организацията и на органа по информационна сигурност по внедряването на съответните механизми за контрол и тяхното изпълнение;
- обучение на персонала;
- измерване на ефективността на избраните мерки и механизми за контрол.

През седмия етап от разработването на СУИС най – общо се извършва одит на системата, като целта на този одит е да се извърши преглед, контрол и мониторинг на системата с цел: идентифициране на успешните и неуспешните пробиви и инциденти в системата; вземане на решение дали дейностите по сигурността, делегирани на служителите, се изпълняват съгласно изискванията и очакванията; да се определи дали предприетите действия за справяне с пробив в сигурността , ако е имало такъв са били ефективни.

Документите които трябва да се изготвят са следните [2] :

1. Документирани декларации за политиката и целите на СУИС
2. Обхватът на СУИС.
3. Процедури и механизми за контрол с цел поддържане на СУИС;
4. Описание на методиката за оценка на риска.
5. Доклад за оценка на риска.
6. План за третиране на риска.
7. Документирани процедури, необходими на организацията да осигури ефективното планиране, действие и контрол на процесите , свързани с информационната сигурност и описание на това как се измерва ефективността на контролите.
8. Записи, изисквани от самия стандарт.
9. Декларация за приложимост.
10. Политика за информационна сигурност на организацията.

В заключение мога да обобщя, че успешното разработване на системи за управление на информационната сигурност е ефективен начин за справяне с предизвикателствата породени от развитието на комуникационните и информационните технологии и съпроводените с тях рискове и заплахи за сигурността на информацията използвана от тези устройства и технологии.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Млеченков, М. Методика за разработване на системи за управление на информационната сигурност, Информационно–издателски и мултимедиен комплекс на факултет “ Артилерия, ПВО и КИС“, Шумен 2010, 64 стр.
2. ISO/IEC 27001:2005.
3. ISO/IEC 27002:2005
4. ISO/IEC TR 13335 – 3:1998

ХАРДУЕРНА РЕАЛИЗАЦИЯ НА ГЕНЕРАТОР НА ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ ИЗПОЛЗВАЩ АТРАКТОР НА ЛОРЕНЦ*

Борислав П. Стоянов, Николай Р. Николов

Шуменски университет "Епископ Константин Преславски", факултет "Математика и информатика", катедра "Компютърна информатика", Шумен, България, bpstoyanov@abv.bg

Шуменски университет "Епископ Константин Преславски" Факултет по технически науки e-mail niki2_1974@abv.bg

HARDWARE IMPLEMENTATION OF PSEUDO-RANDOM SEQUENCE GENERATOR USING OF LORENTZ ATTRACTORS

Borislav P. Stoyanov, Nikolay R. Nikolov

Konstantin Preslavski University of Shumen, Department of Computer Informatics, Shumen, Bulgaria, bpstoyanov@abv.bg

Konstantin Preslavski University of Shumen, Department of Technical Sciences Shumen, Bulgaria niki2_1974@abv.bg

Abstract: *Stream ciphers as a modern means of information protection possible to ensure a relatively high reliability in the cryptographic realization of the information process. Traditional ways of achieving this goal is the realization of generators using LFSR systems with nonlinearities and indivisible polynomials of high degree and the introduction of a priori not defined nonlinearity. A new method for the realization of the PN is to use the house attractors [1,2,3]. As a major advantage of the algorithm presented indicating the possibility of obtaining high performance and ability to work in real time.*

Key words *hardware implementation, pseudo-random number generator, stream cipher*

Въведение

Поточните шифри като съвременно средство за защита на информацията позволяват да се осигури относително висока криптографска надеждност при реализацията на информационният процес. Традиционните пътища за постигане на тази цел е реализацията на генератори на ПСП (псевдослучайна последователност) използващи LFSR (Linear feedback shift register) описвани с неразложими полиноми от висока степен и въвеждането на априори недефинирана нелинейност. Един нов метод за реализацията на ПСП е използването на хаус атрактори [1,2,3]. Като основно предимство на алгоритъм използващ хаус атрактор е получаването на висока производителност и работа в „реално време". Алгоритмите на използващи генератори на ПСП чрез хаус атрактор използват нелинеен оператор което намалява

* Докладът е изнесен на пленарна сесия

ефективността на криптографската атака на Берликамп-Меси.

Изложение

Известно е, че атрактора представлява компактно инвариантно множество в тримерното пространство което притежава дефинирана сложна топологична структура, явяваща се устойчива по критерия на Ляпунов за динамични системи. Всички точки от множеството са разположени в ограничена област от тримерното пространство. Един от първите атрактори представени през 1963 г. е динамичната система описана от Лоренц. Тази динамична система е намерила приложение при описанието не редица процеси в природата и техниката.

Атрактора на Лоренц използван при създаването на генератори на ПСП в [1,2,3] е с описан чрез система от нелинейни диференциални уравнения (1):

$$\frac{dz}{dt} = \sigma(y - x)$$

$$\frac{dy}{dt} = x(r - z) - y \qquad (1)$$

$$\frac{dz}{dt} = x.y - b.z$$

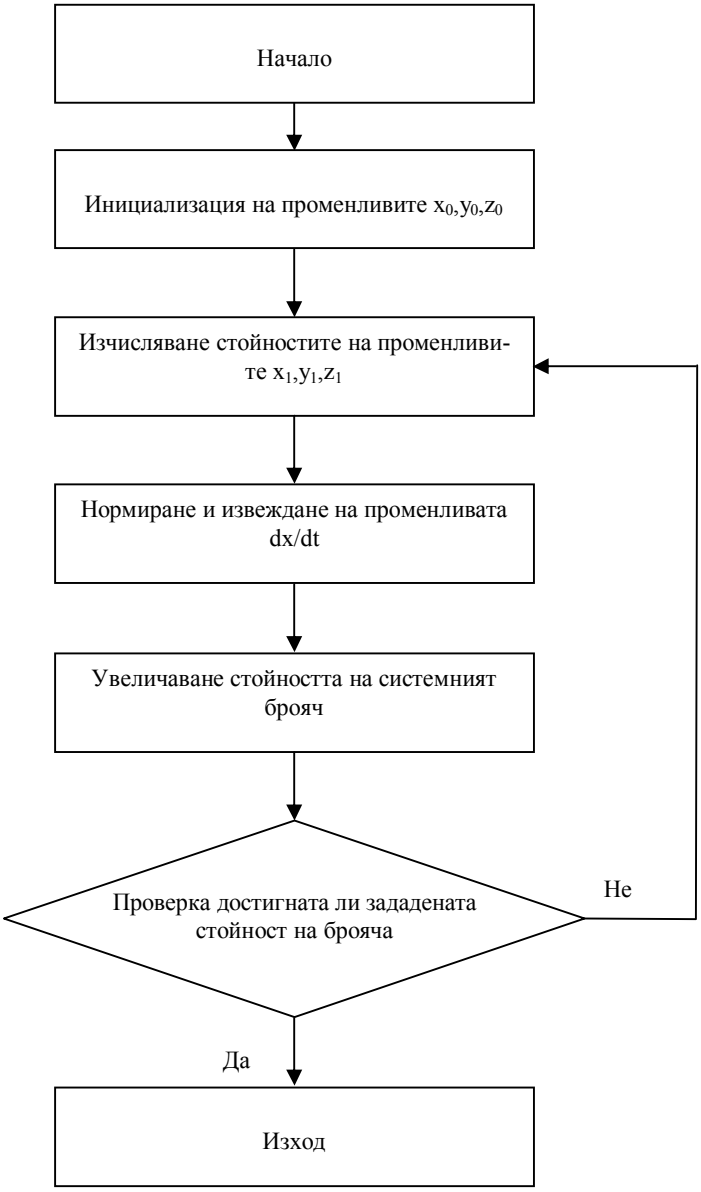
Решението на системата от уравнения (1) е извършено в Matlab използвайки вградените числови методи. Полученото решение на системата е записано като функция на Matlab която е използвана реализацията на хардуерната система. Получените резултатите са представени в (2) и са верифицирани и са аналогични с представените в [4,5].

