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 2

ЗАЩИТАТА НА ИНФОРМАЦИЯТА - СЪСТОЯНИЕ И ПЕРСПЕКТИВИ

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2012

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Защитата на информацията – състояние и перспективи", проведена във Факултет "Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Националния военен университет "Васил Левски" - гр. Шумен, на 7 и 8 юни 2012 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.

Съгласно чл. 31 от Закона за защита на класифицираната информация авторите сами определят грифа на докладите си и носят лична отговорност за публикуване на класифицирана информация в тях.

От редакционната колегия

Редакционна колегия:
полк. инж. доц. д-р Нелко Петров Ненов – председател;
проф. двн Манол Петков Млеченков,
доц. д-р Жанета Николова Савова-Ташева - членове;
Светлана Маркова Зотова, Христо Пеев Христов - сътрудници

Рецензенти:
полк. инж. доц. д-р Нелко Петров Ненов
подп. инж. доц. д-р Андрей Илиев Богданов;
проф. д.в.н. Манол Петков Млеченков;
доц. д-р инж. Жанета Николова Савова-Ташева

©НВУ "В. Левски" – Факултет "Артилерия, ПВО и КИС"
Шумен, 2012.
c/o Jusautor, Shumen

ISBN 978-954-9681-49-9

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ

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 и господа,

От името на ръководството и академичната общност на Националния военен университет „Васил Левски", Факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи" Ви приветствам с *добре дошли* на научната конференция, провеждаща се тази година под надслов „Защитата на информацията – състояние и перспективи".

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

Целта, която си поставяме, е обмен на експертни знания и опит в областта на защитата на информацията.

С удоволствие искам да отбележа участието в настоящия форум на председателя на Комисията за защита на личните данни – г-жа Венета Шопова, разбира се - на директора на Дирекция „Сигурност на информацията" в Министерството на отбраната полк. Иван Иванов. За съжаление поради заболяване в последния момент не можа да пристигне нашият добър приятел и съмишленик директорът на Дирекция „Вътрешна сигурност" в ДКСИ г-н Димитър Гуцалски. Тук са комисар Любомир Христов - директор на Областна дирекция на МВР; г-н Стоян Тонев – директор на Териториална дирекция „Национална сигурност"; г-н Йордан Първанов - главен експерт в Център за реакция при инциденти във връзка с информационната сигурност в Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" на Министерството на транспорта, информационните технологии и съобщенията; г-н Диян Гатев от Главна дирекция „Борба с организираната престъпност" на МВР; капитан първи ранг Петър Петров - служител по сигурността на информацията на ВМС; подполковник Владимир Цанков – началник на Център за документално осигуряване на Командването на Сухопътните войски; служители по сигурността на информацията в областните управи в Шумен, Разград, Русе и Добрич; преподаватели, студенти и докторанти от висши училища и други експерти.

Очакваме всички научни доклади, съобщения и презентации 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.

През последните години у нас се работи по обединяването на усилията на всички структури, имащи отношение към киберсигурността, по изграждането на национален орган по киберсигурност и по правно-нормативна база за неговата работа.

Киберсигурността на критичната комуникационна и информационна инфраструктура на страните членки е основна приоритетна задача за НАТО и Европейския

съюз и в тази връзка постигането на оперативни способности в кратки срокове е важен елемент в решаването на тази задача. Вече стана ясно, че междуведомствена работна група по проблемите на кибернетичната защита, сформирана със заповед на министър-председателя, ще предложи състав, правомощия, мисия, функции и задачи на националния орган. Това обяви г-жа Августина Цветкова, заместник-министър на отбраната, по време нарегионална конференция по киберсигурност и киберпрестъпност за държавите от Югоизточна Европа. Националният надведомствен орган ще координира и консолидира усилията на държавните структури по разработването на национална стратегия за киберсигурност**,** която ще обхваща както обществените мрежи, така и мрежите за класифицирана информация. Създаването на такъв орган се обуславя преди всичко от необходимостта да бъдат координирани действията на всички ведомства, както и да бъде приложен всеобхватен системен подход за решаването на проблемите, свързани с киберзащитата в нашата страна. Ще бъде предложено на Националния орган по киберсигурност да бъдат делегирани правомощия за вземане на решения за управление и реагиране при компютърни инциденти у нас, изразяване на национална позиция и взаимодействие с органите на НАТО и Европейския съюз за кибернетична защита и за планиране изграждането на национален център за реагиране при компютърни инциденти в критичната информационна инфраструктура на България (за това е необходимо надграждане на Правителствения център за реагиране на инциденти в компютърната сигурност CERT).

Тук е важно да отбележим, че работната група е създадена по инициатива на Министерството на отбраната, като в нея участват не само представители на военното ведомство, но и на Министерството на вътрешните работи, Министерството на външните работи, Министерството на транспорта, информационните технологии и съобщенията, Министерството на правосъдието, Държавната комисия по сигурността на информацията, Държавната агенция „Национална сигурност" и Националната лаборатория по компютърна вирусология към Българската академия на науките.

Госпожи и господа,

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 *сигурност* и по-конкретно в направление на информационната сигурност.

Ето защо и тази година направихме необходимото за подготовката и организацията на конференцията по проблемите на информационната сигурност, която се превръща в добра традиция и печели все по-голяма популярност и престиж сред експертите в сектора.

С гордост можем да отбележим факта, че през тази година Националният военен университет „Васил Левски" получи от Националната агенция за оценяване и акредитация за втори пореден път максимална оценка на обучението по специалности от професионално направление „Национална сигурност", включително и по специалност „Административна и информационна сигурност", по която Факултетът в Шумен провежда обучение в образователно-квалификационна степен „бакалавър" и „магистър", както и в образователна и научна степен „доктор".

До сега при нас успешно се дипломираха 60 студенти по специалност „Административна и информационна сигурност" в образователно-квалификационна степен „бакалавър" и „магистър".

В настоящия момент се обучават по същата специалност 206 студенти бакалаври и 15 студенти магистри, а двама докторанти се обучават в образователна и научна степен „доктор".

С решение на Държавната комисия по сигурността на информацията N50-I от 28.07 2011 година нашият Факултет получи разрешение да обучава служители и лица, придобили право на достъп до класифицирана информация. За този период, по-малко от една година, успяхме да обучим в курсове по „Защита на класифицираната информация - първоначално обучение" и курс „Защита на класифицираната информация – текущо обучение - Сигурност на автоматизирани информационни системи и мрежи" специалисти от Община Русе, Областна администрация Разград, Община Върбица, Териториална дирекция „Държавен резерв" - Велико Търново, Областна администрация Шумен, Община Смядово.

В продължение на вече седем години работим по подготовката на кадри по информационна сигурност в тясно сътрудничество с Държавната комисия по сигурността на информацията и Дирекция „Сигурност на информацията" на Министерството на отбраната, за което изказвам своята искрена благодарност лично на г-жа Цвета Маркова и полк. Иван Иванов, както и на всички останали колеги от другите институции.

Уважаеми гости, уважаеми участници в научната конференция,

Днес и утре ще имате възможност да видите и чуете най-новите изследвания, проучвания и постижения в областта на криптографските методи за защита на информацията, предизвикателствата пред специализираните държавни структури в сектора „Сигурност и отбрана", свързани с информационната сигурност, новите тенденции в способите и технологиите по защита на информацията, както и политиката на държавата за защитата на информацията в информационните системи.

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 институции, които притежават различни функции и имат различни отговорности и правомощия.

Изключително съм удовлетворен, че в работа на конференцията се включиха много млади хора – курсанти, студенти и докторанти. Тази тенденция се очерта на миналогодишната конференция. Силно се надявам, че тя ще се запази и задълбочи в бъдеще.

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

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

Откривам Научната конференция „Защитата на информацията – състояние и перспективи".

СЪСТОЯНИЕ И НОВИ ТЕНДЕНЦИИ В КРИПТОГРАФСКИТЕ АЛГОРИТМИ И КРИПТОГРАФСКИТЕ СРЕДСТВА

полк. Иван Иванов*

Позволете първо да благодаря на организационния комитет за учтивата покана да участвам на този научен форум, където думата "сигурност" съм убеден, че ще присъства в почти всяко изречение и на второ място да изкажа своето удовлетворение, че участието на дирекция "Сигурност на информацията" в Министерството на отбраната на Република България се превръща в устойчива традиция.

Думата криптографията или тайнопис произлиза от гръцките думи:

κρυπτός (криптос - "скрит"), и γράφω (графо - "пиша").

Криптографията е наука, която се занимава с теорията и практиката на скриване на информация.

Първоначално криптографията е изучавала методите за шифриране (и дешифриране) на информацията или обратимото преобразуване на открит (изходен) текст на основата на секретен алгоритъм и/или ключ в шифрован текст (шифротекст). Тази, т.н. традиционна криптография, обхваща обаче само раздела Симетрични криптосистеми, в които шифроването и разшифроването се извършва с използването на един и същ секретен ключ. Освен този раздел съвременната криптография включва и раздел Асиметрични криптосистеми, както и системите за електронен цифров подпис, хеш-функции, получаването на скрита информация и квантовата криптография.

В днешно време криптографията се счита за клон едновременно на математиката и информатиката и е тясно свързана с теорията на информацията, компютърната сигурност и инженерното дело.

Криптографията е математическа наука и изучава методите, способите, средствата за преобразуване на данни с цел:

- да се скрие семантичното значение на данните;
- да се предотврати неправомерното им използване;
- да предотврати откриването на евентуални, случайни или преднамерени изменения в данните.

Основните понятия в областта на криптографията са:

- Криптиране (шифриране) – процес на преобразуване на данни (открит или некриптиран текст-изобразен на схемата със съкращението о.т.), чрез специални криптографски трансформации, в резултат на което се получава т.н. криптиран или шифриран текст (ш.т.).
- Декриптиране (дешифриране) – обратен криптографски процес. Процес на преобразуване на шифриран текст в явен текст или в открит текст с използване на т.н. криптографски ключ, за получаване на откритият текст.

---

* *Авторът е директор на Дирекция „Сигурност на информацията" и служител по сигурността на информацията в Министерството на отбраната*

- Криптографски алгоритъм – служи за функционално преобразуване на открития текст, разбираема последователност от символи и съответно тяхното правилно възстановяване.

- Криптографски протокол – съвкупност от правила за използване на криптографски алгоритъм и правила за обмен на данни.

- Криптографска система (крипто система) – съвкупност от два или повече криптографски алгоритъма съответно криптографски протоколи.

- Криптографски ключ – множество от символи и/или числа, което се използва за криптиране/декриптиране на данните. Чрез него се управляват процедурите по криптиране/декриптиране на данните. Има две групи криптографски ключове: секретни – ако изискванията на крипто системата са да бъде запазен в тайна и несекретни – ако изискванията на крипто системата налагат той да бъде публично оповестен и достъпен.

- Криптографско средство – техническо средство (апаратура, хардуер) и/или програмно средство използвани за криптиране/декриптиране на данни и/или за генериране и тестване на криптографски ключове.

- Криптографска мрежа – съвкупност от съвместими криптографски средства с общо администриране на криптографски ключове осигуряващи криптографска защита на съхраняваната или обменяна информация.

- Криптографска защита/криптографска сигурност – прилагане на криптографски методи и средства за защита на данните при тяхното съхранение и обмен (защита срещу разкриване от неоторизирани лица, неправомерно ползване и неправомерна промяна).

На слайда са показани общите (принципни) схеми на процеса на криптиране при двата основни криптографски алгоритъма (симетричен и асиметричен), за които ще говоря по-късно в брифинга.

Основните принципи на криптографията са два.

Първият принцип осигурява скритост на криптографските ключове. А вторият осигурява и разработва методи, способи и средства за обмяна на криптографските ключове.

На базата на тези принципи са изведени пет постулата:

- първи постулат – сигурността на криптографската система не зависи от секретността на използваните криптографски алгоритми, а зависи основно от опазването на криптографския ключ;

- втори постулат – сигурната, силна криптографска система притежава голямо пространство на криптографските ключове;

- трети постулат – сигурната, силна криптографска система произвежда шифриран текст, който притежава напълно случайно статистическо разпределение на символите в него, и който шифриран текст не подлежи на статистически анализ;

- четвърти постулат – цената на "разбиване" криптографския алгоритъм, трябва да бъде много по-висока от цената на защитаваната информация;

- пети постулат – времето за "разбиване" на криптографския алгоритъм трябва да бъде по-дълго от времето, за което защитаваната информация запазва своята актуалност и представлява интерес.

За постигане на устойчивост или строгост на криптиращия алгоритъм съществено значение играят криптиращите ключове и техните дължини.

Дължината на криптографския ключ се определя така че да е защитен от пълно изброяване – комбиниране (т.нар. “атака на грубата сила”).

ТАБЛИЦА 1.

Дължина на ключа	Пространство на ключовете в двуйчна бройна система	Пространство на ключовете в десетична бройна система	Криптоанализ 10 на 20-а 1 ключ 1Ms	10 на 6-а/1Ms
32 бита	2 на 32-а степен	4,3x10 на 9-а степен	35,8 минути	2,15 Ms
128 бита	2 на 128-а степен	3,4x10 на 38-а степен	3,4x10 на 24-и години	5,4x10 на 18-а години

От таблицата се вижда, че**:**

- при дължина на ключа 32 бита са възможни комбинации от ключове – 2 на 32-а степен.

- при дължина 128 бита – комбинациите са равни на 2 на 128 степен.

Дължината на криптографския ключ определя т.н. горна граница на устойчивост на криптографската система срещу атакуваща система, която използва т.нар. “груба сила” (извършване на проверка с всички възможни ключове) за да намери верния ключ.

Към момента използваните изчислителни средства и технологии са в състояние да решат в приемливо време задачата за намиране на верния брой ключове до 10 на 20 степен варианта. В този контекст Ключ с дължина 128 бита се определя, като гаранция за създаване на алгоритъм устойчив на атаката “груба сила”.

Вижда се от последната колонка при наличните изчислителни мощности-колко време е необходимо за да се разбие този ключ (5 пъти по 10 на 18-та степен години).

Класификация на криптографските алгоритми (шифър).

Криптографския алгоритъм се базира на функциите шифриране и дешифриране на данните. При шифриране се използва ключ за шифриране, който е известен само на шифриращата страна или е всеобщо достъпен. Ключът за дешифриране може да е същия, с който е извършено шифрирането или за дешифриране да се използва друг ключ известен само на приемащата страна.

Всяка една криптографска система се състои от два или повече базови криптографски алгоритъма и се характеризира с избраните режими за тяхната реализация. Съответния базов криптографски алгоритъм и реализираните режими подлежат на класификация по различни класификационни признаци. Като класификационен признак на първо ниво най-често се използва свойството симетрия на криптографския ключ. По този признак базовите криптографски алгоритми се разделят на симетрични и несиметрични.

Към симетричните и несиметричните криптографски алгоритми се прибавят и алгоритмите без ключ. Те са разделени на хеш алгоритми (hash функции – хеширане) и генератори на ключов поток или на случайна последователност.

При симетричните криптографски алгоритми процеса на шифриране и дешифриране се извършва с използване на един и същи криптографски ключ. Те се нари-

чат още алгоритми със секретен (таен) ключ. В този механизъм на криптиране и декриптиране изпращача и получателя предварително се разбират кой ключ да използват. Тъй като изпращача и получателя са единствените, които знаят този симетричен ключ, то компрометиране би могло да възникне при тези две страни. Друг проблем се явява и безопасното разпространение на ключа. От друга страна симетричното криптиране не използва дълги ключове, което позволява бързо да се криптират голям обем от данни.

Първата група Симетрични алгоритми са Субституционните и транспозоционните блокови алгоритми

Субституционните блокови алгоритми представляват математическа операция извършена еднозначно и обратимо съпоставяне на символи в открития текст с други символи в шифрирания текст или блок символи в отворения текст се съпоставят на друг блок символи в шифрирания текст.

Субституционен блоков алгоритъм – още се нарича “Шифър на Цезар” .

ТАБЛИЦА 2.

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ ы Ю Я

ы ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ

п о т р е б и т е л

м л пн в юе п в и

Субституционните блокови алгоритми още се наричат заместителни алгоритми.

Транспозиционният блоков алгоритъм/шифър представлява математическа операция, която се състои в еднозначно и обратимо преобразуване на блок от краен брой символи, чрез пренареждане (пермутиране) по определена схема с определен ключ.

ТАБЛИЦА 3.

	1	2	3	4	5
1	с	ъ	о	б	щ
2	е	н	и	е	с
3	ъ	о	б	щ	е
4	н	и	е	с	ъ

Ако използваме например ключ 42135 текста “съобщениесъобщение” придобива вида “бещсъноисеъноибещсеъ”.

В този случай символите от отворения текст се запазват, но само се разменят. Затова транспозиционните блокови алгоритми още се наричат разместителни алгоритми.

Втората група Симетрични криптографски алгоритми са Поточните алгоритми.

При поточните алгоритми всеки символ от открития текст се шифрира и дешифрира независимо от останалите или преобразуването не е функция на една и съща криптографска трансформация. Следователно се налага създаване на секретен ключ, като последователност от символи, с която се реализира алгоритъма. За целта се използват букви, цифри и други разрешени символи, при което отворения текст се преобразува в съответствие на криптографския ключ. Размера на криптографския ключ трябва да е по голям или равен на размера на открития текст.

Една и съща гама не би следвало да се използва повторно във времето и в пространството, тъй като това би довело до значително снижаване в устойчивостта на алгоритъма.

Алгоритъмът трябва да бъде устойчив на атаки установяващи се на статистически анализ.

Принципът е използване на основен криптографски ключ за получаване на различен брой гами за гамиране. Най-сигурен способ за постигане на сигурност е честата смяна на ключа.

Примери за симетрични криптографски алгоритми са: Data Encryption Standard (DES); 3DES (Triple DES); Blowfish; Twofish; IDEA (International Data Encryption Algorithm); AES (Advanced Encryption Standard); SAFER (Secure and Fast Encryption Routine) и др. Най-използваните от тях са: DES, TripleDES и AES.

DES (Data Encryption Standard) е разработен от фирмата IBM и утвърден от правителството на САЩ като официален стандарт - FTPS 46-3.

DES работи с 64-битови блокове от съобщенията. Алгоритъмът използва серия от стъпки за преобразуване на 64-те входящи в 64 изходящи бита.

В своя стандартен вид алгоритъмът използва 64-битови ключове - 56 бита от които се избират случайно. Останалите 8 бита са за контрол по четност (по един за всеки 7-битов блок от 56-битовата случайна стойност). Алгоритъмът използва комбинация от нелинейни (S-блокове) и линейни (заменящи E, IP, IP-1) преобразования.

DES има няколко режима:

- режим електронна кодова книга (ECB — Electronic Code Book),
- режим свързване на блокове (CBC — Cipher Block Chaining),
- режим обратна връзка по шифротекст (CFB — Cipher Feed Back),
- режим обратна връзка по изход (OFB — Output Feed Back).

3DES (TripleDES) по същество е DES алгоритъм, който се изпълнява 3 пъти с различни ключове. По тази причина дължината на ключа се получава 168 (3*56) бита.

AES (Advanced Encryption Standard -„Подобрен стандарт за шифриране“) е стандарт за шифриране, приет през 2002 година от американския Национален институт за стандарти и технология. Към 2009 година това е един от най-широко използваните симетрични криптографски алгоритми. Стандартът включва приложение на алгоритъма Рейндал, разработен през 1998 година от белгийските криптографи Винсент Реймен и Жоан Дамен, като използва ключове с три дължини: 128, 192 или 256 бита.

Вторията основен вид криптографски алгоритми са Несиметричните, по-известни като асиметрични криптографски алгоритми

Идеята за асиметрични криптографски алгоритми е разработена още през 1976 г. независимо от два екипа – Уитфийлд Дифи и Мартин Хелмън.

Фундаменталната разлика при използване на системи с асиметрични ключове от тези със симетрични е, че шифриращия механизъм не съвпада с разшифроващия. Кодирането на информацията е едностранен процес – некодираните данни се шифроват с помощта на зашифриращия ключ, докато с негова помощ не може да се осъществи обратното взаимодействие – да се разшифроват данните до четаем вид отново. За тази цел е необходим разшифроващ ключ, който е свързан с шифриращия но не съвпада с него. Подобна технология на шифриране на информацията предполага, че всеки има на разположение двойката ключове – откритият ключ (public key) и частния ключ (private key).

Затова асиметричните алгоритми се наричат още и алгоритми с публични ключове. При тях криптирането и декриптирането се извършва с различни ключове -

частен ключ и публичен ключ. Освен това декриптиращият ключ не може да бъде (за обозримо време) пресметнат от криптиращия ключ. Криптиращият ключ се нарича публичен ключ и той не се пази в тайна. Всеки може да го използва, за да криптира съобщение, но само който знае съответстващия му декриптиращ ключ може да декриптира съобщението. Декриптиращият ключ се нарича личен (частен) ключ. По изключение съобщението се криптира с личния ключ и се декриптира с публичния.

Криптографски алгоритми с публичен ключ се базират на шифриращи функции характеризиращи се със свойството еднопосочност.

Принципната схема за работа на алгоритъма с публичен ключ е показана на първата картинка.

За предаване на криптирани съобщения от страна А до страна В, страната А използва публичния ключ на получателя (страната В), който е общодостъпен. За декриптиране на съобщението страната В използва своя частен ключ.

Използването на алгоритъм с публични ключове има следните особености, както е показано на втората картинка:

- двойката ключове се генерира едновременно
- за частния ключ особеностите са следните: използва се подписване и декриптиране; съхранява се на отделен физически носител и се защитава от собственика (потребителя).
- за публичния ключ особеностите са следните: разпространява се публично; използва се за проверка на валидността на цифровия подпис; използва се криптиране и се съхранява в сертификати на компютъра.

Най известните асиметрични алгоритми са:

- RSA (Rivest-Shamir-Adelman)
- Elliptic Curve Criptography, ECC – шифриране с елиптична крива
- DSA – Digital Signature Algorithm
- DiJfieHetleman (D-H)

Най-използваният от тях е **RSA**. Наименованието идва от фамилните имена на създателите му Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman. Патентован е през 1983 г, освободен е от патент през 2000 г. Ключът с дължина от 512 до 1024 бита се използва за кодиране и е различен от ключа, използван за декодиране. Алгоритъмът на RSA предоставя процедура за подписване на електронен документ и за проверка на автентичността на подписа. Подписът на електронен документ не е константа - той е реквизит на електронния документ, на който е „положен“.

Операциите на RSA, независимо дали кодирането, декодирането, подписването или проверката, всъщност представляват модулно експоненциране. Това изчисление се извършва като серия модулни "умножения".

RSA в момента е използван широко в много продукти, платформи и промишлености по света. Той намира разпространение в много търговски софтуерни продукти и е планирано да бъде използван в много повече.

RSA е приложен в операционни системи на Майкрософт, Епъл, Сън и Новел. В практиката RSA може да бъде открит в телефони, на мрежови карти за Интернет и на смарт карти. Като цяло, RSA е внедрен като мярка за сигурност във всички главни протоколи за сигурни интернет-комуникации, включвайки S/MIME формат, SSL, и S/WAN.

RSA е също така използван вътрешно в много институции, включително клонове на американското правителство, водещи корпорации, национални лаборатории и университети.

Лицензът за технологията на RSA е придобит от около 350 компании, а приблизителният брой на машините за кодиране на базата на RSA е около 300 милиона. Това го прави най-широко използвания алгоритъм за криптиране в света досега.

За ефективно използване на криптографията с публични ключове и осигуряване услугите като строга идентификация и автентификация, цифров подпис и криптиране на съобщения е необходима Инфраструктура на Публичните Ключове (Public Key Infrastructure, PKI).

Всяка PKI се състои от пет елемента:

- орган издаващ сертификати- Certificate Authority (CA);
- орган регистриращ сертификати - Registration Authority (RA);
- хранилище за сертификати - Certificate Repository (CR);
- носител на сертификат - Certificate Holders (CH);
- системни потребители (клиенти)- System Users (Clients).

Най-добрият начин да се представи функционирането на PKI е да се проследи стъпка по стъпка жизнения цикъл за издаване и използване на сертификатите на основата на типични комерсиални PKI продукти-показан на слайда:

- първо потребителят се свързва към Web Certificate Server за да получи формата на заявка за издаване на сертификат (Certificate Request form).
- след това потребителя използва своя browser за генериране двойката публичен/частен ключ, които се съхраняват в собствена локална база данни, защитена сигурно със зададена от потребителя ключова фраза;
- след това потребителя попълва формата на заявка и я изпраща до Certificate Server;
- органа за регистрация на сертификатите (Registration Authority) автоматично се свързва към Web Certificate Server и преглежда заявката. След проверка на информацията в заявката Registration Authority я автентифицира и я изпраща в Web Certificate Server;
- Certificate Authority достъпва до Web Certificate Server за преглед на заявката. Certificate Authority утвърждава (одобрява) заявката, генерира подписан сертификат, поставя го в Web Certificate Server и го въвежда в X.509 Directory;
- накрая потребителят се свързва към Web Certificate Server и получава (изтегля) своя сертификат, който Web Browser съхранява в собствената локална база данни.

Голямото значение на криптографията с публичен ключ произтича от липсата на необходимост от предварително разпределяне или обмяна на ключове между комуникиращите страни. Това прави възможно предлагането на редица онлайн услуги като електронни разплащания, сигурен обмен на данни и др. Поради поголямата изчислителна интензивност, необходима за реализиране на алгоритмите за криптиране с публичен ключ, понякога методът се прилага за кратък комуникационен обмен, при който двете страни обменят ключове за продължаване на понататъшната комуникация чрез криптиране със симетрични ключове.

Целта по-нататък в доклада е да се изложат основните изисквания на НАТО в тази област, какви протоколи се разработват и каква е визията за едно бъдещо криптографско устройство.

Регламентиращите документи в областта на криптографската сигурност на НАТО са:

- PO(99)47 - NATO Information Management Policy (NIMP);
- C-M(2002)49 - Security within the NATO;
- C-M(2002)60 - The Management of Non-classified NATO Information;
- MC 74/3 - Communications Security for NATO;
- MCM-059-02 - NATO Role of the Military Committee Distribution and Accounting Agency (DACAN);
- AC/35-D/2004 and AC/322-D/052 - NSC and NC3B Primary Directive on INFOSEC;
- AC/35-D/2005 - INFOSEC Management Directive;
- AMSG 293 - NATO Cryptographic Instructions;
- AC/322-D/0047 - INFOSEC technical and implementation directive on cryptographic security and cryptographic mechanisms.

Последният документ разглежда конкретно криптографските механизми и криптографските алгоритми, които се използват в НАТО.

Криптографските механизми трябва да осигуряват следните услуги:

- конфиденциалност (тайна);
- цялостност (интегритет);
- достъпност;
- автентичност;
- невъзможност от отказ от авторство.

Услугите за тайна (конфиденциалност) осигуряват невъзможност за неоторизиран достъп до данните, съхранявани в работните станции и сървърите или предавани по мрежата. Използва механизмите за контрол на достъпа и криптиране.

Услугите за цялостност осигуряват невъзможността данните да бъдат променени или разрушени от неразрешени действия. Механизмите, които осигуряват това, са хеш-функции, цифров подпис и контрол на достъпа.

Услугите за достъпност гарантират, че необходимите ресурси са достъпни и използваеми за потребителите, които имат право на това. Най-често се използват механизмите на цифровия (електронния) подпис.

Услугите за автентичност гарантират, че вие сте това, за което се представяте. Исторически в компютърните системи автентичността се осигурява от парола. Съществуват много техники за доказване на автентичност (идентификация и автентификация), но всички достоверни се базират на криптографските методи. Използва се също и цифровия подпис.

Услугите, свързани с невъзможността за отказ от авторство, са предназначени за осигуряване на взаимодействията в компютърните мрежи. Те не дават възможност изпращачът да отрече изпращането, а получателят - получаването на дадено съобщение. Основната техника е цифровият подпис.

Криптографските алгоритми са 3 типа: A, B и C

- Type A са криптографските алгоритми, които са разработени, оценени и одобрени от NCSA на НАТО и се използват при стриктно спазване на принципа "необходимост да се знае".
- Type B са криптографските алгоритми, които са оценени и одобрени от NCSA на НАТО или страна членка на Алианса.

- Type C са криптографските алгоритми, които са одобрени от NCSA на НАТО или страна членка на Алианса и са предназначени за защита на публични услуги в публичните мрежи.

ТАБЛИЦА 4.

	ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ		
	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET
within NATO	Type B	Type A, Type B	само Type A
NATO – non-NATO Nation	Type B	Type B	Type B

ТАБЛИЦА 5.

	ЗА НЕКЛАСИФИЦИРАНА ИНФОРМАЦИЯ		
	НИСКА ЗАЩИТА	СРЕДНА ЗАЩИТА	ВИСОКА ЗАЩИТА
within NATO	Type B	Type A, Type B	само Type A
NATO – non-NATO Nation	не се прилага	Type B	Type B

На таблица 4 е показано разпределението на алгоритмите за защита на класифицирана информация (по нива на класификация), а на таблица 5 е показано разпределението на алгоритмите за защита на некласифицирана информация.

Това разпределение е продиктувано от следните допълнителни изисквания:

- Type A трябва да са под контрола на националния орган;
- Type A не се използват извън НАТО;
- Type C не се използват за защита на класифицирана информация на НАТО.

За да отговорят на изискванията на НАТО водещите държави в областта на критпографията (САЩ и Франция) разработиха нови протоколи за криптиране, съответно HAIPE и RIP6.

Съкращението RIP6 идва от абревиатурата мрежов интернет протокол (Routing Internet Protocol) и от съвместимост със стандартите за сигурност (Security Interoperability Standarts). RIP6 не е мрежов протокол и не се ограничава само с използването на IPv6.

RIP6 е разработен на основата на стандарт разработен от IEFT (Internet Engineering Task Force), като са добавени допълнителни ограничения и е адаптиран към мрежите за отбрана. При разработването му са спазени всички изисквания и е съобразен с всички характеристики на мрежите за отбрана.

RIP6 поддържа няколко критпографски алгоритъма едновременно и може да се използва за криптиране на всички нива на класификация на класифицираната информация.

RIP6 е разработен от група от фирми (консорциум) THALES – производител на критпографски средства за отбраната, Сертифицирани експерти по критпография от SILICOMP-AQL и Експерти по защита на мрежи от AmosSys.

RIP6 осигурява трите основни характеристики на класифицираната информация – конфиденциалност, достъпност и интегритет, еднозначна идентификация на изпращача пред получателя, повторна защита и енкапсулация в транспортен и тунелен режим, както и IPv6 върху IPv4 и IPv4 върху IPv6.

Криптографските средства, които използват RIP6 протокола имат 5 интерфейса - интерфейс 1 и 2 са физически интерфейси, за свързване към WAN (черно) и LAN мрежи (класифицирани). Другите три интерфейса са логически и са предназначени за свръзка между две устройства и към центрове за управление – на мрежовата (комуникационната) част от устройството и на криптографските ключове.

Протоколът HAIPE IS (High Assurance Internet Protocol Interoperability Specification) е разработен по програмата за модернизация на криптографските алгоритми на Националния орган по сигурността на САЩ - NSA (National Security Authority).

HAIPE IS използва Type 1 на САЩ и точно по тази причина не може да се намери повече информация, още по-малко – да се предостави на този форум. Алгоритъм Type 1 се използва за криптиране на класифицирана информация на правителството на САЩ. HAIPE IS поддържа алгоритмите на НАТО – Type A и B, за които вече Ви споменах.

HAIPE IS е разработен на основата на IPSec, разбира се с направени изменения и допълнително включени ограничения с цел повишаване на неговата надеждност. Едно от тези подобрения включва способността за криптиране на multicast data с помощта на “pre-placed key” – това е много голям набор от числа, които могат да се използват за криптиране на информация години наред, но при HAIPE IS този огромен брой числа се използват за честа смяна по случаен допълнителен алгоритъм.

Устройствата, които са изработени по тази спецификация поддържат: IPv4, IPv6, Information Assurance Service и осигуряват: контрол на достъпа, конфиденциалност, достъпност и интегритет на информацията в жични, безжични, сателитни и хетерогенни мрежи.

За да отговори на най-съвременните изисквания за криптографска сигурност и с цел използване на едно криптографско устройство за защита на комуникационните и информационните системи (знаете, че различните криптографски средства не могат „да си говорят” помежду си) НАТО предприе редица инициативи, бяха формирани няколко работни групи и с помощта на публично-частния сектор се стигна до специфициране на бъдещото криптографско средство – **NINE** (**N**etwork and Information Infrastructure **I**nternet Protocol **N**etwork **E**ncription) = по схемите ще го видите изобразено с числото **9**.

Освен основните изисквания, към устройството са поставени следните допълнителни изисквания:

- Защита срещу отваряне (физическа сигурност)
- Защита от паразитни електромагнитни излъчвания (ПЕМИ) – устройството ще е TEMPEST
- Защита от влажност, повишена температура и пикове и спадове в напрежението

Интерфейсите на устройството са 4, номерирани от 2 до 5:

- интерфейс-2 ще бъде физически интерфейс предназначен за свързване с транспортната среда (мрежата). Той трябва да поддържа протоколите показани на слайда (IPv4, IPv6, BGP+, Multicast, Security Architecture for IP и др.)

Този интерфейс трябва да поддържа скорост не по-малка от 100 Mbps да пропуска не по-малко от 100 000 пакета/сек.

- интерфейс-3 ще бъде логически интерфейс за свързване на NINE устройства. Протоколите, които трябва да поддържа са показани на слайда (IPSecv4, multiple algorithm и multiple key types, VPN, AES-128-bit и др.)

Този интерфейс трябва да поддържа:

- 40 Internet Key Exchange (IKE);
- 80 IPSec Security Associations за 1 сек. за всеки „червен" порт.
- до 1000 IPsec тунела за 10 сек.

- интерфейс-4 ще бъде логически интерфейс между NINE устройство и Центъра за управление сигурността на мрежата (пълно конфигуриране на устройствата и управление на криптографските ключове). Протоколите, които трябва да поддържа са показани на слайда (SNMPv3, Alarm management, Transport Performance, IPv6, NetConfig, IPSec и др.)
- Интерфейс-5 ще бъде физически интерфейс за свързване на NINE устройството и защитаваната ("червената") мрежа

Този интерфейс трябва да поддържа маршрутизиращите протоколи: RIPv3, OSPFv2 (IPv4) и OSPFv3 (IPv6)

Най-общо погледнато се предвиждат 3 сценария за използване на устройството NINE:

- 1-ви сценарий – стандартното свързване на една LAN мрежа към WAN
- 2-ри сценарий – защита на няколко отдалечени LAN мрежи при свързването им към защитена WAN мрежа (Protected Core Network). Характерното тук е, че се предвижда използването на Център за управление на сигурността на мрежата и криптографските ключове)
- 3-ти сценарий – осигуряване на защита на LAN мрежи за различен тип класифицирана информация (NATO SECRET, MISION SECRET и National SECRET). Тук интересен е факта, че ще се използва по едно NINE устройство на LAN мрежа (а не по 3).

ЕДНА ВЪЗМОЖНОСТ ЗА ИЗПОЛЗВАНЕ НА НЕДВОИЧНИ ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ В ПОТОЧНИТЕ ШИФРИ

Жанета Н. Ташева

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

A POSSIBILITY TO USE NON-BINARY PSEUDO-RANDOM SEQUENCES IN STREAM CIPHERS

Zhaneta N. Tasheva

ABSTRACT: *Nowadays with the introduction of many new communication technologies, new problems, related to the provision of reliable and efficient communications via Internet, telephone, wireless, satellite and other channels, are arised. A method for using non-binary pseudo-random sequences in stream ciphers, which increases the period of pseudo-random sequence and remains their balance property, is proposed in the paper.*

KEY WORDS: *PRS, LFSR, SG, GSMG, Stream Ciphers*

Въведение

Актуалността на проблема за сигурността в комуникационно-информационните мрежи и системи произтича от важността на изискванията за получаване на достоверна и точна информация за изпратеното съобщение, неговия подател и получател, при условия на канали за връзка с възможност за подслушване и преднамерени шумове, организирани от престъпни и терористични групировки.

Псевдослучайните последователности PRS (Pseudo-Random Sequences) широко се използват в комуникациите и криптографията още от създаването на теорията на информацията през 1948 г. от Клод Шенон. Научните изследвания на псевдослучайни последователности могат условно да се разделят на три периода:

Период преди тяхното практическо приложение.

Преди 1948 г. изследването на псевдослучайните последователности е имало само теоретичен характер, поради тяхната елегантна математическа структура. Били са изучавани като линейни повтарящи се последователности, дефинирани над пръстен, около 1930 г. и като комбинаторен проблем в 1894 г., известни по-късно като последователности на De Bruijn.

Златен период на последователностите с максимален период на повторение.

В 1948 г. Шенон доказва, че еднократно използваемият ключов поток е неразбиваем. Ако псевдослучайният генератор работи като ключов генератор в криптосистема с поточен шифър и периодът на генерираната последователност е достатъчно дълъг, за да се гарантира, че по всяко време ще се използват отделни различни сегменти на генерираната последователност за криптиране. Така в началото на 50-те години на миналия век критичен проблем е било как да се генерира псевдослучайна последователност с голям период. Решението до 1969 г. са били линейните

премествaщи регистри с обратни връзки LFSR (Linear Feedback Shift Registers), които са се използвали като псевдослучайни генератори в криптосистемите с поточни шифри, защото LFSR с дължина n може да генерира последователност с дължина $2^n - 1$. По-голямата част от ранните разработки на LFSR и Bruijn последователности са събрани и обобщени в популярната книга "Shift Register Sequences" на професор Golomb. LFSR регистрите са били използвани в много приложения, като например поточните шифри, радарните системи и CDMA комуникациите.

Период на нелинейни псевдослучайни генератори.

В 1969 г. Massey прави изключителното откритие, че ако двоична последователност има линейна сложност n, тогава цялата последователност може да се реконструира от $2n$ последователни известни бита посредством алгоритъма на Berlekamp-Massey. От този момент учените търсят нови методи за генериране на нелинейни последователности. Изследователите се обръщат към следните два основни начина за генериране на нелинейни последователности [3]:

1. Структури, основаващи се на LFSR регистри:
   - Филтър генератори;
   - Комбинационни генератори;
   - Тактово управлявани генератори, включително и каскадни.
2. Генератори в крайни полета:
   - GMW (Gordon, Mills и Welch) последователности, включително каскадни;
   - Последователности с бент функция.

В статията се предлага метод за използване на недвоични псевдослучайни последователности в поточните шифри, което увеличава периодът на повторение на нелинейната псевдослучайна последователност, като същевременно с това запазва тяхната еднородност.

Недвоични псевдослучайни последователности

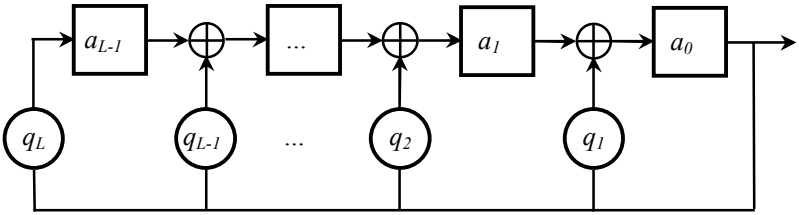
В реалните криптосистеми pLFSR регистрите, като и LFSR регистрите, могат да се конструират по две различни архитектури, наречени регистри на Фибоначи и Галоа. За целите на разработката ще бъде разгледана само архитектура на Галоа на pLFSR регистър [4].

Определение 1. *P-ичният линеен преместващ регистър с обратни връзки* (*pLFSR*) *с архитектура на Галоа* и дължина L (фиг. 1) се състои от L *елемента за закъснение* a_i, $i = 0, 1, \ldots, L - 1$, с един вход и един изход и множителите на обратните връзки $q_1, q_2, \ldots, q_L$. Всеки елемент може да запомни едно p-ично число ($p = 1, 2, \ldots, p - 1$). По време на всеки тактов цикъл се извършват следните операции:

1. Съдържанието на елемент 0 се извежда и формира част от изходната последователност.
2. Съдържанието на елемент i се премества в елемент $i - 1$ за всяко i, $1 \le i \le L-1$, при което са изпълнени следните рекурентни зависимости:

$$\begin{aligned} a'_i &= (a_{i+1} + q_{i+1}a_0) \bmod p, \quad за \ \ 0 \le i \le L-2 \\ a'_{L-1} &= q_L a_0 \bmod p \end{aligned} \tag{1}$$

3. Изходът от най-младшия елемент се въвежда във всеки множител на обратните връзки и се прибавя по модул p към съдържанието на предходния елемент.



Фиг. 1. pLFSR регистър с архитектура на Галоа

Архитектура на Галоа на *pLFSR* регистъра се описва с помощта на полинома на обратните връзки $q(x)$,

(2) $$q(x) = q_L x^L + q_{L-1} x^{L-1} + \ldots + q_1 x - 1$$

и полинома $h(x)$

(3) $$h(x) = a_0 + a_1 x + \ldots + a_{L-1} x^{L-1},$$

определен от началното състояние $(a_0, a_1, \ldots, a_{L-1})$ на регистъра.

Основни свойства на pLFSR регистрите

Едно от най-важните техни криптографски значими свойства е периодът на генерираната p–ична псевдослучайна последователност T. Максимално възможният период T на pLFSR регистрите се определя от дължината им L посредством неравенството

(4) $$T \le p^L - 1.$$

Основно свойство на pm–последователностите (p–ични последователности с максимален период) е равномерното разпределение на p–ичните числа и сериите в техния период. Изпълнени са следните твърдения [2]:

- Броят на появата на всички ненулеви елементи N_i в максималния период $T = p^L - 1$ е $N_i = p^{L-1}$, за $i = 1, 2, \ldots, p-1$, а броят на нулевите елементи е $N_0 = p^{L-1} - 1$. Това свойство определя приблизително еднаквата вероятност за поява на всеки елемент в последователността, следователно тя е балансирана.
- Всяка ненулева p–ична серия B с дължина s, $1 \le s \le L$ се появява p^{L-s} пъти в един период на A или $p^{L-s} - 1$ пъти, ако е нулева.

Друго криптографско значимо свойство на pLFSR регистрите е тяхната линейна сложност [3]. Линейната сложност $\lambda(A)$ на p–ичната периодична последователност A е равна на дължината на най-късия pLFSR регистър, които може да генерира A. Понеже генерираната p–ична периодична последователност A се определя еднозначно от пораждащия полином $A(x)$, то линейната сложност $\lambda(A)$ е равна на степента на минималния полином $m_A(x)$, пораждащ A.Линейната сложност $\lambda(A)$ на p–ичната периодична последователност A удовлетворява неравенството

(5) $$\lambda(A) \ge \log_p(T+1).$$

Теорема 1. [3] Автокорелационната функция на pm–последователността, генерирана от pLFSR с дължина L, е с две нива:

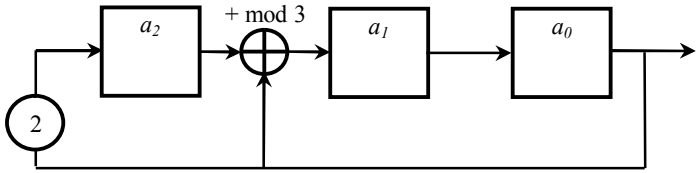
(6) $$C(\tau) = \begin{cases} p^L - 1 & \text{ако } \tau \equiv 0 \bmod (p^L - 1) \\ -1 & \text{ако } \tau \not\equiv 0 \bmod (p^L - 1) \end{cases}.$$

Математическите доказателства на свойствата на *p*LFSR регистрите може да се намери в [3], където са разгледани недвоични последователности в полето GF(p^n).

Пример 1. Троичен LFSR (3LFSR) в поле на Галоа GF(3^3).