$$\begin{aligned} x_1 &= x_0 + a(-x_0 + y_0)dt \\ y_1 &= y_0 + (b.x_0 - z_0.x_0)dt \qquad (2) \\ z_1 &= z_0 + (-c.z_0 + x_0.y_0)dt \end{aligned}$$

Началните условия и коефициентите с който са направени тестовете са аналогични на апробираните в [1,2,3].

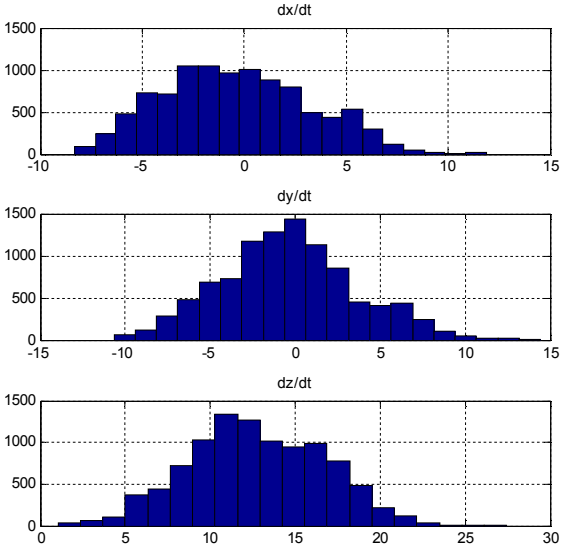
Проведените тестове показах, че при едни и същи изходни условия резултатите от изследването са силно зависими от типа променлива с която се изчисляват параметрите x, y и z. С цел получаване на максимална точност при реализацията на алгоритъма и редуциране грешката от закръгленията при хардуерната реализация на алгоритъма се използват променливи от тип double

Хардуерната реализация на генератора е възможно да се опише с блоковата схема на фиг. 1.


Начало
Инициализация на променливите x_0,y_0,z_0
Изчисляване стойностите на променливите x_1,y_1,z_1
Нормиране и извеждане на променливата dx/dt
Увеличаване стойността на системният брояч
Проверка достигната ли зададената стойност на брояча
Не
Да
Изход

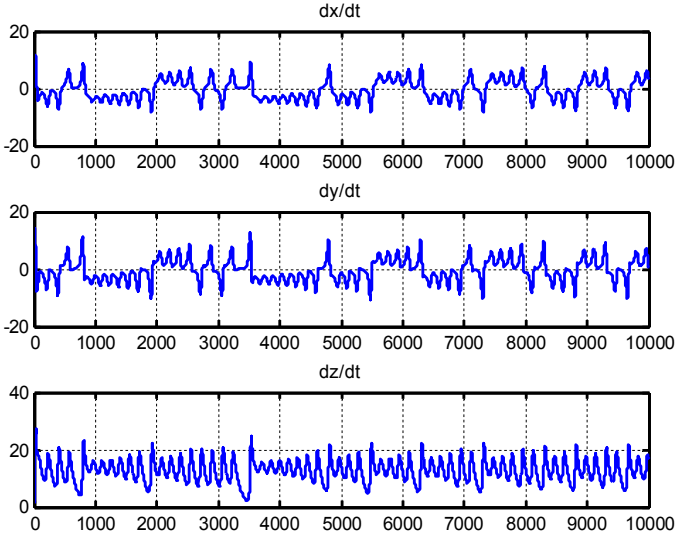
фиг. 1

На фигура 2 са представени хистограмите на получените изходни поредици dx/dt, dy/dt и dz/dt.



фиг.2

Закона по който се изменят стойностите на изходните поредици е представен на фигура 3.



фиг.3

Хардуерна реализация на предложеният алгоритъм.

За да се оцени реалната изчислителна сложност на алгоритъмът и неговата реална скорост на работа, същият е интегриран в сигнален процесор на фирма Microchip - dsPIC 30F4011, работещ с тактова честота 40 MHz /външен кварцов генератор на 10 MHz и вътрешно умножение/. Използвана е средата за програмиране е MPLAB, C-30. Максимална производителността на избраният сигнален процесор е 30 MIPS. В таблица 1 са резултатите от направената хардуерна реализация на посоченият алгоритъм. Тестовете се проведоха при включен и изключен модул за серийна комуникация.

Таблица 3

	Време за генериране на бит с включен RS-232 (9600 bp/s)	Време за генериране на бит в инструкционни цикли /с включен RS-232 (9600 bp/s)	Време за генериране на бит в сек. [s] /без включен RS-232	Време за генериране на бит в инструкционни цикли /без включен RS-232
Генериране на бит	2,83 [mS]	28324	2,44 [mS]	24365

Заключение

1. Проведеното софтуерно моделиране позволява да се оценка реалната производителност и приложимост на предложеният в [1,2,3] алгоритъм.

2. Направените тестове и хардуерен модел позволява да се проведат статистическите тестове на получените поредици.

3. Реализирането на алгоритми използващи атрактор на Лоренц налага използването на данни от тип double, което не позволява да се реализира ускорените алгоритми вградени в сигналният процесор.

Литература

[1] Alvarez G., Li S., Breaking network security based on synchronized chaos, (2004) Computer Communications, 27 (16), pp. 1679-1681.

[2] Kanso, A., Search-based Chaotic Pseudorandom Bit Generator, International Journal of Bifurcation and Chaos (IJBC) in Applied Sciences and Engineering, Volume: 19, Issue: 12(2009) pp. 4227-4235

[3] Kanso, A., Self-shrinking chaotic stream ciphers, Communications in Nonlinear Science and Numerical Simulation, Volume 16, Issue 2, February 2011, Pages 822-836

[4] Marco, A., Martinez, A. Bruno, O., Fast, Parallel and Secure Cryptography Algorithm Using Lorenz's Attractor, International Journal of Modern Physics C, Volume 21, Issue 03, pp. 365-382 (2010)

[5] http://paulbourke.net/fractals/lorenz/

ЗА ЗАЩИТАТА НА ЖУРНАЛИСТИТЕ ПО ВРЕМЕ НА ВЪОРЪЖЕН КОНФЛИКТ*

Христина И. Братанова

Национален военен университет "Васил Левски", Факултет "Общовойскови"

ON THE PROTECTION OF JOURNALISTS DURING AN ARMED CONFLICT

Hristina I. Bratanova

Abstract: Examination of the regulations of the International Humanitarian Law that govern the activities of journalists under the circumstances of an armed conflict.

Key words: Journalist, International Humanitarian Law, civilians

В наши дни конфликтите от различни точки на земята привличат вниманието на най-разнообразни средства за масово осведомяване от всички краища на планетата. На практика всеки журналист рискува да се окаже на място, където се водят военни действия или има безредици, извънредно положение, напрежение. Безпристрастните правдиви репортажи предизвикват широк обществен интерес и в ерата на информацията могат да изиграят решаваща роля за изхода на въоръжения конфликт. Опитите да се попречи на журналистите да изпълняват професионалните си задачи по време на конфликт се случват много често и по най-различни начини – от забрана на достъпа до определени райони, въвеждане на цензура и незаконно задържане под стража до преки нападения на представителите на пресата. Оказвайки се в зона на военни действия или екстремални условия, често журналистът не знае какво трябва да прави, как да се държи, каква помощ може да окаже на хората и на самия себе си, какви са възможностите му да съдейства на пленници, бежанци или колеги.

Във всички случаи от знанието и поведението на журналиста може да зависи не само обективното осветляване на дадена ситуация, не само навременното предаване на информация, но и собствения му живот. Това налага всеки професионален репортер да има най-обща представа за правилата, които се прилагат по време на въоръжени конфликти.[1]

Положението на журналистите в условията на война е предмет на обсъждане и внимание от много конференции и документи, отнасящи се до правото на въоръжения конфликт. Още в чл. 13 на Приложението към Хагската конвенция за законите и обичаите на войната от 1907 г.[2], както и в Женевската конвенция от 1929 г. за военнопленниците (Раздел VII, чл. 81)[3], става дума за "кореспонденти на

* Докладът е изнесен в секция "Държава и сигурност"

вестници" и "репортери". В тези документи журналистът се отнася към неясно определената категория лица, които следват военните сили, без да влизат в личния им състав. Като представители на тази група лица журналистите имат право, в случай на залавяне, на същото отношение, както военнопленниците, макар да съхраняват статута си на граждански лица. Но трябва да е изпълнено най-важното условие – те трябва да имат удостоверение, издадено от военните власти на армията, която следват (съпровождат).

След Втората световна война ООН предлага да се установи определено положение за защита на журналистите. В частност, ООН предлага да се направят специални опознавателни знаци за журналистите, да се въведе определен отчет чрез база данни, да се създаде международна организация, която би могла да регулира изпращането на журналистите в различни "горещи точки". Обаче самите журналисти и техните международни организации се обявяват против инициативата на ООН. Една от причините е опасението, че подобна защита би могла да бъде инструмент за оказване на натиск над журналистите и да възпрепятства тяхната професионална работа в зоната на въоръжените конфликти. Тези опасения не са били неоснователни, доколкото много примери на международно ниво потвърждават наличието на опити да не се допускат журналисти да осветлят един или друг проблем, свързан с въоръжените конфликти.

Журналистите, освен това, смятали, че специалните опознавателни знаци, предлагани от ООН, биха имали обратно действие, тъй като биха привлекли вниманието на снайперистите или на определени сили, които се стремят да унищожат на първо място именно журналистите. И в това имало определен резон. Така специална защита за журналистите не била приета и днес защитата им в зоната на въоръжения конфликт се предоставя от нормите на международното хуманитарно право (МХП).

По времето на преразглеждането на МХП след Втората световна война, в резултат на което се приемат Женевските конвенции от 1949 г., идеята за защита на журналистите намира своето въплъщение в Третата Женевска конвенция за третирането на военнопленниците (ЖК III). Съгласно тази конвенция (чл. 4А, т. 4) военните кореспонденти, които придружават въоръжените сили, без да се числят в личния им състав, попаднали във властта на противника, се явяват военнопленници. Те са длъжни да имат карта за самоличност, издадена от същите въоръжени сили.[4]

Общото в документите от 1907 г., 1929 г. и 1949 г. е, че журналистите са свързани по определен начин с военните, но не влизат в структурата на въоръжените сили.

Въпросът за подобряване на защитата на журналистите по време на опасни командировки дълго време след 1949 г. не слиза от дневния ред. С този въпрос се занимават Генералната Асамблея на ООН, Икономическият и социалният съвет на ООН, Комисията по правата на човека. Когато се свиква Дипломатическата конференция през 1974 г. и се приемат през 1977 г. двата Допълнителни протокола към Женевските конвенции от 1949 г., този процес завършва.

Член 79 (т. 1, 2, 3) на Първия Допълнителен протокол от 1977 г. (ДП I) - "Мерки за защита на журналисти" - гласи: "Журналисти, които изпълняват задачи в райони на въоръжени конфликти, ще бъдат считани за граждански лица по смисъла на чл. 50, т. 1. Те ще бъдат закриляни като такива в съответствие с конвенциите и

този протокол, ако те извършват никакви действия, съвместими със статута им на граждански лица и без да се нарушава правото на военните кореспонденти, акредитирани към въоръжените сили, съгласно статута им, предвиден в чл. 4 А (4) на Третата конвенция. Те могат да получат карта за самоличност, подобна на образеца в Приложение II на този протокол. Тази карта, издадена от правителството на държавата, чийто гражданин е журналистът или на чиято територия той живее постоянно, или където се намира информационната агенция, в която той работи, ще удостоверява неговия статут на журналист."[5]

Както се вижда от чл. 79 на ДП I, особен статут за гражданските журналисти не се предвижда. Те се ползват със защита в същата степен, както и всички останали граждански лица. Важно е да се подчертае, че те могат да загубят правото на такава защита след като вземат оръжие и участват в бойните действия (чл. 51, т. 3 на ДП I), т.е. всяко непосредствено участие във военни действия лишава журналиста от неговата неприкосновеност. Но при това положение той не получава "автоматично" статут на комбатант. А само комбатантите, съгласно МХП, имат право да използват оръжие в случай на въоръжен конфликт (за да бъде признат за комбатант човек трябва да съблюдава редица условия, залегнали в Женевските конвенции от 1949 г. и Допълнителните протоколи от 1977 г., в частност открито носене на оръжие, носене на униформа или ясно видим от разстояние отличителен знак, да се подчинява на отговорно командване и пр. - чл. 43, 44 на ДП I). Гражданските лица, към които се отнасят и болшинството журналисти, нямат право да воюват и ако направят това поведението им може да бъде признато за вероломство, т.е. за престъпление. Използването от страна на журналистите на оръжие може да бъде признато и като нарушение на професионалната етика.