Примитивният полином, определящ разширението на полето на Галоа GF(3^3), е $p(a) = a^3 + 2a^2 + 1$. Схемата (фиг. 2) на 3LFSR се определя от полинома на обратните връзки $q(x) = 2x^3 + x^2 - 1$. Периодът на линейната псевдослучайна последователност е $T = 3^3 - 1 = 26$, като елементите на един период са:

[10121120111002021221022200].



a_0.2 mod 3

Фиг. 2. 3LFSR регистър с архитектура на Галоа от пример 1.

Равномерното разпределение на *p*–ичните числа и сериите в периода е показано на фиг. 3, като:

- всяка наредена тройка се повтаря по веднъж с изключение на нулевата, която не се появява;
- всяка ненулева наредена двойка се появява по 3 ($3 = 3^{3-2}$) пъти, а нулевата – по два ($2 = 3^{3-2} - 1$);
- всеки ненулев елемент се появява по 9 ($9 = 3^{3-1}$) пъти, а нулевият – 8 ($8 = 3^{3-1} - 1$) пъти.

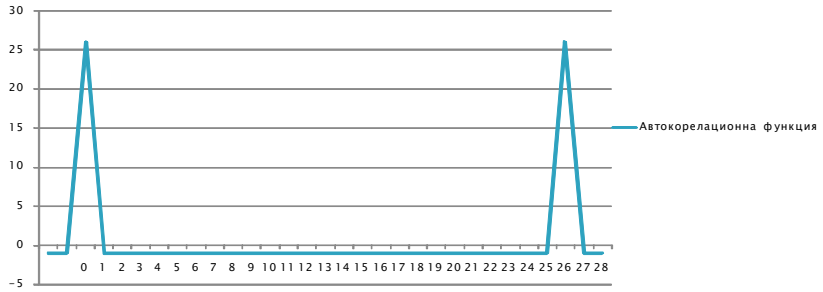
10121120111002021221022200 1, 2 - 9 бр.; 0 - 8 бр.

10121120111002021221022200 00 -2 бр.
10121120111002021221022200 01 -3 бр.
10121120111002021221022200 02 -3 бр.
10121120111002021221022200 10 - 3 бр.
10121120111002021221022200 11 - 3 бр.
10121120111002021221022200 12 - 3 бр.
10121120111002021221022200 20 - 3 бр.
10121120111002021221022200 21 - 3 бр.
10121120111002021221022200 22 - 3 бр.

10121120111002021221022200 1 101, 201, 020, 210, 001 - 1 бр.
10121120111002021221022200 211, 110, 212, 222 - 1 бр.
10121120111002021221022200 10 012, 011, 202, 102, 010 - 1 бр.
10121120111002021221022200 112, 100, 122, 220 - 1 бр.
10121120111002021221022200 121, 111, 021, 022 - 1 бр.
10121120111002021221022200 120, 002, 221, 200 - 1 бр.

Фиг. 3. Равномерното разпределение на 3-ичните числа и серии

Автокорелационната функция на троичната m–последователност, генерирана от *3*LFSR от пример 1, е с две нива: +26 и -1 (фиг. 4).



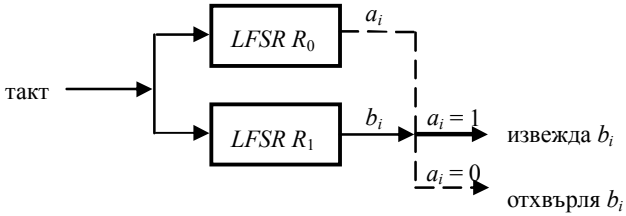
Фиг. 4. Автокорелационна функция на последователността от пример 1

Приложение на недвоични псевдослучайни последователности в поточните шифри

Предложената през 1993 г. от американските учени Coppersmith, Krawczyk и Mansour нова конструкция на свиващ генератор SG (Shrinking Generator) [1] е добър избор за практическа реализация на ефективна криптосистема за поточно шифриране поради своите привлекателни свойства: простота на реализацията, експоненциален период и линейна сложност, добри статистически свойства и имунитет към известните досега атаки.

Общата идея, заложена в SG генератора, е използване на изхода на една псевдослучайна последователност за управление на избора на битове от друга псевдослучайна последователност. Авторите са анализирали конструкция, която се състои от два LFSR регистъра (фиг. 5). Алгоритъмът на работа на SG генератора се състои от следните стъпки:

1. Регистрите R_0 и R_1 се тактуват.
2. Ако изходът на R_0 е 1, изходният бит от R_1 формира част от изходната ключова последователност.
3. Ако изходът на R_0 е 0, изходният бит от R_1 се отхвърля.



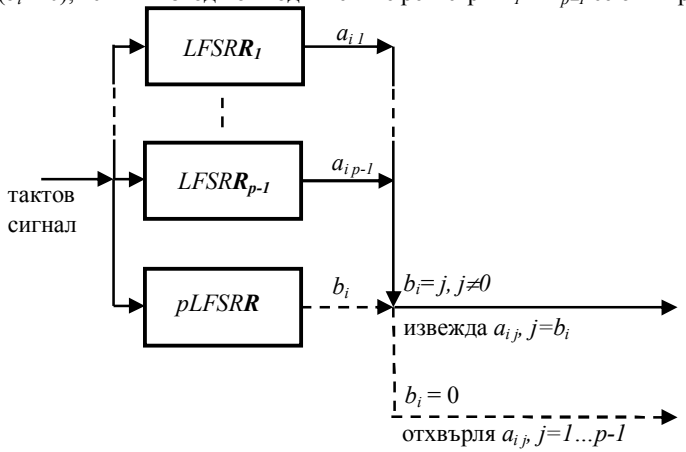
Фиг. 5. Свиващ генератор

Идеята на SG обобщаваме за случая на управляващ недвоичен pLFSR регистър и $p-1$ на брой подчинени LFSR регистри [5]. Генераторът е наречен обобщен

свиващ мултиплексиращ генератор *GSMG* (Generalized Shrinking-Multiplexing Generator).

Определение 2. Архитектурата (фиг. 6) на *GSMG генератора с градивни* LFSR *регистри* се състои от един управляващ *p*LFSR регистър с дължина L и $p-1$ подчинени LFSR регистри съответно с дължини $L_1, L_2, \ldots, L_{p-1}$. При подаване на тактов сигнал за преместване на данните всеки регистър генерира на своя изход едно p–ично число. Алгоритъмът за работа на GSMG генератора се състои от следните стъпки:

1. Всички подчинени LFSR регистри $R_1 \div R_{p-1}$ и управляващият регистър R се тактуват.
2. Ако p–ичният изход на управляващия регистър R не е равен на 0 ($b_i = j$, $j \neq 0$), младшото число от регистъра R_j формира част от изходната двоична последователност.
3. В противен случай, ако изходът от управляващия регистър R е равен на 0 ($b_i = 0$), всички изходи от подчинените регистри $R_1 \div R_{p-1}$ се отхвърлят.



Фиг. 6. Архитектурата на GSMG генератора

Архитектурата на GSMG генератора предлага бърз, ефективен и икономичен метод за получаване на двоични псевдослучайни последователности. Включването на управляващ *p*LFSR регистър внася нелинейност в работата на генератора като превръща генерираната последователност в свита и мултиплексирана версия на генерираните от подчинените регистри двоични последователности.

Пример 1. GSMG генератор с управляващ троичен LFSR и два подчинени LFSR (таблица 1).

Входни последователности:

Две двоични подчинени последователности с периоди $T_1 = 7$ и $T_2 = 3$.

Една управляваща 3-ична последователност 3PRS с период $T = 8$.

Изходна двоична последователност S с период $T_S = 126$.

Таблица 1. Входни и изходни последователности от пример 1

$2PRS_1$ (T_1=7)	11101001110100111010011101001110100111010011101001110100111010011101001110100
$2PRS_2$ (T_2=3)	11011011011011011011011011011011011011011011011011011011011011011011011011011
$3PRS$ (T=8)	11202210112022101120221011202210112022101120221011202210112022101120221011202210112022101120221011202210112022101120221011202210112022101120221011202210
S (T_S=126)	11010011111110101101010110111000101101010011111011101110010001011110101000010101111011101011010111101101110010000111101101

Периодът T_s на генерираната от GSMG последователност удовлетворява следната теорема [6].

Теорема 1. Ако подчинените двоични PRS_i и управляващата p-ична PRS последователност са последователности с максимален период (т.е. обратните връзки се определят от примитивен полином) и периодите им T_i са взаимно прости с периода на управляващата последователност T, т.е $gcd(T_i, T) = 1$ за $i = 1, 2, \ldots, p-1$, то изходната свита и мултиплексирана последователност от GSMG генератора има максимален период:

$$T_S = N_{(\neq 0)} \cdot \prod_{i=1}^{p-1} T_i \,, \tag{7}$$

където $N_{(\neq 0)}$ е броят на ненулевите елементи в един период на управляващата троична PRS.

Таблица 2. Примери за период на GSMG генератора при p = 3

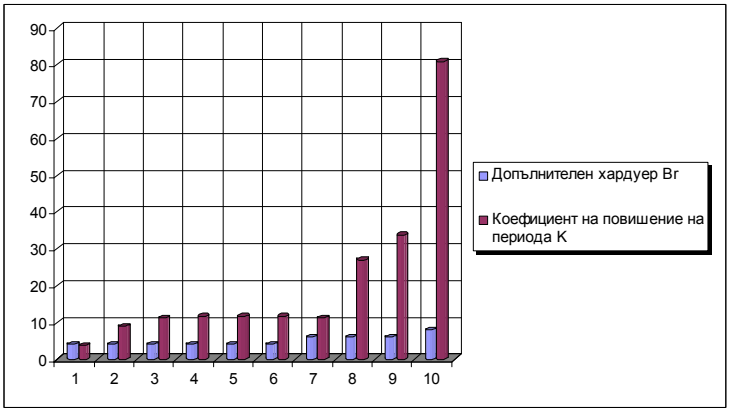
№	*PRSs*	Примитивни полиноми	Период на $m-$последователностите	Период T_S на *GSMG/LFSR*	Период T на *SG*
1	$PRSA_1$	$1 + x + x^3$	$2^3 - 1 = 7$	7.15.18 = 1890	8.7 = 56
	$PRS\ A_2$	$1 + x + x^4$	$2^4 - 1 = 15$		
	$3PRS\ B$	$1 + 2x^2 + x^3$	$3^3 - 1 - 8_{(0)} = 18$		
2	$PRS\ A_1$	$1 + x + x^2$	$2^2 - 1 = 3$	3.15.18 / 3 = 270	8.3 = 24
	$PRS\ A_2$	$1 + x + x^4$	$2^4 - 1 = 15$		
	$3PRS\ B$	$1 + 2x^2 + x^3$	$3^3 - 1 - 8_{(0)} = 18$		
3	$PRS\ A_1$	$1 + x + x^3$	$2^3 - 1 = 7$	7.3.18 = 378	2.7 = 14
	$PRS\ A_2$	$1 + x + x^2$	$2^2 - 1 = 3$		
	$3PRS\ B$	$1 + 2x^2 + x^3$	$3^3 - 1 - 8_{(0)} = 18$		
4	$PRS\ A_1$	$1 + x + x^3$	$2^3 - 1 = 7$	7.15.6 = 630	8.7 = 56
	$PRS\ A_2$	$1 + x + x^4$	$2^4 - 1 = 15$		
	$3PRS\ B$	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		
5	$PRS\ A_1$	$1 + x + x^2$	$2^2 - 1 = 3$	3.15.6 / 3 = 90	8.3 = 24
	$PRS\ A_2$	$1 + x + x^4$	$2^4 - 1 = 15$		
	$3PRS\ B$	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		
6	$PRS\ A_1$	$1 + x + x^3$	$2^3 - 1 = 7$	7.3.6 = 126	2.7 = 14
	$PRS\ A_2$	$1 + x + x^2$	$2^2 - 1 = 3$		

№	*PRSs*	Примитивни полиноми	Период на *m*–последователностите	Период T_S на *GSMG/LFSR*	Период *T* на *SG*
	3PRS ***B***	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		
7	*PRS* A_1	$1 + x + x^3$	$2^3 - 1 = 7$	7.3.54 = 1134	27 = 14
	PRS A_2	$1 + x + x^2$	$2^2 - 1 = 3$		
	3PRS ***B***	$2 + x + x^4$	$3^4 - 1 - 26_{(0)} = 54$		
8	*PRS* A_1	$1 + x + x^3$	$2^3 - 1 = 7$	7.31.6 = 1302	16.7 = 112
	PRS A_2	$1 + x^2 + x^5$	$2^5 - 1 = 31$		
	3PRS ***B***	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		
9	*PRS* A_1	$1 + x + x^2$	$2^2 - 1 = 3$	3.31.6 = 558	16.3 = 48
	PRS A_2	$1 + x^2 + x^5$	$2^5 - 1 = 31$		
	3PRS ***B***	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		
10	*PRS* A_1	$1 + x + x^4$	$2^4 - 1 = 15$	15.31.6 = 2790	16.15 = 240
	PRS A_2	$1 + x^2 + x^5$	$2^5 - 1 = 31$		
	3PRS ***B***	$2 + x + x^2$	$3^2 - 1 - 2_{(0)} = 6$		

Примери за периода на GSMG генератора при различни примитивни полиноми и $p = 3$ са показани в таблица 2. В колоната за периода на управляващата 3PRS последователност са представени броят на елементите различни от нула в рамките на периода. В пример 1. са представени реалните последователности на GSMG генератора от ред 6 в таблица 2. За сравнение на всеки ред от таблицата е показан периодът на съответния SG генератор, при който A_2 е управляваща, а A_1 – подчинена 2PRS.

Първо е сравнен периодът на генерираната последователност с тази на класическия свиващ генератор SG чрез коефициент на повишение на периода $K = T_s/T$, където T_s е периодът на генерираната от GSMG/LFSR последователност, а T – периодът на съответния SG. Многократното увеличаване на периода е за сметка на използване на допълнителен хардуер, изразен в брой тригери *Br*. На фиг. 7 са представени данните за периодите от таблица 2.

От фигурата се вижда, че използването на малко количество допълнителен хардуер при предложената архитектура води до експоненциално увеличение на периода на генерираната 2PRS.



Фиг. 7. Повишаване на периода на GSMG/LFSR спрямо класическия SG

Последователностите, генерирани от *GSMG/LFSR*, са ***еднородни***. Това означава, че вероятността за поява на нулите и единиците в тях е еднаква и е приблизително 1/2. Това свойство се потвърждава от направените честотни статистически тестове, които доказват, че броят на нулите и единиците в изследваните последователности и техните подблокове е приблизително еднакъв. Средният им брой при всички 300 последователности е показан в таблица 3.

Таблица 3.Среден брой на нулите и единиците в GSMG последователностите

GSMG	**Средно от 100 последователности по 1 000 000 бита**	
	брой на нулите	**брой на единиците**
GSMG 1	499974,4	500025,7
GSMG 2	500000,4	499999,6
GSMG 3	500004,6	499995,4
Средно	**499993,1**	**500006,9**

Заключение

Доказана е експоненциалната зависимост на периода T_s на генерираната от GSMG последователност от дължината на управляващия pLFSR и подчинените LFSR регистри. Това позволява предложената архитектура да генерира нелинейни псевдослучайни последователности с големи периоди на повторение при сравнително проста схема на управление.

Анализът на опитните резултати доказва, че последователностите, генерирани от GSMG, притежават свойствата еднородност и голям период. Повторяемостта на резултатите доказва постоянството на поведението на GSMG генератора при различни ядра (начални състояния на неговите градивни елементи).

Гореизброените свойства на GSMG генератора показват, че той работи като напълно случен генератор, т.е. неговият изход във всеки един момент не може да се предскаже. Следователно, GSMG генераторът постига основните цели на псевдослучайните двоични генератори и може да се използва в криптографските симетрични поточни шифри.

Литература:

1. Coppersmith D., H. Karwczayk, Y.Mansour, The Shrinking Generator, Crypto'93, http://imailab-www.iis.u-tocio.ac.jp/ limit/Papers/ Crypto_Eurocrypt /HTML/PDF/C93/22.pdf.

2. Golomb S.W., Gong G., Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.

3. Gong G., Sequence Analysis, University of Waterloo, 1999, p. 137, http://calliope.uwaterloo.ca/~ggong.

4. Goresky M., A. Klapper, Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers, IEEE Trans. on Inform. Theory, vol. 48, pp. 2826−2836, November 2002.

5. Tashev T., B. Bedzhev, Zh. Tasheva, The Generalized Shrinking-Multiplexing Generator, Proceedings of the International Conference on Computer Systems and Technologies - CompSysTech'07, 14-15 June, 2007, Rousse, ISBN 978-954-9641-50-9, pp. IIIB.1-1 - IIIB.1-6. The awarded Best Paper for Section IIIB.

6. Tashev T., The Period of the LFSR Based Generalized Shrinking-Multiplexing Generator, Proceedings of the International Conference on Computer Systems and Technologies - CompSysTech'07, 14-15 June, 2007, Rousse, ISBN 978-954-9641-50-9, pp. IIIB.8-1 - IIIB.8-6.

7. Желев, Ст. Приложение на рекурсивните систематични конволюционни кодове в турбо кодери. Национална конференция с международно участие – ШУ, 2011.

СИГУРНОСТТА ПРЕЗ ВТОРОТО ДЕСЕТИЛЕТИЕ НА XXI ВЕК И РОЛЯТА НА ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ" В ОТГОВОР НА ПРЕДИЗВИКАТЕЛСТВАТА НА РЕФОРМАТА В СЕКТОРА „СИГУРНОСТ"

Стоян Г. Тонев

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ - СОФИЯ
ИНСТИТУТ ЗА НАУЧНИ ИЗСЛЕДВАНИЯ И ОБУЧЕНИЯ НА ДОКТОРАНТИ

THE SECURITY IN THE SECOND DECADE TO TWENTY FIRST /21-ST/ CENTURY AND ROLE TO STATE AGENCY "NATIONAL SECURITY" IN PROVOCATION RESPONSE TO REFORM IN SECTOR /BRANCH/ "SECURITY"

Stoyan G. Tonev

Abstract: The defends of the national security if responsibility and obligation to all the authorities and home self-government, secret and public services, non-governmental organizations and the civilians.

The purpose is to support stable not only security environment in Republic of Bulgaria, but the Balkan region, Europa and all over the world as well.

***Key words*:** Security, risk, threat, danger, crisis, National security

Сигурността е неотменна човешка ценност и е първостепенно условие за мирно, свободно и перспективно развитие на държавата и нейните граждани.

Демократичната държава е тази която защитава, както суверенитета, териториалната цялост, икономиката и финансова стабилност на страната, така и правата, честта, достойнството, живота и здравето на своите граждани и носи отговорност за тяхната сигурност.

Основополагащ документ за политиката на държавната за национална сигурност е Стратегията за национална сигурност на Република България /РБ/, която се основава на Конституцията на РБ, както и на международните ангажименти на страната произтичащи от членството ни в ЕС, НАТО, ООН и други международни организации.

Законова регламентация на задачите и правомощията на Държавна агенция „Национална сигурност" и институционалното и изграждане като част от системата за защита на националната сигурност

Изчерпателната законова регламентация на задачите и правомощията на Държавна агенция „Национална Сигурност" чрез Закона на Държавна агенция „Нацио-

нална Сигурност" е основа на реформата в сектора сигурност в контекста на изграждането на правова държава.

На основата на закона Държавна агенция „Национална Сигурност" /ДАНС/ се изгражда като специализиран орган към Министерски съвет на Република България за изпълнение на политиката по защита на националната сигурност. ДАНС изпълнявайки законовите си функции самостоятелно или съвместно с други държавни органи и са делегирани права, задължения и отговорности по извършване на контраразузнавателна и информационно-аналитична дейност по наблюдение, разкриване, противодействие, предотвратяване и пресичане на замислени, подготвени или осъществявани посегателства срещу и от значение за националната сигурност, включително и в структурите на Министерство на отбраната на основание чл.77, ал.2 от Закона за отбраната и въоръжените сили на Република България. ДАНС извършва дейности по защита на националната сигурност свързани със дейности касаещи разузнаване в полза на чужди сили; опасност за суверенитета, териториалната цялост на държавата и единството на нацията; противоконституционна дейност; корупционни прояви на лица, заемащи висши държавни длъжности; прилагане на сила или използване на общо опасни средства с политическа цел; предотвратяване на опасности за икономическата и финансовата сигурност на държавата; опасности за екологичната сигурност на държавата; нарушаване функционирането на Националната система за защита на класифицираната информация; застрашаване сигурността на стратегически за страната обекти и дейности; деструктивно въздействие върху комуникационни и информационни

системи; международен тероризъм и екстремизъм, както и финансирането им; международна търговия с оръжия и изделия или технологии с двойна употреба, производство, съхраняване и разпространение на общоопасни средства; дейности на групи и лица, подпомагащи чужди служби, терористични или екстремистки организации; и миграционни процеси.

Промени в средата за сигурност

Изграждането на системата за защита на националната сигурност е основен проблем за всяка държава, утвърждаваща ново демократично общество – политическо устройство, като ДАНС се утвърждава като основно звено от системата за национална сигурност.

В организацията по практическото осъществяване на защитата на националната сигурност участват всички органи на държавната власт и местно самоуправление, специални служби, служби за обществен ред, неправителствени организации и отделни граждани, които използват различни средства, форми и методи.

Конституционно отговорни за националната сигурност са Народното събрание, президентът на републиката и Министерски съвет. Министерствата и другите държавни органи осъществяват дейности съобразно определените им от закона функции, които пряко или косвено са свързани с устойчивостта на отделни елементи на националната сигурност.

Системата за национална сигурност е основана на партньорството на държавата, местната власт, организациите и гражданите, като индикатори със способности за оценка и анализ на казуса и предлагане на държавнически управленски решения. Системата за национална сигурност следи в реално време и мащаб състоянието на средата за сигурност, както и своето собствено състояние, като реагира адекватно и своевременно на промените.

Дейността на ДАНС, другите държавни органи, неправителствените организации и гражданите в процеса на защитата на националната сигурност взаимно се допълва, т.е. се осъществява на съвременния етап само по пътя на концентрираните усилия на службите за сигурност с възможностите на другите публични и частни институции. ДАНС осъществява координация и взаимодействие с международните задължения на Р.България и в интерес на националната сигурност и с чужди специални служби за защита на националната сигурност на страната, както и защитата на контингентите ни изпълняващи мисии в различни точки на света.

Основните задачи и структурите на службите за защита на националната сигурност пряко зависят както от Стратегията за национална сигурност, конкретната историческа обстановка, от вътрешнополитическите и външнополитическите й измерения. Ефективността от дейността на тези служби се определя от способността им да се адаптират към промяната на конкретната обстановка. Свидетели сме на значимостта на тази способност при социално-икономически и обществено – политически преход и изменения на геополитическите и икономическите реалности в регионален, континентален и глобален мащаб. В тези условия рязко се повишава значението на службите за защита на националната сигурност, особено за държави, които не са включени в колективни системи за сигурност и не разполагат с действащи международни гаранции за защита от рискове, заплахи и опасности срещу националната сигурност.

Специфично за Р България в условията на преходния период бе натрупването и едновременното въздействие върху националната й сигурност на множество рискове, заплахи, кризи и опасности. Това обстоятелство до голяма степен предопредели остротата, с която сред българската общественост се поставяха и обсъждаха аспектите на проблема за защита на националната сигурност.

За кратко време и без наличието на теоретична база и практически опит трябваше да бъдат дефинирани нови и предефиниране съществуващи понятия от концептуалната основа на системата за национална сигурност като „национална сигурност", "риск", „заплаха", „криза", „опасност", „противник". Процесът на преосмисляне на съществуващите понятия включва въвеждането в речника на специализираните служби на думи, които са дефинирани в съответните области на знанието. Това включване, разбира се, не стана механично и се изрази в коректна според нас интерпретация за целите на дейността ни. Като пример може да бъдат посочени термините „риск", „заплаха", „опасност".

„Рискът" разглеждаме като явление на системите. Проблемът за сигурността на системата възниква тогава, когато рискът нарушава мярката, която от своя страна отразява степента на способностите и ресурсите, с които системата разполага, за да неутрализира негативните последствия Така разбирано, понятието „риск" задава защитните функции на ДАНС във вътрешносистемен /национален/ аспект. В този смисъл службата има за задача да наблюдава състоянието на най-важните за националната сигурност обекти, връзки, подсистеми и своевременно да уведомява висшите държавни управленски структури за възникването на рискове, които са опасни за националната и регионална сигурност.т.е риска е неопределен във времето и може да доведе до опасност-криза. Риска може да се управлява.

„Заплахата" като понятие от концептуалната основа на националната сигурност разглеждаме като явление. Заплаха представляват действия, интереси, намерения и т.н. на други системи от същия, по-нисък/но с по-висока хомогенност/ или по-

висок ранг – например други държави, международни организации, транснационални компании, международно структурирани организации, които застрашават националната сигурност.

„Заплахата" и „рискът" могат да се проявяват като потенциални и действащи, открити и прикрити и т.н. При наличието на остри прояви на заплаха и риск можем вече да говорим за опасност на националната сигурност.

„Опасност" е понятието, което отразява такова състояние на националната сигурност, изразяващо се в остра нестабилност и вероятност от разрушаване на основни елементи, отношения, подсистеми на държавата.

„Криза" – състояние на сигурността при което контролът върху вредните въздействия е силно занижен или невъзможен.

„Сигурност"- състояние на задоволителен контрол над вредните въздействия върху гражданите, обществото и държавата, което гарантира нормален живот т.е. живот в приемлив риск.

„Среда за сигурност" – съвкупност от вредни въздействия върху страната, които окозват влияние върху стабилността и обществото, държавата и живота на гражданите.

„Система за национална сигурност"- интегрирана съвкупност от инструменти за разработване и осъществяване на политиката на Р.България в областта на сигурността.

Ценности и принципи на политиката за национална сигурност

Политиката на Р. България с сферата на сигурността се базира на основните ценности на демокрацията и националната ни идентичност и култура. Водещи са човешките права, възможностите за развитието на всеки, независимо от религия, етност или расова принадлежност, равнопоставеност на различните видове собственост, върховенство на закона, разделение на властите и гражданския им контрол. Изпълнение на поети международни задължения и ангажименти в името на мира в света.

Новите реалности наложиха преосмисляне, което намери израз в Стратегията за национална сигурност на Р България и на понятието „национална сигурност". В началото на XXI век националната сигурност непосредствено се обвързва с европейската и евроатлантическата сигурност. Става дума не само за това, че реализацията на сигурността на България трябва да генерира сигурност и за региона, но и за това, че все повече са необходими съвместни международни усилия и ефективни действия за защита на общочовешките ценности и правата на човека, които са основата на съвременната демокрация.

Именно това разбиране е в основата на виждането, че реализацията на националната сигурност в България е неотделима от постигането на стабилна среда за сигурност както на Балканския полуостров, цяла Европа, така и в света.

В този контекст са наложителни координацията и взаимната допълняемост на усилията и действията със службите за сигурност на държавите от евроатлантическата общност. Това се налага извода на база анализите, че **средата за сигурност в началото на XXI век е значително променена в сравнение с предходните десетилетия**

Успехът в постигането на стабилна среда за сигурност и на базата на съвместни усилия е в значителна степен в зависимост както от правилното и точното оценяване на съществуващите рискове и заплахи, така и от способността за прогнозиране на възникването на нови в обозрима перспектива /включително на съдържащия се в тях деструктивен потенциал/, на формите на възможната и вероятната им проява.

Предизвикателства пред Държавна агенция „Национална сигурност" като служба за сигурност

Днес ние сме изправени пред нови рискове и опасности, които ще оказват негативно влияние върху международната сигурност и върху сигурността на отделните държави. Сред международната общност се формира съгласие относно техния вид и характер.

Необходимо е да се подчертае възникването на качествено ново явление, застрашаващо сигурността, което може да се определи като „трансорганизирана или стратегическа престъпност". Това сравнително ново понятие отразява процеса на превръщане на даден вид организирана престъпност от криминална дейност и заплаха за обществения ред в непосредствена опасност за националната, регионалната и международна сигурност.

В България като застрашаваща сигурността дейности са свързаните опасности за икономическата и финансова сигурност на държавата.

В Югоизточна Европа не са загубили своя разрушителен потенциал и някои от характерните за XX век конфликти на етническа и религиозна основа.

Национализмът все още се използва от отделни страни или политически сили в тях в региона за неутрализиране на социални противоречия и псевдосоциална консолидация на обществото.

Политиката за противодействие на невоенните рискове и заплахи и в Р България се реализира, от една страна, чрез инкриминирането на определени дейности или деяния в наказателното законодателство, а от друга и чрез изграждането и функционирането на системата от специални, специализирани и правозащитни служби и органи.

Обществените потребности наложиха и промени в наказателното законодателство. В Наказателния кодекс бяха направени редица изменения, насочени най-общо към прецизиране и дефиниране на някои от съвременните деяния, включително с въвеждане на квалифициран състав или увеличаване размера на санкциите във връзка с производството, съхраняването, трафика и продажбата на наркотични и психотропни вещества, огнестрелни оръжия, трафик на лица, както и на някои деяния, характерни за организираната престъпност.

Законова задача за ДАНС е противодействие на международния тероризъм и екстремизма, както и финансирането им.

Тероризмът като съвкупност от особено опасни за живота на физическите лица действия и дейности, насочени към постигане на политически или идеологически цели, не е нова заплаха за сигурността и стабилността. В последното обаче сме свидетели на значително разширяване на обхвата на явлението, включително трансграничното му разпространение, което го превръща в един от основните рискове за сигурността и стабилността. Налице е финансиране на тероризма чрез използване на приходи от търговия с наркотици и от други форми на криминална международна организирана престъпност.

Проблемът се задълбочава и от разрастването на нелегалната търговия с различни видове оръжия с висока обществена опасност, включително в нарушение на установен с резолюции на Съвета за сигурност на ООН забранителен и ограничителен режим. Все повече нараства опасността от използването на оръжия за масово унищожение за целите на терора. Ако преди двадесет години разработката и използването на тези технологии бяха монопол на държавите, понастоящем достъпът до тях по редица причини, включително глобализацията в информационната сфера, е значително облекчен. Заплахата от държавно спонсориран тероризъм ще продължи да бъде голяма, доколкото е свързан с възможността за използване от теро-

ристите на оръжия за масово поразяване, което поставя въпроса за **неосъзнатия трансфер на технологии**. Тероризмът на етническа и религиозна основа е обхванал редица региони на света. Опасността от него произтича от факта, че той не може да бъде възпрян или ограничен да прехвърли границите на конфликтната страна или регион. Тя се увеличава и от бруталността и жестокостта на терористите, действащи по етнически или религиозни подбуди. Вероятността те да предприемат акции, причиняващи масови човешки жертви, включително с използване на оръжие за масово унищожение, е много по-голяма, отколкото при терористите с политическа мотивация. Посоченото не само буди тревога, но и налага спешно да се предприемат съгласувани мерки, чиито обем и обхват просто не са по силите на една отделна страна, независимо от нейния потенциал.

Борбата с тероризма като явление, включително и в маркираните свързани с него сфери, е в независимост от решаването на някои проблеми, действията по които имат превантивен характер. Задълбочаването на процеса на дезинтеграция в цели региони също крие риска той да се превърне в траен дестабилизиращ фактор.

Риск за определени региони и европейската сигурност е налице и от увеличаващият се поток от бежанци и емигранти от засегнатите от конфликти региони и държави. Искаме или не, емигрантите носят със себе си проблемите на своите страни и народи. При сблъсъци в страните на произхода си тези общности могат да се превърнат в опасност за обществения ред и сигурността в приютилите ги държави. Факт е, че емигрантските общности от развиващите се страни се използват и като среда за създаване на бази на международни терористични организации.

Предвид горното могат да се направят следните **ИЗВОДИ:**

1. ДАНС се изгражда и укрепва като един от основните елементи на системата за ранно сигнализиране на рисковете, заплахите и опасностите и защита на националната и международна сигурност.

2. ДАНС изпълнява законовите си функции самостоятелно или съвместно с компетентни органи по защита на националната сигурност.

От направените изводи може де се изведе препоръката, че реализирането на националната сигурност в България е неотделима от постигането на стабилна среда за сигурност около нас, както на Балканския полуостров, така в цяла Европа, и в света и е приоритет на всички служби за сигурност и обществен ред в страната.

Литература:

1. Стратегия за национална сигурност на Р. България.- 2011 г.

2. Концепция за национална сигурност на Р. България /ДВ, бр.46/22.04.1998 г./.

3. Закон за Държавна агенция „Национална сигурност"- /ДВ, бр. 109/2012/

4. Закон за отбраната и въоръжените сили на Република България

5. Закон за експортния контрол на оръжия и изделия и технологии с двойна употреба - /ДВ, бр. 11/.2007 г./

6. Трифонов, Т, Търкаланов Ю. Тероризмът – рисков фактор за сигурността в Европа. В: новата архитектура на сигурността в Европа и ранното сигнализиране и предотвратяване на конфликти С., 1997.

7. Стоянов, Г. Рискове и заплахи за вътрешната сигурност на Р. България, С., 2000 г.

ПОЛИТИКАТА НА ДЪРЖАВАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Йордан Я. Първанов

София 1000, ул. Гурко № 6,

Дирекция "Център за реакция при инциденти във връзка с информационната сигурност"
Изпълнителна агенция "Електронни съобщителни мрежи и информационни системи"

STATE POLICY ON INFORMATION SECURITY

Yordan Y. Parvanov

Sofia 1000, ul. Gurko № 6

Main Expert in Directorate" Computer Security Incident Response Team"
Executive Agency "Electronic Communication Networks and Information Systems"

ABSTRACT: *In this article 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.*

KEY WORDS*: Information security, Cyber security, CERT*

Бързото развитие на информационните технологии и интеграцията на телекомуникационните системи през последните десетилетия доведе до тяхната глобализация, намираща изражение в появата на редица информационни мрежи. Използването на Интернет предоставя на всеки потребител достъп до електронни информационни услуги от всякакво естество, независимо в коя държава се намира той. Чрез свързването на тези системи, предоставящи тези услуги на потребителите създаде пространство, наречено "кибернетично пространство".

Значението на 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.

Кратко определение за **киберсигурността** – това са мерките, които се предприемат за защита на компютрите или компютърните системи срещу нерегламентиран достъп, 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.

След 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)".

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) 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. **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 сигурност", 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.

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. Това 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.

4. Закон за защита на личните данни
5. Закон за електронния документ и електронния подпис
6. Закон за електронната търговия

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.

Тази политика е във функциите и задълженията на Държавната комисия по сигурността на информацията. Контролни функции по спазването изискванията на посочените нормативни актове осъществява Държавната агенция "Национална сигурност".

II. Документи, свързани с информационната/киберсигурността и задължения за държавата, произтичащи от членството ни в 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.

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.

През 2004 г. НАТО осъзнава важността и започна активна дейност в областта. Започва се с подготовка на основополагащи документи по киберсигурността, изготвят се политики и дейности срещу последствията от кибер-тероризма, 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). Атакише 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 Cyber Defense 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 „Стратегическата концепция на НАТО-2010" приета в Лисабон миналата година.

Република България подписа 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 широко мащабни 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.

ЕС е подготвил проект на директива [1] с която да се отмени Рамково решение 2005/222/ПВР от 24.02.2005 г. относно атаките срещу информационните системи, като в нея ще се запазят нейните разпоредби и ще се включват следните нови елементи:

- в директивата се включват тестове за наказание производството, продажбите, доставките за употреба, вноса, разпространението или друга форма на предоставяне на устройства/инструменти, предназначени за извършване на компютърни престъпления;

- на широкомащабния аспект на атаките — "ботнети" или други подобни инструменти, ще се отговори с въвеждането на ново утежняващо вината обстоятелство, в смисъл че актът на създаване на ботнет или на подобенинструмент ще бъде утежняващ фактор при извършване на престъпленията, посочени в съществуващото рамково решение;

- когато такива атаки са извършени с прикриване на истинската самоличност на извършителя и нанасят щети на законния собственик на идентичността.Всички такива правила ще трябва да отговарят на принципите на законност и пропорционалност на престъпленията и наказанията и да бъдат в съответствие с действащото законодателство за защита на личните данни.

- въвежда се престъплението "незаконно прихващане";

- въвеждат се мерки за подобряване на европейското сътрудничество в областта на наказателното правосъдие чрез укрепване на съществуващата структура от звена за контакт, които са достъпни 24 часа в денонощието и седем дни в седмицата;

- разглежда се необходимостта да бъдат предоставяни статистически данни за престъпленията в кибернетичното пространство, като държавите-членки се задължават да направят необходимото за въвеждане на подходяща система за записване, производство и предоставяне на статистически данни за престъпленията, посочени в действащото рамково решение и за нововъведеното престъпление „незаконно прихващане".

Основната цел на директивата е да сближи правилата относно наказателното право на държавите – членки, в сферата на атаките срещу информационни системи и да подобри сътрудничеството между съдебните и другите компетентни органи, в това число полицията и други специализирани правоприлагащи служби на държавите - членки.

В дадените в директивата определения на престъпленията, изброени в членове 3, 4, 5 (незаконен достъп до информационни системи, незаконна намеса в системите и незаконната намеса в данните), се съдържа разпоредба, която позволява в процеса на пренос на директивата в националното законодателство да се инкриминират само „случаи, които не са маловажни".

До момента директивата не е влязла в сила и предстои нейното отразяване в националното законодателство.

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 – Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи – ИА „ЕСМИС" (преди това ДАИТС), 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:

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.

1. 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.

2. 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 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.

3. 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.

4. 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 кибер-заплахите 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.

Като страна - членка на ЕС, нашата страна положи усилия за прилагане на една от ключовите мерки за подсилване на способностите за кибернетична защита – провеждане на учение за отработване на компютърни инциденти. През ноември 2011 г. МТИТС беше домакин на първото учение за отработване на компютър

инцидент „Киберзима 2011". Основната цел на проведеното учение да тества някои мерки които ще се предприемат от Националния център за реагиране на компютърни инциденти и МТИТС, заедно и шест свои изпълнителни агенции, в отговор на възникнал инцидент в информационната сигурност.

Учението беше предшествано от някои основни насоки дадени от ENISA.

Основните ползи от проведеното учение могат да се обябощят така:

- Придфобиване на опит за съвместна работа на представители от различни организации;
- Споделяне на добри практики за защита на информацията в ИС;
- Тестване на процедури за реагиране на инциденти;
- Тестване на лицата за контакти и различните канали за обмен на информация при възникване на инцидент в информационната сигурност;
- Тестване на степента на готовност за реагиране на инциденти в информационната сигурност;

Резултатите от проведеното учение ще се използват като база за провеждането на подобни бъдещи учения.

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 сигурност/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.

БИЗНЕС РАЗУЗНАВАНЕТО – ОСНОВА НА КОРПОРАТИВНАТА СИСТЕМА ЗА СИГУРНОСТ

Красимир П. Манев

Русенски университет "Ангел Кънчев", Катедра: "Телекомуникации", тел.: 082/888 780, e-mail: kmanev@uni-ruse.bg

BUSINESS INTELLIGENCE –CORPORATE SECURITY SYSTEM BASE

Krasimir P. Manev

ABSTRACT:*This paper focuses on business intelligence as a key point for increasing organization's security. Business organization's security is a complex state between its internal and external environment, in which threads against organization's survival and development are minimized and necessary measures are taken to compensate harm of possible losses. To comply with the influence of the environment and to respond appropriately, instead of standing idly, the management of business organization needs information about it and here business intelligence is applied. The product or result of competitive intelligence analysis is the information, which helps to make correct and timely management decisions and, thus, to achieve competitive advantage.*

Key words: *Information security, Risk, Data warehouse, Network accounts.*

Съвременната икономическа и социална ситуация е многомерна и сложна, подложена на чести изменения. Множество различни събития в бъдеще могат както да противодействат, така и да способстват за успеха на планираните действия. При вземането на управленски решения е невъзможно да се получат точни и пълни знания за всички действащи и потенциални вътрешни и външни фактори. Поради това планираните от бизнес организациите стопански мероприятия се реализират в условия на неоднозначно протичане на реални социално-икономически процеси, в многообразието на възможните състояния и ситуации, в които може да се окаже самата бизнес организация. Неточността, неопределеността на необходимите за планирането данни могат да доведат до съществени разминавания между плана и реалността.

Вземането на решения винаги се осъществява в условия на непълна информация. Непълната информация за предпочитанията на лицата вземащи решения и непълната информация за съвкупността от алтернативи, се явяват важни характеристики на реалния процес за вземане на решение. Неопределеността, свързана с бъдещето поведение на потребителите на продукцията, доставчиците, партньорите, конкурентите, с бъдещето състояние на общата конюнктура, с бъдещето търсене и предлагане на работна ръка, с постиженията на научно-техническия прогрес, с достъпността на запасите от ресурси, значително усложняват проблемите, свързани с вземането на управленски решения.

1. Бизнесът и несигурността

„Единственият „риск“, който води до печалба, е уникалната несигурност... Печалбата се поражда от вътрешно присъщата абсолютна непредвидимост на нещата.“
Франк Найт,
икономист от Университета в Чикаго, 1921 г.

Бизнес организациите (фирмите, предприятията, компаниите) функционират под въздействие на външната и вътрешна среда, т.е. държавните органи, обществените организации, националната политика, партньори, потребители и персонала на самата организация - фиг. 1.

Фиг. 1. Функционална среда на бизнес организацията

Това предполага необходимостта от вземане под внимание на всички техни интереси и изисквания.

Характеризирайки днешните реалности като „турболентни“ реалности на информационната епоха У. Бек пръв доказва тезата за „рисковото общество“, т.е. за съвременното общество като общество на „серийно произвеждани несигурности“. Впоследствие несигурностите, с които се сблъскват ръководителите и експертите в българското общество, са анализирани през призмата на четири основни характеристики [2]:

- непостоянство на човешкия разум;
- неоднородност на действащите критични фактори;
- неоднозначност на моделите за текущата ситуация;
- недостатъчността на информацията за промените и закономерностите в еволюцията на обкръжението.

Тези четири „не“, лежащи в основата на несигурностите, имат както субективен, така и обективен характер.

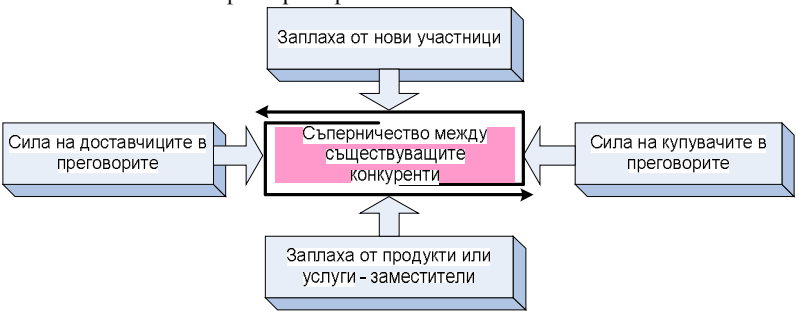
Комплексният, концентрираният източник на несигурностите в пазарната икономика като цяло е неопределеността. Това понятие може да бъде охарактеризирано като състояние достатъчно сложно и динамично, когато към неяснотата по отноше-

ние на действащите фактори и механизми, се добави неяснотата по отношение на желаното състояние на бизнес организацията и на методите и начините за неговото постигане. Увеличаването на несигурността е резултат от различни фактори.

На първо място, става дума за неопределеност, произтичаща от външната среда на бизнес организацията – фиг. 2.

Фиг. 2. Външна среда на бизнес организацията

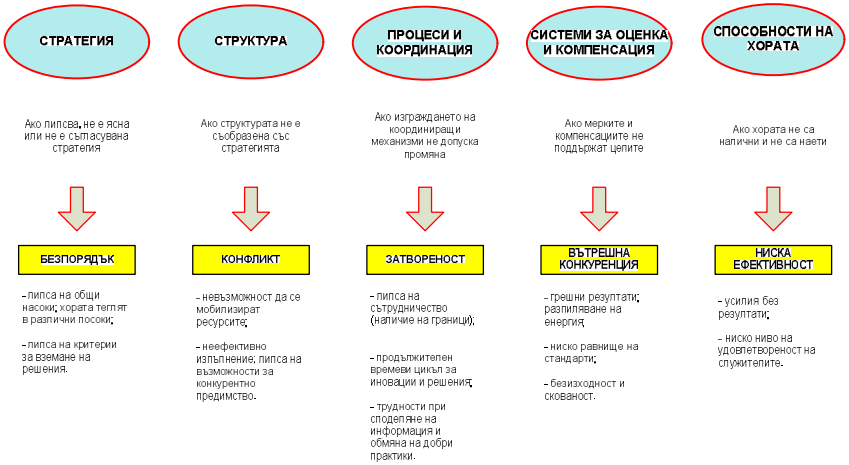
Според М. Портър върху бизнес организацията в рамките да даден пазар влияние оказват пет основни фактора – фиг. 3.



Фиг. 3. Конкурентни сили на пазара

На второ място, става дума за неопределеност, свързана с вътрешната среда на организацията – фиг. 4 и фиг. 5.

Фиг. 4. Фактори дефиниращи вътрешната среда в бизнес организацията



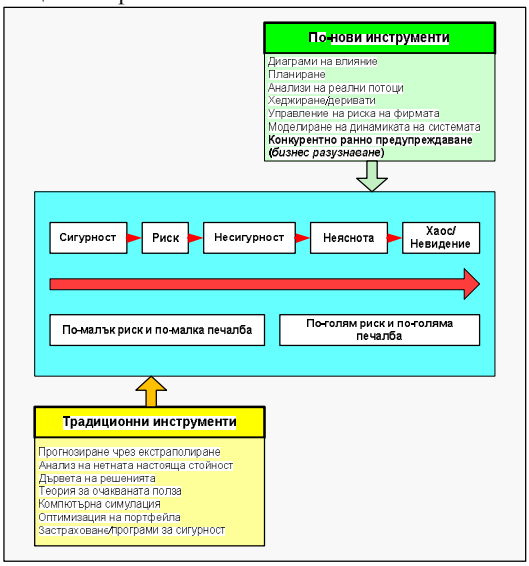
Фиг. 5. Неопределености, вследствие несъгласуваността на вътрешната среда

За да може да се съобрази с влиянието на средата и да реагира адекватно, вместо да стои безучастно, мениджмънтът на бизнес организацията се нуждае от информация за нея. Същият се интересува особено много от два нейни параметъра – стабилност и сложност.

В обкръжението на бизнес организацията постоянно настъпват изменения. За нейното управление е съществена скоростта на измененията и възможността да се прогнозира направлението им. От тази гледна точка се разграничават устойчива и динамична среда. От позициите на сложността на характеризиране и прогнозиране се разграничават проста и сложна среда – фиг. 6.

Фиг. 6. Природа на средата

Предизвикателствата са свързани не само с размера на несигурността, но и с променливата й същност – фиг. 7.



Фиг. 7. Промяна в посока на по-голяма неяснота

Лявата страна на спектъра е най-управляема и поддаваща се на аналитичен подход. В средата на спектъра се сблъскваме с неяснотата, за която настоящите инструменти и техники са по-малко приложими. Предизвикателството в средата в по-малка степен подлежи на изчисляване, отколкото на познание, за да може да се постигне сигурността, че проблемите се установяват точно.

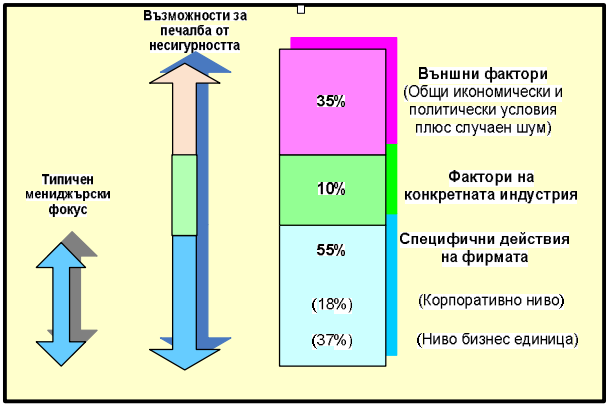
Голямото предизвикателство е във факта, че светът като цяло се движи надясно към по-високи нива на неяснотата и дори на хаос в много сектори и индиустрии. Несигурността в дясната част на спектъра е много по-трудна за управление в срав-

нение с поддаващите се на определение рискове в лявата му част. С колкото по-малко неяснота се сблъскваме, толкова по-сигурни сме, че проблемът може да бъде структуриран, управляван, планиран и контролиран. Но конкуренцията също може да направи това, така че възможността за предимство е намалена. Необходимо е да се научим как да приветстваме и наистина да се радваме на неяснотата. При неяснотата се сблъскваме с риска не само от вземането на решение, но и с нещо по-дълбоко – което е наречено епистемичен риск – риска от незнанието. С придвижването на света от относителна сигурност към по-високи нива на неяснотата епистемичният риск нараства – фиг. 6.

Защо е важно да се акцентира върху несигурността?

- Първо, защото тя засяга част от бизнеса, който мениджърите често дори не се и опитват да управляват – външната среда – а именно това е мястото, където се създава или разрушава голяма част от потенциалната стойност на бизнеса.
- Второ, степента на несигурността в бизнес средата се увеличава значително.
- Трето, човекът е вътрешно ограничен при боравене с несигурността.

Докато мениджърите концентрират вниманието си върху съществуващият бизнес, управлението на външната несигурност би могло да има далеч по-голям потенциал за печалба. Проучванията в широк спектър от индустрии разкриват, че специфичните за дадена фирма дейности ú носят само половината от печалбата. Около половината от възвращаемостта от инвестициите се дължи на общите икономически условия (макросредата) и условията в дадената индустрия (микросредата) както е показано на фиг. 8.



Фиг. 8.Половината от бизнеса е оставен на благоволението на съдбата[1]

Виждането, което доминира в съвременната теория на организацията е, че тя е социално-икономическа цялост, която:

- преследва определени цели;
- представлява по определен начин структурирана и координирана активна система;

[1] Процентът отразява каква част от дисперсията на възвращаемостта на активните средства се дължи на различни фактори.

- постоянно се приспособява и въздейства върху средата – външна и вътрешна.

От най-общи позиции сигурността отразява начините и равнищата на взаимодействие на организацията с външната и вътрешната среда, в която тя работи и се развива. В тази връзка, българският изследовател проф. д.ик.н. Д. Йончев, пише: „Разбирането на сигурността изисква познаване на средата на сигурност… Средата е пряко свързана със сигурността на присъстващия, тъй като присъствието е съвкупност от взаимодействия на присъстващия с неговата среда. Когато той ги контролира говорим за сигурност, когато губи контрола върху тях (става въпрос за взаимодействията със средата) говорим за криза. Средата на сигурност, когато е в норма, влияе на сигурността чрез три типа взаимодействия – предизвикателства, заплахи и рискове.“

Следователно, когато говорим за сигурност на една или друга организация в условията на рисковото общество, неопределеността трябва да се разглежда като конституиращ признак, т.е. като среда за проява на предизвикателства, заплахи и рискове.

Връзката между средата – вътрешна и външна – и организацията се свежда до две основни състояния на средата:

- състояние на норма;
- състояние на криза.

Сигурността на организациите изисква взаимодействие със средата и тогава, когато нейното състояние е в норма, и тогава, когато състоянието й е в криза. Следователно:

Сигурността на организацията (корпоративна сигурност) представлява такова комплексно състояние на средата (външна и вътрешна), при което възможностите да се актуализира силата на факторите, насочени срещу оцеляването и развитието на организацията, са минимизирани и са взети необходимите мерки за компенсиране на вероятни загуби.

Уточнявайки определението „сигурност на организацията“ е необходимо да се отбележи, че едва ли е необходимо да се доказва, колко по-важно и по-ефикасно за организациите е създаването и поддържането на сигурност, основана върху „улавянето“ на симптомите и адекватната реакция при предизвикателства, заплахи и рискове, отколкото да се създава сигурност, когато вече е нестъпило състоянието криза.

ИЗВОД:

Бъдещето на обществото и фирмите става невъзможно без непрекъснато придобиване на знания и умения необходими за стратегически прозрения по овладяване на несигурностите и противопоставяне на вредните тенденции и прояви.

2. Система за конкурентно ранно предупреждаване

„Разузнаването е част от съвременната бизнес култура“
адмирал Пиер Лакост, бивш шеф на Френското разузнаване,
преподавател по управление на фирмената сигурност
в Университета Марк-ла-Вале, Франция

Основната причина, според която бизнес организациите и техните мениджъри така често се оказват неспособни систематично да управляват стратегическите рискове, се заключава в това, по какъв начин самите бизнес организации идентифицират самите рискове.

Робърт Саймън определя стратегическият риск като „*неочаквано събитие или съвкупност от условия, които съществено намаляват способността на мениджърите за практическо осъществяване на приетата бизнес стратегия*“. Той различава три основни типа стратегически риск:

- операционен риск;
- риск за обезценяване активите;
- конкурентен риск.

Последният тип риск има отношение изключително към външните фактори, т.е. към измененията в конкурентната среда. Именно поради тази причина, стратегическият риск представлява по същество, рискът за това, че самата стратегия не е съгласувана с пазарните условия.

Съществуват два основни метода за управление на стратегическите рискове:

- до тяхното възникване;
- след тяхното появяване – известен още като риск-мениджмънт.

Първият метод е насочен към предотвратяване на кризисните ситуации. Това означава, че рисковете трябва да се управляват проактивно, т.е. още при възникването на първите проблематични признаци, или в краен случай, бързо реагиране на настъпващото опасно обстоятелство, докато загубите все още не са така големи.

За да се постигне тази цел е необходима силна интеграция в действията на бизнес разузнаването, стратегическото планиране и мениджмънта за постигането на системна, непрекъсната, осъществявана в рамките на цялата бизнес организация идентификация на рисковете, осъществявани достатъчно рано, за да се игнорира или минимизира тяхното въздействие. Този подход по същество изразява същността на системата за конкурентно ранно предупреждаване.

Механизмът на конкурентното ранно предупреждаване се базира на три взаимно свързани стъпки, водещи към непрекъснато подобряване на бизнес стратегията съобразно въз основа на своевременното разкриване както на рисковите признаци, така и на разкриващите се възможности. Тези стъпки схематично са изобразени на фиг. 9.

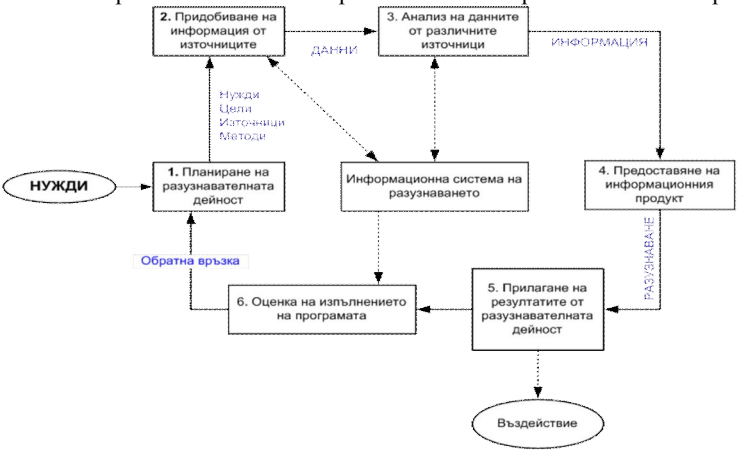
Фиг. 9. Компоненти на системата за конкурентно ранно предупреждаване

Тези три стъпки в структурата на системата за конкурентно ранно предупреждаване започват с идентификацията на зоните за стратегическите рискове (естествено и на зоните за разкриващите се възможности), след това се преминава към разузнавателния мониторинг на признаците и се приключва с предприетите действия от страна на мениджмънта.

За идентификация на ранните рискови признаци, с помощта на методите и средствата на бизнес разузнаването се осъществява постоянен мониторинг както на

факторите от външната среда, негативно въздействащи върху бизнес организацията, така и на разкриващите се възможности.

Бизнес разузнаване (Business Intelligence) представлява дейност, свързана със събирането и обработката на информация (фиг. 10) с цел снижаване ефекта на неопределеността в процеса на изработване и вземане на управленски решения, осъществявана в рамките на закона и при спазване на морално-етичните норми.



Фиг. 10. Същност на бизнес разузнаването

Окончателен тест в процеса на приоритетизацията на рисковете, се явява оценката на измененията във външната среда въз основа на измененията на фона на петте сили на М. Портър – фиг. 11.

Фиг. 11. Приоритетизация на рисковете въз основа на модела на М. Портър

ИЗВОД:

Целта на дейността по обезпечаване сигурността на фирмата е, преди всичко така да се взаимодейства с предизвикателствата, риска и заплахата, че да не се достига до криза, а ако това се случи – тя да се ограничи максимално във времето, да се намалят до минимум жертвите и загубите, а бизнес организацията да излезе колкото може по-бързо и по-съхранена от нея.

ЗАКЛЮЧЕНИЕ

Бизнес разузнаването като вид дейност тепърва прохожда в нашата страна. Независимо от своята младост, то придобива все по-осезаемо своето развитие. Все повече стават тези, в чиито функционални задължения влиза вземането на решения, които достигат до убеждението, че единствено с помощта на бизнес разузнаването те могат оперативно да получат необходимите им информационни ориентири, позволяващи им да направят правилният избор. Много често – единствено правилен.

ЛИТЕРАТУРА

1. **Георгиев Р.** *Делови решения и сигурност на организацията*. София, „Софтрейд“, 2007. ISBN 978-954-334-056-9.

2. **Джилад Б.** *Конкурентная разведка. Как распознавать внешние риски и управлять ситуацией.* Москва: ПИТЕР, 2010. ISBN 978-5-49807-304-0.

3. **Сариев И.** *Мениджмънт на информацията.* София, „Класика и Стил“, 2007. ISBN 978-954-327-041-5

4. **Станчева А.** *Основи на управлението.* Варна: СТЕНО, 2006. ISBN-10: 954-449-277-1. ISBN-13: 978-954-449-277-9

5. *Международни отношения*, брой 3, 2010 г. ISSN 0324-1092

ДЪРЖАВА И СИГУРНОСТ

УПРАВЛЕНИЕТО ПРИ КРИЗИ КАТО ФАКТОР ЗА ЗАЩИТА НА НАЦИОНАЛНАТА СИГУРНОСТ

Георги Г. Гоцев

CRISIS MANAGEMENT AS A FACTOR IN NATIONAL SECURITY PROTECTION

Georgi Gr. Gotsev

Abstract: *The report reveals the problem of a crisis as a social phenomenon which needs to be developed and studied not only in terms of scientific interest but also because of the need of adequate population response in cases of critical situations. Furthermore, the interrelation between crisis management and national security protection has been explicated.*

Key words: *crisis management; national security protection.*

Още от своето възникване човешкото общество постоянно е било съпътствано от необичайни и внезапно възникващи събития, които са били източник на заплахи за основните ценности на хората. Разрушителната сила на природните явления и постоянната опасност от предизвикани от самите хора инциденти формират динамична и рискова среда, в която живеем и сега. Няма сфера на обществения живот, която да е защитена от негативни катаклизми, защото предизвиканите от тях кризи са производна и съставна част от еволюционното развитие на хората и обществените системи. Животът показва, че колкото по-високо е нивото на общественото развитие, толкова по-често обществото ни ще бъде съпътствано от кризи от различен характер.

В тази връзка предизвикателството да живеем в такава среди обуславя острата необходимост от преосмисляне на съществуващите възгледи за кризите и критичните ситуации, свързани с тях. Още повече, че в условията на изграждане на нова, по-надеждна и широкообхватна международна система за сигурност въпросът за кризите е все по-актуален, особено за региони и страни като Балканите и България, в които съществуват фактори, които могат да ги предизвикат и в бъдеще.

Понятието "криза" е известно от дълбока древност. В най-общ смисъл с него се обозначава разстройването на функционирането на дадена система, нарушаването на обичайно протичащите в нея процеси и необходимостта да се вземат решения за справяне с това състояние. Тя се предизвиква от внезапно възникнали събития, вследствие на които се нарушават възможностите на отделната личност, социална група или общностна система да се ориентира нормално в създадената нова среда.

Кризата е промяна на установеното състояние на живот, обхванала територии, обекти, сектори и сфери на икономиката и обществения живот или околната среда, предизвикана от човешка дейност или природни явления, в резултат на която условията за съществуване и за осъществяване на дейност в променената среда са силно променени [1].

Без да се спирам задълбочено върху същността на кризата като социален феномен, трябва да посоча, че възникването на кризи е възможно само в човешка среда. Две са нейните основни характеристики: първо, че кризата е състояние на човека или дадена социална система и второ, че това състояние е различно от обичайното, нормалното. Широкото определяне на кризата като състояние в известна степен ограничава нейното разбиране в динамика и не показва достатъчно пълно нейната зависимост от човешката дейност. Вероятно причина за това е обстоятелството, че най-често терминът "криза" натоварва съзнанието на хората с отрицателна енергия и те я свързват с бедствия, аварии, катастрофи и други, застрашаващи сигурността им катаклизми. Без да се противопоставят тези понятия трябва да се подчертае, че кризата е промяна в дадена обществена система, породена от действия, инциденти, явления и процеси, възникващи и отразяващи се в нея, докато бедствията, авариите и катастрофите са конкретните причини за възникване на кризите. Възприемането на тази дълбока причинно-следствена връзка би спомогнало за изграждането на единен подход при оценяването и справянето с тези събития или за организиране на съществуването в условия, породени от тях.

По своя характер и мащаб кризите могат да имат да имат различни измерения, но от гледна точка на националната сигурност интерес представляват тези, които засягат жизненоважни интереси на обществото и пряко или косвено са свързани с тяхната защита. Въпреки тяхната неопределеност, съчетаващи различни типове събития, възможните кризи могат да бъдат сведени до четири основни вида: военнополитически, вътрешнополитически, кризи вследствие на природни бедствия или предизвикани от човек инциденти и кризи с наши граждани зад граница. Независимо от характера на кризата обаче, за управлението при създадените от нея условия е най-важно да се направи всичко възможно за минимизиране на отрицателните за обществото последствия.

Управлението при кризи е основна функция на държавата. В исторически план главната причина за възникване на държавата е била нуждата на дадена човешка общност да се защити срещу външни опасности, да гарантира сигурността си във всички възможни аспекти на това понятие и да се управлява ефективно, ако тази сигурност бъде нарушена . От своя страна състоянието на системата за управление при кризи на държавата е основен критерий за състоянието на държавността в нея.

Умението да се управлява в условия на кризи е един от основните подходи за гарантиране на националната сигурност и международната стабилност. Съвременното разбиране на този проблем предполага реагирането на кризи да става организирано, при взаимно сътрудничество между институциите, с ясно определени компетенции на всеки орган и целесъобразно използване на националните ресурси.

В голяма степен възможностите на държавата да предотвратява и овладява кризи, както и да преодолява последици от такива, се определят от наличието на функционираща система за управление при кризи, получаване на информация за рисковете от възникването им и поддържане на подготвени органи и добре екипирани сили за действие в случаи на кризи. Спецификата на кризата като явления, отразя-

ващо се основно върху човешкото общество, задължава държавните институции и обществото да реагират адекватно на рисковете и заплахите от тяхното възникване и да развиват способности да защитават гражданите, материалните и културните ценности в случаи на такива.

Във връзка с горното, през последните години и в нашата страна значително нараства потребността от създаване на национална система за реагиране при кризи, чрез която да се осигурят функциите на държавата за гарантиране на живота и здравето на населението и опазване на духовните и материалните ценности на страната и нейните граждани. В отговор на това бяха предприети конкретни законодателни действия за регламентиране дейността при кризи, в резултат на което през февруари 2005 г. 39-то Народно събрание прие Закон за управление при кризи.

До приемането на Закона за управление при кризи в Република България беше създадена и функционираше система, свързана главно със защита на населението при бедствия, аварии и катастрофи. Това беше регламентирано с Правилника за организацията и дейността по предотвратяване и ликвидиране на последствията при бедствия, аварии и катастрофи, приет с ПМС № 18 от 23.02.1998 г. Създадената с правилника организация, наред с положителните си страни създаваше определени трудности при управлението при кризи, свързани главно със социални конфликти, въоръжено насилие, масово нарушаване на обществения ред или други остри прояви на организирана престъпност. Тя не определяше реда за действие на Министерския съвет като централен орган на изпълнителната власт в случаи, когато кризата обхване по-голяма част от територията на страната или застраши във висока степен интересите на обществото или държавата. И не на последно място, тя не съответстваше в пълна степен на изградените в страните от Европейския съюз, НАТО и други международни организации и държави системи за реагиране при кризи.

Посочените пропуски се преодоляваха в голяма степен с приетия през 2005 г. Закон за управление при кризи (ЗУК). Негов предмет бяха организацията, основните функции, задачите, правата и задълженията, както и принципите на взаимодействие на органите на държавната власт и местното самоуправление, на физическите и юридическите лица в условията на кризи. Уреждайки обществените отношения, свързани с предотвратяването и овладяването на кризи и ликвидиране на последиците от тях, законът регламентираше изграждането на Национална система за управление при кризи. Нейната основна задача беше интегрирането на способностите на системата за сигурност на страната в единна система за реагиране при кризи. В закона се акцентираше върху повишаване на възможностите за превенция и прилагането на мерки за реагиране в широк спектър от кризи, включително и на специални мерки при провеждане на антитерористични операции, операции за реагиране при нарушаване на държавната граница, въздушното и морското пространство на Република България, за защита на критичната инфраструктура, а така също и прилагането на мерки за ликвидиране на последствията от кризи и осигуряване на възмездяване на щетите при такива.

Съгласно § 14 от преходните и заключителни разпоредби на ЗУК в срок 6 месеца след неговото приемане правителството трябваше да издаде подзаконовите документи по неговото прилагане (2 правилника и 6 наредби). Тъй като крайния срок за приемане на тези актове не беше спазен, след приемане на закона системата за действие при кризи в страната, включително в следствие на бедствия, аварии и катастрофи, не функционираше пълноценно.

След създаването на Министерството на държавната политика при бедствия и аварии, независимо от декларираните намерения, неговото ръководство поде инициативата за разработване и приемане на изцяло нов закон, уреждащ обществените отношения в тази област. Беше подготвен, а през декември 2006 г. и приет Закон за защита при бедствия. Той беше внесен в Народното събрание с мотива, че е специален закон, допълващ ЗУК и уреждащ обществените отношения само във връзка с осигуряването на защитата на живота и здравето на населението, както и имуществото при бедствия. Постепенно в процеса на неговото приемане по настояване на вносителите беше внесено и предложение за сериозно изменение на Закона за управление при кризи, с което неговите предимства на основен, функционален закон, бяха премахнати. В същото време беше направено всичко възможно подзаконовите актове за прилагане на ЗУК да не бъдат приети, с което на практика не се позволи той да функционира нормално и да изпълни предназначението си.

Стремежът на определени среди в страната да не допуснат Законът за управление при кризи да функционира беше реализиран с решението на Народното събрание за приемането на § 2, т. 3 на Закона за отбраната и въоръжените сили на Република България (обн. ДВ бр. 35 от 12 май 2009 г.) и отмяната на Закона. По този начин единственият закон, който в момента урежда част от отношенията в тази област, е Закона за защита при бедствия.

Отмяната на Закона за управление при кризи доведе до невъзможност обществените отношения в тази сложна област да се регулират цялостно със сегашното законодателство. Законът за защита при бедствия урежда дейността основно за защита на живота и здравето на населението, опазването на околната среда и имуществото при бедствия. Той не създава регламент за организиране дейността на съответните органи в условия на сложни кризи, особено вследствие на социални конфликти. Законът за МВР като устройствен закон регламентира само задачите, дейностите и правомощията на органите на министерството по осигуряване на обществения ред и защитата при бедствия, но не и общото управление на страната при кризи с висока обществена опасност.

Състоянието на националната система за управление при кризи беше обсъдено на заседанието на Съвета по сигурността към Министерския съвет на 30.03.2011 г. На заседанието беше потвърдена необходимостта от законова регулация на обществените отношения в условия на кризи и по принцип се прие да се предприемат мерки в тази посока, включително да се подготви нов закон за управление при кризи.

За да се изясни доколко управлението при кризи е фактор за защита на националната сигурност е необходимо да сме наясно с това как се защитава тя. Трябва да си припомним, че основните документи в областта на националната сигурност целят формиране на обществен консенсус относно националните интереси и цели, които и да определят пътищата за тяхното осъществяване. Политиката за сигурност на страната ни и стратегията за нейното реализиране са насочени към осъществяване на няколко дългосрочни цели:

- осигуряване на благоприятна жизнена среда на българските граждани;
- осигуряване на защита срещу посегателствата върху демократичните права и свободи на гражданите и обществото и тяхната сигурност;
- активно участие във формирането на благоприятна външнополитическа среда и ефективно интегриране на страната в колективните системи за сигурност;

- адекватен отговор на текущи предизвикателства и защита на националните интереси в условия на кризи.

Както се вижда, националната сигурност трябва да бъде осигурена при всякакви условия, включително при кризи. Националната сигурност като състояние на благоденствие на обществото винаги може да бъде подложено на негативно въздействие и в една или друга степен да бъде изменено. По същество нарушаването на някой аспект на националната сигурност е криза на това състояние и налага определени мерки за неговото стабилизиране. Управлението на този процес е кризисно управление, целящо преодоляване на възникналите проблеми и възстановяване на стабилността.

Системата за защита на националната сигурност включва различни органи, осъществяващи националната политика за сигурност. Тази система е изградена и функционира в съответствие с изискванията на Конституцията и законите на страната и отразява политическата воля на обществото да бъдат гарантирани суверенитета, независимостта и териториалната цялост на държавата и защитени основните права и свободи на нейните граждани. Нейното основно предназначение е:

- да определя и оценява рисковете и заплахите за националната сигурност;
- да взема решения за пътищата и средствата за тяхното предотвратяване;
- да поддържа постоянни материални и човешки ресурси за провеждане на необходимите действия за защита на интересите на обществото чрез адекватни на средата за сигурност средства и способи.

Съгласно законите на страната основната отговорност за националната сигурност на страната е възложена на Народното събрание, на Президента на републиката и на Министерския съвет. Особено значима за това е ролята на изпълнителната власт, която реализира основните политики в областта на националната сигурност. Системата за национална сигурност в голяма степен зависи от съществуващите рискове и заплахи и трябва да създава способности за тяхното неутрализиране. Ако я съпоставим с Националната система за управление при кризи ще видим, че двете системи имат идентични органи за управление и се различават по особености, свързани с кризисното управление

Доказано е, че защитата на националната сигурност е приоритет, който винаги ще доминира в обществото, независимо от нейното временно състояние. А възможността стабилността на държавата и обществото да се съхранят и в условия на върхови изпитания в голяма степен зависи от способността им за управление при кризи. За да бъде реален фактор за защита на националната сигурност, е необходимо управлението при кризи да бъде поставено на здрави нормативни основи. Ето защо законовото регламентиране на това управление е първостепенно условие за защита на националната сигурност. Това е посочено и в приетата през 2011 г. Стратегия за национална сигурност, където необходимостта от такъв закон е поставена редом с нуждата от Закон за национална сигурност. Какво друго е необходимо за ефективно управление при кризи, засягащи националната сигурност?

На първо място управлението при кризи се нуждае от ясен понятиен апарат, от единност на концептуалните подходи за осъществяване на тази дейност и точно определени цели пред това управление. При сложните кризисни ситуации, в които може да изпадне обществото и държавата, това е още по-необходимо, защото във всички случаи крайната цел на това управление е минимализиране на обществено опасните последици от кризите. Ето защо целият управленски процес от предотв-

ратяването, през овладяването до преодоляването на последиците от кризите трябва да се осъществява по ясни правила, с общоприети цели и при взаимодействие, почиващо на пълно разбирателство между участващите в него. Точният понятиен апарат предопределя правилното възприемане на задачите и тяхното успешно решаване без съществени различия или противопоставяне при планирането, организирането и осъществяването на дейностите.

На следващо място управлението при кризи се нуждае от стройна система с ясно определени елементи, с точно регламентирани отговорности и взаимни връзки. Задачите на участващите в кризисното управление често са свързани с дейности, налагащи значителни ограничения на правата и свободите на гражданите, както и промени в създадените обичайни обществени отношения. Това важи особено за органите за управление, които в условия на кризи ще трябва често да вземат и непопулярни мерки, понякога на ръба на закона. Съществуващата в момента организация до голяма степен е свързана с дейността на Единната спасителна система и с реакциите на нейните съставни части при една или друга ситуация. Не е регламентирана ясно връзката между органите за управление и участващите в самите операции сили, особено взаимодействието им при възникване на сложни кризисни ситуации.

На трето място успехът на кризисното управление в голяма степен зависи от предварителната му подготовка. Създаването на единна система за планиране и подготовка, разработване на методики за оценка на риска във всички области на обществения живот, почиващи на експертни оценки и на прогнозни сценарии, изискват ясна законова регламентация на отговорностите. Всяко ниво от системата трябва да е предварително готово да действа при възникване на криза и да сведе до минимум изненадата от нейните отрицателни въздействия. Това до голяма степен беше решено с отменения Закон за управление при кризи. При него бяха очертани отговорностите на различните управленски нива, техните задачи и правомощия. Докато въпросите на планирането бяха регламентирани сравнително пълно, то и в него създаването на временни специализирани органи за управление при кризи беше маркирано бегло, без отчитане на първостепенното им значение при организиране и ръководство на дейностите при възникване на кризисна ситуация. Това е проблем, без решаването на който е немислимо успешното управление при кризи.

На четвърто, но не на последно по значение място, успешното управление при кризи се нуждае от ефективна система за ранно предупреждение. Непрекъснатото наблюдение на рисковите фактори, денонощната ситуационна осведоменост и постоянната готовност на дежурни сили ще позволи своевременно и адекватно реагиране на негативните процеси и в голяма степен ще предопредели успешното управление. Наличието на единна национална система от дежурни оперативни центрове, в които ще се поддържа необходимата информация за рисковете и за готовността за реагиране, ако те прераснат в заплахи, трябва да се създаде със закон, с който както да се възложат задачите, така и да се осигурят ресурсите за тяхното изпълнение.

Може би най-важния въпрос, свързан с успешното управление при кризи е този с подготовката на всички елементи от системата да реагират адекватно в целия управленски процес. Поради важното им място в процеса това се отнася най-вече до органите за управление. Тяхната подготвеност да планират и организират изпълнението на плановете до голяма степен предопределя успеха на кризисното управление. От друга страна подготовка е необходима и на специализираните

структури, които участват в управлението при кризи главно чрез провеждане на различни по характер операции. На трето място подготовка е необходима и за населението, което поема тежестите на възникващите кризи и трябва да знае какво поведение да има при тяхното въздействие. Това налага приемане на законови разпоредби за организиране на подготовката на всички посочени категории, с което процесът на изграждане на цялостна система за реагиране при кризи да бъде завършен. В сегашното законодателство този въпрос не е решен и създава сериозни проблеми пред управлението при кризи.

Разбира се, могат да се посочат достатъчно други пътища за повишаване ефективността на управлението при кризи като фактор за защита на националната сигурност. Такива са необходимостта от регламентиране на степените на опасност от възникване на различни по характер кризи и действията, които трябва да се предприемат в случаи на такива. Успешното управление при кризи се нуждае от единни стандартни процедури, единна комуникационно-информационна среда и единни критерии за оценка на готовността и на действията на органите и силите при кризи.

Всички изброени по-горе насоки за усъвършенстване на националната система за управление при кризи са важни предпоставки за нейното утвърждаване като фактор за защита на националната сигурност. Съществуващите реалности и тенденциите за повишаване на риска от природни, техногенни, екологични и социални катаклизми категорично поставят изискването за оптимално използване на управленския потенциал и ресурсите на страната за развитие на нейните способности за овладяване на различни по характер кризисни ситуации. За целта е необходимо да се предприемат преди всичко правно-нормативни мерки за оптимизиране на системата за реагиране при кризи, която да отговаря на изискванията на съвременните предизвикателства и да бъде в съответствие със системите на другите страни, членки на ЕС и НАТО. Въпросът е тази система да не се изгражда самоцелно, а да бъде подсистема на системата за защита на националната сигурност и да работи в интерес на сигурността на страната.

Литература:

1. Закон за управление при кризи. ДВ, бр.19/1 март 2005г., отм. ДВ, бр. 35 от 12 май 2009 г.

ВЪТРЕШНАТА СИГУРНОСТ КАТО ФАКТОР ЗА ГАРАНТИРАНЕ НА НАЦИОНАЛНАТА СИГУРНОСТ

Георги Г. Гоцев

THE INTERNAL SECURITY AND ENSURING OF THE NATIONAL SECURITY

Georgi Gr. Gotsev

Abstract: *The development of society is accompanied by the appearance of negative processes, making favorable conditions for organized resistance or other forms of illegal behavior. In order to ensure society's security a system for protection of the internal security has been developed.*

Key words: *national security; internal security.*

Всяка държава в зависимост от нейния международен статут, политически и икономически суверенитет и специфични национални ценности и интереси определя националната си сигурност. "Стратегията за национална сигурност на САЩ се основава на тясно очертания американски интернационализъм, който отразява единството на нашите ценности и национални интереси. Целта на стратегията е да помогнем на света да стане по-мирен, но и по-сигурен. Тази цел ще постигнем по пътя на прогреса, постигане на политическа и икономическа свобода, на мирни взаимоотношение с другите страни и зачитане на човешкото достойнство" [1]. В Закона на Руската федерация "За сигурност" националната сигурност е дефинирана като "Състояние на защитеност на жизнените интереси на личността, обществото и държавата от вътрешни и външни заплахи" [2]. В националната концепция за сигурност на Република Латвия, одобрена от парламента на страната през месец януари 2002 г. "националната сигурност на Република Латвия е способността на държавата и обществото да защитят и обезпечат националните си интереси и основни ценности" [3].

Според официалната, приета през 1998 г. от Народното събрание на Република България, Концепция за национална сигурност: "Национална сигурност има, когато са защитени основните права и свободи на българските граждани, държавните граници, териториалната цялост и независимостта на държавата, когато не съществува опасност от въоръжено нападение, насилствена промяна на конституционния ред, политически диктат или икономическа принуда за държавата и е гарантирано демократичното функциониране на държавните и гражданските институции, в резултат на което обществото и нацията запазват и увеличават своето благосъстояние и се развиват. Сигурността е гарантирана, когато страната успешно реализира националните си интереси, цели и приоритети, и при необходимост е в състояние ефективно да ги защити от външна и вътрешна заплаха" [4].

Макар и дефинирани различно, общото в многото съществуващи определения за националната сигурност е, че националните измерения на сигурността обхващат всички онези предизвикателства, рискове, заплахи и опасности за сигурността,

които възникват и действат, или на които се търси отговор и биват преодолявани на нивото на националната държава. Макар и национални, тези измерения на сигурността отчитат влиянието на регионалните и глобалните фактори, но запазват националната си същност и преди всичко националния си характер, история, нрави, традиции, националното целеполагане и управление.

Националната сигурност в нейната многоаспектна същност предполага тя да бъде разглеждана като комплексно явление, което се декомпозира на сфери на сигурност в зависимост от различните аспекти на обществения живот. Тази комплексност е породена от самата системност и интегралност на обществото и зависи от различни фактори, свързани с националната сигурност. Това дава основание съдържанието на националната сигурност да се представи като съвкупност от сфери за сигурност: политическа, икономическа, военна, социална, екологична и т.н.

Комплексността на националната сигурност се определя и зависи от различни фактори: географски, икономически, социално-политически, военно-политически, демографски, етнически, религиозни и др. Главни елементи на тази система са личността като биосоциална система, социалната група, обществото, държавата. В тази връзка може да определим националната сигурност като съвкупност от връзки и отношения, характеризиращи такова състояние на личността, социалната група, обществото и държавата, което осигурява устойчиво и стабилно съществуване, удовлетворяване и реализиране на жизнените потребности, способност за ефективно париране на вътрешните и външни опасности, саморазвитие и прогрес.

Теорията за сигурността в голяма степен е построена върху тезата, че държавата има жизненоважна роля за осигуряване на националната сигурност. Това, че цялата система за национална сигурност е създадена и продължава да съществува така, че държавата да е главен фактор за обезпечаване на сигурността на обществото и на отделния човек, е продукт на определен етап на историческото развитие. В отделни периоди тази роля се е променяла и е естествено тя постепенно да намалява с повишаване ролята на международната сигурност. Факт е обаче, че системата за национална сигурност все още е така структурирана, че дели предизвикателствата за нея на външни и вътрешни. Така например армията се грижи главно за противодействие на външни заплахи, а силите за вътрешна сигурност се грижат за противодействие основно на вътрешни заплахи. Но размиването на границите между структурите за вътрешна и външна сигурност обективно не би могло да следва динамиката на процесите в света и промените в глобалната сигурност. Държавата със своята система за сигурност е значително по-устойчива структура и нейното разрушаване, без да са изградени други механизми за защита на сигурността, може да доведе до опасни, непоправими щети и за националната сигурност. Не случайно през годините се е утвърждавала (и доказвана многократно) тезата, че съюзите на държавите са временни, а самите държави - вечни.

В системата за национална сигурност обикновено се определят три равнища (обекта) на сигурността: личностно, обществено и държавно. Сигурността на личността се постига чрез осигуряване на правни и нравствени норми и изграждане на институции, позволяващи развитието на способностите и задоволяване на потребностите на всеки гражданин. Сигурността на обществото означава развитието на институти, норми и обществено съзнание с цел реализация на правата и свободите на всички групи от населението. Сигурността на държавата означава наличие на ефективно управление на обществените групи и политическите сили, и действени

механизми за тяхната защита. Посочените структурни компоненти, взаимодействайки със средата за сигурност, формират условно два основни аспекта на националната сигурност: външна и вътрешна.

В исторически план сравнително доскоро основен обект на изучаване и защита беше външната сигурност. Водещ фактор за нея беше опасността от военно нападение срещу територията на страната. Вътрешната сигурност беше разглеждана преди всичко като сигурност на властта (особено авторитарната), т.е. на режима в държавата. В демократичните общества това понятие има друг смисъл и е свързано със сигурността на обществото и на неговите отделни членове.

Съществуват редица дефиниции за понятието "вътрешна сигурност". Общото при тях е, че те я определят като състояние на гарантирани интереси на гражданите, обществото и държавата и възможност да бъде защитен конституционно установения в страната правов ред. Най-общо вътрешната сигурност е съвкупност от взаимноопределящи се групи фактори: политически, икономически, социални, информационни, екологични, властови и др. Същите при определени условия могат да бъдат риск, заплаха или опасност за националната сигурност, и по-точно да породят процеси и явления, застрашаващи законната публична власт в държавата.

Сигурността на държавата, обществото и отделните граждани на една страна са в пряка връзка със състоянието на конституционно установения правов ред в нея. Съблюдаването на този правов ред изключва всякакво насилие и произвол, и утвърждава властите на правовата държава на основата на самоопределението на народа, съгласно волята на мнозинството и в името на свободата и справедливостта. Към основополагащите принципи на този ред спадат: зачитането на регламентираните в конституцията човешки права, народният суверенитет, разделението на властите, законосъобразността на управлението, независимостта на съдебната власт, принципът на многопартийността и равенството на шансовете на всички политически партии и др.

В правната теория е прието, че конституцията действа чрез нейното съблюдаване в отношенията, които възникват при конституирането, организацията и дейността на органите на законодателната, изпълнителната и съдебната власт. Дейността на органите на държавната власт по привеждане в действие на конституцията обаче е функция и на прилагането на още редица правила, регламентирани от други правни отрасли. Въобще конституцията се привежда в действие в живота чрез реализация на съвкупност от обществени отношения, регламентирани както от конституционни, така и от широк кръг други норми. В литературата често системата от всички обществени отношения, регламентирани от обществени норми - правни, политически, обичайни и морални, се определя с термина "обществен ред". В този смисъл е логично, че много автори определят конституционния ред като съставна част на обществения ред.

Някои автори обаче с основание твърдят, че разширителното тълкуване на понятието "обществен ред" е недопустимо в правовата държава. Според тях "в съдържанието на понятието могат да бъдат включени само обществени отношения, регламентирани с правни норми. Това е съществуването различие на правното понятие "обществен ред" от понятието "обществен ред" в широкия смисъл на думата" [5] .

В подкрепа на подобно разбиране е фактът, че в демократичното общество правозащитната дейност се характеризира с няколко съществени признака, нито един от които не може да бъде пренебрегнат. Тя е дейност на държавата, извършваща се

с цел защита на правото, осъществявана от специално упълномощени органи чрез прилагане на юридически мерки за въздействие в строго съответствие със законите на страната и при стриктно спазване на реда, установен по законодателен път.[6]

Конституцията е основен закон на държавата и подлежи на пряко изпълнение от всички в нея. Нито един гражданин, политическа организация или обществена група, нито който да е представител на държавната власт, независимо от положението си, нямат право да игнорират конституцията или ако допуснат в своята дейност тя да бъде нарушена, подлежат на санкциониране.

Правово поведение е това, което следва предписанията на нормите на правото или заповедите на длъжностните лица. В практическата дейност по защита на конституционния ред не може да не се отчита фактът, че в живота има закони, които се спазват, и закони, които често не се спазват. Затова в демократичното общество е предвиден мощен инструмент за привеждане на Конституцията и законите в действие - съдебният контрол.

Подриването на обществените отношения, които съставляват конституционния ред в държавата, в крайна сметка е насочено срещу нейната сигурност, тъй като последиците се изразяват най-малко в дискредитиране на вътрешната и външната политика на нейното ръководство пред обществото и пред международната общност. Независимо от какви фактори е предизвикано това враждебно въздействие върху обществените отношения, институциите или отделни хора и социални групи, то засяга националните интереси във вътрешно държавен план или вътрешната сигурност на страната.

Без да се омаловажават другите направления на дейност по защита на националната сигурност на страната трябва да се посочи, че при съществуващата вътрешна и външна политическа обстановка функциите по опазването на конституционния ред или вътрешната сигурност на страната придобиват все по-голямо значение. Развитието на обществото е съпроводено с възникване на негативни процеси и явления на политическа, социална, етническа, религиозна и друга основа, пораждащи условия за организирана съпротива и насилие или други форми на противоправно поведение, които застрашават нейната вътрешна сигурност. Ако към това се прибавят катаклизмите от природен и техногенен характер, картината става пълна. Това налага усилията на компетентните държавни органи да бъдат насочени към своевременно придобиване на информация за тези негативни предимно социални процеси и явления и предприемане на целенасочени мерки за ограничаване на рисковете, заплахите и опасностите до степен, която да гарантира защитата на сигурността на държавата, обществото и на всеки отделен гражданин до общоприето ниво. За това се изгражда система за защита на вътрешната сигурност.

В синтезиран вид съдържанието на термина "защита на вътрешната сигурност" може да се определи като комплекс от дейности за придобиване на информация за реални и потенциални заплахи за сигурността на страната и организиране на противодействие за тяхното предотвратяване или неутрализиране. Нейната основна цел е постигане на стратегическо превъзходство над източниците на заплахите чрез тяхната постоянна оценка и прилагане на адекватни мерки.

Системата за защита на вътрешната сигурност е организационно и функционално определена от закона. Между отделните нейни компоненти съществуват връзки съобразно функциите, целите и основните им задачи. Взаимодействието

между тях е делово сътрудничество на основата на взаимопомощ с цел най-ефективно решаване на задачите по защита на вътрешната сигурност на страната.