Що се отнася до сътрудниците на военните пресслужби или други армейски подразделения, изпълняващи информационни функции, то те, разбира се, споделят участта на останалите комбатанти. Така че за военните кореспонденти, акредитирани към въоръжените сили, се запазва тяхното положение, признато от чл. 4А, т. 4 на ЖК III.

Удостоверението на журналиста, намиращ се в опасна командировка, съгласно образеца в Приложенията към ЖК III и ДП I, се смята за общопризнат международен документ и позволява да се идентифицира личността му в зоната на въоръжения конфликт. Международните хуманитарни организации препоръчват на журналистите преди да се отправят към такава зона да оформят въпросното удостоверение, което може да се получи от различни организации, за да се знае, че това е именно журналист, а не шпионин или разузнавач.

Но журналистът не губи правото на защита даже ако няма у себе си такова удостоверение, което, разбира се, би предизвикало сериозни подозрения у военните и може да доведе до неприятни последствия.

До такива последствия може да се стигне и при придвижване на журналисти с военна техника, предоставена от командири на подразделения, в чиито райони те се намират. Но машината, в която е настанен журналистът, може да попадне в засада и никой не би разбрал дали в нея е имало военнослужещ или журналист, който може да бъде убит заедно с другите комбатанти. При това придвижване журналистът не губи правото на защита като гражданско лице, но рискува да се окаже "съпътстваща жертва" при нападение на законна военна цел. Т.е. той няма да може да се ползва от защитата, на която има право, ако дадено формирование

стане обект на нападение от страна на противника.

Същото може да се случи и когато журналистът е твърде близо до военни обекти (командни пунктове, складове с боеприпаси, артилерийски системи и пр.) или ако следва въоръжените формирования на твърде близко разстояние. При тези обстоятелства той действа на свой риск.

До неприятни последици може да доведе и желанието на журналиста да използва военна униформа. От гледна точка на международното право това би дало повод журналистът да се приеме за военнослужещ с всички произтичащи от това последствия.

Изводът е, че журналистът може да загуби не правото на защита, която има в съответствие със своя статус на гражданско лице, а фактически предоставената му защита.

По принцип редакциите на средствата за масова информация (СМИ), телевизионните центрове и радиостанциите не се смятат за военни обекти. Нападението над тях е забранено, даже ако те се използват за целите на пропагандата (например, призовават народа да се вдигне на борба с агресора или изобличават жестокостите на врага). Тази забрана може да престане да действа в два случая: На първо място, ако СМИ се използват за военни цели. Например, ако в телевизионния център или радиоцентъра са разположени команден пункт, огнева точка и пр. или СМИ служат за предаване на информация от военен характер (такъв център в Сърбия бил включен към военна мрежа К3 - командване, контрол, комуникация - което дава основание на Международния трибунал за бивша Югославия да оправдае унищожаването му от самолети на НАТО през 1999 г.).

На второ място, офис на СМИ може да се превърне в законна военна цел, ако се използва за подстрекателство към извършване на сериозни нарушения на МХП, актове на насилие или геноцид.

Въпреки това практиката показва, че и журналисти, и редакции на СМИ нерядко стават обекти на незаконни военни нападения или случайни жертви. Във всички случаи работата на хората в офисите и сградите на подобни центрове в зоните на въоръжени конфликти е достатъчно опасна, както, въобще, работата на журналистите в "горещите точки".

Журналистите и всички, които се окажат в зоната на военни действия, могат да бъдат задържани от военните. Участта на задържания журналист зависи от много фактори, в частност от неговата националност или гражданство, наличието на документи и пр.

В отношението към журналиста, задържан от властите на собствената му страна, действат нормите на вътрешнодържавното законодателство. При това може да се твърди, че основните гаранции, предвидени в чл. 75 на ДП I (за третиране на лица във властта на участваща в конфликта страна), са приложими в случай на задържане на журналиста във връзка с въоръжен конфликт, ако нормите на вътрешното право са по-неблагоприятни по отношение на задържания.

Що се отнася до журналисти, принадлежащи към една от воюващите страни и попаднали във властта на другата, съществува различие между акредитираните военни кореспонденти, които стават военнопленници (за които стана вече дума), и "свободните" журналисти. Ако свободен журналист е задържан на територията на своята страна, т.е. на територия, окупирана от противника, той трябва да бъде задържан на тази окупирана територия (чл. 76 на ЖК IV) и не може да бъде пре-

местван на националната територия на окупиращата държава. Задържащата държава може за започне наказателно разследване срещу журналиста, ако е извършил някакво нарушение или да го интернира "по повелителни съображения за сигурност". Ако няма основание за възбуждане на дело или за интерниране, журналистът трябва да бъде освободен.[6]

По отношение на журналистите, принадлежащи към трета държава, неучастваща в конфликта, в случай на тяхно залавяне от една от воюващите страни, действат нормите на мирновременното право. Те могат да бъдат арестувани, ако задържащата държава може да им предяви обвинения. В противен случай тези журналисти трябва да бъдат освободени.[7]

Във всички посочени случаи задържащата държава е задължена да съблюдава редица конкретни норми, които обезпечават хуманно отношение по време на задържането, както и да осигури всички юридически гаранции в случай на съдебен процес. Както и другите задържани, журналистите имат право на връзка с близките си. Журналистите от държави, които не са страна в конфликта, се ползват с поддръжката на дипломатическите и консулските представителства на своята страна или, при отсъствие на дипломатически отношения, от поддръжката на трета страна, поела задължението за защита на интересите на тази държава.

Имуществото на гражданските лица (вкл. оръдията на труда на журналистите - видеокамери, фотоапарати, диктофони и пр.) трябва да се ползва със защита и уважение и без нужната военна необходимост не могат да се изземват, унищожават и пр.

Посочените по-горе норми се отнасят до международни въоръжени конфликти. В нормите на МХП, отнасящи се до вътрешните въоръжени конфликти (разгледани в общия за всички Женевски конвенции от 1949 г. чл. 3 и във Втория Допълнителен протокол към тях от 1977 г.), не е казано нищо конкретно за журналистите. Но това не значи, че журналистите, работещи в районите на немеждународни въоръжени конфликти, са лишени от правна защита. Всяко гражданско лице, в т.ч. и журналистът, трябва да се ползва с уважение и защита и не трябва да става обект на нападение.

В известна степен неопределен и двусмислен днес е статутът на т. нар. "прикомандирован", "прикрепен" журналист или "командирован към военната част журналист" **(**"embedded")[8]. Това понятие за първи път се появява по време на влизането в Ирак през 2003 г. То не фигурира все още в нито едно положение на МХП.