Обичайно в документи, в литературата или в ежедневния език в термина "защита на вътрешната сигурност" се влага различно съдържание. Най-често в него се включва комплекс от дейности със следното съдържание:

а) придобиване и обработка на информация относно реални и потенциални заплахи за вътрешната сигурност;

б) информиране на компетентните държавни органи относно заплахите и подготовка на предложения за начина на реагиране;

в) оперативно противодействие чрез предотвратяване и пресичане на заплахите, неутрализиране на последиците от тях и създаване на възможност и за прилагане на други мерки за противодействие - политически, правни, дипломатически и т.н.;

г) защитни действия на полицейските и другите правозащитни органи за разследване на престъпления в тази област.

Заплахите за конституционния ред в една съвременна демократична държава могат да бъдат породени от различни фактори. От една страна това могат да бъдат външни сили - чуждестранни служби, международни терористични и други престъпни групировки, задгранични центрове на екстремистки религиозни и националистически организации. Реализацията на техните планове би могла да е предназначена и да предизвика негативни последици вътре в страната. Източници на непосредствена заплаха за конституционния ред и условия, които да благоприятстват подривната дейност на външните сили, могат да възникнат и под въздействието на вътрешни фактори - политическо, социално и етническо напрежение, засилване влиянието на организираната и конвенционалната престъпност в страната и др.

Това, което определихме като защита на вътрешната сигурност, е функция на всяка съвременна демократична държава, регламентирана законово. Ако се обобщи съдържанието на действащите закони в тази област ще се установи, че защитата на вътрешната сигурност в съвременни условия е дейност на държавата, насочена срещу:

- целенасочено противоправно скрито вмешателство от страна на чужди държави и престъпни организации във вътрешния живот на страната, насочено срещу националните интереси;
- дейността на незаконни, политически или военизирани формирования, престъпни групи и отделни лица, поставили си за цел насилствено изменение на установения в страната конституционен ред;
- терористични действия и други крайни екстремистки прояви, насочени срещу нормалното функциониране на държавните органи, общественото спокойствие, живота, здравето и имуществото на гражданите;
- опитите за проникване на криминални структури в държавния апарат и тяхното сращване със законодателната, изпълнителната и съдебната власт;
- развитието на корупцията, "сивата икономика" и организираната престъпност и свеждане на тези явления в допустими за обществото граници.

В предвид многообразието на заплахите за вътрешната сигурност на страната, нейните институции са длъжни да прилагат съвкупност от взаимосвързани и насочени към една цел мерки от различен характер за тяхното предотвратяване и неутрализиране. Тези мерки могат да са политически, икономически, правни, дипломатически, административни, оперативно-издирвателни и др., и трябва да се провеждат системно, последователно и постоянно.

От горната система от мерки за защита на сигурността се потвърждава тезата за единодействие на всички елементи от системата за вътрешна сигурност. Придобитата информация от специалните служби се използва за планиране на действия за предотвратяване или неутрализиране на заплахата, като тези действия често се предприемат съвместно с други органи, особено с полицията и органите на съдебната власт.

Организационно системата за защита на вътрешната сигурност включва държавните органи, които чрез определените им от Конституцията и другите закони на страната функции осъществяват националната политика в този сектор на сигурността. Съгласно конституционния принцип за разделение на властите, отговорности за вътрешната сигурност имат законодателната власт (Народното събрание), изпълнителната власт (Министерския съвет) и съдебната власт - следствие, прокуратура и съд.

Често обект на спорове е разграничаването на работата на службите за сигурност от тази на полицията. В това отношение законът е най-добрия арбитър. Законодателят е този, който решава колко и каква власт да даде в техните ръце. Има страни със специални служби без полицейски правомощия, а с полиции, които имат ограничена информационно-разузнавателна дейност. В други страни специалните служби съвместяват и оперативни, и полицейски функции, с което концентрират много власт в себе си. Какво ще бъде съотношението на правомощията на службите в системата за защита на вътрешната сигурност зависи в голяма степен от обективните условия, в която се изгражда тя и целите, които им поставя държавното ръководство.

Историята на Третото българско царство и на страната след 1944 г. е показателна за съотношението на значимостта на ораните за сигурност и на полицията за гарантиране на нейната вътрешна сигурност. В края на XIX и началото на XX век, когато военната сила на държавата е била решаваща за нейното развитие, от голямо значение е била мощта на нейните военни разузнавателни и контраразузнавателни органи. Следвоенната политическа и икономическа криза (1918-1926 г.) създава условия за увеличаване на политическата и криминалната престъпност. Тогава са създадени специални военно-полицейски органи, които да компенсират слабостта на Министерството на вътрешните работи и народното здраве (МВРНЗ) да се справи с криминално-политическите прояви. По такъв начин военното министерство, респективно неговия Разузнавателен отдел поема освен военното разузнаване и контраразузнаване и вътрешната сигурност на страната, макар и частично. Все пак основната тежест на борбата за вътрешен ред и сигурност в страната понася МВРНЗ. През този период функционират различни полицейски органи и институции за опазване на обществения ред и сигурност. Те носят различни наименования: Отделение обществена безопасност (1925-1927 г.); Отдел за държавна сигурност и криминален (1927-1931 г.); Отдел за държавна сигурност (1931-1944 г.). След 1934 г. за тези органи се налага популярното име "Политическа полиция" [7].

След 1944 г. връзката между полицейските органи (Народната милиция) и специалните служби се запазва. При укрепване на тоталитарната държава и при поспокойна оперативна обстановка, органите на Държавна сигурност са били отделяни от полицията и са били ориентирвани към работа в интерес на партийно-държавното ръководство. За такива цели полицията (милицията) най-често се оказ-

ва неподходяща и затова съвместната им организационна структура е била неприемлива. Като цяло тези опити за разделяне на органите за сигурност с органите за обществен ред не са давали траен положителен резултат. Всички опити за извеждане на специалните органи за сигурност от отделните министерства и обособяването им в самостоятелна организационно-щатна структура могат да бъдат ефективни само при наличие на ред предварителни условия. Историческият опит в организацията и управлението на полицейските и специалните служби в България досега показва, че успехите на разузнаването и контраразузнаването и особено защитата на вътрешната сигурност на България са били възможни, когато органите за сигурност и полицейските органи са били с общо ръководство.

В смисъла на казаното дотук специализираните правозащитни органи са пряко ангажирани с провеждането на държавната политика за гарантиране на вътрешната сигурност на страната. Тяхната дейност се осъществява въз основа на нормативно възложени им функции и задачи. Именно задачите, които закона им е регламентирал, определят основните различия, които съществуват между тях. Независимо от аспекта, в който се защитава националната сигурност нейното гарантиране е крайната цел, основната причина, която осмисля и самото съществуване на тези органи.

Според приетата през 1998 г. от Министерският съвет Единна система за противодействие на престъпността, вътрешната сигурност на Република България се гарантира в значителна степен от "защитата на правата и интересите на гражданите, на обществото и държавата. Равнището на вътрешната сигурност максимално зависи от ефективния контрол над престъпността". За това се формира система за защита на вътрешната сигурност, в която влизат основно службите за сигурност и за обществен ред на страната. Това представлява системата в нейния тесен смисъл. В широкия смисъл в тази система освен висшите и другите специализирани органи на държавна власт участват органите на съдебната власт, на финансите, на частните охранителни формирования и др. Ето защо в по-широк смисъл защитата на вътрешната сигурност може да се определи като сложна система от специализирани органи, сили, средства и механизми.

В предвид на това, че всички елементи на системата за вътрешна сигурност имат една обща цел - да защитят интересите на страната и да допринесат (всяка по своему) за гарантиране на конституционния ред в Република България, то системата се нуждае от общо, единно ръководство. Това ръководство, изхождайки от устройството на държавата и на опита на развитите европейски страни, следва да се концентрира основно в правителството като висш орган на изпълнителната власт.

Най-голямо значение за вътрешната сигурност на страната имат социално-икономическата, социално-психологическата и етно-социалната стабилност на обществото и ефективността на дейността на институциите за сигурност и правова защита за тяхното осигуряване. В условията на преход защитата на националните икономически интереси е едно от приоритетните направления за гарантиране на вътрешната сигурност. Стратегията за нейното осъществяване обхваща преориентиране на част от потенциала на службите за сигурност и за обществен ред към сферата на икономическата престъпност,защитата на научно-техническата и интелектуалната собственост на страната.

Борбата с престъпността и особено с организираната престъпност са сред приоритетите на стратегията за сигурност и обществен ред. Това е така, защото органи-

зираната престъпност, особено в големи размери, е сериозна заплаха за вътрешната сигурност на страната.

Основната цел на политиките за вътрешна сигурност е да се формулират и прилагат принципите, свързани със защитата на демократичните основи на държавата и обществения ред в нея. Посредством институциите, оторизирани от закона, се оценяват рисковете, идентифицират се заплахите и се инициират предложения за тяхното резултатно преодоляване чрез ефективни мерки от законодателен и незаконодателен характер. Всички компоненти на системата за вътрешна сигурност участват в нейното обезпечаване като акцента се поставя върху професионализма и високите стандарти в дейността на правозащитните органи, при важната роля на гражданската отговорност, контрол и подкрепа.

В заключение може да се обобщи, че вътрешната сигурност е състояние на гарантирани интереси на гражданите, обществото и държавата, както и възможност да бъде защитен конституционно установения в страната правов ред. Тя е съвкупност от взаимно определящи се политически, икономически, социални, информационни, екологични, властови и други фактори, които при определени условия се явяват риск, заплаха или опасност за националната сигурност, и по-точно пораждат процеси и явления застрашаващи публичната власт в страната. За това се изгражда система за защита на вътрешната сигурност като подсистема на общата система за защита на националната сигурност и като основен фактор за гарантиране на самата национална сигурност.

Литература:

1. Информационен бюлетин на НСС-МВР, бр. 62, ноември 2002, с.8
2. Годжев, К.,Геополитика. М., Международной отношения, 1997, с. 201
3. Стратегии за колективна и национална сигурност. Сборник, Академия на МВР, С, 2005, с.301
4. Концепция за националната сигурност на РБългария, ДВ, бр. 46 от 22.04.1998 г.
5. Тодоров, В., Понятието обществен ред и неговите полицейски аспекти. Годишник ВИПОНД-МВР, 1994 г., стр.18
6. Закон за обществения ред в Англия, НИКК, С., 1990 г.
7. Симеонов С., Полиция и закон, София 1996, стр. 15

ГОТОВНОСТ НА СИСТЕМАТА ЗА ВЪТРЕШНА СИГУРНОСТ ЗА УЧАСТИЕ В ОТБРАНАТА НА СТРАНАТА

Георги Г. Гоцев

PREPAREDNESS OF THE SYSTEM FOR INTERNAL SECURITY PROTECTION TO PARTICIPATE IN THE DEFENSE OF THE COUNTRY

Georgi Gr. Gotsev

Abstract: *The defense of the country requires all state authorities to be prepared to participate in it. The internal security system also maintains such preparedness, which has certain peculiarities.*

Key words: *defense; system for internal security protection.*

В съвременни условия значението на готовността на отбранителните компоненти в системата за национална сигурност да изпълняват задачите си във военно време не намалява. Характеристиката на съвременните войни и въоръжени конфликти, както и промените в стратегическата среда за сигурност показват, че България ще отстоява интересите си и ще защитава националната си сигурност в сложна, динамично променяща се и трудно предвидима среда. Макар, че през следващото десетилетие глобални военни конфликти да са малко вероятни, съществуващите и потенциални противоречия извън и в държавите продължават да влияят върху развитието на международните отношения и военната сила запазва значението си на инструмент за постигане на политически цели и интереси. "Партизанските войни, тероризмът и другите форми на въоръжен протест срещу съществуващото разпределение на властта не само ще продължат, но дори могат и да се увеличат. Най-много, което може да се очаква поне столетие, … е да се сложи край на широкомащабната световна война. Даже и ако всички законни правителства още утре прехвърлят своите въоръжени сили под егидата на ООН, това няма да сложи край на вътрешните конфликти и на регионалните войни" [1].

При определяне на готовността на отбранителните компоненти, в това число и на тези от системата за вътрешна сигурност, да изпълняват задачи във военнополитически кризи и конфликти, е необходимо да се отчитат няколко изходни твърдения, които през последните години експертите в областта на сигурността и отбраната приемат като доказани:

Първо. Отговорността за сигурността и отбраната и в бъдеще ще продължи да бъде национална, въпреки протичащите интеграционни процеси. Това е исторически проверено и изпитано твърдение, защото се оказва, че коалициите и съюзите са временни, а държавите ги надживяват. Без да се вглеждаме дълбоко в историята е достатъчно да хвърлим бегъл поглед на големите международни конфликти през последния век. И Първата, и Втората световна война бяха конфликти между големи коалиции, които след техния край или изчезваха (особено загубилите войната), или се трансформираха основно. Самата най-нова история на нашата страна през последното столетие показва участие в три подобни съюза. Последният - Варшавс-

кият договор дори изчезна без да е участвал във военен конфликт, под силата на глобалните международни промени. Какви са последиците за България като държава не е трудно да бъдат разбрани, тъй като те наложиха коренен поврат в нейната отбранителна политика.

Второ. Войната като явление и процес не е функция на въоръжените сили, а на държавата. Въоръжените сили изпълняват само част от задачите, планирайки и водейки военни операции, за което разполагат с точно определен потенциал. В действителност до 1806 г., когато Прусия за първи път разделя военната професия като отделна такава, винаги войната се е смятала за дейност на самата държава. Наложилата се специализация не променя същността на това, но довежда до общественото съзнание (а понякога и практика), че военните са тези, които решават въпросите за войните. В действителност въоръжените сили са тази част от държавната мощ, която може и прилага въоръжено насилие при военен конфликт или служи като военна заплаха при решаване на междудържавни проблеми.

Трето. В съвременните и бъдещите военни конфликти ще се засилва участието на гражданските структури. Това води до нарастване на числеността на организирано заетите в тях хора и системи, интегрирайки военните с невоенни методи и потенциал. Неслучайно в последните години конфликтите се определят като военно-граждански, като процес на "хуманизация" на войната.

Четвърто. Визията за войната на бъдещето и използването на сила излиза извън разбирането за разрушения или завладяване на територии, а се свързва с употреба на гъвкави стратегии, основани на асиметрични преимущества за постигане на бързи благоприятни резултати. Предимствата са свързани с информационното господство, технологичното и организационно развитие.

Пето. Бъдещите въоръжени конфликти ще предполагат сътрудничество на военните и граждански държавни органи, местното самоуправление и неправителствените организации за организиране на прецизно премерени, синхронизирани и високоефективни съвместни операции за постигане на общи цели. "През следващите десетилетия се очаква появата на три големи промени, които биха могли да върнат международната система обратно към старата анархия: природните предизвикателства на промените в климата, политическите предизвикателства на възхода на новите велики сили и технологичните предизвикателства на увеличаване на ядрената мощ. В комбинация - а те със сигурност ще пристигнат повече или помалко заедно - те ще подложат разнебитената система за поддържане на световния мир, която успяхме да измислим, на огромно напрежение. И би било неимоверно трудно да се измъкнем от всички тези промени без катастрофална война" [2].

Шесто. Войните на третото хилядолетие (или поне в неговото начало) няма да приличат на войните от миналото. Понятието "бойно поле" ще загубва своето буквално значение. Сраженията се пренасят в населените места, които стават предпочитано място за воюване. Този тип войни са най-кръвопролитни, водят до големи разрушения и до масови жертви сред гражданското население. Това са войни, в които единствения закон е отсъствието на всякакви закони.

Следващите войни ще се водят не само по бойните полета, но и в световните компютърни и комуникационни системи. Съществува тенденция - днес информационните технологии са толкова важни по време на война, че преобладават над всичко останало. Побеждава тази страна, която разбира как да използва информационните технологии по-ефективно. Днес способността да се събира, обменя, об-

работва и ползва информацията е един от най-важните фактори, определящ отбранителната мощ. “При всички случаи в бъдещи войни атакуването на компютърни мрежи вероятно ще е рутинна част от военни операции главно защото е тактика с явен ефект и няма причина да не бъде част от военните действия. Много чуждестранни военни ръководители вече признават, че използват тази възможност и тя често се дискутира във военните трудове в Китай, Русия и Индия - да спомена само три от държавите” [3].

Характерът на бъдещите войни поставя нови, повишени изисквания и към участващите в тях сили. На преден план излиза личната подготовка на състава, а веднага след това идват технологиите. Средствата за водене, за разузнаване и защита ще повишат относителната самостоятелност на отделния служител, ефективността на неговите действия и личния му принос в крайния успех на операцията. Новите оръжия и средства за водене ще му позволяват да получава постоянна информация в звук, текст и картина за оперативната обстановка, както и повишена лична защитеност чрез системи за идентификация и предпазване от “приятелски огън”. Като цяло в бъдещите въоръжени конфликти ще се отива към масово възприемане на несмъртоносни оръжия, главно за въоръжаване и ползване от полицейските служители.

Трансформацията на силите за отбрана, както беше вече посочено, е процес на придобиване на напълно нови оперативно-бойни способности или на тотална модернизация на най-доброто от съществуващото в тях. Способностите не са само технологии. Това са и доктрини, образование и подготовка, организация, комплектуване, инфраструктура, всестранна логистика. Само разглеждането в пакет на тези няколко императива може да даде пълна представа както за реалните, така и за бъдещите отбранителни способности на структурните звена от системата за вътрешна сигурност.

Очевидна е диалектиката между посочените компоненти. Изменението на всеки един от тях води до повишаване на общите оперативни способности само ако се съпътства от съответното развитие и на останалите. Един бъдещ модел предполага еволюционна модернизация на активните и поддържащите сили на системата за вътрешна сигурност и революционно развитие на мисленето и подготовката на личния състав. Прилагането на такъв подход е реалистично, тъй като бързите промени в мисленето ще мотивират нов тип поведение, който ще определя и темповете на развитие на материалния компонент.

Готовността за работа във военно време е една от основните категории на военната наука. Тя представлява главното съдържание на отбранителната способност на дадена система (държава, общност) и е в пряка зависимост от целите на провежданата политика, от господстващата военна доктрина, от степента на развитие на средствата и способите за водене на въоръжената борба. Тази категория характеризира определено количествено и качествено състояние на отбранителните сили и тяхната способност при всякакви условия на обстановката своевременно и организирано да се приведат в състояние да изпълнят задачите си по отбраната на страната.

Готовността на системата за вътрешна сигурност за работа във военно време е състояние, осигуряващо незабавно или след кратка подготовка в определени срокове планомерно нарастване на способността й за изпълнение на военновременни задачи. Тя е в пряка зависимост от политическото, икономическото, военното и моралното състояние на страната и се определя от няколко фактора:

- обективната оценка на военнополитическата и оперативната обстановка;

• количеството на личния състав в отбранителните елементи, тяхната окомплектованост с въоръжена и бойна техника, запаси от материални средства и средства за управление;

• подготовка и сглобеност на органите за управление и силите;

•равнище на оперативно-бойната подготовка и тренираност на органите и силите;

• поддържането на въоръжението, оперативната и бойната техника в постоянна готовност за използване;

• организация и състояние на оперативното дежурство във всички структурни звена;

• организация на оповестяването на органите и силите;

• състояние на системата за управление на органите и силите;

• поддържането на дисциплина, организираност и ред в силите за вътрешна сигурност;

• морално състояние и бдителност на личния състав.

В съвременни условия значително нарасна значението на времето като количество. То става стратегически фактор и оказва съществено влияние върху готовността да се реагира при нетрадиционни заплахи. Затова е недопустимо да се недооценяват или подценяват въпросите на оперативно-бойната готовност или готовността да се изпълняват оперативни и бойни задачи. Това налага постоянни усилия на ръководителите, щабовете и силите за съкращаване на времето за изпълнение на мероприятията по привеждане от мирно във военно положение. То налага и сериозни изисквания към готовността.

Готовността за работа във военно време трябва да се разглежда освен като състояние и в процес на развитие, постоянно да се оптимизира и се поддържа в съответствие с изискванията на военно-политическата и оперативната обстановка, развитието на средствата и способите за водене на въоръжената борба и преди всичко в съответствие със схващанията на вероятните ни противници за водене на война.

Основните изисквания към готовността на силите за работа във военно време са:

• своевременно привеждане на органите за управление и силите от мирно във военно положение и подготовката им за незабавни оперативно-бойни действия;

• скритост при привеждането на органите за управление и силите от мирно във военно положение;

• способност за организирано провеждане на планираните оперативно-бойни действия и мероприятия;

• организиране и поддържане на непрекъснато и твърдо управление на органите и силите при привеждането им в различни степени на готовност;

• всестранно осигуряване на органите и силите при привеждането им от мирно във военно положение;

• непрекъсната оперативно-бойна подготовка на органите за управление и на останалия личен състав;

• подробно разработвани планове за привеждане на силите в различните степени на готовност, за провеждане на мобилизация, поддържането им в съответствие с настъпилите изменения, и способност да се въвеждат в действие;

• пълно окомплектоване на структурните звена по военновременните щатове с личен състав, въоръжение, оперативна и бойна техника, автотранспорт и запаси;

• подготовка на мобилизационните ресурси за срочно и качествено окомплектоване на военновременните формирования;

• организиране на взаимодействие между държавните органи на централно и териториално, органите на местното самоуправление и обществото;

• организирано изпълнение на мероприятията по защита от ОМУ и провеждане на спасителни и възстановителни работи за поддържане на системата за управление и отбранителната способност на силите при необходимост;

• поддържане на висока морална устойчивост, дисциплинираност и бдителност в личния състав на структурните звена.

Развитието на военнополитическата обстановка в света и региона, характеристиките и схващанията за водене на съвременна война или провеждане на военни действия показват, че времето за подготовка за тяхното разкриване и отразяване ще бъде ограничено. Ето защо постоянната готовност на силите за организирано и своевременно провеждане на оперативно-бойни действия ще спомогне за минимизиране на негативните последици от евентуална внезапна агресия или опити за дестабилизиране на страната с военни средства.

Привеждането на системата за вътрешна сигурност в готовност за работа във военно време е сложен комплекс от дейности за преминаване на силите от мирновременен към военновременен състав и организация. Привеждането се явява заключителен етап на тяхната мирновременна подготовка и може да започне и да се проведе при различни условия. Привеждането на силите се извършва организирано и може да се осъществи в следните условия: в мирно време, т.е. до началото на войната (военния конфликт); да започне в мирно време и да завърши в хода на военните действия; да започне и да се проведе в хода на войната (военните действия).

Привеждането на силите от мирно във военно положение до започване на военните действия създава най-благоприятни условия за последователно провеждане на всички мероприятия в съответствие с предварително разработените планове и своевременната им подготовка за изпълнение на оперативно-бойни задачи. В този случай силите ще се привеждат последователно в по-високи степени на готовност при спазване на изискванията за защита на информацията. Това осигурява висока степен на окомплектованост, организирано провеждане на всички мероприятия по оперативното, организационно-строевото и оперативно-бойното сглобяване на силите и тяхното развръщане. Привеждането по този способ е възможно при наличие на сравнително продължителен застрашаващ период и своевременно разкриване на признаци за предстояща военно-политическа криза или въоръжена агресия. В този случай планирано ще се проведат организирани действия за преминаване от мирно във военно положение и пълно реализиране на планираните оперативно-бойни мероприятия.

По-сложни ще бъдат условията за привеждане на силите от мирно във военно положение, когато застрашаващият период е сравнително кратък и през него ще бъдат проведени само част от мероприятията, предвидени за различните състояния и степени на готовност. Значителна част от тях ще се проведат в хода на започналите военни действия под въздействие на противника. Това ще бъдат основно мероприятията за завършване на мобилизационното развръщане на силите и изпълнението на военновременни задачи.

Най-сложни условия за привеждане на силите от мирно във военно положение ще се създадат при внезапно нападение от страна на противника. При наличието на

съвременните информационно-разузнавателни средства такава внезапност е малко вероятна, но не изключва напълно възможността от внезапно нападение. В този случай силите ще бъдат приведени от постоянната си готовност направо в пълна такава. В кратък период под въздействието на противника те ще трябва да изпълнят основните мероприятия, предвидени за междинните степени на готовност, част от които ще се провеждат под въздействието на високоточни и ефективни оръжия, и усложнена оперативна обстановка, налагащо комплекс от мерки за защита на силите.

Бързото и организирано преминаване в готовност за работа във военно време е от решаващо значение за отбраната на страната. То се осигурява чрез:

- предварителна подготовка на ръководителите и органите за управление за работа във военно време;
- правилно разработени планове за привеждане в готовност за работа във военно време, тяхното поддържане в съответствие с настъпилите изменения в обстановката и способността на ръководния състав да ги въвежда в действие;
- своевременно оповестяване за привеждане за работа във военно време;
- надеждно и ефективно управление на силите при привеждане в по-високи степени на готовност и реагиране при конфликти с различна интензивност;
- подготовка на мобилизационните ресурси за срочно и качествено комплектуване на силите по военновременните щатове с личен състав и техника;
- организиране и поддържане на взаимодействие и координация на действията на елементите на системата за вътрешна сигурност в нея и с другите компоненти на системата за сигурност и отбрана на страната;
- поддържане на висока морална устойчивост, дисциплинираност и бдителност на личния състав на елементите от системата за вътрешна сигурност за бързо и успешно изпълнение на поставените им военновременни задачи.

Привеждането на страната и неговите органи за сигурност и отбрана в по-високи степени на готовност се извършва по решение на органите за ръководство на отбраната на страната. Съгласно Конституцията и законите на страната това са Народното събрание, Президента на републиката и Министерския съвет.

При обявяване на военновременните режими "положение на война" или "военно положение" осигуряването на вътрешния ред в страната преминава под ръководството на Президента на републиката. Системата за защита на вътрешната сигурност се ръководи от него пряко и непосредствено от членовете на ВГК в техните сфери на дейност. В своите актове за обявяване на съответния военновременен режим или в последствие при ръководенето на отбраната, президентът на републиката посочва конкретно нормативните актове, които влизат в сила или се отменят. Всички актове и решения на органите за ръководство на отбраната се обявяват и влизат в действие със заповеди на ръководителите на съответните нива.

Надеждното управление на привеждането от мирно във военно положение винаги е било един от основните фактори за неговия успех. Неговото значение нараства значително в съвременните условия, когато информационното превъзходство е определящо за успеха на военните действия. Затова и качествено нова черта на съвременните операции е стремежът на всяка една от воюващите страни да наруши системата за управление на противоположната страна.

Известно е, че управлението се заключва в целенасочена дейност на ръководителите, органите за управление и останалия личен състав на силите за поддържане на постоянна готовност за работа във военно време, подготовка на оперативно-

бойните действия и тяхното ръководене при изпълнение на поставените задачи. То трябва да осигурява ефективно използване на оперативните възможности на силите за успешно изпълнение на задачите в срок, при всякакви условия на обстановката.

За осъществяване на управлението на привеждането на системата за вътрешна сигурност в готовност за работа във военно време още в мирно време се създава система за управление. Като част от системата за управление на държавата във военно време и тя включва органи за управление, пунктове за управление и комуникационно-информационна система. Те са функционално свързани и позволяват управлението на системата за вътрешна сигурност при участието ѝ в отбраната на страната да се осъществява на три нива:

- стратегическо - ръководствата на министерствата и ведомствата, чиито структури са елементи на системата за вътрешна сигурност;
- оперативно - ръководствата на национални служби и органи, чиито правомощия обхващат територията на цялата страна;
- тактическо - ръководствата на териториалните структурни звена и органи, чиито правомощия обхващат съответната част от територията на страната.

Ръководителите от всички степени в системата за вътрешна сигурност носят пълна и еднолична отговорност за готовността на подчинените им за работа във военно време. Те са длъжни да управляват твърдо и непрекъснато структурните си звена при привеждането им от мирно във военно положение и в хода на евентуални военни действия.

Ръководителите осъществяват ръководството на подчинените си лично или чрез органите за управление, главно щабове. Поради специфичния характер на задачите, изпълнявани от елементите на системата за вътрешна сигурност в мирно време, повечето от тях нямат щатни щабове, които да са основен орган за управление на силите. Такива щабове има създадени от длъжностни лица по съвместителство, които се подготвят за изпълнение на задачи по привеждането от мирно във военно положение в системата на отбранително-мобилизационната подготовка.

Създаването на помощен специализиран управленски орган, какъвто е щабът, е продиктувано от огромната по количество и качество информация, която в хода на привеждането изправя единоначалника пред тежка управленска задача. Това е основната причина за възникване на щаба в управлението. Без такъв помощен специализиран орган ръководителят не винаги може своевременно да се ориентира в оперативната обстановка, да взема решения и да организира тяхното изпълнение. Щабното звено е помощна управленска структура, която е непосредствено до ръководителя и носи отговорност само пред него. Щабната работа е преди всичко организационно-управленска, защото щабът осигурява в организационно отношение подготовката и реализацията на управленските решения, особено тяхната координация и контрол [4].

В мирновременния период създадените щабове извършват подготовка за изпълнение на военновременните си задачи, усвояват плановете за привеждане и участват в тяхното актуализиране. За началник на щаба обикновено се назначава ръководителя на звеното за отбранително-мобилизационна подготовка, а в него се включват служители от основните направления на дейност на структурното звено.

При привеждане в по-високи степени на готовност създадените щабове започват работа като екипи. Техни основни задължения са непрекъснатото събиране, изучаване и оценка на данните по обстановката, подготовка на необходимите до-

кументи и предложения пред ръководителите за вземане на решения за провеждане на операции (оперативно-бойни действия); своевременно свеждане на задачите до подчинените; водене отчет на изпълнението на мероприятията от плановете; изготвяне на доклади и информации до старшите ръководители; организиране на системата за управление; упражняване на постоянен контрол върху дейността на подчинените органи и сили.

Организацията, съдържанието, последователността и методите за работа на ръководителите и щабовете при привеждането от мирно във военно положение и в хода на оперативно-бойните действия се определят от обстановката и характера на поставените задачи. При всички случаи организацията и методите за работа трябва да осигуряват твърдо и непрекъснато управление на силите, своевременно вземане на решение, пълно и качествено планиране на оперативно-бойните действия.

При вземане на решението, поставянето на задачите и планирането на оперативно-бойните действия могат да се използват различни методи. Възможна е последователност на работата, паралелност в работата или тяхното съчетаване (в различни звена и на различни нива). Важно е в резултат на този процес на подчинените звена да се предоставя по възможност достатъчно време за непосредствена подготовка за изпълнението на поставената задача.

Едно от най-важните задължения на ръководителите и щабовете е организиране на взаимодействието и непрекъснатото координиране в хода на подготовката и провеждането (осъществяването) на оперативно-бойните действия. По време на организирането на взаимодействието се съгласуват действията на органите и силите по цел, време, място и способ за изпълнение на поставените задачи. Въпросът за организиране на взаимодействието е особено важен за системата за вътрешна сигурност, в която участват различни структури и органи, провеждащи сложни оперативно-издирвателни, охранителни, разследващи и правораздаващи дейности. Този въпрос е още по-актуален във военно време, когато оперативната обстановка ще бъде усложнена и ще има опити от страна на противника за сериозно дестабилизиране на нормалното функциониране на цялото държавно управление.

При привеждане на системата за вътрешна сигурност в по-високи степени на готовност ръководителите са длъжни своевременно да организират и осигурят своевременното провеждане на всички планирани мероприятия, да вземат мерки за активиране на оперативно-издирвателната, охранителната и режимната работа и изпълнението на поставените задачи. Със започване и в хода на оперативно-бойните действия ръководителите и щабовете са длъжни своевременно да получават и анализират данните по обстановката, бързо да уточняват взетите решения и да организират тяхното изпълнение. Нарушеното в хода на операциите (оперативно-бойните действия) управление трябва да се възстановява максимално бързо.

Литература:

1. Дайър Г., Войната., "Кръгозор", София, 2005, с.469-470
2. Дайър Г., Войната., "Кръгозор", София, 2005, с. 452
3. Бъркоуиц Б., Новото лице на войната, ВИ, С. 2003, с.177
4. Илиев, И. Управление на полицейските и специалните служби, изд. "Албатрос", 2000.

ГЕОКОД, КУЛТУРА И НАЦИОНАЛНА СИГУРНОСТ

Евгени П. Манев

evgeni_manev@yahoo.com

GEOCODE, CULTURE AND NATIONAL SECURITY

Evgeni P. Manev

ABSTRACT: *The article argues that the "GeoCode" is an element of the "organizational code and software of the mined". The conclusion is made based on the organizational culture theory and Edgard Schain's model of the culture. The article stipulates that the multidisciplinary study of the organization is appropriate way of understanding the economic problems and geopolicy and geoeconomy better.*

KEY WORDS: geopolicy, geoeconomy, organizational culture*.*

През втората половина на 20-ти и в началото на 21-ви век се появиха нови субекти и обекти на глобалната икономика, формираха се и се формират нови полюси, процеси и явления. Протичат активни процеси на геоикономизация и геоплоитизация на международните отношения. Геоикономиката все повече става реално стратегическо средство за провеждане на политика на глобално, регионално и национално ниво.

Понятието геополитика произлиза от гръцки език и се състои от две думи geo (земя) и politicos (всичко свързано с държавата, града и техните граждани). Геополитиката по своето съдържание е сложно явление, което включва исторически, политически, икономически, социални, културни, етнически, религиозни и други фактори. Съществуват множество определения за термина геополитика, като подходящо за целта на изложението може да се приеме определението, че *геополитиката е наука в доктринален и стратегия в практически аспект за разпределение и преразпределение на сферите на влияние и световните ресурси с цел установяване на водещи позиции, контрол, доминиране и хегемония на водещите субекти в локалните, регионални и глобалното пространство* [1].

Генезисът на понятието *геополитика* се свързва с "био-социалната кодираност на развитието на човечеството", според която възникват и се развиват социалните организации (П. Ганчев). Тази постановка се базира на виждането, че тезата за кода за зараждане и развитие е валидна за всяко начало в живата природа, като се "прехвърля" и в социалната сфера. Доколко това е основателно и дали е правилно ще бъде обект на нашите разсъждения по-нататък. В този контекст е възприето и се използва понятието „гекод". Необходимостта от този термин се обосновава от „презумпцията за първоначалната кодираност при възникването всеки социално-обществен организъм" [2]. Основното внимание на геокода се насочва към субекта държава, която е основен играч в международните отношения. По този начин се допълва и разширява понятието геополитика, като за целта се лансира „тезата за кодирания генезис на субектите (б.а. социалните субекти), която „може да бъде

основа за интегриране в цялостна хипотеза на по-значими класически и нови геополитически и геоикономически теории" [3].

Обективната необходимост в глобализиращия се свят все повече налага и с усилени темпове ще ускорява мултидисциплинарния подход в търсене на все по-широки по обхват и обединяващи специализирани понятия и теории за обяснения на съвременните глобализиращи процеси. Несъмнено тези нови „обвиващи" многостранните процеси теории ще се нуждаят от нови термини и категории, все повече знания от научните дисциплини ще се включват в „пакета", необходим за изграждането на теориите за по-пълното изучаване на социалните организации (субекти). В изложението ще разширим, допълним и разкрием още една страна на геокода, отнесена към социалната организация. Ще направим връзката на геокода с културата на социалната организация, т. е с нейната организационна култура, като от тази гледна точка ще допълним обяснението за генезиса на геокода. Хипотезата е, че *геокода на социалната организация, в това число и на държавата, е културно придетерминиран*. С други думи, възприятията, убежденията и вижданията на лидерите на дадена държава, произлизат от културно-историческите и съвременни особености на населението на тази държава и в този смисъл те са „ културно кодирани" или както ги нарича Хеерт Хофстеде, програмирани чрез „софтуера на ума".

В съдържанието на понятието ГеоКод се влага интегрираната същност на паметта за произхода (генезиса) на един социо-обществен субект (например държавата или друга социална организация), неговата еволюция и развитие (прогрес, регрес или деградиране) в процеса на историческото му развитие. С това определение се визират субекти като държава, нация, народ, етнос, но характеристиката принципно е валидна за всеки политически, икономически и индивидуален субект. Всеки обществено-социален субект има генерализиран ГеоКод, който се базира на три фундамента: генетична памет, геостратегическа визия и генетичен механизъм, които в своята цялост определят качествената характеристика на субекта и го правят устойчив в обкръжаващата го природна, икономическа и политическа среда" [4]. Съдържанието на генетичната памет от своя страна се разглежда условно в няколко аспекта: генерирана памет, историческа памет и социокултурна памет. Генерираната памет е процес, чрез който се натрупват през целия жизнен цикъл на социалния субект знания, авангарден опит и традиции, които се наследяват по *„генетичния канал"* всъщност е процесът на постоянна адаптация на организацията спрямо външната и вътрешна среда. В този смисъл геокодът е отражение на културата на социалното общество и организационната култура на субекта принадлежащ към същото общество. Историческата памет е наследството от генезиса до съвременната точка на неговото развитие, а социокултурната и психологическата памет идентифицира субекта, и се обуславя от духовната, културна, етническа, езикова, религиозна и други принадлежности. Геостратегическата визия, като втория елемент на ГеоКода дава информация за вижданията на субекта както в исторически план, така и за неговото бъдещо развитие, чрез възприетото виждане за развитие и неговото позициониране на локално, регионално и глобално ниво във времето. Генетичния механизъм за комуникиране и предаване на информация между поколенията, в този смисъл, се характеризира с традициите, родовата етническата памет за предаване на кодирана памет, което е част, елемент от културата на социалното общество и субекта „потопен в неговата култура".

Съдържанието на един генерализиран код се представя като закодирани същности, които следствие развитието си стават „кодекси", правила и своеобразни закони за поведение на субекта в околната географска, политическа и икономическа среда. Те се трансформират в стратегически вярвания, убеждения и предположения за устойчиво развитие на субекта във времето и геопространството и на тази основа се разработват доктрините на субекта за собствената му роля и позициониране в геопространството. Устойчивостта на геокода се базира на приемствеността и на неговото актуализиране, което става чрез процеса на адаптация към външната и вътрешна страна за субекта (организацията). Приемствеността се заключава в исторически придобитата геостратегическа визия за развитие на субекта в континуума на неговия жизнен цикъл, която обхваща базисните елементи на генералния код, който също е елемент от културата на субекта и обществото, към което той принадлежи. Актуализирането на основните елементи на геокода или на отделни негови „кодекси" се осъществява спрямо действащите външни и вътрешни фактори. Тези две условия осигуряват оцеляването и успешното развитие на субекта в геополитическата и геоикономическата среда. Генерализираният геокод се проявява в различни направления (сектори) чрез негови „специфични" геокодове, като основни са: геополитически, геоикомически, геовоенен и други.

Геополитическият код е водещ, има основно влияние и сравнително дълъг период на неизменност в континуума на времето при формирането и функционирането на генерализирания геокод, формира неговата обществено-политическа значимост в обкръжаващата геосреда и отразява виждането и предопределя стратегическото развитие на субекта (държавата) в бъдещ период. Геокода формира трайната матрица за геополитическото развитие на субекта, който определя своята цел, мисия визия за развитие, която матрица е елемент от матрицата на организационното развитие на субекта. Последните се отразяват във формираните геополитически интереси, които отразчват икономическите, а те от своя страна отразяват жизнените интереси на субекта. Икономическите интереси оказват решаващо влияние върху изработването на доктрината и извеждането на приоритетите за субекта, определяне на сферите на влияние, разработването на стратегии, политики, приемственост и адаптиране в геосредата.

Икономическият аспект (елемент) на генерализирания геокод, се представя от геоикономическия код, за който е възприето, че доминира и е водещ спрямо геополитическия. Неговото съдържание се свежда до възприети и споделени представи, виждания, предположения, хипотези и доктрини на даден субект за неговото собствено развитие в обкръжаващата го икономическа среда на съответни равнища: национално, регионално и глобално. Като съставна част на генерализирания геокод, геоикономическия код формира и в същото време следва неговите „указания", създава база за геополитическия код. Геоикономическия код се основава на исторически сложилите се отношения между субектите в обкръжаващата среда на съответните равнища и създава базата за геоикономически отношения. Неговата стабилност и развитие се основава на приемственост, адаптация и развитие в съответствие с обкръжаващата среда и вътрешните интереси на субекта. Геоикономическия код също се „изработва" на локално (национално), регионално и глобално равнище.

Ефективността на управлението на субекта зависи от способностите на управляващия политически елит на държавата (нацията) за разработване на геополитически стратегии за развитие и увеличаване способностите на субекта да акумулира

национален, регионален и глобален материален и интелектуален капитал и умения да управлява ефективно приоритетните ресурси от стратегическо значение – капитал, знание, високи технологии, алтернативни енергийни източници от ново поколение и други.

В контекста на споменатата в началото теза, че генезиса на понятието геополитика се свързва с "био-социалния код за развитието на човечеството", според която възникват и се развиват социалните организации се базира на виждането, че тезата за кода, за зараждане и развитие на социалните субекти, е валидна за всяко начало в живата природа се "прехвърля" индуктивно и в социалната сфера (П. Ганчев). Зад посочената накратко теория за кодовото развитие на социалните структури, прозира фундаменталната научна теория за културата и за организационната култура, която уместно е адаптирана за нуждите на геополитическите и геоикономически теори и практики. Кодовете, създаващи кодекси (норми и правила), които формално и неформално регламентират дейността на субекта от гледна точка кое е правилно и кое не, кое е позволено и кое не в дадения субект, всъщност за метафори за изразяване на определни модели на геоикономическо и геополитическо поведение. Това е така, но тяхното приемане на като даденост, като нещо което е спуснато в субекта от някъде отвън и обяснено с неговия генезис (развитие) не изяснява същността и съдържанието на геокода като понятие. Именно на този въпрос ще спрем нашето внимание. За целта ще разгледаме най-основните теоретични постановки на теорията за културата с акцент на организационната култура в необходимия за целта обем.

Най-често с категорията *култура се означава комплекс от възприети вярвания, убеждения, оценки, допускания, предположения и очаквания, позволяващи на личността да разбира, осмисля и обяснява околната среда, които са общо възприети и споделени в социалната организация*. За нашия случай тази социална организация се разглежда като субект и по-точно се визира държавата като такава. Така възприетите вярвания и убеждения на субекта дават целенасочеността и смисъла на действията му и по този начин осигуряват хармония с обкръжаващата среда, което интуитивно формира чувство за удовлетвореност и равновесие и мотивира за по-нататъшни действия в унисон с обкръжаващата външна и вътрешна среда, които се проявяват под формата на външна адаптация и вътрешна интеграция.

Културата е особен механизъм и основа за манипулиране и целенасочено въздействие по определен начин върху членовете на субекта, т. е. културата на субекта „направлява и формира" в общ план, в рамките на своя контекст цялостната дейност на субекта, в това число и геоикономическата и геополитическата, чрез общо възприетите виждания, вярвания и убеждения за това как трябва да се развива субекта (държавата). Културата се проявява като споделено акумулирано знание на субекта, определящо поведенческите, емоционалните и когнитивните елементи на груповото психологично функциониране на неговите членове, появило се в резултат на исторически натрупан и споделен опит. От своя страна опитът осигурява стабилност на членовете на социалната група. В този аспект културата е съвкупност от споделени базови възгледи на групата (организацията, субекта-държава), които се създават в процеса на решаване проблемите на вътрешната интеграция и адаптацията в обкръжаващата геополитическа и икономическа среда. Когато тези възгледи работят достатъчно добре и се смятат за валидни, те се възприемат от новите членове като правилен начин на мислене, поведение и действие,

включително в геосферата, геополитиката и геоикономиката като се отразяват в тях. По тези причини културата е като *"терен на съзнателност, разгърнат на основата на конкуренция и борбеност, специфичен начин на организация и развитие на човешката дейност, представена чрез продуктите на материалния и духовния труд, в система от социални норми и учреждения, в духовните ценности, в отношението на човека към останалите и към самия себе си"* [5]. Всички тези компоненти на културата пряко или косвено влият на формирането и управлението на геополитиката и геоикономиката на субекта (държавата), чрез своя "културен код", който е по-общ и обхваща в себе си геокода на субекта.