Ако журналисти, явяващи се граждански лица, преминат процедура по акредитация, даваща им право на преимущества при получаване на информация от военните и на особена защита от една от воюващите страни, от правна гледна точка стават военни кореспонденти. В съвременните въоръжени конфликти много работници на СМИ се отнасят към тази категория. Понякога военните власти изискват всички журналисти, работещи в зоната на дадения конфликт, да преминат подобна акредитация. Позициите по въпроса за защитата, от която се ползват те в случай на залавяне от другата воюваща страна, са различни. Например, според Ръководните принципи, регулиращи отношенията със СМИ, разработени от военното министерство на Великобритания през 2003 г., на такива журналисти трябва да се предостави статут на военнопленници. Международният комитет на Червения кръст (МКЧК) смята, че "прикомандированите" имат право на такава защита, както и другите граждански журналисти (и въобще гражданските лица). Подобно мнение

изразяват и редица автори в областта на МХП.[9]

В светлината на въоръжените конфликти в Ирак, Ливан, Афганистан и в други региони на света все по-често се изказва мисълта за необходимостта от приемане на нов международноправен акт, който би засилил защитата на журналистите и средствата за масова информация, както и професионалната журналистическа апаратура, отчитайки реалностите в съвременните въоръжени конфликти и дейността на СМИ по тяхното осветляване. Освен това подобен документ би обозначил по-точно статута на "прикомандированите" журналисти.

Все пак трябва да отбележим, че международното хуманитарно право се занимава не с проблемите за обезпечаване на свободата на словото и печата, а с въпросите за физическата защита на хората, в т.ч. и на журналистите. Казано другояче, МХП защитава не дейността на журналистите, а хората, занимаващи се с тази дейност. [10]

Документите, отнасящи се до защитата на правата на човека, гарантират свободата на словото или информацията – Всеобщата декларация за правата на човека (чл. 19) и Европейската конвенция за правата на човека (чл. 10). Но нито един документ не гарантира по време на кризисна ситуация пълното осъществяване на тази свобода. В тази област, в съответствие с вътрешнодържавното право и съгласно чл. 10, т. 2 на споменатата Европейска конвенция за правата на човека, властите могат да установят ограничения.

Важен въпрос, който е актуален днес, е за свободата на преместване на журналиста в зоната на въоръжения конфликт. Всяко командване се опитва да установи в това отношение някакви ограничения: или въвежда комендантски час, или специален пропуск, за да не може външен човек да види онова, което не биха искали да му покажат: неизбирателния характер на военните действия, нарушението на нормите на МХП, унищожението на гражданското население и други действия, за които по принцип се носи юридическа отговорност. Това усложнява работата на журналиста в зоната на конфликта, в прилагането на положенията на МХП за защитата му като гражданско лице. Много въоръжени формирования изискват от журналиста да премине през процедура на акредитация при някой щаб, политическа група или армия, с цел да се контролира неговата работа в зоната на военните действия. В тази връзка се появяват и други обвинения срещу журналистите: Чеченският конфликт, например, остави много свидетелства за най-честото обвинение по адрес на журналистите в шпионска, разузнавателна дейност.

Във връзка с прилагането на МХП изисква осветляване и въпросът за използването на съвременната техника за събиране и предаване на информация. Едва ли някой се съмнява в констатацията, че отдавна живеем в епохата на информационните и психологическите войни. Съществуват много примери, когато едно новинарско съобщение може да доведе до огромни жертви, да създаде атмосфера на паника и пр. По-съвършените средства за събиране и предаване на информация със силата на своето въздействие могат да предизвикат по-големи последици отколкото, да кажем, прилагането на обикновени оръжия. Тъй като това е съществен въпрос, вероятно той ще доведе до преразглеждане и допълване и на Женевските, и на Хагските конвенции със специални положения за регулиране на прилагането именно на информационните и психологическите средства за водене на война.

Като пример може да се посочи едно техническо изобретение, което се прилага вече, в частност от журналистите от "ВВС" – една от водещите световни информа-

ционни служби. Става дума за малка телевизионна камера, съвместена с портативна спътникова антена. Такава система позволява на оператора да води пряко телевизионно излъчване непосредствено от зоната на бойните действия, защото спътниковата антена може да бъде скрита зад всякакво естествено укритие. Човек може да си представи какъв психологически ефект може да окаже това предаване и до какви последствия да доведе.

Много специалисти днес изследват явлението, наречено "ефектът CNN". Това са преки предавания, организирани от тази компания от зоната на бойните действия (може и да са денонощни) с показване на ужасите на войната. По този начин се оказва психологическо въздействие върху политиците, които имат ограничено време, за да реагират в тежка ситуация и да вземат адекватно решение и затова могат да допуснат сериозни грешки чрез прибързани, необмислени, не съвсем правилни решения, взети под въздействието на телевизионното изображение. Във връзка с това се поставя въпросът какво значение може да окаже този ефект на бъдещето не само на отделна страна, но и на бъдещето на планетата и на характера на въоръжените конфликти. [11]

Ролята на журналистите във въоръжените конфликти е много важна. Със своите репортажи, статии или други материали те могат не само да привлекат вниманието на световната общественост към хода на военните действия, съдбата на населението, намиращо се в зоната на въоръжения конфликт, на бежанците и военнопленниците, героизма на сражаващите се, ужасите на войната, но и да спомогнат за разкриването на военни престъпления или да съдействат за тяхното предотвратяване, особено при използване на забранени видове оръжия.

В своята професионална дейност журналистът е принуден постоянно да влиза в правоотношения, свързани с получаване, събиране и разпространение на информация в екстремални ситуации. Незнанието на правата и неумението да се ползва от тях може да постави под въпрос по-нататъшната му професионална съдба и даже да доведе до трагични последици. Според МКЧК съществуващото законодателство предоставя достатъчна и реална защита за журналистите. Без съмнение тяхната работа в хода на международния или вътрешния конфликт винаги ще е свързана с риск, при това нерядко журналистите съзнателно се подлагат на опасност. Правото не винаги може да ги защити от последствията на риска, който те са избрали по собствена воля. Изменение на посочените по-горе норми засега не се очаква.

Най-сериозният проблем не е, че няма правила, а в неспособността за тяхното прилагане и системно да се разследва, наказва и преследва нарушението. Хората носят наказателна отговорност за военните престъпления, които извършват и всяка страна в конфликта трябва да уважава и съблюдава международното хуманитарно право.