Културата определя начина на действие на хората за постигане на определени резултати. Тя отразява опита, нормите, стандартите и моделите, определени от възприетите духовни и материални ценности, които неизбежно се отразяват в геокода. Ориентирана е към решаване задачите на социалния субект-държава с цел по-добро задоволяване на жизнените потребности.

На пръв поглед културата изглежда, че тя съществува като абстрактно понятие, което не би могло да бъде измерено по някакъв начин, а на тази база и управлявано. Широко разпространено е разбирането, че културата е многостранно, многопластово понятие, включващо артефакти, поведения, ценности, емоции и мотивиращи причини [6]. На по-вътрешно ниво, културата се състои от ценности, които са негласни, традиционно установени, сраснали се със самата същност на организацията предпочитания, за които тя полага усилия да ги получи, както и знанията за начина, по който ще го постигне [7]. Културата има многопластова структура, като на най-вътрешно, централно ниво се разполагат най-трудно откриващите се и в същото време най-устойчивите нейни елементи като интуитивно подразбиращи се и споделени възприетия и вярвания в социалната система (субекта - държава, обществото, организацията, групата).

Културата е приоритетна категория в антропологията, социологията, организационната психология, в която навлиза с приемането на ценностните и символните аспекти на организацията и тяхното влияние върху поведението на хората. Това поставя началото на културологичния подход в изследването на организациите и използването на термина *организационна култура* (Pedttigrew, 1979). На съвременния етап теорията за организационната култура все повече навлиза в практическото управление на социалните организации на макро ниво. Организационната култура е феномен, който осъществява интеграцията и изравняването между индивидуалните и социалните ценности. Логиката предполага изследване на ценностите на три нива на анализ: *индивидуално, организационно и национално*. Според Хофстеде (2001), индивидите постъпвайки в организацията, вече са "ментално програмирани" в резултат на придобития опит в процеса на социализацията и под влияние на националните различия и особености, т. е., организациите в този смисъл са кодирани за спецификата на своето бъдещо развитие. В този смисъл може да се твърди, че организацията като цяло има свой код, който може да има много аспекти, а геокода е само един от тези аспекти. Това обуславя сходните организационни култури в рамките на дадено общество (нация, държава, регион) и съответно сходни субкултури в рамките на дадена организационна култура (държава, регион), което обуславя сходни геокодове на субекти от един ранг (големина).

Организационната култура е феномен, отразяващ същността и закономерностите на съществуването на дадена организация (държава), тя е духовната сила, движеща и поддържаща единството на организацията, "лепилото", което я държи сплотена. *"Организационната култура* има своите философски, антропологични, психологически, социологически, лидерски и мениджърски измерения. От тук произлизат и различните или сходни характеристики на гекодовете на различните субекти.

В литературата е възприето, че социалната организация е мрежа от споделени идеологии (съвкупност от понятия, философии и ценности), набор от форми и практики, чрез които значенията се изразяват, предават, приемат и потвърждават към и от членовете на организацията. Този модел представя съществуващите две главни страни при изучаването на организационната култура и нейните "приложни стратегии" [8].

Според тристепенния модел на организационната култура на Едуард Шейн, тя се състои от три пласта, като най-външният пласт са артефактите, които са най-лесно забележими, отразяват видимата организационна структура и процеси. На следващото (ниво по-скрити) на организационната култура са разположени възприетите ценности, които „кодират" философията, стратегията и целите на организацията в общ и специфичен план, включително и в сферата на геокода, който отразява специфично направление от дейността на субекта държава, като социална организация. На трето и най-вътрешно ниво са разположени скритите основни подразбиращи се предположения, които отразяват подсъзнателно възприетите убеждения, идеи, мисли и чувства и се отразяват в „кода на субекта", а чрез него и в геокода.

Организационната символика се отнася до артефактите, или видимите прояви на културата, и включва ритуалите, символите, церемониите, разказите, митовете и легендите, материалната среда, т.е. цялата съвкупност от лесно наблюдаеми, но трудно обясними аспекти на културата. Смисълът, който се придава на символите, се детерминира от ценностната система. Това означава, че един и същ символ може да се интерпретира по различен начин в зависимост от ценностната система. Нормите присъстват в организационната символика чрез определяне неформалните роли, статута и начина на комуникация. Всичко това е „кода на субекта", който дефинира неговия геокод.

Според посочения модел на организационната култура, дейността на хората и най-вече на лидерството на организацията, неизбежно в своята дейност се влияе от организационните ценности, второто и възприетите и подразбиращи се основни положения в субекта (държавата). От своя страна лидерството на организацията има своето реверсивно влияние върху организационната култура. То от своя страна, определяйки „програмата за действие" в организацията базирана на възприетите норми, организационната култура поставя рамката за сегашните действия на организацията, както и модела на бъдещите нейни действия. Този модел е кодиран в от самата организационна култура в нашия случай на субекта (държавата). След като организационната култура създава общия код на дейността в организацията от това следва, че генерализирания геокод е един от многото съставни кодове на генералния организационен код на модела на организацията. Моделите на възприетите и споделени вярвания, убеждения и ценности предетерминират генералния кода, ако използваме тази метафора, на организацията. Той от своя страна определя позволената рамка на действие на генералния (общия) геокод на субекта (държава-

та). Последният предетерминира рамките на геополитиката и геоикономиката в контекста на организационната култура в крайна сметка.

Този подход показва, че теорията за ГеоКода е частен случай на приложение на теорията за организационната култура за нуждите на икономическата теория. Това е още едно потвърждение, за необходимостта от многодисциплинарен подход в изучаването на различните области от дейността на държавата и организациите.

Националната сигурност е неразривно свързана със защитата на интересите на държавата от външни и вътрешни заплахи. Мъдрото държавно управление на нейните икономически аспекти на сигурността на глобално, регионално и национално ниво задължително е свързано с нейната геополитика и геоикономика, от една страна. От друга страна националната сигурност се придерминира или ако се кодира от рамката на организационната култура на субекта (държавата). Този код и „програма" на организационната култура определят геокода, в рамките, на който се дефинира геополитиката и геоикономиката на държавата. Същият код и „програма" на организационната култура определят каква сигурност е необходима на държавата. Следователно, специфичните кодове (генерален за държавата – организационната култура (национална култура), кода за сигурността, геокода и т. н.) „работят" единствено в рамките на организационната култура на държавата, формална и неформална. Следователно използването на организационно-културния подход за развитие теорията на геополитиката и геостратегията на държавата е още една крачка напред към многодисциплинарния подход за изучаване на икономическите проблеми на държавата. Това показва богатите възможности на организационно-културната теория и полезността на нейното използване както в теоретичен така и в мениджърски план за изучаване проблемите на сигурността.

Литература:

1. Маринов, Г. Геоикономикс: Трансформациите., С., 2010, с. 17
2. Пак там, с. 18
3. Пак там, с. 18
4. Пак там, с. 19-20
5. Семерджиев, Ц. Стратегическо лидерство. С., 2000.
6. Hawkins, P. Organizational Culture: Sailing between Evangelism and Complexity. – Human Relations, 50, 4, 1997, pp. 417–440
7. De Long, D., L. Fahey. Diagnosing Cultural Barriers to Knowledge Management. – Academy of Management Executive, 14, 4, 2000, pp. 113–127; Bloor, G., P. Dawson. Understanding Professional Culture in Organizational Context. – Organization Studies, 15, 2, 1994, pp. 275–295
8. Семерджиев, Ц. Стратегическо ръководство. Лидерство. С., 2000, с.359

ОСНОВНИ ТЕНДЕНЦИИ В МЕЖДУНАРОДНИТЕ ОТНОШЕНИЯ И ГЛОБАЛНАТА СИГУРНОСТ

Евгени П. Манев

evgeni_manev@yahoo.com

GLOBAL PERSPECTIVE OF THE INTERNATIONAL RELAYIONS AND GLOBAL SECURITY

Evgeni P. Manev

ABSTRACT: *The global perspectives of the international relations and global security are explored by the author. New situation in the World creates a new opportunities and at the same time provokes new challenges to the world players. Based on known theories article analyzes three main characteristics of the current and future development of the international relations: new security paradigm, new cultural paradigm and new information technology dominance.*

KEY WORDS: *international relations, security, culture, technology.*

Колкото повече световен ред се въдворява, толкова по-несигурен светът става. Римата е случайна, но изводът е закономерен! Това е тезата на изложението по темата.

Международните отношения (МО) са система от геополитически, геоикономически и кратополитически отношения между субектите на съвременния глобален свят и следват логиката на историческите епохи: генезис, еволюция, развитие (прогрес или регрес) деформиране или деградиране на субектите [1]. Общоприета е теоретичната постановка, че закономерностите на развитие на природните процеси, явления и феномени са общи със закономерностите на развитие на обществата, т.е. тезата за единство на природата е фундаментът на разсъжденията в изложението по-нататък. Развитието на субектите върви по възходяща спирала (според Хегел) като в даден момент може да има връщане на зад, но на ново по-високо ниво на развитие. Тази постановка се отнася също и за социалния субект държавата разглеждана като социална организация със своите закономерности от гледна точка на развитие на социалните процеси в нея.

Различни видове отношения в глобалния свят представят съдържанието на „световния ред" в неговите два основни аспекта: геополитически и геоикономически. Разбира се има и други типове отношения като: международните отношения, международните икономически отношения, междукорпоративни и фирмени отношения, междуличностни отношения. Освен тези легитимни отношения има и друг тип отношения в света – нелегитимни отношения, които са извън установените формални и неформални международни стандарти. Представители на нелегитимния тип отношения са субектите на сенчестата икономика, „криминалния бизнес", световния тероризъм, етническото предприемачество.

В зависимост от историческата зрялост на етапа на развитие всяка епоха се характеризира със своя модел на световен ред, като за сега са познати следните модели: еднополюсен, двуполюсен, многополюсен и хармоничен (желания бъдещ модел, за сега хипотетичен). За целите на изложението ще опишем основните моменти от съдържанието на някои теории, които ще използваме.

Теорията на руския учен Нукилай Кондратиев за „циклите на световната конюнктура", която е известна още и като теорията за „дългите вълни" на развитие на световната икономика. Според тази теория световната икономика се развива циклично, с период на цикличност между 40-60 години. През този период настъпват разместванията в позициите на субектите в международните икономически отношения във водещи отрасли на световната икономика и групи стоки на световния пазар.

Друга теория е известна като „Моделът Кондратиев-Уолърстейн", която свързва модела на геополитиката със световния цикъл на дългите вълни на геоикономиката (теорията, модела на Кондратиев). В комбинация тези две теории формират цикъл, който е наречен „*цикъл на хегемония*". Според тази теория продължителността на един цикъл на хегемония е от порядъка между 100-150 г. Следователно в един геополитически цикъл се вместват два и половина геоикономически цикъла, като цикълът на хегемония включва три фази:

- Етап на зараждаща се и *възходяща хегемония*, в който субекти-държави, които имат технологично предимство постепенно придобиват позицията на световен хегемон.
- Следващият логичен етап е „*етапа на истинската хегемония*", в който субектът с технологично предимство се превръща в световен икономически, финансов, банков и политически център. Обикновено този етап се характеризира с нарастваща ресурсна и кризисна несигурност, провежда се агресивна и активна геополитика основно с инструментите на геоикономиката. Глобалната стратегия на субекта-държава (хегемона) е подчинена на неолибералната теория и принципи.
- Етап на „*постепенна загуба на хегемонизма от субекта*". В този етап е характерно изоставане в технологично и икономическо отношение на досегашния субект-хегемон и излизане на тази позиция на друг субект. Става смяна на стария субект-хегемон с изгряващия на световната сцена нов хегемон.

На основание на тази теория в новата история на човечеството са определени няколко цикъла на хегемония. Първият е с център Англия (18-19) век, вторият Германия (до първата световна война) и САЩ от средата на миналия век до момента. Ако се вгледаме в модела и поставим мащаба на циклите на оста на времето, ще видим, че хегемонизмът на САЩ се намира в края на своя геополитически цикъл. Именно тези теории са основание за прогнозите на много учени, които предвиждат края на американската хегемония в глобалния свят към средата на 21-ви век и излизането на сцената на новия хегемон, който се очаква да се измести на Изток и най-вероятно това ще е Китай, както повечето специалисти прогнозират.

Имайки предвид тази тенденция, отчитайки реалните устойчиви темпове на развитие на китайската икономика, икономическите съюзи в този регион, включително и Япония, САЩ преместват центъра на своите „жизнени интереси" в Азиатско-Тихоокеанския регион. Формалната „фасада" за това преместване е опасността от придобиването на ядрено оръжие от Иран, но дълбоките същностни мотиви са появата на новият Евразийско-Тихоокеанския хегемон, който застрашава хегемо-

низма на САЩ в света и те са принудени да защитават своя хегемонизъм чрез смяна на досегашната си стратегия.

Английският учен Питър Тейлор създава теорията за „икономическото превъзходство", в която постановките съвпадат с модела на Кондратев-Уолърстейн като авторът въвежда постулата за „икономическото превъзходство" като основа за геополитическата и геоикономическа хегемония. Той също извежда три геополитически цикъла в съвременната човешка история, като счита, че хегемонът в първия цикъл е Холандия (17 век), във втория е Англия (19 век) и в третия цикъл - САЩ (средата на 20-ти и началото на 21-ви век). Питер Тейлор въвежда понятието геополитически код в науката за първи път[1].

От посочените теории се вижда, че моделът за световния ред се подчинява на множество сложни фактори, които на свой ред влияят и определят съвременните тенденции в развитието на света. В края на всеки „*цикъл на хегемония*" се заражда и развива нов субект с нови технологични възможности, който измества предишния субект от хегемонната му позиция, т. е измества се центъра на световния хегемон. Базирайки се на посочените теории могат да се изведат три, на-главни тенденции в развитието на света [2].

- Първата тенденция е към промяна на парадигмата за сигурност изразяваща се в промяна на статуквото на националното, регионално и глобално пространство по отношение на различните нива на сигурност. Радикално се промени виждането за национална сигурност и неговото място в международната система за сигурност, която може да се разгледа, макар и в недостатъчно изчерпателен вариант, като национална сигурност, регионална сигурност, международна (колективна) сигурност, глобална, корпоративна и индивидуална сигурност[2]. Процесът на „смяна" на хегемона не върви „по вода", а е свързан с преразпределение на сфери на влияние, материални и финансови активи в света. Това поражда нови интереси на зараждащия се хегемон, които влизат в конфликт с интересите на настоящия хегемон. Това поражда остра геополитическа и геоикономическа борба в световен мащаб, внася качествено нови отношения между субектите в света. В този контекст се изменят и разбиранията, възприятията и вярванията за (не)сигурност, които са отражение на еволюцията на ценностите на световните субекти (играчи) на политическата сцена. Сигурността отдавна не е прерогатив само на националната държава в такава степен, каквато е била преди. Измени се съдържанието и относителното тегло на аспектите на сигурността, като интегралната „стойност" на всички нейни компоненти придобива все по-голямо значение за националната сигурност, като се повишава неговият дял в сигурността на държавата. Повишава се международният компонент на националната сигурност. Сигурността вече не прерогатив на националната държава и концепцията за широкото разбиране на сигурността надхвърля

[1] Манев, Е. Геокод, култура и национална сигурност, доклад, 2012

[2] За повече подробности виж:

Н. Слатински - пет равнища на анализ на сигурността: сигурност на индивида, сигурност на групата от индивиди, сигурност на държавата, сигурност на общността от държави и сигурност на света.

Е. Манев различава четири нива за анализ на сигурността на социалния субект: общо теоретично ниво на анализ на сигурността, аспектно ниво на анализ на сигурността, секторно ново на анализ на сигурността, обектово-функционално ниво на сигурност, Сигурност на организацията и нейните функции.

своите доскорошни граници. Навярно дошло е време да се говори за глобална сигурност, като националната сигурност е пряко и силно зависима от нея.

Водещите субекти разработват своите нови цели, основани на геокода си, за осигуряване на своята сигурност в пълния спектър от аспекти, като издигат нови доктрини за енергийна, екологична, водна и друга сигурност. Всеки аспект на сигурността поражда необходимост от специализирани доктрини и стратегии са целите на нейното постигане. Те от своя страна предизвикват адекватно управленско поведение и политики за определени времеви хоризонти с цел адекватно посрещане на новите заплахи. Независимо от формите и съдържанието на доктрините и управленските форми и методи за нейното реализиране, крайната цел на силните световни субекти си остава непроменена: *установяване на хегемония в глобалния свят и доминиране над него*. Това налага „деполитизиране" и „декорпориране" на науката, за да не се допуска целенасочено манипулиране на общественото мнение в интерес на користни субектни хегемонистични цели.

В този контекст Г. Маринов „улавя" парадигмата на първата тенденция към усложняване, дефинирани от промените (адаптация и актуализация) в геополитическите и геоикономическите кодове на претендентите за хегемон субекти и настоящия хегемон, изразяващи се във функционално сливане на националните граници в някои аспекти като физически, икономически социокултурни, като се формират се нови виртуални граници с регионални и глобални статусни характеристики (БРИК, Евразийско-Тихоокеанското сътрудничество). В тези новоформиращи се регионални геополитически и геоикономически пространства се включват национални държавни територии, които формират регионални статуква с нова геополитически и геоикономически характеристики. Все по-голяма степен на национален суверенитет (политически, икономически, военен, социален) се преотстъпва на наднационални глобални структури, упълномощени да изпълняват стратегически функции, които неизбежно водят и до упражняване и на оперативни функции в много случай. Това несъмнено влиза в остро и трудно разрешимо на сегашния етап противоречие с най-устойчивата културна парадигма на националната държава, за духовния, интелектуален и социокултурен суверенитет. Това е следствие от втората тенденция в новия световен ред.

- Втората глобална тенденция в развитието на света е *промяна в културната парадигма*, която чрез геокода „въвежда в експлоатация" нови съществени характеристики и параметри на съвременния свят. Използват се нови както технологични „твърди" така и „меки" средства за постигане стратегическите цели. Новите технологии „изместиха" тоталната война, но все още тя не е изключена от арсенала на средствата окончателно постигане на политическите цели. Високоточните оръжия в съчетание с политическата, финансова и материална подкрепа на опозиционните режими от „силните на деня" замениха употребата на въоръжените сили на хегемона и неговата коалиция като средство за превземане на властта в „недемократичната" държава – обект на интерес на хегемона. За тази цел се използват „бунтовническите организации" като им се оказва материална, финансова и морална подкрепа. Това става с подкрепата и на силите за „специални операции", като не е задължително тези операции да са с чисто военно действие и пряко използване на въоръжение. Използват се информационни операции като средство за манипулиране на общественото мнение, с цел представяне благовидно, хуманно лице на действията на хегемона в дадени региони, който под маската на загриженост за светов-

ния ред, защитата на свободата и демокрацията преследва с всички сили и средства своите геополитически и геоикономически цели. Нарасналите технологични възможности и икономическа мощ „увеличава" апетита на хегемона и неговите поддръжници, което води до разширяване мащаба и обхвата на геоконфликтите, които винаги са в зоните на икономически интерес. Съвременните технологични възможности доведоха до нови количествени и качествени характеристики на националните, регионални и глобални конфликти. Увеличи се честотата, интензитета и се нарастна броя на локалните конфликти след периода на „Студената война". Те придобиват все повече геоикономически характер и ухаят на „нефт". Надмощието на субекта хегемон, укрепващ с тези си действия ролята си на световен „творец на реда', който не признава редица международни легални, юридически правораздавателни организации и актове, влиза в „тих, негласен конфликт" с останалите субекти на световната сцена, което е „бомба със закъснител", която той сам за себе си залага.

- Другата нова глобална тенденция е все по-дълбокото навлизане е информационната ера на човечеството. Тя води до нови качествени и количествени промени на света и в другите сфери на живот чрез новите нано и био технологии, за които се знае повече за ползите от тях и по-малко за предсказуемите или непредсказуеми рискове, пред които е изправено човечеството. Новите генно модифицирани храни, изкуствен интелект, нано и биотехнологиите ще донесат на човечеството един ден нови, непознати досега „сиви или черни лебеди"[3], с които ще трябва да се справя. За пример може да се спомене въвеждането преди доста време на ефективния химически препарат ДДТ за борба с вредителите по селскостопанските култури. Наистина беше много ефективен, но се оказа, че нанася непоправими злокачествени вреди на човешкото здраве, поради което е забранен и спрян от ползване. Но докато се прояви този „черен лебед" много хора загубиха живота си.

Не е ясно как ще се преодолее наследената от индустриалната епоха и задълбочаваща се през информационната ера поляризация и икономическа стратификация на субектите, нерешените проблеми като бедност, пандемии, екокатастрофи, климатични промени и др. Около 10% от световното население, живеещо на територията на групата от най-развитите държави, наречена Г-7, консумира две трети (66,6%) от световния брутен вътрешен продукт. Трислойният модел на света на И. Уолърнстейн (САЩ) състоящ се от ядро, полупериферия и периферия, държавите са представени както следва: 20% от държавите в ядрото са развитите държави, а в полупериферията и периферията са останалите 80% от средно и слабо развитите държави. Въпреки „голямата грижа" на развитите държави за повишаване жизненото равнище на страните от полупериферията и особено от периферията ефектът, е точно обратен – все повече богатства от бедната периферия се стичат към богатия център. Богатите стават по-богати, а бедните по-бедни. Поради това страните от богатия център начело с хегемона водят агресивна по съдържание и „демократична" по форма геополитика и геоикономика, която помага на населението от бедните страни чрез различни програми, като Борба с глада и други. Разбира се това ще

[3] У Бек нарича „сиви лебеди" събития, които са изненадващи, но предсказуеми. Н. Талеб нарича „черни лебеди" събития, които са непредсказуеми и когато се случат, имат рязко отдалечена стойност, огромен изненадващ ефект и последствия спрямо обичайните очаквания. Могат да се обяснят само след като са се случили.

доведе до много други последици, като имиграционен натиск от населението в периферията към страните от центъра, пандемии по всички точки на света, които не могат да се контролират с икономически, политически или военни средства. Съотношението 20 към 80, води до другото съотношение, че в 25% от населението живеещо в богатия център е концентрирано 85% от световното богатство.

Изложените по-горе основни тенденции в развитието на света ще определят парадигмите за сигурност в света на различните нива. На глобално ново общата картина на сигурността ще бъде на фона на новата стратегия на хегемона за изместване центъра на жизнения му интерес от Европа в Азиатско-Тихоокеанския регион. Както беше посочено от разгледаните теории, всички мотиви за по-висока степен на сигурност в света ще се оценяват и представят през ценностната система на субекта хегемон да запази своята асиметрична доминираща позиция в света с всички сили и средства. Това ще се подсилва и от теоретично обоснованото и очаквано събитие за смяна на субекта хегемон към средата на 21-ви век. Това ще води до постоянно нарастващи противоречия между него и новия субект набиращ икономическа мощ и способност да стане следващия хегемон. Предстои глобална икономическа надпревара, която въпреки загрижеността за световния мир поставя в риск сигурността в глобален мащаб. Предстои следващото преразпределение на световното богатство. В тази надпревара твърде вероятно е светът отново да стане двуполюсен. От едната страна да са сегашните страни от НАТО начело със САЩ, а от другата да са страните от Евразийско-Тихоокеански регион, като водещи могат да се очертаят Китай, Русия, Индия и други.

Важно влияние върху водещия глобален „спор" за смяната на субекта-хегемон ще играят други два процеса. Единият е отношението на Япония с Евразийско-Тихоокенаското геополитическо и икономическо пространство и другият е отношението на европейския съюз с НАТО и Евразийското-Тихоокеанското геопространство.

Япония ще разширява връзките си с Евразийските страни, което е в ход. Япония и Китай започнаха търговски обмен, без да използват американския долар както беше досега[4]. Освен това водят се преговори основните страни от този регион, между които и Русия да преминат кум търговски обмен, без да използват американския долар. Това има двустранно икономическо значение за страните от Евразия, прави сделките по-ефективни и негативно влияе върху финансовите приходи за САЩ от неизползването на американския долар като обща търговска валута от тези страни.

Европейският съюз не е в състояние да решава самостоятелно въпросите си за сигурността в глобален мащаб извън рамките на НАТО, поради това, че не разполага със съюзни въоръжени сили способни да изпълняват такива задачи. Той още е далеч от самостоятелността си във военно отношение. Поради това и много други

[4] http://bulgarian.ruvr.ru/2012_06_01/76674097/, Китай и Япония започнали пряка взаимна търговия във валута без използването на долара. При това коридорът, в който юанът и йената ще търгуват, ще бъде по-широк, отколкото двойката юан-долар. Според договореностите, китайските регулатори всеки ден ще определят курса, а борсата ще има възможност да го променя с 3% в едната, или другата страна. В двойката долар-юан промените не могат да бъдат повече от 1%. Търговските сделки ще се извършват на пазарите в Шанхай и Токио. Най-вероятно между курса в Япония и Китай отначало ще има разлика, но в бъдеще те ще трябва да се изравнят.

икономически и политически причини, още дълго време ще трябва да разчита на този модел. Но вътрешно-интеграционните процеси в съюза, на определен етап неминуемо ще доведат до необходимостта от създаване на хомогенни европейски въоръжени сили, ако Европейския съюз иска да се превърне в многонационална федеративна или щатска държава. Това означава по модела на САЩ, да си има свои въоръжени сили, експлоатиращи оръжейни системи собствено производство. Ако иска да бъде самостоятелен играч, това трябва да стане. Не е възможно субекта Европейски съюз да няма собствени въоръжени сили като такъв. Без тях, той разчита на НАТО основно и на националните въоръжени сили на държавите от съюза. Вярно е, че политическите условия не са назрели и, че един такъв подход би създал проблеми със САЩ, но ако не иска да е в позиция на зависимост и сигурността му да е зависима от други държави и политически конюнктури, следва да се създават условия за решаване на този въпрос без да се създават конфликти, но и без да се изчаква чуждо благоволение за това.

На регионално ниво, в Европейския съюз проблемите със сигурността ще са поставени от икономическите рискове за имиграционна вълна, особено след „арабската пролет". Важни са енергийната независимост, която е се решава в две генерални направления. Едното е диверсификацията, която под натиск извън Европа се преекспонира, за да се „вкарат" технологиите за шистовия газ, за които няма ясни и еднозначни научнообосновани, от политически независими научни институти технологии, които да не са екоопасни. Под миловидната форма на полезната за Европа и България диверсификация на енергоизточниците, упорито се настоява от външни за Евросъюза държави да започнат проучвания в съюза и основно в България и Румъния. Тази политика, може да застраши както регионалната така и националната сигурност на Евросъюза и на България. Зад лицето на този „мек" натиск за обработка на общественото мнение в ползата от добиването на шистов газ у нас и Европа има двоен позитивен икономически ефект на първо място за компаниите, които ще проучват и евентуално добиват газа, негативен икономически ефект от сегашния доставчик, при евентуално намаляване на количеството на вноса спрямо сегашния. Освен това, по някои данни цената на шистовия газ с многократно поскъпа от внасяния за сега газ.

По-добрият вариант е да се развиват високотехнологични възобновяеми алтернативни източници на енергия в Европейския съюз и България. Най-добрата независимост е собственото производство. За целта е необходима насърчаваща съюзна и национална политика и финансиране.

На национално ниво сигурността ще се обуславя в рамките на ЕС и НАТО. България ще продължава да е под миграционен натиск от страните извън европейския съюз и от полупериферията. Основен проблем в близко бъдеще ще е безработицата и почти липсата на индустрия, разпокъсаното и нископроизводително селско стопанство. Това създава условия за изтичане на най-ценния капитал на България - младите висококвалифицирани хора в трудова възраст. Този процес води до двойни щети върху българската икономика. От една страна разходваните финансови, материални и морални ресурси за отглеждането, възпитанието и образованието на тези млади хора няма да се възпроизведат в България никога, от друга те започват да носят двойна печалба за страната, в която се установят на работа. Първо, тази страна не е разходвала преди споменатите ресурси за тяхното отглеж-

дане и образование и второ, принадената стойност от техни труд остава като печалба отново за чуждата страна вместо за България.

В заключение, пряка опасност от военен конфликт срещу България в близко бъдеще няма, но икономическите и демографски рискове не са на ниско ниво.

Литература

1. Маринов, Г. Геоикономикс: Трансформациите., С., 2010, с. 34
2. Пак там, с. 36-41

СЪВРЕМЕННИ ВОЕННИ АСПЕКТИ НА НАЦИОНАЛНАТА СИГУРНОСТ

Евгени П. Манев

evgeni_manev@yahoo.com

MODERN MILITARY ASPECTS OT THE NATIONAL SECURITY

Evgeni P. Manev

ABSTRACT: *The article argues that the hegemony in the world policy is an objective process. The position of the hegemonic country requires such kind of policy. That makes it predictable and can be used for planning small country future policy in order to fallow and reach its goals and strategy. That defines the military aspect of national security of the small countries.*

KEY WORDS: *hegemony, militaru aspekt of the security*

Националната сигурност на съвременния етап става все повече зависима от международната общност и е все по-пряка функция на международните отношения. Страните в света все повече се обвързват в икономически и политически организации, разширяват икономическото си сътрудничество, което оказва съществено влияние на подходите за осигуряване на националната сигурност на държавите. В бъдеще все по-голяма част от националната сигурност ще се генерира от участието на страните в коалиционни икономически и политически формати за сигурност, в това число и военна. Условията на глобализация произтичащите световни процеси оказват все по-значително влияние върху аспектите на сигурността, в това число и на военния аспект на сигурността. Глобализацията ще определя спецификата на развитие на съвременните военни аспекти на националната сигурност. Това е единият от важните фактори, които ще предопределят бъдещите изисквания към военния аспект на националната сигурност.

Съюзните отбранителни формати, съществуващи и зараждащи се, в които държавата участва ще предопределя изискванията към военните компоненти на военния аспект на националната сигурност като ще определят отговорностите и задъл-

женията на отделната държава в тях. По този въпрос се преувеличава ролята на член пети от Вашингтонския договор, и умишлено се пренебрегва член трети, според който всяка съюзна държава е длъжна сама да си гарантира националната сигурност. Политическите спекулации в това направление са много, но истината е, че договорът задължава всяка държава-членка да поддържа необходимия капацитет за осигуряване на националната си сигурност сама. Останалото е „качване" на гърба на партньорите.

Третият определящ фактор в развитие на компонентите на военния аспект на сигурността е политиката на хегемона в света, която ще определя дали дадена държава е в сферата на неговия интерес или не от което зависи до каква степен тази държава ще бъде покровителствана или не.

През последните 20 години, след епохата на Студената война, политическия и икономически живот в света се доминира от новия хегемон САЩ, от неговата политика, която е отражение на неговите интереси. Независимо под каква форма се провежда политиката и икономиката на САЩ по света, тя защитава неговите интереси. Очакванията на изследователите са, че следващите 10-20 и повече години светът ще се доминира от САЩ като световна икономическа и военна сила, въпреки че се зараждат нови сили, които ще се опитата да се противопоставят на хегемона.

В голяма степен външната политика на САЩ, като президентска република се определя и провежда от самия президент. Каква политика може да се очаква от американския президент през следващите години (разглеждаме институцията) ще зависи не само от неговите лични и партийни качества, виждания и амбиции, но и от обективните закономерности и изисквания на имперската същност и хегемонната позиция на САЩ в света. Последното ще играе основна, водеща роля поради своята обективна даденост. Освен това тези процеси силно ще са зависимо и от надигащите се нови сили (Русия, Китай, Индия и др.), стремящи се да се противопоставят на хегемона и да го изместят от позицията му.

Кои ще са най характерните черти на бъдещата политика на президента на САЩ, които той ще следва в политиката си. След 1991 г., когато Съветския съюз се разпадна, САЩ останаха без коректив. В известна степен, активиралия се тероризъм, може да се разглежда като опит за такъв коректив. Доколко, той ще изиграе такава роля или ще легитимира политиката на САЩ да стъпят в страните, където има терористични бази, да създадат свои бази там и да останат за дълго време преследвайки стратегическата си цел да заздравят хегемоните си позиции в света и да затягат обръча около надигащата се противостояща на хегемона сила е обект на други анализи, с които сега няма да се занимаваме. Политиката за борба с тероризма и режимите в страни, в които се нарушават човешките права се рафинира през имперските амбиции, интереси и позиция на САЩ в света, независимо от същността на политиките в „нарочените" страни. Единствено „правилният" критерий за определяне на политиката е, имперския и хегемонен интерес на САЩ. Как се стигна дотук и обективен процес ли е това или политически повлияно заключение на ангажирани учени и медии?

В началния етап на американската държава, през 1796 година Джордж Вашингтон декларира: „Най-важното правило за нашето поведение спрямо другите държави трябва да включва разширяване на търговските връзки и колкото е възможно по-малко политически отношения". Тогава в началото, отделяйки се от колониялната си зависимост от Англия, още слаба държава, е имало резон за

такава политика, която не е би могла да бъде агресивна или имперска. Това не е въпрос на политическо желание или амбиция на държавното ръководство, а обективна даденост на определен исторически етап. Днес нещата стоят по съвсем друг начин, независимо колко привлекателна изглежда тази перспектива, "вече е невъзможно една нация с толкова могъща икономика да поддържа търговски връзки с другите държави, без това да влече след себе си политически отношения и поледици. Антимонополисическият патос на Джордж Вашингтон е напълно достоен за основател на републиката като него. Иронията в случая е, че невероятният успех на същата тази република направи неговата красива визия невъзможна"[1]. Икономиките на много страни от гледна точка на вноса и износа зависят от икономиката на САЩ в рамките от 5 до 10 процента от брутния вътрешен продукт. Това налага останалите страни в света да се опитват да прогнозират развитието на САЩ за да прогнозират собственото си поведение, с цел да спечелят предимство или да избегнат бъдещи неприятни последици за себе си. Очакването на света, че високата степен на икономическата зависимост между държавите прави войната невъзможна се оказа илюзия. Свидетели сме, че след 1991 г. Военните конфликти зачестяват. Причините са комплексни, но видимо липсата на коректив отвързва ръцете на хегемона да използва асиметричната си сила и статукво и да си позволява да води войни, за които в условията на паритета не би и помислил дори.

„Онова, което превръща САЩ в неформална империя на света, е броят на държавите, върху които те влияят, както и интензитетът на това влияние. И макар и в центъра на американското могъщество да стои икономиката – колкото и разбита де изглежда тя в този момент, директно зад гърба и е военната мощ на САЩ. Главната цел на американската военна доктрина е да не позволи на нито една нация, огорчена от американското икономическо влияние, както нито на една коалиция от подобни държави, да използва военна сила, за да се опитат да пренаредят условията, които са ги поставили в неизгодна позиция. Подобно на римските легиони, и американските войски се разврьщат превантивно по целия свят, тъй като най ефективния начин да контролираме събитията е да унищожим надигащите се противници, много преди те да са се превърнали дори в маргинална заплаха". В крайна сметка могъществото на американската икономика и разпределението на американските въоръжени сили превръщат съюза с тях в необходимост за много страни. Именно тази необходимост е факторът, който обвързва държавите със САЩ много по-ефективно, отколкото която и да е формална имперска система." Тази логика на реалността, отразена от Джордж Фридман, „макар че САЩ все още отказват да видят империята (бел. авт. формално), в която са превърнати (бел. на авт. не без тяхното желание и усилие) всеки път, когато доловят нейния капан, се ужасяват. Но вече е крайно време да признаем, че американският президент управлява империя с безпрецедентна мощ и влияние, пък било то и неформално и недокументирано. Едва когато приемем този факт, ще можем да формулираме такава политика за настоящето десетилетие, която ще ни позволи да управляваме разумно и мъдро света, с каквато отговорност очевидно сме натоварени." Тук възникват въпроси от кого са натоварени легитимно? Очевидно нямя такова нещо и по-коректно би било да се счита, че САЩ се самонатоварват с тази отговорност, което би било много добре, ако тази орговорност не се филтрираше през цедката на хегемонните американски интереси. За да се извличат правилни и обосновани изводи трябва да

не се разделят идеите на американската политика от фокуса на американския интерес и стратегическите цели на САЩ да поддържат позицията си на асиметрична сила в света, която по своята същност сама се явява заплаха за сигурността на света и движи към ускорено развитие на военния аспект на националната сигурност на много държави към нови по-съвършенни технологии за унищожение, сравнявана с условията на паритета, независимо дву или многополюсен е той. Поради това изгряващата конкуренция на суперсилата, като нещо ново в диалектиката на развитието на света ще влиза във все по-остри форми на противоречие с хегемона, който може да загуби своята мощ само чрез война за което Джордж Фридман пише "Дори ако допуснем, че имперската мощ на САЩ някой ден намалее, силата на подобни мащаби не се сгромолясва толкова лесно, освен чрез война."[2]. Какво странно заключение или по-точно предупреждение към света, което означава, че ако не сте съгласни и искате да станете новия хегемон гответе се за война със сегашния.

Имперската позиция на САЩ, макар и неформална, през следващите десетилетия ще бъде насочена към запазване на водещата си роля в света в икономиката, политиката и военната сфера чрез експанзия на своето влияние с използване на меки и твърди средства за постигане на тази цел. Основното внимание ще бъде насочено към надигащият се опонент от Евразия. Това обуславя възприетата от САЩ нова стратегия за преместване фокуса на своя интерес от Европа в Азия – по-близо до надигащия се претендент за нов хегемон. Съсредоточаването на военна сила в тези региони е, силовия инструмент за провеждане на тази политика, която вече е в ход.

Налагащата се имперска позиция на САЩ в света създава обективните условия на този неформален статус, който ще изисква от президента да полага грижи за управление на света, независимо от неговото желание дали иска или не защото няма друг избор от тази позиция, която го задължава да защитава хегемонния статус. Могъществото не прави САЩ всемогъщи, поради което грижейки се за световния ред ще трябва да държат сметка за рисковете и евентуалните последствия, които трябва да минимизират. За това ще им се наложи да балансират и взаимодействат с другите играчи на световната сцена. Хегемонизмът освен предимства носи и рискове и ако САЩ допуснат да се изправят срещу света, без да се съобразяват с останалите играчи рискуват да им се случат неприятности.

„В прощалното си обръщение Джордж Вашингтон казва: „Нация, която изпитва към друга нация омраза или любов, е до известна степен роб на другата нация. Тя е роб на нейната враждебност или любов, като и двете са напълно достатъчни, за да я отклонят от нейния върховен дълг и от нейните интереси." Джордж Фридман продължава тълкуването; „Това означава, че НАТО няма уникално значение за САЩ извън европейския си контекст и че Европа не може да бъде считана за поважна от останалата част на света. Това означава, че президентът ясно и точно трябва да очертае най-опасните врагове на САЩ, след което да създаде коалиции, за да се справи с тях. На практика това означава окончателно да се скъса с цялата система от алианси и институции, останала от студената война, в това число НАТО, МВФ и ООН. Някои от тях може и да имат бъдеще, но само в контекста на новите институции, които биха могли да се появят на тяхно място. А те трябва да бъдат регионални и да служат на стратегическите интереси на САЩ. Тези институции следва да решават следните задачи: На първо място да поддържат в макси-

мална степен баланса на силите в света, да контролират енергетиката на всеки отделен регион и да отклоняват заплахите от САЩ. На следващо място съюзите да са способни да поемат основния товар при евентуални конфликти, като САЩ поддържа тези държави с облаги, военна технология и обещания за военна намеса при необходимост. На трето място, САЩ да използват военна интервенция само в краен случай, когато балансът на силите е изчезнал и съюзниците вече не са в състояние да се справят сами с проблема. Това е политиката, която американският президент ще бъде длъжен да институционализира през десетилетието, като не забравя, че САЩ ще продължават да пораждат ненавист и враждебност сред останалия свят според Джордж Фридман.

В отговор на американския хегемонизъм отношението на света към Америка се отличава с неодобрение и дори съпротива и докато правителствата на отделните страни се опитват да извлекат икономически дивиденти от това отношение, а ако не успеят то поне да избегнат негативните му последици. Във вътрешен план болното място на американците е да бъдат харесвани и обичани, а във външен – необходимостта САЩ да са по-отстъпчиви и не толкова арогантни в своите действия. Това, че е дефиниран проблемът и че Обама се опита да се справи с него, съпротивата спрямо властта на империята остава проблем без окончателно решение. И причината за това е, че проблемът произтича не от политиката на САЩ, а от самата същност на имперската власт. След като вече САЩ нямат съперник в надпреварата за световно господство, президентът трябва да започне да мисли за света като за ясно очертани региони, да създава регионални баланси, както и коалиционни партньори. Главната стратегическа цел вече е предотвратяването на евнтуална стратегическа сила, която би могла да се опълчи на Америка [3].

След като днес Европа не е по-важна от останалите страни за САЩ, какво следва да е отношението на Европейския съюз, който няма още свои въоръжени сили обединени под единно командване, обучение, и логистика. Каква трябва да бъде стратегията на България в частта й за поддържане и развитие на военния аспект на сигурността? Колко про-НАТО елемент, колко про европейски елемент, колко национални и какъв да е балансът между тях? Първичната реакция е да се каже, че те не трябва да се противопоставят. Никой не оспорва това, напротив те трябва да се синхринизират и дистрибутират в разумни съотношения, функционалност и предназначение. Това не означава, че за всяко "направление" трябва да се готвят сили и средства само за него и да не се преувеличават международните ангажименти за сметка на чисто националните отговорности. Какво става, ако член пети на Вашингтонския договор не сработи или сработи със закъснение?. Според закономерностите на хегемонизма и историческия опит, член пети сработва веднага, ако са засегнати пряко интересите на САЩ и не сработва при останалите случай. Погледнете Кипър. Тогава беше добрата политика за България докато Европа беше приоритет за САЩ. Това вече е история, стратегическия фокус е Азия. Този нов момент поставя още една дилема – колко проруска и азиатска политика, ориентация и в контекста на темата, колко военен компонент съвместим с нейният? Тази нова стратегия на САЩ, която е вече реалност, поставя България пред още по-трудни решения. Така разработените основни документи като Стратегията за национална сигурност, Националната военна стратегия и от там основополагашите документи за военното строителство вече изостават от времето

макар и приети преди около година. За да се преодолее този постоянен спътник в българската политика следва да се изработи закон, по подобие на някои развити страни, за нормативно адаптиране на голямата (Стратегията за национална сигурност) и малката (Насионална военна/отбранителна стратегия) стратегии, както ги наричат в някои страни. Такър опит, за изработванена иден проект и виждане (разписани) на такъв закон беше изработен през 2005-2006 г във ВА "Г. С. Раковски", който не получи развитие на по-високото ниво. Ако този закон беше факт, то както е нормално на всеки четири години голямата и на всеки две години малката стратегия щяха да се доразвиват и адаптират към изключителната динамика на световните процеси, които засягат България дълбоко. Независимо, че е загубено много ценно време, необходимо е да се изработи такъв закон. Това ще е важна крачка за поддържане на военния компонент на националната сигурност на България на по-адекватно ниво, състояние и способности.

В тези стратегически документи ясно трябва да се определят целите и инересите на българската нация. С достатъчна яснота трябва да се определят целите на нацията в икономиката и от там и във военната сфера, която през последните години се неглежира, опирайки се само на политическото очакване на недостатъчно надеждния член пети от Вашингтонския договор. На този член може да се разчита само след като са изчерпани възможностите на член трети от същия договор.

В чисто военен аспект на националната сигурността, основавайки се на принципа за баланс на силите в региона, България трябва сериозно да преоцени своята политика по отношение на въоръжените си сили. Въпреки финансовия си колапс Гърция не приема "българския вариант на демократично" драстично съкръщаване на въоръжените си сили и особено на авиацията си. Интересното е, че Европа не им поставя такива изисквания и условия. Това са въпроси, които следва да предизвикват по-сериозни анализи и намиране на адекватни решения. Българския политически "елит", който изобщо не заслужава това световно прието обръщение към политиците ръководещи дадена нация, некомпетентно оценява настоящата ситуация и не е в състояние да прогнозира бъдещето на дистанция по-голяма от един мандат (комат). Военната експертиза, която е на служба е длъжна да "марширува в крак с мажорния политически тон" водещ България къмто наникъде. Инак мислещите биват смазвани в зъбите на корупционната машина използвана от властта за лични саморазправи с тях. Развихрила се форма на корупцията в макроуправлението на държавата. Войнството от резерва, освободено донякъде от това си притеснение, е притиснато от социално незавидното си положение с отчаяно и апатично безразличие търси решение за собственото си оцеляване. Това заедно с условията на финансовата криза поставя под реална заплаха България да има необходимия адекватен на задаващите се нови реалности в региона и света военен компонент на националната сигурност, за което един ден днешните деца на България ще плащат за недалновидността на своите бащи и майки, най-вече на тези, които са заемали високите политически и държавни постове. Практиката показва, че каквато и власт да дойде, тези деца са пак в "управляващия ели", а плащат децата на останалите "простосмъртни" люде.

За да се решават правилно тези жизнено важни въпроси за държавата трябва да се изгради система в България за подготовка на и кариерно развитие на ръководни кадри – лидерски и административни, за да не се налага на бъдещите лидери на

държавата да ги намират по кръстопътищата на страната или да ги изваждат от "ръкава си". Щом ще управляват държава, те трябва да имат подготовка и по военното стоителство и използване на военния инструмент в политиката и икономиката на държавата. За това трябва специален подбор базиран на равнопоставена конкуренция, целенасочена подготовка и обучение, съчетани с практическо кариерно развитие на принципа на равните възможности при кандидатстване, професионалния успех, който да е основта за развите според способностите. Да се отстрани в максимално възможна степен партийното и корпоративно протежиране и назначение.

По отношение на компонентите на военния аспект на ационалната сигурност, България трябва да прогнозира тенденииите в световното тразвитие и да формира правилното си, точно и своевременни поведениие като прокарва своите интереси в световните процеси. Българската политика не трябва и не може да прави изключение от закономерностите на политическите процеси, отражение на икономическите и да води сляпа и тесногръда политика на вечната дружба и предност към хегемона, който и да е той, за която лорд Палмерсън, казва, че "Признак на тесногръдна политика е да се приеме, че една или друга страна са вечни съюзници или постоянни врагове на Англия (бел. на авт., ако интерпретираме това за България е абсолютно вярно) Ние нямааме нито вечни съюзноци, нито постоянни врагове. Едиственo интересите ни са постоянни". Това е основното нещо, което българските управници не са научили, а тези, които са го научили, заменят интересите на държавата с личните си интереси.

Какво наблюдаваме, за илюстрация, в днешно време – същата по съдържание политика в сравнение с тази беше преди 1989 година по отношение на новия ни покровител, само дето не се скандира "вечна дружба", но и за това има време. Политиката НАТО, ЕС или еди кой си иска така, не е държавнически изгодна за България, а е политика в угода на другите и ущърб на нацията. Само един пример ще приведа за авиационния компонент на военния аспект на националната сигурност. Чувате от най-висшите инстанции пропагандното уверение, че България има въоръжени сили, които са в състояние да гарантират националната ни сигурност, военния й компонент. Но никой от тези високопоставени дами и господа не казва срещу коя потенциална заплаха, ако се появи, Българската армия гарантира военната сигурност? Защо? Отговорът е ясен за компетентните професионалисти - това не е вярно. Нашата политика на „красивото" говорене е насочена във вътрешен план вместо във външен.

Заместването на националните интереси на България с политическото плонжиране и създаване нагласи за закупуване на средства за въоръжените сили по-стари от тези, които имаме е равносилно на предателство спрямо България. Погледнете, една Полша, която през 2011 г пое курс на модернизация, макар и лека, на съществуващи технически средства. Това е по-изгодния вариант за държавата. Истината е проста, като нямаш пари за нови дрехи, кърпиш старите докато изкараш парите, които ти трябват за новите. В условията на стратегическия курс на държавата за развитие на транспортната инфраструктура, е целесъобразно да се мисли и действа в тази посока, но да не се допуска България да загуби необходимите й отбранителни способности. Мандатите минават и заминават, България остава и тя трябва да е все по-добра за живеене на българите в нея след всеки мандат и всяко правителство. Единственият лесно измерим и видим критерии за правилната политика на Президента и Премиера

(като институции) това е броят на емигрираните българи за постоянно устройване и живот в други държави. Друг измерител е политическо бръщолевене.

Световните тенденции на развитие, ще диктуват регионалните тенденции в Европа и на Балканите. България трябва да балансира умело в тази турбулентна, понякога и бурна обстановка. От изместването стратегията на САЩ към Азия, все повече ще се налага на България да се интегрира с Европейския съюз в по-висока степен, отколкото с НАТО. Това означава, че трябва да се внедряват повече европейски технологии и да се балансира в използването на изгодните налични такива докато се изчерпи пълният им технически и морален ресурс. Това ще доведе до икономии на държавата и намаление на емиграцията на българите.

Литература:

1. Фридман, Джордж. Следващите 10 години, С. 2011, с. 21
2. Пак там, с. 24-28
3. Пак там, с. 33-37

ДЪРЖАВНА ПОЛИТИКА В ОБЛАСТТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Радослав Д. Узунов
Величка Д. Станчева

Шуменски университет „Еп. К. Преславски“
veli4ka_stan4eva@abv.bg

GOVERNMENT POLICY IN THE FIELD OF INFORMATION SECURITY

Radoslav D. Uzunov
Velichka D. Stancheva

ABSTRACT: *Have described the basic principles of information security policy. CERT Bulgaria is an element of state policy in the field of information security at home.*

KEYWORD: *Basic principles of state policy, information security, information security policies.*

Базови принципи на политиките за информационна сигурност

Политиките включват: общи принципи, които определят подхода към сигурността; конкретни правила за работа - определят това, което е разрешено и това, което е забранено. Правилата могат да се допълнят с конкретни процедури и различни ръководства, а техническият подход е анализ, който подпомага изпълнението на принципите и правилата.

Основният принцип на политиките за информационна сигурност е прилагането на ефективен контрол, който е измерим със стандартите за сигурност и

изискванията за съответствие. Контролът е насочен към постигане на следните изисквания:

1) **Достоверност** - Потребителите на информационните активи да бъдат идентифицирани по уникален начин при получаване на достъп до информация;

2) **Цялостност** - Наличие на адекватни защитни контроли и предпазни мерки, които да осигуряват точността на информацията по време на получаване, съхранение, обработка и предоставяне/представяне на информацията;

3) **Конфиденциалност** - Наличие на адекватни защитни контроли и предпазни мерки, които да осигуряват разкриване на информация само пред оторизирани потребители;

4) **Отговорност** - Наличие на адекватни защитни контроли и предпазни мерки, които да гарантират поемането/носенето на отговорност от страна на доставчици и потребители на информация;

5) **Управление** - Информационните активи, независимо от това дали са наети или собственост на организацията, да бъдат използвани единствено и само за осъществяване на основната й дейност, като не се допуска използването им за лични нужди или за други цели освен за основното им предназначение;

6) **Квалификация и обучение** - Осъзнаване на важността на квалификацията, компетентността и необходимостта от непрекъснато провеждане на обучение на персонала, клиентите и бизнес партньорите на организацията по отношение на информационната сигурност.

Извод: Политиката за сигурност е множеството от правила и практики, които определят как една организация управлява, защитава и разпределя информацията. Това е рамката, в която една система осигурява защитата и се изразява в описанието на средствата за защита, обектите на защита, служби, механизми и основни практически принципи.

Политиките за информационна сигурност се създават, прилагат и периодично преглеждат. Принципно те са специфични за всяка организация. Под политика за сигурност може да се разбира съвкупност от управленски решения по отношение защитата на класифицираната информация и присъединените към нея ресурси. От практическа гледна точка политиката за сигурност може да се раздели на три нива – горно, средно и долно.

Често в практиката се наблюдава ситуация, при която под натиска на нормативни и поднормативни документи формално се приемат политики, без да се мисли дали те могат да бъдат приложени реално или дали са необходими изобщо. Това налага да се постави изискването за приложимост и необходимост.

Изискването за адекватност се поставя, за да се осигури възможността на политиките да отговарят на бързо сменящите се условия за осигуряване на защита на информацията. Постига се, като периодично се преразглеждат и коригират.

Контрола на изпълнението на политиките за информационна сигурност осигурява обратната връзка при прилагането им. Не може да се установи ефективността им, ако не може да сме сигурни, че са приложени правилно.

Необходимостта от защита на информацията се определя от функциите на организацията, чрез които се постигат целите и задачите й.

Дейността по опазване на важната за сигурността на организацията информация придобива нови измерения, изправя се пред нови заплахи и налага различни подходи за предотвратяване, овладяване и преодоляване на предизвиканите от тях

неблагоприятни последици. Политиките трябва да са ориентирани към функционалността на организацията. Ако се допусне разминаване, се появяват два нежелани ефекта: непълна защитеност или излишни мерки.

Държавна политика в областта на информационната сигурност

Информацията винаги е била и остава най-търсената и скъпа стока. Това особено важи за съвременното информационно общество. В тази връзка усилията за създаване на сигурност на информацията добиват драматични размери. С развитие на информационните взаимодействия и увеличаване на атаките върху компютърните системи въпросите за компютърната сигурност стават все по-сериозни.

На държавно, европейско и световно ниво се провеждат редица форуми и дискусии за постигане на необходимата информационна сигурност.

Целта на разработката е да се направи предложение за повишаване на информационната сигурност в компютърните мрежи и системи от гледна точка на политиката за сигурност на държавата.

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение.

Едно от предназначенията на всяка информационна система е предоставяне на пълна, достоверна и своевременна информация. Тази информация е уязвима както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи), което налага да се вземат мерки за нейната защита.

Под защита на информацията трябва да се разбира постоянно използване на средства и методи, прилагани с цел:

- **Защита на конфиденциалността (тайната)** – да не се допуска разкриването на информация от неоторизирани лица;
- **Защита на цялостността** – да не се допуска неоторизирана преднамерена или случайна модификация на информацията;
- **Защита на достъпността** – да не се допуска отказ на информация или ресурс.

Обект на защитата е структурен компонент на информационната система, в който има информация, подлежаща на защита. Такива обекти са компютрите (работни станции на потребители и администратори на системи, локално използвани персонални компютри, периферни устройства), мрежови средства (модеми, апаратура за предаване на данни, рутери, мрежови сървъри, комуникационни канали) и помещенията**. Компютърните системи са техническата база на информационните системи.**

Компютърната и мрежова сигурност е свойство на компютърните системи и мрежи да противодействат на опитите за несанкциониран достъп до обработваната и съхраняваната информация, водещи до деструктивни действия и получаване на лъжлива информация.

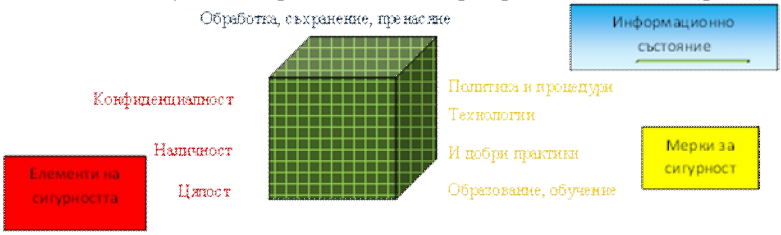
Тя се гради върху следните концепции:

- Идентификация – потребителите използват компютърните приложения чрез потребителски идентификатор (ID);
- Автентификация – доказване на самоличността на потребителя;
- Оторизация – присвояване на права за достъп на всеки потребител (например за запис, четене или изпълнение на файл);

- Контрол на достъпа – присвояване на права за достъп до мрежови ресурси и предпазване на ресурсите чрез лимитиран достъп (кой, как, кога и при какви условия има достъп).

Информационните системи се нуждаят от сигурност на информацията при обработката, съхранението и нейното пренасяне.

За постигане на конфиденциалност, цялостност и наличност като елементи на сигурността на информацията е необходимо да се реализират определени мерки за сигурност. По-характерни от тях са политика и процедури за сигурност, технологии за защита, както и обучение и прилагането на добри практики за защита (фиг. 1).



Фиг. 1

Информационната сигурност е комплексно понятие. В него влизат административната и IT сигурност. Административната сигурност е за осигуряване на непрекъснатостта на управлението.

IT сигурността е свързана с комуникационната сигурност, както и със сигурността на данните (фиг. 2).

Фиг. 2

Административна сигурност представлява система от правила и мерки регламентирани в нормативни актове, регулиращи защитата на чувствителна информация, нарушаването на които води до носене на отговорност.

Физическа сигурност е свързана със система от организационни, физически и технически мерки за предотвратяване на нерегламентиран достъп до критична (чувствителна) информация.

IT сигурността защитава компютъра и всичко, свързано с него – сградата, стаите, терминалите, принтерите, кабелите, дисковете или всичко, което е свързано със защитата на информацията, затова често се слага равенство между компютърна и информационна сигурност.

Data Centre-Сигурност е свързана със сигурността на базите данни в информационните системи включващи центрове за съхранение на данни.

Комуникационна сигурност, представлява система от мерки за сигурност, прилагани с цел защита на класифицираната информация от нерегламентиран достъп при нейното пренасяне по комуникационни системи. Системата от мерки включва защита с криптографски методи и средства, защита от излъчвания и защита при пренасяне на информацията.

От съществено значение за информационната сигурност е правната уредба. Основна задача на законодателството е грижата за защита на данните на организацията. От друга страна трябва да се спазват правилата за тайната на личната информация. От съществено значение също така са и мерките за защита на интелектуалната собственост.

Важна роля в сигурността на мрежите и информацията се отрежда на така наречените Центрове за реагиране при компютърни инциденти (Computer Emergency Response Team - CERT).

Първият център от този тип е създаден от американската агенция Defense Advanced Research Projects Agency (DARPA) през ноември 1988г., в отговор на потребностите възникнали след поредица от Интернет атаки с появата на червея на Робърт Морис. Още тогава функциите му включват 24 часова техническа помощ при реагиране на компютърни инциденти, изследване на уязвимостите на софтуера, предоставяне на техническа документация и провеждане на семинари.

Понастоящем, в света има повече от 250 организации, които се занимават с превенция и реагиране на компютърни инциденти.

По своята същност CERT представлява структура, звено, което предоставя на определени потребители услуги по защита и предпазване от инциденти в компютърната сигурност.

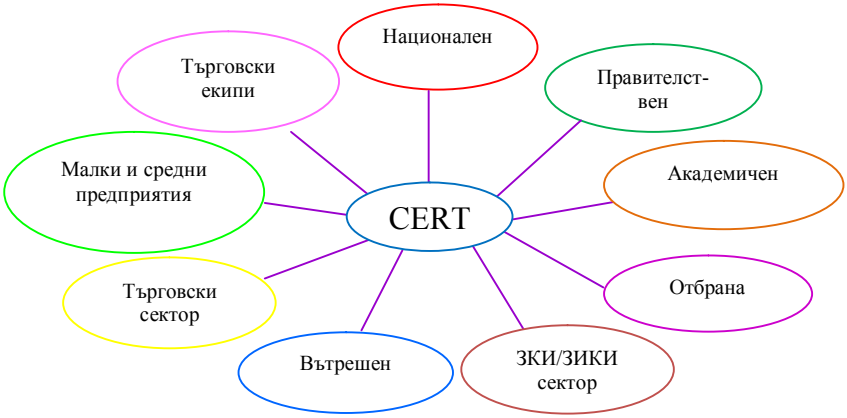
Като елемент от държавната политика в областта на информационната сигурност у нас се създава Национален център за действие при инциденти в информационната сигурност (CERT Bulgaria). Основната цел на центъра е да подпомага потребителите на услугите му в извършването на проактивни дейности за намаляване на рисковете от инциденти в информационната сигурност, както и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали.

Националният център предоставя централизирана база данни с обобщена информация, свързана с осигуряване на сигурна и защитена информационна среда в интерес на правителството, научните среди, отбраната, сектора за защита на класифицирана информация, МВР, търговския сектор, малките и средните предприятия, както и в интерес на търговските екипи. На фиг. 3 са показани видовете CERT у нас и връзките между тях, включително и този по отбраната.

Началото на успешното партньорство между България и Европейската агенция за мрежова и информационна сигурност (ENISA) датира от есента на 2006г., след посещението на г-н Андреа Пироти, изпълнителен директор на ENISA, в Държавната агенция за информационни технологии и съобщения.

През юни 2007 г. ДАИТС, ENISA и CERT-Унгария подписват тристранно споразумение за оказване на съдействие и подкрепа при изграждането на български правителствен CERT.

Първите стъпки за изграждането на правителствен CERT в България започват година по-късно. Причина за това е в регулаторната рамка в България, която до този момент не е достатъчно развита по отношение на информационната сигурност. Във връзка с това, като регулаторната рамка, през юни 2007г. в България бе приет Законът за електронното управление.



Фиг. 3

След изграждането на регулаторната рамка ДАИТС се заема с мащабен проект, целящ институционално укрепване на агенцията за посрещане на нейните нови отговорности, развивайки портал за информационна сигурност и, което е още по-важно, поставяйки основите на правителствен CERT.

Мисията на звеното е синтезиран израз на идеята за съществуването му, мястото му в обществото и ползите, които то носи. Обикновено тя представя накратко основните функции на звеното, изразени чрез идеята за предоставяне на конкретните услуги към аудиторията от ползватели.

Мисията не трябва да се променя много във времето, а да остава относително постоянна и по тази причина е необходимо да бъде достатъчно широкообхватна, за да позволява промените в услугите или функциите на звеното.

Съществуват множество услуги, които едно CERT звено може да предложи на своите потребители. Практиката обаче показва, че няма CERT, който да предлага пълния набор от услуги. Затова изборът на услуги трябва да се направи достатъчно прецизно и с нужното внимание. Наборът от избрани услуги ще определи ресурсите, уменията и взаимовръзките, от които CERT-екипът ще има нужда, за да функционира правилно. Избраните за предоставяне услуги трябва да са такива, каквито новоизграденият екип може реалистично да предложи, съобразно мисията и поставените цели, както и съобразно своя размер и компетентност. По-добре би било да се предложат по-малко и качествени услуги, отколкото да се дефинира широка гама и екипът да се сблъска с невъзможността за предоставяне на необходимото

качество. С натрупването на авторитет и уважение от страна на потребителите, екипът може да разшири обхвата на услугите, персонала и бюджета си.

В заключение може да се посочи, че Националният център за действие при инциденти в информационната сигурност предоставя базови услуги, които са особена важност за потребителите като: сигнализиране и предупреждение, управление на инцидентите, публикуване на информационни бюлетини, разпространение на информация свързана с осигуряването на сигурна информационна среда, единна база данни, централен информационен портал, реактивна и проактивна помощ при справяне с инциденти в сигурността, координация между различни национални и международни CERT звена, както и обучение с цел осъзнаване на необходимостта от осигуряване на сигурна информационна среда.

Литература

1. Национален център за действие при инциденти в информационната сигурност (www.Govercert.bg)

2. http://www.enisa.europa.eu/

3. Веселина Гагъмова, Т. Николова-Коцева – статия: „About government policy in the field of information security”

СОЦИАЛНА СИГУРНОСТ

Маргарита К. Бонева

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет

SOCIAL SECURITY

Boneva Margarita

Univesity of Shumen, Faculty of Education

Abstract: *It the presents current but not enfugh social security and problems in accordance with the globalizing world.*

Key words: *social, security, globalization.*

Понятието за “ социална сигурност ” олицетворява идеята за обществена солидарност. Могат да бъдат разграничени три принципа и основополагащи елементи на социалната сигурност: принцип на солидарност и субсидиарност принцип на осигуряване, обезпечаване и подпомагане социална мрежа На базата на тези принципи се развиват идеите за социално осигуряване, за социална помощ, както и мерките на държавата и на гражданското общество за постигане на равнопоставеност и социална справедливост. Социална сигурност съществува тогава, когато на всички членове на едно общество е осигурен достоен стандарт на

живот чрез преодоляване и предотвратяване на икономическите рискове. Реализацията на тази цел се постига най-вече чрез системите за: социално осигуряване, социални компенсации, обезщетения и социални помощи. Под социална сигурност следва да се разбират всички мерки на държавата и на гражданското общество, свързани с реализацията на социални цели и преодоляване на социални проблеми:

- защита на социалните права гарантиране на равни възможности;
- преодоляване на глада и бедността;
- равен достъп до образование;
- намаляване на неграмотността;
- здравеопазване.

Концепцията за социална сигурност признава, че всеки индивид в качеството си на член на човешкото общество се нуждае от социална сигурност, необходима за запазване на неговото достойнство и за свободното развитие на личността му. Основната цел е да се дава на индивидите и семействата уверение, че тяхното равнище и качество на живот няма да бъдат сериозно засегнати, доколкото това е възможно. Социалната сигурност включва съвкупност от условия, мерки и институции, които в своето взаимодействие са насочени най-напред за предотвратяване на тези нужди. Това, което е най-важно в тази концепция, е не средствата, с които се дава гаранция, а именно самата гаранция. Политиката на социална сигурност цели да покрие съвкупността от населението и да надхвърли рамките на т.нар зависим труд, т.е. наемните работници. Тя си поставя за цел покриването на всички социални рискове, а не само на някои от тях. Покриването на рисковете почива върху идеята за солидарност, реализирана чрез преразпределение на националния доход. В определена степен социалната сигурност цели също да съдейства за прегрупиране на отделните институции, които допринасят за самата нея, както и за въвеждане на принципа на единни вноски и приобщаване. Особено важни са две откроявщи се нейни характеристики - универсалност и отвореност. Социалната сигурност е универсална, защото включва всички социални рискове и всички индивиди. Освен това тя е еднаква за всички категории от общността, тъй като това е въпрос на елементарна социална справедливост. Социалната сигурност е човешко право. Системата за тази сигурност може да бъде организирана на равнище общество, на основата на специфични групи или индивиди. Концепцията за социална сигурност е отворена и по отношение на въпроса за финансирането. Тя не познава преференции на вноски или държавни субсидии и съсредоточава своето внимание изключително върху обезщетенията. Социалното подпомагане е форма за сигурност, която се предоставя на определени лица след проверка на доходите им, при някаква неблагоприятна жизнена ситуация. Финансирането в този случай е за сметка на държавата и обществото. Специфично при нея е, че средствата се предоставят не на всички нуждаещи се, а само след като се направи проверка, т.е. ако доходите на лицето или семейството не превишават определена граница, като тази граница в повечето случаи се нарича граница на бедността. Социалното подпомагане е форма за сигурност, която се базира на солидни колективни усилия. Наред със социалното подпомагане друга форма, която е възникнала пред повече от един век е формата наречена социално осигуряване. Постепенно тя е разширила своя обхват, както по отношение на самите осигурителни рискове, така и по отношение на самите лица,

които ще ползват тази защита. До възникване на социалното осигуряване индивидите са получавали защита като са използвали следните форми: спестовност; формите на застаряване; помощ от самите работодатели, както и самото социално подпомагане. Иновационен момент в появата на социално осигуряване се явява задължителен характер на защititата. Друга характерна черта на социалното осигуряване е нейното финансиране. Това става чрез така наречените осигурителни вноски, а не чрез данъците. Вноските се акумулират в специални фондове, от които се изплащат и съответните осигуровки, но само по отношение на лицата, които са засегнати от рискове. Тази форма за сигурност, подобно на първата почива на солидни колективни сила. Става дума за система, която предоставя сигурност на всички срещу всички неблагоприятни обстоятелства. Така се въвежда едно ново понятие - социална сигурност, което постепенно измества понятието социална осигуреност.

Гарантирането на икономическата и социалната сигурност винаги е било една от най-важните функции на държавата. Социално-икономическите аспекти на сигурността и на националната сигурност в съвременни условия трябва да бъдат разгледани по нов начин, тъй като в света се осъществяват фундаментални икономически промени. В процеса на преход към пазарно стопанство главната задача се състои в това да се гарантира мирно и нормално развитие при отчитането на социалния ефект от промените и запазване на основните параметри на вътрешната и външната сигурност на страната. Социалната сигурност – включва "свобода от дискриминация на базата на възрастта, пола, етноса и социалния статус. Става дума за система, която предоставя сигурност на всички срещу всички неблагоприятни обстоятелства.

Членството на Република България в ЕС поставя на преден план оптимизирането на социалния модел и задълбочаването на реформите за подобряване гъвкавостта на пазара на труда.

Социалната политика се формира на базата на диалог между социалните партньори с участието на правителствата. Смята се, че социалният диалог до известна степен може да предложи икономическа ефективност, сигурност и разпределение на доходите.

Задължителна е законовата защита на заетостта. Стачниците, например имат право да се върнат на работните си места след решаване на спора.

Основният източник на сигурност в САЩ е да си на работа, обезщетенията за безработица са умерени и с кратък срок, здравното осигуряване е частно или при заетост. Държавата подпомага бедните и възрастните хора, но подкрепата на доходите на самотните родители е в тесни граници. Основното и средното образование там са финансирани от щатските и местните правителства, а голяма част от висшето образование се заплаща от студентите и техните семейства.

В ЕС обезпечаването на социални грижи от страна на държавата се разглежда като основен източник на икономическа защита. Страните от ЕС предлагат сравнително щедри обезщетения при безработица за дълъг период. Налице е национално здравно осигуряване под някаква форма. Осигурява се безплатно основно и средно образование. Предлага се държавна подкрепа за университетите и таксите за висше образование са много по-ниски.

Социалният диалог се разглежда като допълващ националните практики диалог. Споразуменията между социалните партньори и колективното договаряне

имат национален характер и могат да се наблюдават съществени различия в отделните страни.

Човек е свободен да мисли каквото пожелае, но не е свободен да прави каквото пожелае. В такъв смисъл правото се отнася към дейността на човека. Никой закон не може да предпише какво да мисля, но може да предпише да мисля така, че мисленето да не доведе до действието "престъпване на закона".

"Днешното положение на човечеството повдига въпроса за това, каква е целта на цивилизацията и дали е възможно цивилизацията да бъде променена и спасена. Нашият морален проблем е безразличието на човека към самия себе си. В основата му е фактът, че сме загубили усещането за значителността и уникалността на индивида, превърнали сме се в инструменти на цели извън нас, преживяваме и третираме себе се като стока, а собствените ни сили са се отчуждили от самите нас. Резултатът е, че се чувстваме безсилни и се презираме за своето безсилие.

Върховната доброта – източник на истинско щастие – се разкрива пред човека, само ако се придържа към съответните правила. Положителният ефект от тях може да породи необходимата мотивация за цялостното му възприемане. Тези правила на поведение не са измислени от никого. Те са вписани в паметта на Природата и до тях може да се достигне в състояние на висше съзнание.

Природата е чувствителна към човешките действия и енергиите, излъчвани от човека. Ние сме хибридни същества. Еволюирали сме от животното и сме постигнали определени качества, които ни отличават от него. Наричаме тези качества човешки. Наш морален дълг е да ги развиваме, за да се проявяват в максимална степен. Целта на нашия живот е еволюцията на индивидуалното съзнание, която се състои в развиване и разширяване на истинските човешки качества за разлика от животинските. Ние сме съзидателни същества, тъй като психичните енергии, пораждани от нашето съзнание, от чувствата и от действията ни, са биофотонни импулси, които излъчваме в пространството, и те взаимодействат със силите на космическата Природа, като й влияят и изпитват нейното влияние. Всяка човешка частица променя природата със своите биофотонни излъчвания и съответно приема енергия, която трябва да възстанови космическото равновесие. При разрушително енергийно излъчване, нечисто, нехармонично или престъпно, природното равновесие отвръща на причинителя с равностойна отрицателна реакция, макар и доста по-силна, и това е справедливото наказание за моралното нарушение. "Всеки плаща за делата си", независимо дали намеренията му са били добри или лоши.

Ние излъчваме вибрационни енергии, които насищат енергийната среда. Ако сме песимисти, създаваме и излъчваме песимистични вибрации, при което ставаме чувствителни към други сили от подобно естество, т.е., ако излъчваме вълни на песимизъм, ще привлечем злощастни събития, но ако излъчваме радост и оптимизъм, ние се настройваме на вълните на сходни вибрации, които достигат до нас и се отразяват върху живота ни.

Отчуждението се определя като "процес на промяна на съзнанието на индивида или група хора до степен, в която то стане противоположно на очакваното при техните условия". Всяка дейност и всяко обучение – работа, обществен живот, спорт или развлечения се превръщат в елементи, които могат да засилят процеса на отчуждение. Ние живеем в океан от високочестотни

радиовълни, различни магнитни полета и хипнотични индукции, идващи от околната среда, които напълно могат да завладеят съзнанието.

Отчуждението е като психическа пандемия, която в определен момент поразява всички хора. "Проблемът е в обстоятелството, че образованието превръща хората в обикновени "контейнери за информация". Главите им са пълни с автономна информация, а това наистина предизвиква дълбоко отчуждение. Отчужденият субект прогресивно се механизира и отчуждава. Той започва да изпада в тягостна самота, присъща на хората, загубили истинската посока в живота, защото са се отдалечили от вътрешната си природа и са принудени да вършат това, което им наредят чиповете в паметта, а не това, което желаят в душата си".

Нормалните взаимоотношения между хората, независимо от възраст, пол и обществен статус са елемент с особено голямо значение за социялната сигурност в дадено общество.

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. Слатински, Н., Измерения на сигурността, С., 2000.
11. Слатински, Н., Националната сигурност – аспекти, анализи, алтернативи, С., 2004
12. Слатински, Н., Петте нива на сигурността, С., 2010
13. Хънтингтън, С., Сблъсъкът на цивилизациите и преобразуването на новия световен ред, С., 1999.
14. Ibryamova, N., Migration from Central and Eastern Europe and Societal Security in the Europian Union, The Jean Monnet Chair, University of Miami, Florida, 2002.

ГЛОБАЛНАТА ИКОНОМИКА И СИГУРНОСТТА НА ДЪРЖАВАТА

Маргарита К. Бонева
Шуменски университет „Епископ Константин Преславски”
Педагогически факултет

LUMP ECONOMICS AND SECURITY OF A COUNTRY

Boneva Margarita
Univesity of Shumen, Faculty of Education

Abstract: *Enriched is a theory about the lump economics and security of a country.*
Key words: *globalization, security, migration*

В икономически аспект сигурността се определя като „обществено благо”, достъпно еднакво за всеки член на обществото.

Категорията „*държавен интерес*” е приложима към всяка държава на всяка степен от нейното развитие: държава-класа, държава-бюрокрация, държава-нация, държава-партия. В либералните демокрации възниква своеобразен тандем между държавата и обществото, който създава феномена „национална държава”. В „нацията” държавата съществува дотолкова, доколкото е в състояние да изпълнява делегираните й от обществото функции да осигурява връзката между гражданите. Често за по-голяма прецизност се използва понятието „национално-държавни интереси”, под което се разбират интересите на определена социално-политическа общност, отразяващи конкретно-историческия баланс на интересите на личността, обществените групи и социума като цяло в съотношение с интересите на институциите на властта, политическите партии и др. Жизненоважните интереси гарантират на държавата сигурност, свобода, независимост, защита на държавните институции и укрепване на нейните ценности. Тези интереси изключват компромиса като отразяват въпроси, заради които държавата е готова да воюва. Второстепенните интереси допускат компромис и преговори.

Икономическата сигурност е състояние, при което съществува възможност за защита на държавата и обществото от дискриминация и икономически диктат, осъществявани под формата на санкции, забрани и ограничаване на търговско икономическите връзки, а също така и от други пречки пред прогресивното, постъпателното и ефективното развитие на националната икономика. Тя е мярка за състояние и средство за предпазване от ерозия на икономическите ценности на нацията. Икономическата сигурност има две взаимносвързани измерения – вътрешна и външна. Вътрешната изразява влиянието на негативните фактори влияещи върху стабилността на стопанското развитие. Външната икономическа сигурност изразява двустранната връзка между състоянието на международните отношения и стабилността на икономическото развитие на страната.

Държавата като набор от институции има пряко отношение към глобалната икономика. 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.

В международен план вече е постигнат широк консенсус относно задачите, които предстои да решат всички държави в най-близко време:

- ефективно политическо управление, основано на демократична политическа система, зачитане правата на човека, върховенство на закона и социална справедливост;
- ефективна държава, осигуряваща високи и стабилни темпове на икономическия растеж, произвеждаща обществени блага и гарантираща социална защита;
- разширяване възможностите на хората посредством всеобщ достъп до системите на образование и другите социални услуги и насърчаваща равенството на половете;
- енергично гражданско общество, построено на принципите на свободата на сдружаване и право на мнение, отразяващо и изразяващо разнообразни мнения и интереси;
- социален диалог с представителните организации на работниците и работодателите.

Глобалната цел, в рамките на многостранната система е осигуряването на достоен труд за всички. Необходима е съгласуваност между глобалната икономическа, социалната и екологичната политика.

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. Държавата има водеща роля в:

- здравеопазване, образование и правов ред;
- надзор над дейността на пазарите и корекция на пазарните недостатъци и неуспехи;
- отстраняване на външните недостатъци като влошаване на околната среда;
- осигуряване на социална защита и закрила на уязвимите слоеве на населението;
- инвестиции в области, представляващи обществен интерес, в които не отиват частни инвестиции.

Друга важна роля на *държавата* е ограничаване влиянието на глобализацията върху обществото с помощта на прогресивно данъчно облагане, политика в областта на заплащането на труда, социални програми и други механизми.

Налагащият се глобален икономически модел се основава на:

- абсолютизацията на пазара и частната собственост;
- на конкуренцията и гонитбата на икономически ръст за сметка на солидарността и социалната чувствителност;
- на тоталната либерализация на икономиката и оттеглянето на държавата от нея;
- на свободната от ограничения и граници търговия;
- на безпрепятственото и бързо придвижване на капитали.

В глобален мащаб за първи път в историята цялата власт е под контрола на мощния транснационален капитал. Той сваля и качва правителства, чертае световния дневен ред, определя правилата на играта.

Този 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. Колкото и динамичен да е, той е реакционен, елитарен. Най-важното, не е универсален, защото е твърде добър за т. нар. златен 1 милиард богати и сити хора, които разполагат с 80% от световния БВП, но е твърде лош за останалите 5 милиарда бедни и гладни хора с 20% от световния БВП. Статистиката показва, че докато Западът прекрачва в Третото хилядолетие, голяма част от света страда от недъзи, характерни за Средиземноморието. Семейството на бедните, на водещите мизерно съществуване, на болните телом и духом, на лишените от шанс и перспективи не само не намалява, но дори расте.

Съвременната международна политика не е способна адекватно да реагира на задачите, възникващи в процеса на глобализация. 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 изострящите се глобални проблеми. Недостатъчно ефективно функционира и 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 както и значението, което те придават на глобалната солидарност, са жизнено важни фактори, предопределящи качеството на глобалната система за управление.

Глобалната цел, в рамките на многостранната система, трябва да стане задача за осигуряването на достоен труд за всички. Необходима е съгласуваност между глобалната икономическа, социалната и екологичната политика.

Анализът показва, че глобалната система на управление е в криза, а несъответствието между икономиката и обществото подкопава социалната сигурност на държавите.

Държавата в сътрудничество с гражданите и техните организации планира, организира и провежда дейности за възпиране употребата на езика на омразата и за противодействие срещу прояви на ксенофобия, етническа, религиозна или друга нетолерантност.

През последните години на световната сцена набира сила още едно ново явление, свързано с появата на неправителствени движения, които се противопоставят на глобализацията, предимно в икономиката, и нейните последици.

Вероятно най-убедителният пример за глобализацията в света е икономиката, която всъщност е нейна причина и резултат едновременно. В края на XX век определяща роля в тази система имат механизмите на неолибералната пазарна

икономика, при която стопанската инициатива е насочена към извличане на печалби, реализиращи се в условията на повсеместна конкуренция. Главен инструмент на глобализацията е неотклонното развитие на интернационалните процеси в световната икономика, а техен резултат е нейната все по-нарастваща интернационализация, която обхваща производството на стоки и услуги, пазарите, в т.ч. и пазара на работната сила, банковата и финансовата система. Производството и пазарите до такава степен са се интернационализирали, че често крайният резултат се намира в различни части на света, а потреблението на самото изделие пък се извършва на съвсем друго място на планетата.

В края на XX век се наблюдава преориентация при модернизацията на икономиката, която се изразява в замяна на труда и капитала с информация. Този процес води до:

- увеличение на производителността;
- автоматизация, електронизация и компютъризация на производството;
- нарастване на възможностите за печалба, свързани с използването на информатиката;
- миграция на хора към големите икономически центрове.

Всичко това е свързано с т. нар "троен конфликт на модернизацията", проявяващ се в:

- сблъсъка между стремежа към икономически растеж;
- исканията за социална справедливост и потребността от запазване на националното и културното своеобразие и идентичност.

Пазарната икономика, конкуренцията, световният обмен се признават за фундамент на съвременния растеж и просперитет на обществото. В същото време обаче, в редица страни, предимно високо развити, се дискутират и отрицателните последици от глобализацията на икономиката - унищожаване на околната среда и природни ресурси. На дневен ред започва да се поставя обсъждането на въпроса за цената, която трябва да заплати човечеството за това, което се приема за прогрес на съвременната цивилизация.

Държавата разглежда своите отговорности в сигурността според няколко основни критерия. Според консуматора на сигурността (според бенефициента) тези равнища са:

- лична;
- групова;
- обществена;
- регионална;
- световна.

Според преките сфери на дейност равнищата са следните:

- управление;
- обществен ред;
- отбрана;
- дипломация;
- класифицирана информация;
- специализирано производство;
- търговия;
- кризисен мениджмънт;

- мобилизация и резерв;
- научно и образователно осигуряване.

Повечето европейски икономики се борят с пристъпи на евросклероза, при която държавните сектори се разрастват неимоверно, фискалните условия се влошават, стагфлацията придобива епидемични размери, цената на труда е ниска и трудно подвижна, а прекомерните данъци и регулации буквално задушават предприемачеството. Ниските печалби водят след себе си намаляване на инвестициите, което пък генерира ниска производителност в бъдеще – една зловеща спирала, която сочи надолу към икономически упадък и социални размирици.

Стриктна валутна дисциплина би гарантирала прочистване на капиталовите пазари от инфлационните си очаквания и намаление на лихвените проценти. На пътя на националната икономическа политика в Европа застават приумиците на глобалната икономика, доминирана от американците. Вместо собствен разцвет, ръководен от вътрешни инвестиции, европейците се радват на воден отвън напредък, подхранван от високия долар. Това пак ги връща в позиция на зависимост.

В една глобална система, където правилата са неустойчиви и стабилността е в опасност, е наложителен стабилен глобален режим, глобално партньорство. Спорен е въпросът за евро-американското лидерство, което може да се окаже по-ефикасно при трудното приспособяване, което глобалната система изисква.

Глобалната система изисква конституционни реформи, за постигане на сигурността, необходима за консолидирането на един здрав европейски блок.

Динамични и дълбоко вкоренени тенденции – военни, културни, политически и икономически подтикват европейските държави към консолидиране и поемане на отговорност за обща безопасност.

Националните държави губят контрол, докато многонационалните предприятия, придобили нови сили, в нарастваща степен имат възможността да решават изгоди, да експлоатират работниците и да потъпкват екологичните стандарти. Проблемите, които глобализацията поражда произтичат главно от това, че едновременно с много положителни черти: по бърз растеж, по-евтин внос, нови технологии, стимулиране на конкуренцията, тя поражда загуба на националната идентичност на по-малките държави и засилване сферите на влияние върху тях.

Основна трудност при определяне на цената, заплахите, и негативните последствия от глобализацията е свързана с асиметричната структура на съвременното световно стопанство и често антагонистичните интереси и очаквания на макро- и микроикономическите участници в този процес. Допълнителни трудности създава многообразието от последиците на глобализацията - икономически, социални и психлогически - най-вече поради невъзможността част от тези последици да се интерпретират еднозначно. Едни от най-често срещаните негативни последствия от глобализацията са:

- валутно-финанасови кризи - това е първата и очевидна последица от финансовата глобализация. Мащабите и глобалните последици от последните валутно финансови кризи стоят в основата на аргументите за необходимостта от въвеждане на контрол и механизми за регулиране на международните капиталови потоци;

- глобализация и несигурност - производствената и търговска глобализация оказва неблагоприятен ефект върху разпределението на доходите, сигурността за работните места и жизнения стандарт на ниско квалифицираните работници в условията на ограничаване на миграцията;
- глобализацията и разпределението на доходите - глобализацията променя данъчната тежест и съответно преразпределението на доходите като дескриминира едни в полза на други;
- глобализация и екология - повишената загриженост за състоянието на околната среда в процеса на глобализация е предизвикана от разрастването на мащабите и срока на вредните екологични последици от стопанската дейност. Като изход от ситуацията противниците на глобализацията често предлагат съкращаване на производството и ограничаване на трансграничната предислокация на производствените фактори. Подобно становище пренебрегва обичайната практика в съвременния свят, а именно, че санкционирането на замърсяването на околната среда се извършва преимуществено по силата на националните законодателства без да се компенсират щетите от трансграничния пренос на вредни емисии и от екологичен проблемът се превръща в компетитивен. Заниженитe или често липсващи национални норми за екологосъобразност в отделни страни прехвърлят екологичните разходи за производството от замърсителите в страната върху засегнатите през границита. Освобождавайки местното производство от екологични разходи, страната придобива сравнителни приимущества и привлича инвестиции. От гледна точка на глобализацията може да се твърди, че страните със занижени екологични изисквания имплицитно дотират местните производства и привличат капиталови потоци чрез екодъмпинг.

От развитието на процеса на глобализация и търговска либерализация са заинтересовани всички страни, влизащи в развлични подсистеми на световното стопанство. Необходимо е отчитането, както на положителните така и на отрицателнитея последици от този процес. Глобализацията в съвременни условия е процес, който има противоречиви последици за отделните страни. Целта на страните е минимизиране на вредните последици. Необходимо е международните икономически отношения да се развиват на база съчетаване на интересите на участващите в тях страни независимо от икномическата им сила и големина. В процеса на глобализация трябва да се търси оптималния вариант за съчетаване интересите на държавите и стопанските субекти.

Интегрирането на пазарите за стоки и услуги е противоречиво. Митата на стоките намалява, което води до засилване интеграцията на пазарите, но от друга страна нетарифните бариери оказват голямо влияние. В определени периоди в някои държави те се засилват. Следователно това е причината цените на едни и същи стоки в държави, намиращи се на еднакви или сходни етапи на развитие да са различни. Поради това глобализацията на ценовата конкуренция изостава от глобализацията на търговията.

При търговските преговори в международната търговия целта на страните е да се намалят търговските бариери от страна на партньорите. Ползите от многостранното либерализиране са резултат от усилията на страните да намалят собствените си търговски ограничения.