Литература

1. http://www.dzyalosh.ru/03-toler/books/nasilie/2_melnik.htm;
2. http://www.zaki.ru/pagesnew.php?id=1519&page=4;
3. http://kopilka.wolfschanze.ru/genkon29.htm-;
4. Женевските конвенции от 12 август 1949 г. Допълнителните протоколи от 1977 г., Медицина и Физкултура, С., 1990, с. 84-85. Женевска конвенция III, чл. 4 А, т. 4; Приложение IV към конвенцията;
5. Женевските конвенции от 12 август 1949 г...., с. 324. Член 50 е озаглавен

"Определение за граждански лица и гражданско население";
6.http://www.icrc.org/Web/rus/siterus0.nsf/html/protection-journalists-interview-270710;
7. http://www.jurn.by.ru/zak_2.html;
8. http://www.journ.usu.ru/ucheba/uch.material/mgp-add-on.doc; На български език това понятие няма точен и еднозначно приет превод;
9.http://www.journ.usu.ru/ucheba/uch.material/mgp-add-on.doc;
http://www.icrc.org/Web/rus/siterus0.nsf/html/protection-journalists-interview-270710;
10. От 1985 г. в МКЧК работи гореща линия за журналисти, оказали се в затруднено положение (+ 4179 217 32 85). На адрес press.gva@icrc.org може да се съобщи за изчезването, раняването или арестуването на журналисти и да се поиска помощ: http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/hotline-010106;
11. http://www.library.cjes.ru/online/?a=con&b_id=362&c_id=3657.

ТРАФИКЪТ НА ХОРА И НАЦИОНАЛНАТА СИГУРНОСТ*

Сашо С. Евлогиев

Р. България, Шумен, НВУ "В. Левски", Факултет "Артилерия, ПВО и КИС", катедра "ОУТП от Полевата артилерия"

THE HUMAN TRAFFICKING AND THE IMPACT ON NATIONAL SECURITY

Sasho S. Evlogiev

***ABSTRACT**: Human trafficking is a serious problem in modern society. Unfortunately, this problem is getting bigger and harder day by day. Fundamental human rights violation in developing countries provides favorable environment for the deepening of the problem.*

***KEY WORDS**: human trafficking, human rights, people, rules.*

През последните няколко години сме свидетели на кампании, които да информират обществото за един сериозно разрастващ се проблем - трафик на хора и насилствена проституция. Голяма част от нашето общество не подозира за съществуването на това съвременно робство. Една част от световните обществени институции, организации и органи все още го отричат. Друга част го пренебрегват или омаловажават, но независимо от съпътстващите го обстоятелства това опасно явление съществува. Твърде малко хора си дават сметка, че това е социален феномен с дълбоки корени, който вече има своите пагубни последствия за цялото общество.

Република България, като част от световната демократична общност инициира и участва активно в организираните и провежданите мероприятия в световен, ев-

* Докладът е изнесен в секция "Държава и сигурност"

ропейски, регионален и национален мащаб.

Целта на организираните кампании и проекти е да се ограничи максимално трафика на хора и насилствената проституция като се активират всички съществуващи защитни механизми на съвременното демократично общество. Целесъобразно е в тези мероприятия да се включват, както държавни структури, органи и организации, така и родители и деца, които в голяма степен се явяват обект на насилствени посегателства. Необходимо е да се развърне широка образователна подготовка сред децата и младите хора за да се придобият знания как да се предпазват от въвличане във възможни престъпни схеми и как може да се съдейства на органите на министерството на вътрешните работи (МВР), министерството на правосъдието и други държавни институции в борбата с незаконния трафик на хора.

Трафикът на хора представлява тежко престъпление, често извършвано в рамките на организирана престъпна дейност, грубо нарушение на основните права и е изрично забранено съгласно Хартата на основните права на Европейския съюз (ЕС). Предотвратяването и борбата с трафика на хора е *приоритет* за Съюза и за държавите – членки [1].

В този смисъл, трафикът на хора е противозаконно явление и участващите в него носят пълната наказателна отговорност.

Трафикът на хора представлява набирането, транспортирането, прехвърлянето, укриването или приемането на хора, независимо от изразената от тях воля, чрез използване на принуда, отвличане, противозаконно лишаване от свобода, измама, злоупотреба с власт, злоупотреба с положение на зависимост или чрез даване, получаване или обещаване на облаги, за да се получи съгласието на лице, упражняващо контрол върху друго лице, когато се извършва с цел експлоатация [2].

Анализът на посочената дефиниция показва, че се открояват два основни момента. От една страна, "трафика на хора" се осъществява независимо от изразената воля на лицата, участващи в "трафика", т.е. независимо какво е желанието на дадения човек той се заставя да изпълнява желанието на трафикантите чрез използване на различни методи на принуда и/или измама. От друга страна, трафикантите използват различни похвати за да получат съгласието на лицата за извършване на определена дейност с цел експлоатация.

Жертвите на трафика на хора могат да бъдат продавани, лъгани, насилвани или подмамвани и въвличани в ситуации, от които не могат да избягат. Много от тях са принуждавани да работят в секс - индустрията като проституиращи или в порнографския бизнес. Други са примамвани да напуснат доброволно страната си с обещания и надежда за по-добър живот, но завършват в ситуации, където здравето, психиката и физическата им безопасност са силно застрашени. Използвайки факта, че жертвите са в чужда страна те са малтретирани и експлоатирани жестоко.

Експлоатацията е противозаконно използване на хора за секс, за отнемане на телесни органи, за осъществяване на принудителен труд, за поставяне в робство или в положение сходно с робството. Голяма част от „трафика на хора" заема „трафика на жени".

Според международни и европейски експерти понятието "трафик на жени" означава всички дейности, свързани с набирането или транспортирането на жени в границите на дадена страна или отвъд територията й с цел извършване на работа или услуги, придружени от насилие, заплаха за насилие, унижение, финансова зависимост, измама или друга форма на ограничаване.

Трафикът на хора е световен проблем, защото представлява интернационален, печеливш, престъпен бизнес.

Според данни на Организацията на Обединените нации (ООН) трафика на хора засяга 4 милиона души по света, като 300 000 жени са от страните от Източна Европа. Незаконните приходи от този бизнес са оценени на 3 милиарда долара годишно.

Всяка година около 800 000 души са жертви на трафик, а 90% от тях са жени и момичета. Мнозинството от тях стават обект на сексуална експлоатация. Проблемът е световен, но той е особено голям на Балканите, защото има и своя сериозен социално-икономически аспект.

Гръцкият всекидневник Kathimerini съобщава, че жертвите на човешки трафик в Гърция са нараснали и са около 25 000 души . Това са предимно жени, използвани за проституция, които са докарвани от престъпни групи от Албания, България, Румъния, Молдова и Русия. Данните на гръцкото министерство на обществения ред показват също, че броят на гръцките мъже, ползващи услугите на тези проститутки е нараснал с 600 % след началото на 90-те години.

За България това е криза на ценностите, криза в образованието и промяна в представата за успеха и за оцеляването. Данните сочат, че около 10 000 български момичета по целия свят насилствено са принудени да проституират [3].

Във въображаемото им търсене на щастие не съществува нищо, което би ги задържало по родните им места. Момичетата лесно се доверяват на подозрителни работодатели, но в момента, в който напуснат пределите на страната ни, те се превръщат в стока, която търговците на плът купуват и продават единствено с цел печалба. Момичетата се търгуват от 3 до 8 хиляди долара в зависимост от „качеството". Много често те са крити за няколко дни на тайно място, където са държани гладни, където ги бият, изнасилват и тормозят. Превърнати вече в играчка в ръцете на притежателите си, момичетата трябва да работят по 20 часа на ден и да водят мизерен живот изпълнен с безкраен страх. Ако някоя от тях реши да се защити, тя бива публично наказвана за назидание на останалите. В повечето случаи момичетата са така изплашени от заплахите на сводниците, че дори не смеят да потърсят помощ от полицията. Те нямат паспорти. Сводниците ги вземат, за да изнудват след това момичетата с това, че са нарушили закона и че ако отидат в полицията, положението им ще стане още по-лошо. Реинтеграцията на момичета, успели да се изплъзнат от този омагьосан кръг и да се върнат в света, от който са били отвлечени, е трудна. Те са опетнени и повечето хора смятат, че ситуацията, в която са попаднали, е изцяло по тяхна вина.

Често емоционалният свят на жертвите до такава степен е разрушен, че те се чувстват неспособни да се справят с предизвикателствата на ежедневието им. Звучи абсурдно, но в много от тези случаи момичетата се връщат към проституция, защото никой и нищо не може да им помогне да преодолеят този труден период на промяна в техния живот.

Жените биват препродавани между 3 и 6 пъти, като 55 % от тях са жестоко бити и изнасилвани от трафикантите. Средната им възраст е 21 години. Една проститутка печели между 321 и 642 долара на нощ, което означава, че тя има 10-15 клиента. Годишно, една проститутка заработва за своя господар от 96300 до 160500 долара. С тези пари тя издържа себе си и семейството си в родната си страна. „Вносната" проституция във Франция (включително и от България) е описана в

доклад на парламентарната комисия, който по-късно става основа за приемането на закон против робството на нашето съвремие. Този закон дава шанс на проститутките да се изплъзнат от мрежите на мафията.

Какви са данните за „трафика на хора" за Република България през 2009 година?

Жертви на трафик на хора за периода 01.01.2009 – 31.08.2009 г.

Характеристика	Брой лица
Общо жертви	137
Жени	122
Мъже	15
Непълнолетни	20
Бременни жени	4

Анализът на посочените в таблицата данни показва, че:

- 89 % от жертвите на трафик са жени и само 11 % - мъже;
- 14,6 % от жертвите на трафик са непълнолетни, а 2,9 % - бременни жени.

Видно е, че трафикантите се стремят да въвличат в престъпната схема здрави и работоспособни жени, които могат да бъдат експлоатирани максимално за да се извлекат по-големи печалби. В „трафика" могат да бъдат включени и непълнолетни или бременни жени, но само по изключение или при особени обстоятелства.

Как се разпределят лицата, жертви на трафика на хора според спецификата на извършвания труд?

Характеристика	Брой лица
Общо жертви	137
Жени, използвани за:	118
- сексуална експлоатация	106
- принудителен труд	12
Мъже, използвани за:	15
- сексуална експлоатация	1
- принудителен труд	14
Непълнолетни (всички са жени)	20
- сексуална експлоатация	18
- принудителен труд	2
Бременни жени	4

Анализът на посочените данни показва, че за сексуална експлоатация се използват 90 % от жените и 6,7 % от мъжете; за принудителен труд се използват 10 % от жените и 93 % от мъжете;

Трафикът на хора не се прилага само към възрастни и голяма част от него представлява трафик на деца. По смисъла на закона "дете" е всяко физическо лице до навършването на 18 години. Децата са по-уязвими от възрастните и следователно съществува по-голям риск те да станат жертви на трафика на хора. Трафикът на деца се състои от всички действия, включващи или насочени за транспортирането

на деца в страната или през граница, чрез измама, принуда и насилие, заробване, поставяне на децата в ситуации на злоупотреба или експлоатация, като насилствена проституция, робски практики, побой, или извънредна жестокост, непосилен труд или експлоатационен домашен труд.

Защо се задълбочава проблема с „трафика на хора"?

От една страна, световната икономическа криза и непрекъснато увеличаващата се безработица и евтината работна ръка на пазара на труда в слабо развитите икономически страни и от друга – търсенето на човешка плът на черния пазар са причините, които стимулират разрастването на този световен проблем, като география и като брой на участващите в него лица.

Какви са основните стъпки, които използват трафикантите при манипулиране на жертвите?

Първо, жестоко насилие, което се състои предимно в изнасилване, бой, изтезания, глад. Целта на тези действия е жертвата да се постави в екстремални условия за оцеляване. Атакува се психичния защитен механизъм на човека, който се състои във вярата, че светът около нас може да бъде контролиран. Когато проблемът за смъртта от просто екзистенциален въпрос стане дотолкова личен, че единственото, за което можеш да мислиш е как да оцелееш, тогава, както при високо напрежение, бушонът изгаря, за да предпази от изгаряне цялата инсталация, така и човек "изключва" в такива ситуации на опасност и спира да мисли в името на една единствена цел – физическо оцеляване.

Второ, физическо изтощение, което включва система от манипулации с цел да се лиши лицето от каквато и да е почивка. При тези обстоятелства жертвата няма никаква възможност да остане насаме със себе си, да осмисли възникналите обстоятелства, да анализира своите действия и действията на своите противници, да се възстанови физически и психически и да набележи действия за своята защита. Двадесет часовия работен ден носи големи печалби, но по-важното в конкретния случай е обстоятелството, че продължителният и изтощителен работен ден е важен и за "пречупването" на психиката на жертвата.

Трето, пълен контрол и изолация, което изцяло изолира жертвата от външния свят. Жертват се лишава от физическата възможност да общува с други хора освен с насилника и строго се следи. Повечето от жертвите на трафик обикновено живеят там, където работят. Човек не може да потисне своята потребност от комуникация, но общувайки само с насилника той започва да получава изкривена информация за света и за обкръжаващата го действителност. Единственото послание, което жертвата трябва да възприеме след продължителното физическо и психическо въздействие е следното: "Животът ти не е ценен, ти не струваш нищо!".

В голямата част от случаите на жертвата се внушава чувството за вина. Например, жертвата е виновна, защото "дължи пари", тъй като е "купена" от продавача и трябва да се издължи. Естествено жертвата не може да се изплати и бива продадена на следващия трафикант /сутеньор/. Системата с продажбата е много важна, защото въвежда идеята, че жертвата е стока, роб, който е лишен от основни човешки права, като правото на свобода.

На жертвата се внушава упорито, че тя не е човек като другите и се затвърждава представата, че единствения възможен свят е този, в който живее – свят на насилие и контрол. Всички трафиканти са възприели да работят по един "стандарт". Постоянният тормоз се прекъсва с малки жестове на внимание, с което се цели

привързването на жертвата към нейния насилник. Това почти винаги успява и жертвата постепенно свиква с отредената й роля и със своя господар.