Глобализацията и нарастващата взаимозависимост между отделните икиномически общества са обективно протичащи процеси, които е невъзможно да

бъдат спрени. Този основен извод се признава от мнозинството икономисти, политици, социолози. В днешно време все по ясно се очертава тази взаимозависимост. Глобализацията обаче не се изчерпва със простата взаимосвързаност между страните, тя е процес много по напреднал във еволюционно отношение. Той се свързва не само с пренасяне на ефекти през границите, но и едно много по мащабно и всеобхватно симулативно и синхронизирано функциониране на националните икономики в рамките на унифицирани условия и правила. Повишената загриженост за състоянието на околната среда в процеса на глобализаиция е предизвикана от разрастването на мащабите и срока на вредните екологични последици от стопанската дейност. Като изход от ситуацията противниците на глобализацията често предлагат съкращаване на производството и ограничаване на трансграничната предислокация на производствените фактори. Подобно становище пренебрегва обичайната практика в съвременния свят, а именно, че санкционирането на замърсяването на околната среда се извършва приимуществено по силата на националните законодателства без да се компенсират щетите от трансграничния пренос на вредни емисии и от екологичен проблема се преявръща в компетитивен. Занижените или често липсващи национални норми за екологосъобразност в отделни страни прехвърлят екологичните разходи за производството от замърсителите в страната върху засегнатите през границита. Освобождавайки местното производство от екологични разходи, страната придобива сравнителни приимущества и привлича инвестиции. От гледна точка на глобализацията може да се твърди, че страните със занижени екологични изисквания имплицитно дотират местните производства и привличат капиталови потоци чрез екодъмпинг. От развитието на процеса на глобализация и търговска либерализация са заинтересовани всички страни, влизащи в развлични подсистеми на световното стопанство. Необходимо е отчитането, както на положителните така и на отрицателнитея последици от този процес. Глобализацията в съвременни условия е процес, който има противоречиви последици за отделните страни. Целта на страните е минимизиране на вредните последици. Необходимо е международните икономически отношения да се развиват на база съчетаване на интересите на участващите в тях страни независимо от икномическата им сила и големина. В процеса на глобализация трябва да се търси оптималния вариант за съчетаване интересите на държавите и стопанските субекти. В съвременни условия интензивно протича процес, при който целият обществен живот се поставя на икономическа основа и има икономически измерения, известен като “икономизиране на политиката”. Във вътрешен план това означава: постигане на целите и решаване на политическите задачи с икономически методи и преместване на вектора на стратегическото развитие от политическите, идеологическите и други средства към икономическите.

По отношение на външната среда икономизирането на политиката се изразява в приоритет на геоикономическите интереси над геополитическите и геостратегическите, т.е. икономическата власт диктува свои правила на играта, геополитиката ги оправдава, а военната компонента ги защитава.

В съвременния глобализиращ се свят тя не води до осъществяване на най-елементарните и законни въжделения по отношение на достойна заетост и изграждане на по-добро бъдеще за децата. Преобладаващото мнозинство жени и мъже, се намират в клещите на неформалната икономика и са лишени от каквито и да било формални права или живеят в най-бедните страни, безцелно съществуващи и прак-

тически изключени от глобалната икономика. Подобен глобален дисбаланс е морално неприемлив и политически несъстоятелен. Трансграничната организирана престъпност е една от главните заплахи за сигурността на гражданите и демократичните основи на обществото. Тя включва дейности, свързани с икономически престъпления

производство и трафик на наркотици, трафик и експлоатация на хора, контрабанда, производство и разпространение на неистински парични знаци и документи, киберпрестъпления, пране на пари и други. Организираната престъпност създава предпоставки и се възползва от корупцията.

ЛИТЕРАТУРА:

1. Ангелов, А., Системата за национална сигурност в новите условия. София, 2000. с. 18.
2. Калео Д., Да преосмислим бъдещето на Европа, ВИ, 2003
3. Милина, В. Политически аспекти на сигурността. София, 2003, Министерство на отбраната, ВА „Г.С. Раковски". с.23-28.
4. Милушев, В., Националната сигурност след края на Студената война. В: *Актуални проблеми на националната сигурност.* Годишник на Военна академия „Г.С. Раковски", София, 1995. 15-21с.
5. Рачев, В. и др. Национална и международна сигурност. София, 2005, с.9.
6. Стойчев, С. Политика за сигурност и отбрана – някои теоретични положения. София, Военна академия „Г. С. Раковски", 1999. 5-9 с.
7. McNamara, R., *The Essence of Security* (New York: Harper and Row, 1968)
8. Ivanov, Tilcho K., Confidence and Security in the Balkans: The Role of Transparency in Defence Budgeting: *Research Report No.6, Institute for Security and International Studies*. Sofia, November, 1996.
9. Mesjasz, Czesław. Security as an Analytical Concept. Cracow University of Economics Paper presented at the 5th Pan-European conference on International Relations, The Hague, 9-11 September 2004. pp.4
10. Милина, Величка. Политически аспекти на сигурността. София, 2003, Министерство на отбраната, ВА „Г.С. Раковски". с.23-28.
11. Милушев, Васил. Националната сигурност след края на Студената война. В: *Актуални проблеми на националната сигурност.* Годишник на Военна академия „Г.С. Раковски", София, 1995. 15-21с.
12. Liotta, P. H. Boomerang Effect: The Convergence of Natioanl nad Human Security, in: *Secirity Dialogue*, vol.33, no 4, pp. 473-488.
13. Encyclopaedia Britannica, 1997.

ГЛОБАЛИЗАЦИЯ – МИГРАЦИЯ- СИГУРНОСТ

Маргарита К. Бонева

Шуменски университет «Епископ Константин Преславски»
Педагогически факултет

GLOBALIZATION – MIGRATION – SECURITY

Margarita K. Boneva

University of Shumen
Faculty of Education

Abstract: *Analizing globalization is found a relationship globalization-migration-security.*

Key words: *globalization, security, migration.*

Едни от основните социално-екологични проблеми на глобализиращия се свят са замърсяването на околната среда, икономическите и социални кризи, тероризмът, трафикът на хора и наркотици, организираната престъпност, нелегалната миграция.

Нарастването на миграцията в световен мащаб е функция на глобалните икономически, демографски, екологични проблеми, от засилващата се бедност, безработица, екологични проблеми, незачитане на човешките права. Бързото развитие на технологиите е една от причините за масово движение на населението.

От една страна висококвалифицираните имигранти допринасят за развитието на специфични отрасли в съвременната икономика, от друга – неквалифицираните – се реализират в сектори, нежелани от местните граждани. Сред имигрантите също има безработица, която поражда социални проблеми и застрашава вътрешната сигурност.

За разлика от легалната, която се осъществява според законите на дадена държава и е въпрос на вътрешната й политика, нелегалната имиграция е извън националното право и има отрицателно влияние върху всички области на обществеото развитие. Този вид имиграция е заплаха и е един от новите рискове на вътрешната сигурност. Тя се явява заплаха за културната идентичност и икономическата стабилност в не по-малка степен от трафика на наркотици, организираната престъпност и тероризма.

По – голямата част от нелегалните мигранти не желаят да се интегрират в обществото, а това допълнително повишава недоверието и несигурността. Освен това все повече именно те се възприемат като потенциални участници в престъпни организирани мрежи и като заплаха за обществената сигурност.

Нелегалната имиграция в Европейската общност до голяма степен е организирана от престъпни групировки, специализирани в контрабанда и трафик

на хора. Вярно е, че експлоатацията и обвързването на жертвите с криминални структури изгражда връзка между трафика на хора и други форми на организираната престъпност.

Високата безработица в условията на рецесия в Западна Европа повишава страха от «нахлуване» на евтина работна ръка от «бедните» страни.

Според Европейската стратегия за сигурност именно глобализацията е причина «вътрешните заплахи за сигурността все по-често да имат външни измерения».

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 и по-високи разлики в доходите, а това ще наложи държавната политика да посочи път за териториално сближаване и справяне с негативните последици от урбанизацията.

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;
- потребността от допълнителна работна ръка в приемащите страни;
- 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.

Националната стратегия в областта на миграцията, убежището и интеграцията цели формирането на ефективни и единни национални политики при управлението на миграционните процеси. Феноменът «миграция» е както необходим ресурс за националната икономика, така и потенциална заплаха за социалното единство и сигурността на дадената страна. В условията на демографска и икономическа криза миграцията е ресурс, който чрез прилагането на добре работещи механизми на управление на миграционните процеси, може да окаже положително влияние за развитието на икономиката и сигурността на ЕС. Миграцията е и ще бъде феномен, присъстващ в глобален мащаб. Добре управлявана, от нея могат да бъдат извлечени ползи както за националния трудов пазар и за икономическия растеж на ЕС, така и за благосъстоянието на самите мигранти и страните им по произход.

Политиката на Република България в областта на миграцията, интеграцията и убежището се основава на националните интереси и на европейските принципи за управление на миграционните процеси, а именно:

- законност и защита на човешките права;
- координация и партньорство;
- прозрачност;
- анализ;
- научност и проактивност;
- отчетност;
- мониторинг и контрол;
- равни възможности.

В Република България е изградена институционална система и администрация за изпълнението на държавната политика в областта на миграцията, убежището и интеграцията.

Изпълнението на критериите, заложени в основополагащите директиви на Европейския съюз е ключов елемент за реализиране на обща миграционна политика, целяща да гарантира на всички етапи ефективно управление на миграционните потоци, справедливо третиране на гражданите на трети страни, пребиваващи законно в държавите – членки на ЕС, както и предотвратяване на незаконната миграция и трафика на хора.

Приетата Национална стратегия по миграция и интеграция има две основни цели:

- привличане на български граждани и чужденци с български произход за трайно установяване или заселване в България;
- провеждане на съвременна политика по прием на граждани на трети страни с оглед подпомагане на българската икономика и ефективно регулиране и контролиране на миграционните процеси.

Противодействието на незаконната миграция е един от основните приоритети на българската политика в областта на сигурността и управлението на миграционните процеси. Защитата на човешките права на жертвите на трафик е ръководен принцип на всички усилия за предотвратяване на престъплението «трафик на хора» в Република България.

Сред основните фактори, движещи трафика на хора са:

- бедността и слабото икономическо развитие на някои райони;
- липсата на информираност сред лицата в риск, които се характеризират с ниско ниво на образованост и липса на достатъчно социален опит.

Най-уязвими продължават да бъдат младите жени на възраст между 18 и 30 години, непълнолетните момичета и децата без родители, мъжете и жените в активна възраст за трудова експлоатация. Жертвите на трафик в голяма част произхождат от райони с висока безработица и бедност. Основните методи за въвличане в трафик продължават да бъдат предложения за работа, образование в чужбина за младите хора, обещания за брак.

Република България участва активно в глобалните процеси в областта на миграцията и развитието. Политиката на предоставяне на българско гражданство е ключов елемент в управлението на миграционните процеси от страна на държавата. Тя е съчетана с мониторинг и контрол на процеса и недопускане на действия, насочени срещу националната сигурност на страната.

Интеграцията на имигрантите, които законно пребивават в страната, се провежда съобразно общите принципи за интеграция на имигранти в ЕС. Балансът между правата и задълженията на мигрантите в Република България е гарантиран. Интеграционната политика е неразделна част от държавната политика на страната ни в областта на законната миграция.

Националната политика в областта на миграцията, убежището и интеграцията е комплекс от взаимносвързани приоритети и секторни политики, съобразени с националните интереси и политиката на ЕС. Визовата политика е част от имиграционната политика и има за цел да допринесе за създаването на единно пространство на свобода, сигурност и правосъдие.

Борбата с явлението «трафик на хора» остава във фокуса на националната и миграционна политика и на Република България.

Приоритет в националната политика е трайното привличане и заселване в страната на лица от български произход с чуждо гражданство за целите на трудовия пазар, както и обратното привличане на български емигранти в България с цел окончателно завръщане, укрепване на административния капацитет на работещите в областта на миграцията, чрез системно обучение на държавната администрация, местната власт, социалните партньори, академичната общност и гражданското общество.

В Европейския съюз все по-належаща става необходимостта от прилагане на специфични политики за интеграция, основани на справедливо отношение към гражданите на трети държави, пребиваващи легално в дадена европейска страна, превенцията за социално «изключване», расизма, ксенофобията и уважението към културните различия.

За Република България високото ниво на емиграция е процес, равнозначен на «изтичане на мозъци», защото напускат млади хора, получили добро образование, предоставено им от българската държава.

Основната цел на провежданата политика е «да се повиши чувството за сигурност на гражданите в собствената им страна и така да се демотивира желанието им за емиграция, като едновременно с това ефективно се противодейства на нелегалния трафик, контрабандата на хора и незаконната имиграция». Това азначава, че за постигане на основната цел – повишаване на сигурността – правителството трябва да осъществява политика в две насоки: от една страна то трябва да «задържи» българите в собствената им страна, т.е. да спре емиграцията, а от друга – да предотврати нелегалното пребиваване и преминаване на чужди граждани на българска територия и нерегламентираната миграция на българи в чужди държави, т.е. да ограничи самата миграция.

Намаляването на темповете на емиграцията изисква повишаване на жизнения стандарт на българските граждани, който според прогнозите ще нараства с бавни темпове и успоредно с икономическия растеж и намаляването на безработицата. В този смисъл, мотивацията на българските граждани да останат в страната е пряко свързана с икономическите реформи. Имиграцията е един от малкото въпроси на сигурността, който заедно с политиката за предоставяне на убежище и охраняване на външните граници на ЕС е актуален в цялата Европейска общност. Имиграционната политика е една от най-интензивно развиващите се сфери на европейската интеграция. Всичките страни преживяват частична интернационална миграция - както влизане в страната, така и излизане. За много държави емиграцията се е превърнала в икономически жизнена и широко приета икономическа стратегия. Най - ярък пример за това е САЩ и високоразвитите западноевропейски страни. Това често води до “култура на миграцията”, в която да ходиш да работиш в чужбина става път за млади хора, стремящи се към икономическо благосъстояние и по- добър социален статус. Мнозинството от емигрантите са млади хора в тяхната най-продуктивна възраст. В края ня XIX век повечето от емигрантите са били мъже, но последните няколко декади показват “феминизъм на миграция”. Някои от основно доминиращите миграционни движения днес са от жени. В България се наблюдава обратния процес - имиграция. Резултатите от последното преброяване на населението сочат, че повече от 1 милион българи са зад граница. Голяма част от тях са с висок научен потенциал, току - що завършили висшето си образование. С падането на визовия режим

границите на страната ни се отварят за останалите страни от Европа и се засилва имиграционния поток. Това води до неблагоприятното свиване на потреблението и намаляване на местното производство. В тази насока България трябва да насочи усилията си към производство на конкурентноспособна за външния пазар продукция. Емиграцията включва трансфер на най-ценния икономически ресурс - човешкия - обикновено от бедни към богати държави. Семейството, местното общество и родината понасят загубите от повишаващата се миграция към съседни държави. Главен въпрос за правителствата на емигрантските държави е дали емиграцията допринася за развитие. Въпросът е твърде сложен тъй като емиграцията предизвиква дългосрочни и дълготрайни влияния на всеки сектор от обществото. Миграцията е богатство за страната на имигранта, само когато той се завръща обратно в родината и предоставя своите знания и умения, придобити в чужбина. Най-очевидната причина за миграцията е липсата на висок доход, работа и социално благоденство. Демографските различия в полова, възрастова структура, човешкия прираст и растеж са много важни. Трябва да се очаква отделни хора да максимизират своя доход като се преместват от места с ниска работна заплата към икономики с високо заплащане на труда. Последните проучвания показват голямо влияние на социалната мрежа. Катастрофа като война или природно бедствие може да принуди дори най-бедните да мигрират, обикновено при много лоши условия. Миграцията е едновременно и резултат и причина на развитието. Развитието води до миграция, защото икономическите и научни подобрения улесняват хората да търсят по-добри възможности в останалите държави. Социалните групи със среден доход се изселват най-много. Колкото доходът расте, толкова емиграцията намалява. Миграцията води до развитие, само когато мигрантът се завръща с опит и инвестира в родината.

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 човешкия живот може да се превърне в *сериозен глобален въпрос на сигурността*. В света се оформят нови полюси. Единият е този на благополучието и богатството, на "златния милиард", където населението намалява, а богатствата са огромни. Срещу него се изправя другият, този на бедността, на развиващите се държави, които по население многократно превъзхождат първия полюс. В страните от втория полюс вече се чувства остра липса на храни, територия, природни ресурси. Това може да предизвика фаталната необходимост от нови териториални преразпределения, които едва ли ще се извършат по мирен и цивилизован начин. Подобно на снежна лавина нараства и проблемът с *миграцията на населението* – един от първите признаци на демографския натиск на глобалният Юг върху глобалния Север.

Прогнозата за демографското състояние на човечеството през следващите 50 години показва, че най-гъсто населената страна ще бъде Индия, която по демографски показатели ще изпревари настоящия фаворит Китай. Ще намалее населението на Германия, Япония и Русия. Като нови демографски гиганти ще се появят държави от Третия свят, чието население и сега нараства със застрашителни темпове.

Най-голяма динамика в ръста – около три до четири пъти се очаква в някои африкански държави. Предполага се, че на пето място в демографската статистика ще се издигне Нигерия (339 млн.), на девето–Етиопия (213 млн.), а на единадесето ще се окаже Конго (165 млн.). На трето място ще се окаже Пакистан (357 млн.) пред САЩ (348 млн.). Русия ще се нареди на 16 място (114 млн.), а Япония (110 млн.) на 17 място.

Новото разместване на демографската скала неминуемо ще създаде многобройни проблеми на всички нива на обществения живот и ще се отрази върху въпросите на сигурността във всички аспекти – демографски, етнокултурни, икономически, политически, социални, екологични, военни и др. Прогнозира се залезът на глобалната хегемония на западната цивилизация и все по-нарастващата световна значимост на ислямската и синоистката. Това ще доведе до неминуем "сблъсък" на цивилизациите, съпроводен с всички, произтичащи от него войни и гибелни последици за човечеството.

Според изтъкнатия руски физик академик, Сергей Капица "в обозримо бъдеще центърът на човешкото развитие ще се премести в Азиатско-Тихоокеанския регион". Неминуемо това ще бъде свят, в който Европа завинаги ще се превърне в малочислена по население световна провинция. Тези нарастващи диспропорции в демографското развитие на човечеството могат да доведат и до война. В това се състои най-сериозното предизвикателство на човечеството и световния мир.

Динамиката на световните процеси поставя пред човечеството редица нови проблеми, възникващи в хода на историята. Един от най-важните е демографският, предизвикан от пренаселването на света, застаряването на поколенията, масовата миграция на хората, все по-застрашителното нарастване на населението в слаборазвитите и развиващите се страни, недостига на храни и питейна вода за милиони хора.

През последните 50 години се случва нещо уникално. Хората на планетата нарастват два пъти и са вече над седем милиарда. Това е безпрецедентен ръст в човешката история, който никога повече няма да се повтори, защото човечеството е изживяло своя демографски връх и от тук нататък неговото нарастване ще бъде минимално.

Във все по-глобалния съвременен свят националните демографски проблеми и миграцията 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 се превръща в сериозен *глобален въпрос на сигурността*.

ЛИТЕРАТУРА

1. Калчев, Й., Външната миграция на населението в България, С., 2001.
2. Петров, А., Тероризъм и системи за сигурност, С., 2005.
3. Проданов, В. Глобалните промени и съдбата на България, София, 1999.
4. Стиглиц, Дж., Глобализацията и недоволството от нея., С., 2003
5. A Secure Europe in a Better World, European Security Strategy, 2003.
6. Albuthnott T., Migration in an expanding EU, BBC News online, 2002.

7. Brucker H., Epstein G., Mc Corm B., Saint – Paul G., Venturini D. and Zimmermann K., Managing Migration in the European Welfare State, 2001.
8. leinschmidt, H., EU Migration Policy, Institute of Social Science, University of Tsukuba, 2002.

НЯКОИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА КОНФЛИКТА

Красимир М. Марков

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

SOME ASPECTS OF CONFLICT MANAGEMENT

Krasimir M. Markov

ABSTRACT: *The paper deals with some aspects of conflict management highlighting the possible methods of conflict resolution in organizations.*
KEY WORDS: *management, conflict, resolution*

Когато при хората възникне зона на разногласие, съществуват различни представи за определена ситуация и на тази основа противоречия, породени от невъзможност да бъдат осъществени едновременно мотиви и цели, то е естествено, че тези хора започват да проявяват поведение, при което действията на едната и другата страна влизат в противоречие. Целта на такова действие е да се попречи на другата страна да постигне своите цели. Именно поради това всяка от страните определя действията на другата като враждебни. В тези действия се заключава и реалното протичане на конфликта. Автори, разглеждащи проблемите на конфликта, считат, че основни видове действия на едната от страните, които другата оценява като враждебни, могат да бъдат:

– създаване на преки или косвени пречки за осъществяване на плановете и намеренията на другата страна;

– неизпълняване от съответните страни на обещания и задължения;

– нанасяне на пряка или косвена вреда на имуществото или репутацията на другата страна;

– унижаващи човешкото достойнство;

– заплахи или други принуждаващи действия, които карат човека да прави това, което не иска или не е длъжен да прави;

– физическо насилие.

Особеност в човешкото поведение е, че тези чиито действия се считат за конфликтни могат да не ги смятат за такива или въобще да не подозират, че околните ги смятат за конфликт. В конфликтната ситуация действията на едната страна оказват съществено влияние върху другата, това влияние се състои не само във факта, че отсрещната страна понася някакви вреди, но и в това, че тя на свой ред планира и

предприема ответни действия. В този смисъл конфликтиращите страни така или иначе си въздействат една върху друга. Разглеждайки енергетиката на конфликта, трябва да отбележим, че всеки конфликт съществува дотолкова доколкото хората отделят енергия във вид на време, сили и здраве, за да го поддържат. Би било много просто да се прекрати конфликта, ако престанем да се занимаваме с него, но това не е възможно, когато в зоната на разногласията се намират жизнено важни за хората ценности.

Съществуват различни обективни и субективни фактори, действията на които подтиква хората към конфликт:

Обективни фактори – това са реално съществуващи в живота обстоятелства свързани с условията на бита, като например социално неравенство или с някои съществени социалнопсихични особености на личността, които тя реално има в даден момент и не могат да бъдат коригирани за кратко време (образование, ниво на квалификация, интелектуално развитие, диапазон на способности, потребности и нагласи). Различията в тези качества водят до взаимно неразбиране, а в някои случаи и до разпад на контактите, а доколкото тези качества не съответстват на изискванията на конкретната организация за изпълнение на определени дейности, могат да се явят като основна причина за служебните конфликти.

Наличието на тези обективни фактори, които предизвикват сблъсък на жизнено важни потребности, интереси и цели на хората прави конфликта неизбежен;

Субективни фактори – те представляват стимули за конфликтни действия, които са предизвикани от илюзорни, измислени обстоятелства. Хората приемат изкривено ситуацията в която се намират, като в тяхното въображение обстоятелствата придобиват характер несъответстващ на действителността, дори й се наслагват такива обстоятелства, които в действителността не съществуват. Според американския социолог Томас, тези измислени обстоятелства се възприемат от страната като напълно реални (теорема на Томас). Енергетиката на конфликта, както видяхме се ражда и се подтиква от различни както реални, така и въображаеми източници. Всъщност илюзии имат всички. Когато две страни имат различни представи за едно и също нещо, то всяка от страната смята, че представите на другата страна са грешни и илюзорни, и много често се случва така, че изобщо не е ясно чия гледна точка е по-правилна.

Продължителността и интензивността на конфликта зависи от целите, нагласите, ресурсите, средствата и методите за водене на противоборството между страните, а също така и от реакцията, която околните имат към този конфликт. На определен етап на развитието на конфликта противодействащите си страни могат да изменят съществено представите си за своите възможности и възможностите на противната страна. Настъпва така наречения момент на преоценка на ценностите, на осъзнаване на реалната ситуация водеща до невъзможност за достигане на целите или до прекалена цена за постигане на тези цели, което води до стимулиране на страните за промяна на тактиката и стратегията на конфликтно поведение. В този случай, страните на конфликта започват да търсят средства за изход от конфликта, което води до идеята, че ръководството на организациите следва да познава структурата на конфликта и възможните начини, методи и средства за управление на конфликтите с оглед на тяхното разрешаване.

Необходимостта от управление на конфликтни ситуации винаги е заемала особено място в живота на хората, но в съвременния живот нараства значението на

този процес. В науката и практиката съществуват различни ефективни способи за управление на конфликтната ситуация. Независимо от тяхното многообразие можем да ги разделим на две големи групи: структурни и междуличностни.

Към коя категория методи за разрешаване на конфликта ще се насочи съответния управленец, зависи от анализа на съответните фактически причини за възникването на конфликта. Именно този анализ предполага използването на съответната методика.

По принцип към структурните методи спадат:

- разяснение на изискванията към дейността;
- координационни и интеграционни механизми;
- управление на общоорганизационните комплексни цели;
- използване на стимулиращото въздействие на системата за заплащане.

Разясняването на изискванията към дейността в организационната практика се приема като един от добрите методи на управление, предотвратяващ възникването на дисфункционален конфликт. Неговото съдържание е в разясняване на това, какви резултати се очакват от дейността на всяка структурна единица на организацията и на всеки от сътрудниците в организацията. Тук трябва да бъдат заложени такива параметри на очакванията, като: ниво на резултатите, които трябва да бъдат постигнати; кой ще предоставя и кой ще получава информацията; системата на правомощия и отговорности в организацията; определяне на политиката на организацията, процедурите и правилата. Ръководителят на организацията изяснява тези параметри, от една страна за себе си, а от друга страна, за да може всеки от неговите подчинени да разбере какво се изисква от него в конкретната ситуация и в дейността на организацията като цяло.

Координационни и интеграционни механизми – координационния механизъм за разрешаване на конфликти е разработен още от Макс Вебер в неговия административно-бюрократичен подход. В крайна сметка става дума за установяване на йерархия в организацията, налагане на определен ред във взаимоотношенията между сътрудниците и на определен ред при вземането на решение и обработването на информационните потоци в организацията. Това означава, че ако между двама сътрудници в организацията възникне конфликт, право и задължение на техния началник е да вземе решение и да разреши конфликта. Този така наречен казармен принцип на единоначалието, всъщност облекчава решаването на конфликтните ситуации в организацията, тъй като всеки от сътрудниците много добре знае на чии заповеди и решения трябва да се подчинява.

При управлението на конфликтната ситуация са много полезни средствата на интеграцията като управленска йерархия, междуфункционални групи, целеви групи, междуотраслеви съвещания, създаване на отдели или структури, които да осъществяват връзка между отделните звена на организацията и т.н.

Управление на общоорганизационните комплексни цели – идеята на всяко поставяне на цели в една организация се заключава в мобилизация на сътрудниците в тази организация за достигането на тези цели. Разковничето на конфликтите тук се заключава в това, че са необходими почти съвместни усилия на отделните сътрудници, групи, сектори, служби и т.н. за достигането на общата цел. Ако всеки сътрудник, всяко подразделение на организацията разбере първо своето място в достигането на общата цел, и второ, че тази обща цел може да бъде достигната

само с общите усилия на всички, то вероятността за възникване на неконструктивни конфликти значително намалява.

Използване на стимулиращото въздействие на системата за заплащане – системата за заплащане може и се използва като метод за управление на конфликтна ситуация, доколкото финансовото поощряване или санкциониране оказва влияние на хората за избягване на последствията от конфликтите. В този смисъл е предложената от Б. Скинър, система при която хората, които работят за постигане на целите на организацията, старят се да намерят решение на проблемите и подпомагат останалите, трябва да бъдат стимулиране чрез повишаване на заплащането, допълнителни възнаграждения и т.н., т.е. да се **утвърждава** такова поведение в организацията. От друга страна не по-малко важно е системата на заплащането да санкционира тези сътрудници или служби в организацията, които не работят активно за постигане на целите на организацията и проявяват неконструктивно поведение. В съвременните пазарни условия използването на стимулиращото въздействие на системата за заплащане е един от най-важните икономически лостове, с помощта на който се регулират взаимоотношенията в съответната организация и който в частност способстват за разрешаване на конфликти.

Междуличностни стилове за разрешаване на конфликта:

Американският социолог Томас е един от първите, които предлагат класификация на междуличностните стилове за разрешаване на конфликта. В различните източници се различават несъществено по наименованието си, но в съдържанието няма разлики. За нашите цели ще приемем наименованията: избягване, съгласяване, принуждаване, компромис, разрешаване на проблема.

Избягване – самото наименование на този стил подсказва, че той се използва от хора, които се опитват да стоят на страни от конфликта. Създателите на мениджърската решетка Блейк и Мутон смятат, че един от способите за разрешаване на конфликта е да не се попада в ситуация, която провокира възникване на противоречие, да не се встъпва в спорове, разногласия, за да не се привеждаме във възбудено състояние, което ще ни попречи за разрешаване на проблемите.

Съгласяване – целта на такова поведение произтича от убеждението, че ние все пак сме един екип и не е необходимо да предизвикваме разногласия. Обикновено привържениците на този стил апелират към солидарност, разбирателство и омаловажават значението на конфликтния проблем. Особеното е, че прилагащите този стил могат да постигнат в определен момент съгласие и доброжелателство, но това не означава, че проблемът който е породил конфликта ще бъде разрешен. В този смисъл, съществува реалната опасност от вътрешно натрупване на негативна енергия, която при подходящи условия би предизвикала нова много по-тежка конфликтна ситуация.

Принуждаване – и при този стил на поведение името говори само за себе си. Става дума за стил при който личността се стреми да застави другите да приемат нейната гледна точка, независимо от цената на това приемане. Като правило прилагащите този стил не се интересуват от мнението на другия, обикновено проявяват агресивно поведение и се стремят да наложат властта си по пътя на принуждаването. Този стил може да бъде ефективен в организации със строго йерархирана структура и ясно обозначено ниво на субординация от типа на армията, полицията и други военизирани структури, но може да бъде прилаган и се прилага и в организации, в които по една или друга причина ръководителят има ясно изразена власт

над подчинените си (едноличен собственик на организацията). Недостатък на този стил е в това, че той подтиска инициативата на подчинените, не допуска обсъждане, с което се поражда възможността реални, важни фактори да не бъдат отчетени при вземане на решение. При това подобен стил на поведение обикновено предизвиква негодувание и възмущение, особено сред по-младата и по-образованата част от персонала на организацията.

Компромис – този стил донякъде прилича на съгласяването дотолкова, доколкото в някакви аспекти приемаме позицията на другата страна в конфликта. Но тук това приемане е до известна степен и не на всяка цена. Едно от най-ценните управленски качества е способността на компромиса, тъй като това снема нивото на напрежение в организацията и дава възможност конфликтът да бъде разрешен при оптимално удовлетворяване на претенциите на страните на конфликта. Умението да бъде използван компромиса се заключава в това, не само да се постигне обединение на вижданията на страните на конфликта, но и в това кога ще бъде предложен компромиса като средство за разрешаване на конфликта. Прилагането му в ранен стадий на конфликта може да попречи за пълното изясняване на проблема и за преценяването на различните алтернативи, което свива и възможността за приемане на оптимално решение.

Разрешаване на проблема – тук става дума за това открито да признаем наличието на различие в мненията, да изразим готовност да се запознаем с другите гледни точки, което ще ни помогне по-пълно да разберем причините за конфликта и да набележим план за действие приемлив за всички страни. Прилагащият такъв стил на действие не се стреми да постигне своите цели за сметка на останалите, а по-скоро търси най-добрия вариант за разрешаване на конфликтната ситуация.

От значение е туширането на проявата на емоции в хода на разрешаване на проблема. Това може да се случи само по пътя на преки, директни разговори с лицето което има различни от нашите виждания. Всъщност всички автори сочат, че разрешаване на конфликта е възможно, но за това трябва определена зрялост на ръководителя, в смисъл че той трябва да е овладял изкуството на работа с хората. Проявата на искреност в отношенията е изключително значение за постигане на разбирателство. Вече споменахме, че конфликти е имало и ще има и че конструктивния конфликт проявяващ се в сложна ситуация само очертава различните варианти и възможности на вземане на решение, и поради това е необходимо в една организация дори да се поощряват такива конструктивни конфликти.

От казаното до тук е видно, че останалите стилове за предотвратяване на конфликта могат с успех да ограничат или предотвратят конфликтната ситуация, но няма да доведат до оптимално вземане на решение, тъй като алтернативните възможности и виждания няма да бъдат разгледани. Различните автори, в това число Блей и Мутон предлагат и методика с помощта на която би могло да се тушира конфликта по пътя на разрешаването на проблема. Най-общо тя се състои в следните стъпки:

- определяне на проблема, който се явява конфликтен;
- определянена решение, което е приемливо за страните на конфликта;
- съсредоточаване върху решаването на проблема, а не върху личностните качества на страните на конфликта;
- създаване на атмосфера на взаимно доверие и обмен на информация;

- в хода на обсъждането да се създаде положително отношение с изслушване на мнението на другата страна, като се стараем по всякакъв начин да тушираме проявата на емоции.

Литература:

1. Ангелов, А. Организационно поведение. С. 2002
2. Белинская, А. Б. Конфликтология в социальной работе. Дашков и Ко. 2002
3. Джонев, С. Социална организация – теория, диагностика, консултация. С. 2000
4. Димитров, Д. Конфликтология. УИ. С. 2003
5. Димитров, Д. Социология на конфликта. УИ. С. 1999
6. Дронзина, Т. Разрешаване на конфликти-тенденции и инструменти. С. 1999
7. Илиева, С. Организационно развитие. С. 1998
8. Каменов, К. Мениджмънт. ВТ. 1999
9. Карабельова, С. Управление и развитие на човешкия потенциал. С. 2004
10. Лазукин, А. Д. Конфликтология. Омега-Л. 2010
11. Желев, Ст. и др. Относно практическото обучение по военноспециална подготовка. ВВУАПВО, Трудове Научна сесия 2000.

ВЪНШНА СРЕДА НА ФИРМАТА И СИГУРНОСТ

Красимир М. Марков

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

EXTERNAL COMPANY ENVIRONMENT AND SECURITY

Krasimir M. Markov

ABSTRACT: *The paper deals with some aspects of external environment in terms of management and external environment impact on the company with emphasis on security.*

KEY WORDS: *management, external environment, company, security*

Един от най-важните въпроси на съвременната наука за управлението е въпросът за външната среда на фирмата и нейното влияние върху сигурността на фирмата, разбирана в най-широк смисъл. Всяка една организация като открита система зависи от външната среда както по отношение на ресурсите, които придобива от нея във вид на материали, енергия, информация и т.н., така и по отношение на персонала който организацията наема или освобождава, а също така и връзката с потребителите. След като оцеляването на организацията като такава зависи от нейнитеотношения и нейното място във външната среда, то задължение на всеки ръководител е да умее да определя съществените фактори на тази външна среда, които влияят върху организацията. Това дори не е достатъчно, тъй като той трябва да определи не само факторите, а и начините по които организацията ще реагира на външното въздействие. В

теорията на мениджмънта, понятието за външната среда и отношението й с организацията се появява в края на 50-те години на XX век, тогава се формира и разбирането, че външната среда представлява съвкупност от условия съществуващи извън организацията, които на практика влияят на нейния успех.

Разглеждайки факторите на външната среда, които влияят върху организацията трябва да кажем, че те са много и разнообразни, но което е по-важно те действат взаимосвързано. Тази взаимовръзка се разбира като взаимодействие при което изменението на единия фактор въздейства върху другите фактори. Ако преди време отделните фактори се разглеждаха без взаимна връзка и главно внимание се обръщаше на икономическите и техническите, то сега ръководителите вече не могат да разглеждат външните фактори изолирано, те трябва да отчитат че тези фактори са взаимосвързани и се изменят.

Това налага въвеждането на понятието **сложност на външната среда,** под което се разбират количеството фактори на които организацията задължително реагира, а също така и нивото на вариативност на всеки фактор. Доколкото всяка организация съществува в различна среда ситуативния подход налага извода, че не съществува най-добра организационна структура, а организационната структура трябва да бъде оптимално съобразена със средата.

Подвижност на средата – това е скоростта с която настъпват изменения във външната среда, тази подвижност може да бъде различна за различните организации, за някои организации, които пряко се влияят от пазара тя може да бъде много голяма, а за други организации от типа на административно-бюрократичните тя би могла да бъде много малка. Съвсем естествено е, че ръководителят при необходимостта да взема решение ще го взема много по-трудно при висока подвижност на средата.

Неопределеност на средата – неопределеността се явява функция на количеството информация с което разполага организацията по повод на конкретен фактор, а така също и функция от достоверността на тази информация. Колкото ръководството на една организация повече се съмнява в достоверността на една информация или не разполага с достатъчно информация за действията на един или друг фактор, толкова повече нараства неопределеността на средата. Доколкото в рамките на Европейския съюз се забелязва глобализиране на бизнеса, това налага необходимостта от все повече и повече информация, но колкото повече е информацията, толкова повече увереността в нейната достоверност се намалява.

Среда на прякото въздействие – тя включва фактори, които непосредствено влияят на операциите, които организацията извършва и изпитва върху себе си прякото влияние на резултатите от тези операции. Към такива фактори могат да се отнесат: доставчиците, трудовите ресурси, законовите норми, държавните институции за регулиране, потребителите, конкурентите и др.

Ако използваме системния подход, би трябвало да разгледаме организацията като механизъм за преобразуване на постъпващо на входа въздействие и преобразуването му до излизане на изхода на определен резултат. На входа на организацията могат да постъпват: материали, оборудване, енергия, финансови средства, работна сила. Зависимостта между организацията и мрежата от **доставчици** осигурява въвеждането в организацията на така посочените ресурси и е един от най-добрите примери за прякото въздействие на средата върху организацията. Получените на изхода ресурси могат да бъдат, както изгодни от гледна точка на цени, качество или количество, така и неизгодни следствие на външни влияния като

колебание на цените на международните пазари, политическа и икономическа нестабилност на държавата и др.

Като правило, колкото по-добро е състоянието на компанията или организацията, толкова по-голяма е възможността да се договори с доставчиците за по-благоприятни условия при получаването на необходимите ресурси. Другия елемент **трудовите ресурси** също е необходимо условие за успешното функциониране на организацията, адекватното осигуряване на организацията с работна сила, с необходимата специализация и квалификация е свързано с решаването на задачите на организацията, а оттам и с постигането на целите, което означава, че всъщност е свързано с ефективността на организацията като цяло. В съвременни условия пазара на труда показва, че все повече се търсят кадри в областта на високите технологии като компютърни и комуникационни специалисти или такива, които имат необходимата квалификация и опит за работа с финанси в сложни пазарни и кризисни условия. Практиката показва, че обикновено набирането на такива специалисти във фирмите се извършва на четири очи с договаряне на лични преференциални условия.

Законовите норми и влиянието на държавните институции за регулиране също са от значение за успешното функциониране на организациите. Промяната на тези норми, създаването на нови държавни организации отговарящи за тяхното регулиране, пряко влияе върху успешното функциониране на дадената организация. Интересни парадокси се наблюдават когато държавното законодателство или части от него не е синхронизирано с изискванията на Европейския съюз, които ние като страна членка би трябвало да съблюдаваме. Това по същество затруднява излизането на нашите организации на европейските пазари и съответно свива възможността за тяхната успешна реализация.

Потребителите – в крайна сметка всяка организация съществува, за да удовлетворява потребностите на потребителите. Тук става дума не само за производствени и търговски организации, а и за такива които са в сферата на държавната администрация. Дори правителството на държавата съществува, затова, за да обслужва потребностите на гражданите на страната. Бедата е, че самите граждани не винаги разбират това.

Но в най-общ план потребителите решавайки какви стоки и услуги и на какви цени да закупят, всъщност определят правото на съществуването на организацията и влияят върху резултатите от нейната дейност. По тази причина, масата на потребителите всъщност е обект на атаки от конкуриращи се фирми и организации, в много случаи не самите потребители, а конкуренцията между организациите определят цените на определени стоки и услуги. В някои случаи се получава определени организации като например енергоразпространяващи дружества, В и К и др. да имат монополно за дадения район разпространение, при което от една страна не съществува конкуренция, което пък от друга страна принуждава потребителите да изберат да изберат техните стоки и услуги на цените, на които им се предлагат.

Среда на косвеното въздействие – факторите на косвено въздействие като правило не влияят върху функционирането на организацията толкова забележимо, колкото факторите на средата на прякото въздействие, това обаче не означава, че ръководството на организацията не трябва да отчита влиянието на подобни фактори. Проблемът е, че когато се отчита тяхното влияние обикновено се разполага с непълна информация, което затруднява възможностите за прогнозиране на разви-

тието на организацията. Към тези фактори можем да отнесем развитието на технологиите, състоянието на икономиката, социокултурни и политически фактори, взаимоотношения на местно и регионално ниво.

Технологии – особеното при тях е, че те се явяват едновременно и вътрешна променлива, и външен фактор с голямо значение. Технологичните нововъведения влияят на ефективността, което означава, че могат да влияят на скоростта с която продуктът се произвежда и продава, на скоростта на въвеждане на нови производствени мощности, на възможностите за събиране, обработка и съхранение на инфрмацията. Проблемът тук е, че подобни нововъведения много често са достатъчно скъпи и не всички фирми и организации имат необходимите финансови ресурси за закупуването им. Същевременно както вече беше подчертано, работата с новите технологии и самото въвеждане на новите технологии изисква подготвени кадри за които има недостиг на пазара на труда и съществува доста силна конкуренция за тяхното привличане.

Състояние на икономиката – състоянието на икономиката в световен мащаб влияе върху стойността на стоките и услугите и най-вече върху стойността на енергоносителите, които косвено влияят на стойността на всяка една продукция. Намиращата се в състояние на криза икономика прави значително по-трудно възможностите за прогнозиране на инфлационните процеси, влияе върху формирането на бюджетите на държавите, а оттам и върху възможностите на финансиране на едни или други дейности в дадената държава. Същевременно в условията на криза значително по-трудно става възможно организациите да теглят банкови кредити, тъй като от една страна банките втвърдяват условията за отпускането им, а от друга страна самите организации се затрудняват в изплащането на кредитите.

Социокултурни фактори – болшинството от организациите функционират в една социокултурна среда, по тази причина социокултурните фактори влияят на развитието на организацията като едни от най-значимите от тях са нагласите, ценностите, традициите, религиозните виждания и др. Всъщност едната от идеите е организациите да предусещат нагласите на потребителите и да урегулират своята дейност в съответствие с тези нагласи. За самата организация влиянието на социокултурните фактори се заключава най-вече в организацията на собствената си вътрешна уредба и урегулиране на взаимоотношенията между сътрудниците.

Политически фактори – политическата стабилност във всяка една страна е решаващ фактор за успешното функциониране на организациите. Не по-малко значими обаче са и такива аспекти на политическата обстановка като отношението на администрацията и законодателните органи към бизнеса, всички те са от значение както при привличането на чуждестранни инвеститори, така и при намиране възможностите за по-пълно усвояване на предлаганите европейски фондове. Двама от най-известните икономисти Паскал и Атос сочат, че реалността на управленските действия не е абсолютна, а тя е социално и културно детерминирана. Във всяка една култура и във всяко едно общество на хората се заплаща за изпълняване на определени колективни действия насочени към преодоляване на общ проблем, което налага да се координира, съгласува и организира съвместната дейност, като от съответната култура зависи как тези проблеми ще се възприемат и решат.

Под сложност на външната среда често разбираме и разнообразните действия на органи, институции и организации насочени към разбиване на някоя организационна структура, смазване на конкуренцията, печелене на пазарни позиции, дос-

тъп до информация и т.н. От всичко казано дотук е видно, че външната среда със своите въздействия има пряко влияние върху сигурността и стабилността на всяка една организация, тогава когато се правят преценки на състоянието и влиянието на външната среда върху организацията, те се правят преди всичко и главно от гледна точка на сигурността на съществуването на самата организация. Ако определени фактори повишават тази сигурност те се отчитат като благоприятни за организацията и същата работи за тяхното развитие и обратно, ако фактори влияят върху влошаването на тази сигурност и застрашават едни или други нейни аспекти, те се отчитат като неблагоприятни за организацията, същата се стреми по всякакъв начин да тушира или ограничи тяхното въздействие.