Важно е не само да се разглежда проблема с трафика на хора, но и да се разкрият причините за това явление. Поради това е необходимо да се намери отговор на въпроса: *Защо хората попадат в трафик?*

Причините, които може да се посочат са много, но най-общо те могат да се систематизират в три основни групи, като:

- *Политически,* които предизвикват силно изостряне на междудържавните отношения и невъзможност за постигане на мирно развитие на отношенията, ескалиране на голямо напрежение и избухване на локални войни или конфликти. В резултат на локалните войни или конфликти се създават условия за нарастване на международната организирана престъпност, а реакцията на местното население в застрашените региони се изразява в мощна бежанска вълна, насочена към съседни незастрашени от конфликта (локалната война) страни. Възможно е получаването на бежанска вълна при създаване на напрежение в определени региони в резултат на неспазването на международните правни норми и/или закони от вътрешното законодателство на определена страна, противоречащи на международните. Такива закони могат да разпалват противоречия на етническа, религиозна, расова или друг вид омраза.

- *Икономически* – те се явяват основа на трафика на хора и най-често се изразяват в тежко материално състояние и невъзможност за осигуряване на елементарния човешки минимум от храна, отопление, осветление, дрехи и хигиена. Характеристиката на тази група причини е степента на бедност на хората. До голяма степен масовото обедняване на хора беше констатирано при разпадането на социалистическата икономическа система поради това, че старата система беше разрушена, но нова не беше изградена. Нещо повече, нямаше приет дори модел на новата система в икономиката, селското стопанство, туризма и в другите сфери на икономическия живот, която да замени старата. При това се очерта тенденция за феминизиране на бедността, по-ярко изразена е в малките населени места, планинските и полупланински райони, в региони, където растениевъдството и животновъдството са се развивали приоритетно през годините на социализма.

- *Социално-културни* - включва ниска грамотност и следователно ограничени образователни възможности за работа, патриархален тип семейство, расова и етническа дискриминация, влияние на медиите и Интернет.

Какъв вид може да бъде трафика на хора?

Хората могат да станат жертва, както на вътрешен трафик – трафик в страната, така и на външен, т.е трафик извън територията на страната, който се извършва чрез извеждане през граница и обикновено продължава в друга страна, за да се избегне издирването, проследяването и възстановяването на лицата, жертви на „трафика". В широк смисъл „трафика на хора" може да се разглежда като система за поставяне на лица във финансова зависимост. Хората са насилвани, продавани или подлъгани в чужда страна като доброволни емигранти чрез измама. Предлага им се работа като детегледачки, прислужници, стюардеси, икономи, компаньонки, секретарки и др. Когато става дума за истински трафик, човекът, отишъл да работи в чужбина е натрупал "дълг" към трафиканта, който ще трябва да плати по един или друг начин.

Основните области, в които хората, жертви на „трафик" работят в чужбина при

условия близки до робство или изцяло пленнически са: земеделие, индустрия, домакинство или насилствена проституция.

Каква е връзката между „трафика на хора" и националната сигурност?

От изложеното по-горе е видно, че трафика на хора е съвременна форма на робство. Трафикът на хора е тежко престъпление и сериозно нарушение на основните права на човека. По данни на Съвета на Европа (COE.int) трафикът на хора е третият по големина източник на приходи за организираната престъпност и е най-бързо разрастващата се престъпна дейност в сравнение с другите форми на организирана престъпност в ЕС.

Според доклад на Държавния департамент на САЩ, озаглавен „Трафик на хора 2005 г.", всяка година жертва на трафика на хора в света стават между 600 000 и 800 000 души, 80 %, от които са жени и момичета.

Групировките за трафик на хора в страната са отделно обособени. Трябва да се има предвид, че връзките и възможностите, с които разполагат, довеждат до определен тип „диверсификация", и.к. работят по всички видове контрабанда с изключение на оръжие. Тази престъпна дейност е сравнително нова, поради което за разлика от наркотрафика и разпространението на наркотици монополът и районирането все още са въпрос на близко бъдеще.

За съжаление, няколко от действащи канали за трафик на хора преминават през България и се явяват сериозна заплаха за националната сигурност. Основните канали за трафик на хора са:

- *Индийският канал* - един от подходите да се вкарат в страната индийски младежи под предлог, че учат, като ги снабдяват с различни видове документи – студентски книжки, удостоверения и др. Съществуват основателни подозрения, че представяните като индийци младежи са кюрди. Външният им вид и документите им не позволяват това да бъде надеждно установено. Според експерти тези лица организират транзитен трафик на хора от Турция през нашата страна за Западна Европа – предимно за Франция, Испания, Португалия. Тарифата е около 10 000 щатски долара на човек. Според експерти от Главна дирекция "Гранична полиция" организаторите разполагат с връзки и в служба "Задгранични паспорти" и успяват да доставят оригинални лични карти за чужденци, както и на аерогара София успяват да уредят пускането на лица с нередовни документи.

Пакистанският канал - организира трафик през аерогара София и от Турция през ГКПП Капитан Андреево с хладилни камиони, обикновени камиони с тайници, както и през зелена граница. Обикновено хората, които обслужва, имат проблеми с правосъдието. Успява да ги прехвърли в Англия, където има големи пакистански общности и лесно могат да укрият и легализират пребиваването си.

Африканският канал – организацията му се състои в преминаването на зелена граница с помощна на местни хора – погранични жители от Турция и Гърция. Афганистанският канал организира всякаква контрабанда – на хора, оръжие и наркотици. Използва специални тайници в камионите си или укрива хората в килими и рогозки, направени в Афганистан. Разполага с необходимите връзки сред гранични полицаи и митничари, така че работи в условия на минимален риск.

За *Китайският канал* се предполага, че организацията му е дело на триадите. Той се ограничава в подпомагане на китайци да бъдат трансферирани и заселени в България и страни от ЕС [4].

Проблемът с трафика на хора е изключително сериозен тъй като представлява

търговия с човешки същества. Престъпниците използват своите жертви за да печелят незаконно пари. Те заставят хората да проституира, да просят, да работят при опасни и унизителни условия на труд. Решаването или ограничаването на неговото разпространение изисква усилия на ЕС и всички държави - членки на Съюза за изготвянето и приемането на Единен план за действие за превенция и борба с тази престъпна дейност.

Литература:
1. Директива 2011/36/ ЕС на Европейския парламент на Съвета.
2. Закон за борбата с трафика на хора, ДВ, бр. 74, С., 2009.
3. Н. Михайлова, „Трафикът на жени – правни и институционални механизми за противодействие". С., 2010.
4. www.unodc.org/trafficing human beinqs.html

Българска. Издание първо. Тираж 60

Предпечатна подготовка във факултет “Артилерия, ПВО и КИС” - Шумен