Литература:

1. Виханский О. С. Стратегическое управление. М., 1995.
2. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
3. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
4. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
5. Mintzberg H. Power in and around organizations. N.Y., 1983.
6. Robey P., Sales A. Designing organizations. Burr, 1996.
7. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
8. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical approach. N.Y., 1989.
9. Желев, Ст. Симулатори за обучение на специалисти за ПВО. Факултет А, ПВО и КИС“, Трудове Научна сесия 2004.

ВЪТРЕШНА СРЕДА НА ФИРМАТА И СИГУРНОСТ

Красимир М. Марков

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

INTERNAL COMPANY ENVIRONMENT AND SECURITY

Krasimir M. Markov

ABSTRACT: *The paper deals with some aspects of internal company environment in terms of security.*

KEY WORDS: *internal environment, management, security*

Вътрешната среда на фирмата е тази, която определя техническите и организационните условия на работа и е резултат от управленските решения на ръководството. Всяка фирма анализира своята вътрешна среда с цел да се изследват силните и слабите страни на дейността й. Фирмата не би могла да

използва рационално външните условия, без наличието на определен вътрешен потенциал. При това трябва да се изследват онези слаби места, които могат да застрашат сигурността на фирмата. Като подчертахме, че вътрешната среда е резултат от управленските решения на ръководството трябва да поясним, че всяко действие на фирмата е възможно само ако вътрешната среда допуска неговото осъществяване. В този смисъл вътрешната среда е източника на силите на фирмата и организацията, тъй като тя включва в себе си потенциала, който е необходим за съществуването на организацията, но в същото време може да бъде източник на проблеми, в това число проблеми на сигурността на фирмата. Анализът на вътрешната среда на фирмата се налага, защото: фирмата трябва да определи своя вътрешен потенциал на който може да разчита при постигането на целите си, от своя страна анализа на вътрешната среда позволява по-добре да се изяснят целите и задачите на фирмата, а следователно и аспектите на нейната сигурност.

Самото определение за организация съдържа по презумция идеята, че тя е вид социална общност, състояща се от групи хора, дейността на която съзнателно се контролира за достигане на общите цели. За да съществува вътрешна среда на организацията и за да съществува самата фирма, са необходими някои условия, известни от социологията, социалната психология и мениджмънта по повод на групите, а именно, че трябва да са налични поне двама души, които да се считат за част от група, те трябва да имат поне една цел, която да е обща за тях и съзнателно да работят за нейното постигане. Всяка фирма функционира във вътрешна и външна среда, като външната среда оказва влияние върху структурата, а в някои случаи и върху начините на функциониране на вътрешната среда. Авторите занимаващи се с теорията на мениджмънта се обединяват около идеята, че вътрешна среда са онези основни съставни части на фирмата, които оказват непосредствено влияние върху нейното функциониране.

Всеки уважаващ себе си мениджър трябва да има ясна информация за състоянието на вътрешната среда на фирмата, за да може да определи нейните вътрешни възможности на които може да разчита в условията на конкурентна борба за постигане на поставените цели. Когато се анализира вътрешната среда не бива да се забравя, че наред с организацията на производството или услугите във фирмата, то тя трябва да осигури нормални условия за труд на своите служители и да създаде определени социални условия за тяхното нормално съществуване като хора.

Анализът на външната и вътрешната среда би трябвало да върви паралелно дотолкова, доколкото оценката на външните условия като благоприятни или неблагоприятни за работата на фирмата може да бъде направена само в резултат на анализ на силните и слабите страни на вътрешната среда на организацията. Това налага анализът на вътрешната среда да се провежда периодично. Специалистите по мениджмънт сочита няколко причини, които налагат провеждането на анализ на вътрешната среда на организацията:

- Намиране на най-добрите начини за постигане на поставените цели;
- отчитане на реалните фактори, на които да се основава действието на организацията;
- разкриване на причините, поради които са извършени определени действия в организацията.

При анализа на вътрешните фактори обикновено се разглежда следното (Кэмпбел Д., Стонхаус Д., Хьюстон Б. Стратегический менеджмент:Учебник./М. 2006.):

1. Състояние на пазарите и ниво на обслужването. Тук е необходимо да се разбере кои стоки и услуги отговарят на изискванията на пазара и върху кои да се концентрираме. Тези стоки и услуги се оценяват по следните параметри:

- явяват се подходящи за бързия ръст на фирмата в предела на възможните инвестиции;
- изпълняват се добре, но условията налагат намаляване на производството;
- изискват по-големи разходи, а се получават по-малки приходи.

2. Финансови средства. Тук се оценя следното:

- как са разпределени инвестициите;
- какви средства са вложени в производство с голям риск;
- доколко ефективно се използват текущите финансови ресурси.

3. Оперативна дейност и производителност. Тук трябва да се изясни доколко е ефективна организацията при предоставянето на своите услуги по отношение на време, точност, стойност, разходи за труд.

4. Технология. Да се оцени възможността за понижаване стойността на производството в резултат на инвестиране в нови технологии.

5. Управление и персонал. Да се оцени как се разпределят усилията по отношение на постигането на глобалните цели и че е налице управление и персонал с достатъчна квалификация и опит, за да могат да се постигнат поставените задачи.

6. Организация. Да се оцени доколко организационната структура помага или пречи на изпълнението на задачите и как се осигуряват връзките между отделните звена.

7. Информация. Да се оцени доколко е полезна съществуващата информация за изпълнението на задачите, стига ли тя навреме до хората на които е необходима, има ли влошаване на дейността, поради липса или закъснялост на информацията.

8. Система на обслужване на клиентите. Да се оцени:

- колко време се отделя;
- колко ни струва;
- каква е възможността за усъвършенстването й.

Анализът на вътрешната среда не би могъл да се осъществи без оценката на вътрешните променливи, в повечето случаи фирмите представляват открити системи състоящи се от много взаимозависими части. Кои са най-съществените вътрешни променливи на фирмата. Обикновено към тях се отнасят: целите, структурата, задачите, технологиите и хората (по Минцберг, Г., Альстренд Б., Лэмпел Дж. Школы стратегий. СПб. 2005):

1. Целта като правило е желания резултат, конкретно крайно състояние, което се стремят да постигнат група хора работещи заедно. По правило целите се разработват от ръководството, което ги свежда до знанието на сътрудниците. Това е много важен процес, тъй като дава възможност на персонала да знае към какво трябва да се стреми. Всяка фирма има цели, които се подразделят на стратегическо, оперативно и тактическо ниво в зависимост от тяхната дългосрочност. Другаде ги наричат дългосрочно, средносрочни и краткосрочни цели. Освен тях обект на

внимание на мениджмънта на организацията трябва да бъдат и целите на отделните структурни звена на организацията.

2. Структура на организацията. Най-общо казано всяка фирма се състои от няколко нива на управление и различни подразделения свързани помежду си. Тези подразделения могат да бъдат отнесени към една или друга функционална област, обикновено свързана с дейността на фирмата като цяло напр.: маркетинг, производство, финанси, планиране и т.н. При разглеждане на проблемите за структурата на организацията обикновено се стремим да си отговорим на два въпроса, свързани с разделението на труда и контрола.

Разделението на труда не би трябвало да върви по принципа за използването за определена дейност на този, който е свободен в момента, а за използването на този, който еспециалист в тази дейност. Съществува хоризонтално и вертикално разделение на труда. При хоризонталното – разделението на труда се осъществява по специализации, например: мениджър по продажбите, главен инженер, счетоводител и т.н. При вертикалното разделение на труда търсим възможността за координация при изпълнението на задачите, то всъщност е управленската йерархия и по същество дава формирането на управленските нива в организацията.

Броят на хората подчинени на един мениджър се нарича сфера на контрола. Във фирмата всеки ръководител си има своя сфера на контрол.

3. Задачи. Това е възложената работа, която трябва да бъде изпълнена по установен начин в установения срок. Всяка дейност на фирмата включва в себе си редица задачи, които е необходимо да бъдат изпълнени за постигане на целите на организацията. Обикновено задачите се разделят на три категории:

- задачи за работата с хората;
- задачи за работа с машини, суровини, инструменти и.н.;
- задачи за работата с информация.

В съвременни условия в резултат на въвеждането на информационните технологии и иновациите, задачите стават все по-детайлни и специализирани. От своя страна всяка задача може да бъде твърде сложна.

4. Технологии. Това е принципа, реда по който се осъществява определен процес в организацията за оптимално използване на различните ресурси (трудови, материални, финансови, времеви). В този смисъл технологията представлява начина, по който можем да осъществим някакво преобразование. Обикновено се разглеждат две класификации на технологиите:

Класификация на Удуърт:

- единично, малко серийно или индивидуално производство;
- масово или голямо серийно производство;
- непрекъснато производство.

Класификация на Томпсън:

- технологии характеризиращи се със серии взаимосвързани задачи, които се изпълняват последователно;
- посреднически технологии, характеризиращи се със срещи на групи хора;
- интензивни технологии, характеризиращи се с използването на специални способи за изменение на състоянието на определен процес.

5. Хората. Те са централното звено във сяка една система на управление, съществуват три аспекта на тази променлива във фирмите:

- поведението на индивидите;

- поведението на хората в групата;
- поведението на ръководителя.

Разбирането и управлението на човешкия фактор във фирмата е най-сложния процес от цялостната система на управление и зависи от много фактори.

- способностите на хората. Това е първото което се вижда от ръководителя, когато оценява персонала на една организация. Тази характеристика обаче и най-лесно подлежи на промяна чрез обучение на персонала
- потребностите. Тук трябва да се отчитат не само материалните, но и психологическите потребности от уважение, признание т.н.
- възприятие. Под него разбираме как всъщност хората реагират на събитията в обкръжаващата ги среда. Познаването на този аспект дава възможност да се разработат различните стимули за персонала на организацията.
- ценности. Това са общите убеждения на хората кое е добро и кое е лошо. Общите ценности помагат на ръководителя да обедини персонала за достигане целите на фирмата;
- влияние на средата. Отчитане по какъв начин различните ситуации във фирмата влияят върху хората.

Подобни фактори могат да се изброяват още, но би трябвало да се отчита съществуването на формалните и неформалните групи в организацията и състоянието на лидерството.

Всички вътрешни променливи, които изброихме се явяват ситуационни фактори, които могат да бъдат конторлирани и регулирани, те са взаимосвързани и по своята съвкупнрост представляват социотехническа подсистема на вътрешната среда на фирмата. Изменението на всяка една от тях в определена степен влияе и за промяната на останалите. Мениджърът, управленецът трябва да умее да ги анализира в съвкупност без да изпуска един или друг аспект на вътрешната среда, за да може да вземе вярно решение и по този начин да повиши сигурността на фирмата. Умението да изясни и проанализира елементите на организацията е всъщност залог за успеха и сигурността на фирмата.

Литература:

1. Виханский О. С. Стратегическое управление. М., 1995.
2. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
3. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
4. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
5. Mintzberg H. Power in and around organizations. N.Y., 1983.
6. Robey P., Sales A. Designing organizations. Burr, 1996.
7. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
8. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical approach. N.Y., 1989.
9. Желев, Ст. и др. Computer vision - simulation programs for a video image processing. 7 international conference, Liapaja affiliate, Latvia, May 2010.

РОЛЯТА НА ОРГАНИЗАЦИЯТА И УПРАВЛЕНИЕТО НА ОПЕРАТИВНОТО ПРОТИВОДЕЙСТВИЕ ЗА РАЗКРИВАНЕ И НЕУТРАЛИЗИРАНЕ НА ПОСЕГАТЕЛСТВА СРЕЩУ ФИРМЕНАТА СИГУРНОСТ

Христо Атанасов Христов

Университет по библиотекознание и информационни технологии – София,
hristov63@abv.bg

CHARACTERISTICS IN ORGANIZATION AND MANAGEMENT OF OPERATIONAL REACTION AGAINST ENCROACHMENT UPON COMPANY SAFETY

Hristo A. Hristov

***Abstract*:** *In the new-growing global market the contemporary global environment of company safety is defined by high complexity and chaotic dynamics of changes that are the reason of the collapse in stability and firmness in society and especially business life.*

According to safety of social structures like corporations, companies, firms the new challenges and threats are hardly predicted and appear in complex interdependence so that traditional or other instruments become useless in struggling for company safety. Transformation in security policy of social organizations is necessary in order to create optimal conditions for mission accomplishment and to guarantee sustainable development of society. Counter-reaction management against company security encroachment is a contemporary approach which will allow complex neutralization of various and mutually-dependent sources of threats and also will prevent the negative impact of their effect on social organizations. The discussed security approach will contribute to adequate prioritization of tasks and goals which should be taken in security organizations, along with planned use of their limited resources which will provide the right conditions for effective realization of strategy management.

***Key words*:** *management encroachment, information security, national security, information, security policy, social organizations.*

Развитите икономически страни през XXI век се характеризират с глобализираща се икономика. Във формиралия се глобален пазар се води битка за световни ресурси и локални пазари под формата на икономическа война. С навлизането на XXI век икономиките на напредналите държави навлизат в ерата на интелектуалния мениджмънт, кореспондиращ пряко с епохата на разузнаването. Вземането на решение е подвластно на достиженията на ума, идеите и нововъведенията, а не на технологично ниво. Не случайно Ал. Тофлър в „Революционното богатство" определя „Знанието" за един от дълбинните фактори на днешната глобална революция. По тази причина нараства броя на мениджърите приемащи частната разузнавателна дейност, като задължителен елемент от управлението на фирмите, характеризираща се с изключителна динамика.

В тази връзка противодействието на заплахи и посегателства породени от дейността на частното разузнаване осъществявано от чужди сили е задължителен елемент от управлението на фирмата, то е следствие революцията на глобалната икономика. В съвременните конкурентни условия ефективно противодействие на корпоративното разузнаване може да се гарантира само със собствена специализирана структура

за сигурност. Във всички развити икономики собствените органи за сигурност на социалните организации са станали задължително условие за просперитет и запазване позициите на пазара. Понятието фирмена сигурност е комплексно и покрива няколко различни направления на сигурността. Един от елементите в дейността на фирмените служби за сигурност е оперативното противодействие на посегателства и заплахи. /специфичната дейност на органите на фирмената сигурност, която има за основна цел да разкрива, неутрализира и подпомага откритото пресичане на посегателства, чрез прилагане на специфични средства и методи/

Във формиралия се нов световен пазар, съвременната глобална среда за сигурност се характеризира с висока сложност и хаотична динамика на промените, нарушаваща стабилността и устойчивостта на развитието на обществото.

Новите предизвикателства и заплахи за сигурността на социалните организации /търговски дружества, корпорации, компании, фирми и др./ са с висока степен на неопределеност, проявяват се в сложна взаимозависимост и са трудно предвидими, което определя невъзможността за ефективно противодействие с традиционни сили и средства.

Необходимо е извършване на трансформация в политиката за сигурност на социалните организации, с цел създаване на благоприятни условия за изпълнение на мисията им и гарантиране устойчивото развитие на обществото. Трансформацията в политиката, стратегиите и подходите е свързана с коренна промяна от реагиране на промените в средата за сигурност към формиране на способности за гарантиране на сигурността, основани на целесъобразно проактивно противодействие на съвременните заплахи и посегателства.

Управлението на противодействието на посегателства срещу фирмената сигурност е съвременен подход, чието приложение в сферата на сигурността позволява осъществяването на комплексно неутрализиране на многообразните и взаимозависими източници на заплаха и надеждно предотвратяване на негативното им въздействие спрямо социалните организации. Разглежданият подход в сферата на сигурността позволява извършването на адекватно приоритизиране на целите и задачите на социалната организация, съчетано с планирано използване на ограничените им ресурси, позволяващо създаване на условия за реализация на ефективно стратегическо ръководство.

Във демократичните общества с развита пазарна икономика естествен процес е разширяването на недържавната система за защита на сигурността. Държавата отстъпва част от своите правомощия и функции на собственика, които е най-заинтересован да се гарантира неговия живот, имущество и интереси. В тази връзка фирмените служби за сигурност стават един от елементите на системата за национална сигурност.

Възприето е схващането, че фирмената сигурност в условията на пазарна икономика е част от националната сигурност и съответно защитата на фирмената сигурност е тясно свързана с националната сигурност.

В процеса на утвърждаване като компонент на националната система за сигурност, социалната организация е обект на въздействие на многообразни и сложни съвременни заплахи и посегателства: – шпионаж, -нерегламентиран достъп до чувствителна информация, -фирмената тайна, -международен тероризъм; -корупция; -деструктивни въздействия върху комуникационните и информационни системи и мрежи; -организирана престъпност, -изнудване, -подкупи, кражби в

корпоративния сектор и др. Всички тези дейности са свързани с неетични и незаконни действия, които не следва да бъдат подценявани и пренебрегвани.

Държавните служби за сигурност носят историята, традицията и опита на контраразузнаването, в тази връзка фирмените служби за сигурност в Република България са исторически по млади. В тази връзка е целесъобразно разработваните решения, касаещи проблемите за оперативното противодействие на посегателства срещу фирмената сигурност да са на база теоретичния и практически опит на държавното контраразузнаване, изхождайки от идеята, че те са общовалидни за всяка съвременна контраразузнавателна служба на социалната организация. Контраразузнавателните служби за сигурност в света използват еднакви по своята същност сили, средства, методи и форми на дейност.

В условията на глобализация обстоятелствата все по-често ще принуждават държавата да поема ангажимент за защита на частните икономически интереси. При свободна пазарна икономика тези интереси са съществена част от националната сигурност и тяхната защита става и задача на държавата, а не само на частния собственик. Тази защита ефективно не може да се осъществява само с участие на националните служби за сигурност, работещи за общите интереси на всички компании в страната.

Към момента държавата не оценява голямото значение на сигурността на частните предприятия за своята собствена икономическа сигурност. В условията на глобализираща се пазарна среда конкуренцията се изостря и често има характеристиките на икономическа война дори и между партньорите от ЕС и САЩ. Преобладаващото участие на частния сектор в държавната икономика изисква да се гарантира неговата сигурност, за постигне и гарантиране сигурността на държавната икономика, като цяло. Към момента постановката на държавната власт е, че сигурността на частните фирми си е тяхна работа и тя се дистанцира от съществуващите проблеми в противодействието на посегателства и заплахи срещу фирмената сигурност. По тази причина към момента не са приети всички необходими закони с които се регламентира дейността на частните служби за сигурност и криминализира деянието икономически шпионаж. Успоредно с това фирмите в сферата на сигурността подготвят и разполагат с все по качествени кадри, отделят все по вече средства и се оборудват все по модерно. Като пример Йордан Начев в труда си „Конкурентно разузнаване" посочва съществуването на частна компания с личен състав на службата за сигурност над 10 000 човека., което е по вече от взетите заедно кадрови разузнавачи и контраразузнавачи на държави с мащабите на България.

Анализа на гореизложеното налага приемане на законодателни промени в областта на сигурността благоприятстващи сътрудничеството на държавния и частния сектор, насочени към ефективна защита на националната сигурност в частност сигурността на отделната организация.

Най-голямата заплаха за всяка организация, е изправянето и пред перспективата от изчезване. Компании, както и чужди правителства, сега се състезават един срещу друг за икономическо превъзходство и технологии. Заплахата срещу бизнеса на фирмата и лична информация е сериозна. Дори по време на Студената война, икономическата конкуренция е съществувала. Сега конкуренция между държавите се движи от политико-военно ниво на икономическо и технологично ниво. В икономиката, ние сме конкуренти, а не, съюзници", каза Пиер Марион.

Посегателствата на фирмената сигурност винаги са били част от оперативната среда на организациите. Редовни заглавия за промишлен шпионаж, бизнес разузнаване и кражба на информация показват, че адекватната защита на чувствителна информация за социалната организация, се превръща в световен проблем. Компаниите все по ясно разбират значението на запазването на своите вътрешни секрети и последиците от несанкциониран достъп на конкурентите, терористични организации и чужди разузнавателни сили до тях.

Това е нещо, от което нито един собственик и нито една голяма мултинационална компания не може да избяга. Известно е ,че събитията са свързани помежду си и по този начин средата за сигурност на организацията е в постоянен поток. Международни, национални, регионални събития имат пряко влияние върху това как ще функционира и развива организацията. Показателен пример в това отношение е световната икономическа криза. Несигурността за бъдещето на организацията пряко кореспондира с изпреварващото определяне и предвиждане на възможни заплахи и посегателства.

За управлението на противодействието на заплахите и посегателствата в организациите, са отговорни корпоративните лидери на организацията. За съжаление, много организации са приравнили противодействието само с физическата сигурност, а не с други аспекти в рамките на тяхната оперативна среда и игнорирайки оперативното противодействие на посегателства и заплахи.

[Джон Нолан автор на разузнавателен цикъл на групата „Феникс"] предупреждава, че традиционното опазване на собствеността на компанията от крадци и незаконни действия по отношение на фирмените секрети вече не действа ефективно. Причината е в промяната на интензивността и естеството на заплахите и посегателствата. Държавата целенасочено прави разграничение между борбата с престъпността и противодействието на чужда разузнавателна дейност. Средствата и методите съществено се различават в двата случая и това трябва да се отчита при организиране сигурността и на частния сектор.

Ако се приеме това за изходна база, то естествено е компанията да развива и усъвършенства непрекъснато собствена контраразузнавателна дейност, като елемент на противодействието на разузнаването на чужди сили.

В подкрепа на тези разсъждения и с цел да се гарантира комплексно сигурността на фирмата, е необходимо защитата на фирмената сигурност да се организира в два цикъла контраразузнавателен и разузнавателен. Контраразузнавателният цикъл разглежда организацията и управлението на противодействието срещу посегателства на фирмената сигурност. Контраразузнавателна дейност отговаря за оптималната информационна обезпеченост за потенциални заплахи на средата за сигурност и недопускане посегателства на фирмената сигурност. По този начин частната контраразузнавателна дейност осигурява поглед извън границите на корпорацията. Компаниите, които прилагат ефективна контраразузнавателна дейност, виждат извън себе си.

Частната контраразузнавателна дейност може да се дефинира като „Силно специализиран, непрекъснат процес за информиране на компанията за потенциални посегателства срещу фирмената сигурност и организиране на противодействие и неутрализиране на заплахи и посегателства към компанията.

Това е възможно да се постигне чрез управление на оперативното противодействие, ако се извършва правилно изучаване на средата за сигурност на фирмата и целенасочено се прилагат видовете контраразузнавателна дейност. Фирми с добра

стратегия на противодействието с включена функция за контраразузнаването, имат предимство пред конкурентите, поради възможността за своевременно предвиждане на заплахите и промените в оперативната среда. Стратегията за противодействие на заплахи и посегателства във фирмата може да предостави рамка, за да се ограничи възможността за реализиране на тези посегателства и настъпване на вредни последици за фирмата.

В условията на свободна пазарна икономика сигурността на частните структури става съществен параметър от националната сигурност и това трябва ясно да бъде осъзнато от всяко държавно ръководство. Когато в дадено предприятие има държавно участие би следвало между собствениците да се осъществи ползотворно сътрудничество. Само по този начин може да се гарантира неговата сигурност и просперите в условията на непрекъснато нарастваща конкуренция.

Разликата между частната контраразузнавателна дейност и държавното контраразузнавене не трябва да се търси в методите и средствата, които са известни, а от начина и ограничителните условия за тяхното ползване. Основното различие идва от ограниченията, които съществуващото местно законосателство поставя пред частните структури за сигурност. Забранените действия в етапа на придобиване на информация не влизат в арсенала на професионалиста по фирмена сигурност. Дейността на структурите за фирмена сигурност трябва да не нарушава закона, да се придържа към етичните норми в бизнес практиката и да остане в рамките на откритата конкурентна борба. Това се прави за да не попадне под ударите на закона собствената компания.

Субект на посегателства срещу фирмената сигурност може да бъде държава, всякаква организационна структура и отделна личност.

Повишаване на сигурността на организацията чрез процес на планиране, събиране и анализ на информация за средата за сигурност на фирмата е сравнително евтин начин да се сведат до минимум вероятността от осъществяване на посегателства срещу фирмата. На тази база е необходимо фирмите да разработват корпоративна стратегия/концепция за противодействие на заплахи и посегателства срещу фирмената сигурност и обучение за по-нататъшно реализиране на тази цел. Една добра стратегия може да служи като инструмент за оценка и намаляване на заплахите, без да се компрометира доброто управление**.**

Обобщавайки изложеното по-горе, основателно може да се попита: "Подготвени ли са и готови нашите фирми, за защита на тяхната информация срещу професионални и сложни атаки от местни и чуждестранни сили, както и на конкурентите".

Противодействието на посегателства и защита на бизнес информацията, са корпоративни въпроси и следва да са едни от основните проблеми на днешните бизнес лидери. Приемането на корпоративна стратегия за противодействие и защитата на тайните на корпорацията следва да са ангажимент на нейното ръководство.

Според насоките, на [Стив Уайтхед .] публикувани в доклада "King II, отговорността за управлението на всички форми на заплаха сега живее с корпоративни лидери и директори. Различни хора и функции в компанията могат да им съдействат, но крайната отговорност спира на корпоративни лидери и директори. Те ще трябва също да се ангажират със задачата по приемането на корпоративна стратегия с противодействието и защитата на тайните на корпорацията.

Системата за фирмена сигурност неизбежно има отношение към защита на чувствителната информация във фирмата. Действителният подход към проблема за разработване на мерките по сигурността следва да се изгражда на предположението за

най остри действия от страна на противника/конкурента, и как те ще се отразят на собствената фирма. Ако не се действа срещу конкурента, това не означава, че конкурентът не прави същото срещу нас. Затова опазването на придобитата във фирмата чувствителната информация е съществен проблем.

Икономическата самостоятелност при пазарната икономика заставя частните компании изцяло да отговарят за фирмената сигурност. При съвременните пазарни характеристики политиката на фирмена сигурност трябва да се разглежда, като система от възгледи, решения и действия в областта на сигурността, които създават благоприятни условия за просперитета на бизнеса.

Фирмената сигурност се постига, чрез създаване на собствено подразделение за сигурност, което насочва дейността си в две посоки: –опазване на вътрешно фирмени секрети и придобиване на информация за средата за сигурност, в която фирмата развива своя бизнес. Този подход е целесъобразен за големите транс национални компании. При тях собствената структура за сигурност работи в две направления – разузнаване и контраразузнаване. Процесът по осъществяване на контраразузнавателна дейност в своята цялост може да се нарече контрарзузнавателен цикъл,състоящ се от няколко етапа с различен характер на дейност. Ключов от тези етапи е оперативното противодействие на заплахи и посегателства срещу фирмената сигурност.

Ползата от използването на оперативното противодействие на заплахи и посегателства срещу фирмената сигурност в съвременния бизнес проличава най добре в примерите, където неговото игнориране става причина за големи загуби и обратно-как добре планираното му използване може да даде тласък на развитието на частната структура. Щетите на фирмите, причинени от деиствия на разузнаването на преките им конкуренти са огромни.

Поради изострянето на конкурентното съществуване темата за наличие на собствената структура за оперативното противодействие на заплахи и посегателства срещу фирмената сигурност предизвиква все по малко отхвърляне, неразбиране и опасение. Тази дейност става обичайна в сферата на собствената сигурност на фирмата. Основен неин клиент е частният бизнес, които обръща все по голямо внимание на възможностите и все по често прибягва до услугите на специализираното комплексно звено по осъществяване на оперативното противодействие на заплахи и посегателства срещу фирмената сигурност.

Мениджърите знаят, че всяка преуспяваща фирма не може да продължи да съществува повечо от седмица, ако 20% от нейната търговска вътрешно фирмена информация стане известна на преките и конкуренти.

Заключение:

Управлението на оперативното противодействие е комплексен подход, който може успешно да бъде приложен в сферата на фирмената сигурност, за надеждно противодействие на съвременните глобални заплахи и посегателства, за изграждане на гъвкава динамична система за сигурност, гарантираща изпълнението на мисията на социалната организация.

Моделът за организация и управление на оперативното противодействие на посегателства в сферата на фирмената сигурност /специфичната дейност на органите на фирмената сигурност, която има за основна цел да разкрива, неутрализира и подпомага откритото пресичане на посегателства, чрез прилагане на специфични средства и методи/ си поставя за цел изследване на концепция на контраразузнавателния цикъл -/КРЦ/ на оперативното противодействие срещу посегателства на фирмената

сигурност. Концепцията обединява и определя пътя за изграждане и реализиране на КРЦ с цел развитие на фирмата /защита на секрети, неутрализиране на заплахи, понижаване на риска и предотвратяване на посегателства/, при ясното разграничаване на контраразузнавтеланата и разузнавателна проблематика на сигурността.

Ефективното управление на противодействието на посегателства срещу фирмената сигурност. може да бъде реализирано само при комплексни, синхронизирани действия на органите за фирмената сигурност, съответните органи на изпълнителната, законодателната и съдебна власти, като основна тежест и отговорност за реално противодействие имат органите за сигурност на съответната социална организация.

Приложният характер на изследването се определя от конкретната специфика на социалната организация, разглеждана, като една от основните подсистеми на системата за национална сигурност на Р България.

Литература:

1. Бончо Асенов, Александър Кипров -„Теория на контраразузнането" – Издателска къща „Труд" – София 2000.
2. Проф. д.н. инж. Йордан Начев - „Конкурентно разузнаване", -Сиела –Софт ЕНД Пъблишинг.
3. Тодор Бояджиев, „Шпионажът като занаят" –Издателство „Захарий Стоянов" – София 2002.
4. Алвин и Хайди Тофлър. „Революционното богатство".
5. Марин Стоянов - експерт по фирмена сигурност - „Управление на фирмената сигурност задача с много неизвестни" Ангел Иванов - Ръководител бизнес развитие, Лирекс БГ - Ангел Деспотов –консултант по Фирмената сигурност, Академик проф. д-р Минко Ст. Памукчиев – „Модерните измерения на икономическия шпионаж „ -лекция

9. Румен Дончев –експерт по „ *Физическа сигурност на информационните системи и ресурси"*

10. д-р Невин Фети експерт по национална сигурност –лекция генерал Людмил Маринчевски пред Твоят Бизнес: -„ Етиката е критерий за успешен бизнес" - доцент, доктор по политология Тодор Кобуров –статия „Национална сигурност" д-р инж. Милен Иванов –експерт по охранителна дейност доц. Николай Цапрев –експерт по фирмена сигурност.

15. Майкъл Podszywalow „Съвместимост срещу сигурността на многобройните аспекти на корпоративен шпионаж" Януари 2012 г.

16. Бернар Odendaal, CBIA „ Конкурентно разузнаване - ключът към корпоративното управление на риска „- 1 юли 2003 г.

17. *Мариан Lawlor,* „Корпоративно контраразузнаване" - Публикувано от AFCEA International, Copyright © 2007 AFCEA International.

18. Стив Уайтхед –„Корпоративно контраразузнаване" - 1 юли 2003 г.

MECHANISMS FOR PREVENTION OF CORRUPTION IN BULGARIA

Yordan G. Deliverski

Address for Correspondence:
Jordan Deliversky
deliversky@abv.bg
mobile: +359 888 85 60 73

PhD student at State University of Library Studies and Information Technologies

Abstract: *Corruption exists as major problem in Bulgarian society and it is realized as such by most representatives of the political elite. The fight against corruption must be an organized and long-term process of applying of purpose-defined measures for prevention and suppression of corruption.*

Key Words: *Corruption, Strategy, Legislation, Prevention*

Corruption exists as major problem in Bulgarian society and it is realized as such by most representatives of the political elite. This is an extremely important phenomenon in social consciousness, because it is a main precondition for its determination. Corruption is absolutely considered as threat to national security and that is why its manifestation has to be imitated with every possible legal means.

Combating corruption is part of the effort for creation of public institutions and for the strengthening role of civil society. The results achieved in the prevention of corruption practices is turned into important measure for success in period of translation and for introduction of modern standards for transparency and democratic control.

According to article 8 of the Constitution of the Republic of Bulgaria the power of the State shall be divided between legislative, executive and judicial. The achievement of certain result in combating corruption is a challenge facing all three powers in the State.

The Legislature

In combating corruption there is the issue on necessarily of strong commitment of the National Assembly to the problems of combating corruption through implementation of its main function: the adoption of legislation, parliamentary control and the formation of certain state institutions. Parliamentary committees are formed, directly related to creation of legislation for combating corruption:

- 38th National Assembly (1997-2001) – Parliamentary committee for combating crime and corruption ;
- 39th National Assembly (2001-2005) – Commission on combating corruption;
- 40th National Assembly (2005-2009) - Commission on combating corruption;
- 41st National Assembly (2009-2013) - Anti-corruption, conflict of interests and parliamentary ethics committee

Legislative acts and amendments in active legislation

- National Assembly passed amendments to Law on political parties to ensure greater transparency and control over the financing of political parties;
- There has been introduced a requirement members of governing and supervising bodies of political parties, as well as political parties representatives, to declare their

assets, income and expenses in the country and abroad under the Law on Disclosing the Property of Persons in Senior Government Positions[1].

- National Assembly passed Commercial Register Act, as of July 1, 2007, aiming to limit corruption pressure on business registration;
- There have been passed new procedure codes – Administrative procedure code, Criminal procedure code, Code of civil procedure, in order to expedite justice and to increase its efficiency, as well as to reduce corruption in society and the judicial system.
- It has been passed Law on Prevention and Disclosure of Conflict of Interests, effective of January 1, 2009.

The executive authority

According to Decision No 671 of 01.10.2001 of Council of Ministers, it has been adopted National strategy for combating corruption. The need of developing a National strategy for combating corruption relays on seriousness of this problem, as well as on the need of putting efforts to address it long-term frame of political and social-economic development of the country. By adopting this Strategy are created the foundations of one the first definite measures in combating corruption.

The Strategy focuses on:

- Creation of common institutional and legal environment for curbing corruption;
- Anti-corruption measures in judiciary system and criminal legislation;
- Curbing corruption in the economy field.

On January 12, 2006 Council of Ministers adopts Second Strategy for transparent governance and prevention and combating corruption for the time period 2006-2008. The Strategy defines priority areas for prevention and combating corruption, including high-level corruption through introducing worldwide practices in this field:

- To ensure transparent management and accountability in public administration activity;
- Regulation on clear and effective rules on interaction between citizens and administration personnel.
- Increase the transparency in decision making process at management level;
- Promoting values such as honesty and ethics in public relations;
- Prevention of corruption;
- Increase the public confidence in institutions, strengthening civil control.

The strategy aims to ensure conditions of transparency of financial and property status of civil servants at all levels, including senior officials. In order to distinguish a democratic political parties system and transparent funding of political parties, measures has been taken to distinguish the state of public-and private-party domain and to limit possibilities for party influence in the management of state property for the benefit of parties close to companies and nonprofit organizations and the appointment and dismissal of civil servants in managerial positions in the administration on different criteria from the requirements of professionalism and loyalty.

Coordinator of the implementation of activities under the Strategy for transparent governance is the Committee on prevention and countering of corruption[2]. Chairman of the Committee is the Minister of Interior, while and deputies are the Minister of justice

[1] Article 30, par.3 Law of Political parties

[2] The Committee on prevention and counteracting corruption was established under Decision No 61 of the council of Ministers on 02.02.2006.

and the Minister of public administration. After amendments in 2009[3], the Committee includes: Chairman – the Deputy Prime – Minister and Minister of interior. Deputy Chairmen is the Deputy Prime – Minister and Minister of finance. Members of the Committee are the Ministers of: Justice, Education and Science, Health, Economy, Energy and Tourism, Regional Development and Public Works. Members are also the Chairman of the State Agency "National Security", the Secretary of the Security Council at the Council of Ministers and the Secretary of the Management Council of EU funds in the Council of Ministers.

The Committee fulfills two main functions – creation of state anticorruption policy and control on implementation of the strategy and monitoring basic parameters of the dynamics of corruption on national level.

The Committee creates drafts of decisions, sets the priorities of the government's anti-corruption activities on annual bases and proposes the most effective approaches to combat and prevent corruption in various prerogative areas such as:

- Main priority is the prevention and combating of corruption at the highest levels of government through introduction of mechanisms for accountability and control of senior government positions, ensuring accountability and transparency of political party financing, as well as regulating lobbying activity.
- Another main point in the work of the Committee are the anti-corruption measures in economy field; promoting transparent management and control of public revenues and expenditures of central and local levels (including funding of the European Union) in public procurement, concessions, tax and customs services, public-private partnership between the State and the Business, mechanisms for transparency in the private sector, etc.
- The co-operation with specialized anti-corruption committees in the National Assembly and the Supreme Judicial Council are also set as a priority, in order to improve dialogues with legislative and judicial systems in conducting criminal policy in fighting corruption.
- Of particular importance is the institutionalization of civilian control. Intensive cooperation with civil society in assessing trends in the evolution of corrupt practices is important for the effectiveness of ongoing anti-corruption policies.

In order to improve coordination and interaction between various institutions and organizations working in the field of anticorruption, and other specialized anti-corruption committees at the National Assembly and the Supreme Judicial Council, it is being relied on Council for Coordination of anti-corruption commissions, established in April 2006.

The effect of creating Coordinating Board to conduct a single anti-corruption policy between the three authorities is now observed. This is an implementation of government policy consistently pursued on synergy between institutions in the field of security, for combating corruption.

In the administration of the Council of Ministers it has been created a Main Inspectorate[4]. It is directly subordinate to the Prime Minister and serves as Secretariat of the Committee on the Anti-Corruption to Council of Ministers. The main focus on the func-

[3] Decision No 145 of Council of Ministers of 12.03.2009 amended and supplemented the structure and functions of the Committee. Decision № 760 of 25/09/2009 Council of Ministers have amended the two Decisions

[4] Article 46-a Law on Administration, State Gazette No. 24 of 2006

tion of the Inspectorate is to examine indications of conflict of interest and other acts of misconduct and corruption signals of executive authorities and civil servants in management positions.

To all ministries and government agencies there were established inspectorates, but insufficiency in the legislative framework does not regulate their activities in detail.

By Protocol № 45.32, on 18.11.2009 Council of Ministers has adopted an Integrated Strategy of prevention and combating corruption and organized crime.

The aim of this Strategy is to create a trust of Bulgarian citizens toward rule of law, as well as of European partners and foreign investitures towards Bulgaria through targeted, systematic, consistent, professional and decisive actions in all spheres of governance for:

- prevention of corrupt practices at the highest levels of government and the disruption of connectivity between organized crime, political parties and authorities;
- Achievement of visible results in combating widespread corruption, which penalize citizens, businesses and destroys the state government system;
- Maximum limitation of organized crime activity, effective criminal prosecution and forfeiture of its proceeds.
- Establishing Bulgaria as a reliable partner in the implementation of policies on freedom, security and justice with its contribution to protecting the financial interests of the European Union.
- Outcome of moral and behavioral crisis in the country, confidence in the values of integrity, morality and solidarity and promotion of sustainable value system in society with attitudes towards intolerance of corruption and crime.

Council of Ministers Decree No 158 of July 29, 2010 creates a Centre for Prevention and Combating Corruption and Organized Crime to Council of Ministers. On November 24, 2010 Rules of Procedure of the Center for Prevention and Combating Corruption and Organized Crime have been adopted.

The Center's activity is associated with analysis, planning and development of measures and comprehensive solutions to prevent the possibility of creating corruption and anti-corruption in general. The Center assists State and local governments in developing policies to prevent these phenomenon and to improve cooperation and coordination between public institutions, civil society, media and business. It provides a comprehensive model for combating corruption and organized crime approved German standards and expert elaboration[5].

The Director of the Centre is determined by the Council of Ministers, and is being appointed by Prime Minister's order. The activity of this structure is driven by methodological Advisory Board with representatives of legislative, executive authority and judiciary system. Chairman of the Board is the Deputy Prime - Minister and Minister of interior.

Judicial system

According to the Judiciary system act, promulgated, SG No. 64/7.08.2007, The Supreme Judicial Council shall be a permanent body representing the Judiciary and securing its independence. It shall set the composition and work organization of the Judiciary and shall manage its business without interfering with the independence of the bodies thereof.

[5] Statute of the Centre for Prevention and Combating Corruption and Organized Crime, Council of Ministers.

The Commission for Professional Ethics and Prevention of Corruption in the judicial system is a permanent subsidiary body of the Supreme Judicial Council. It consists of ten members of the Supreme Judicial Council, appointed based on its decision.

This Commission holds regular meetings every week. If necessary it may meet more than once. It is convened by its chairman or at the request of one third of its members.

The purpose and activities of the Commission are aimed at preventing and combating corruption in the judiciary system. Ethics The Commission for Professional Ethics and Prevention of Corruption in the judiciary has the following authorities:

- To conduct studies on individual signals and complains, to inform the competent authorities and the Supreme Judicial Council for the submitted results;
- To analyze information on the existence of instances of corruption in the judiciary bodies;
- To develop and propose for approval by the Supreme Judicial Council practical measures for prevention and combating corruption in judiciary system;
- To sign agreements for joint activities and exchange information with the Commission on Combating Corruption of the National Assembly.

Annually the Commission for Professional Ethics and Prevention of Corruption in the judiciary system presents a report on its activity.

Inspectorate at the Supreme Cassation Prosecution Unit became a separate sector in the administrative department, but directly appointed to the Attorney General. The Inspectorate has the power to investigate all complaints and reports, even anonymous ones, as well as those signals for corruption filed in the prosecution office, the Ministry of interior and the prison facilities. It also investigates signals against judges and prosecutors.

There is insufficient social awareness that every form of corruption is destructive. Corruption destroys the essence of the state and thus its suppression to a level of acceptability commensurate with standards of the world we live in, is a requisite without which the state cannot be identified as a state ruled by law.

Bulgaria has established legal mechanism to prevent and combat corruption. The practical implementation of this mechanism reveals weaknesses, mainly due to poor cooperation between entities involved in preventing and combating corruption.

Bibliography:

1. **Administration Act,** Promulgated, State Gazette No. 130/05.11.1998, effective 06.12.1998

2. **Administrative Procedure Code** - Promulgated, State Gazette No. 30/11.04.2006, effective 12.07.2006.

3. **Code of Civil Procedure** - Promulgated, State Gazette No. 59/20.07.2007, effective 01.03.2008

4. **Conflict of Interests Prevention and Ascertainment Act,** Promulgated, State Gazette No. 94/31.10.2008, effective 01.01.2009

5. **Constitution of the Republic of Bulgaria** - Promulgated, State Gazette No. 56/13.07.1991 (effective 13.07.1991)

6. **Council of Ministers Decree No. 158/29.07.2010** for Foundation of Center for prevention and combating corruption and organized crime

7. **Criminal Procedure Code** - Promulgated, State Gazette No. 86/28.10.2005, effective 29.04.2006

8. **Integrated Strategy of prevention and combating corruption and organized crime**, Council of Ministers Protocol No. 45.32/18.11.2009
9. **Judiciary System Act**, Promulgated, State Gazette No. 64/07.08.2007
10. **National strategy for combating corruption**, Council of Ministers Decision No. 671/01.10.2001
11. **Political parties Act** - Promulgated, State Gazette No. 28/1.04.2005, effective 1.04.2005.
12. **Public Disclosure of Senior Public Official's Financial Interests Act** - Promulgated, State Gazette No. 38/9.05.2000
13. **Strategy for transparent governance and for prevention and countering of corruption 2006-2008,** Council of Ministers Decision No. 60/02.02.2006

ОПРЕДЕЛЯНЕ НА ТЕХНОГЕННАТА И ЕКОЛОГИЧНА БЕЗОПАСНОСТ ЧРЕЗ КОЛИЧЕСТВЕНА ОЦЕНКА НА РИСКА

Христо Ат. Десев

Национален военен университет „Васил Левски",
Факултет „Артилерия, ПВО и КИС", гр. Шумен

DETERMINATION OF TECHNOGENIC AND ECOLOGICAL SAFETY THROUGH QUANTITATIVE RISK ASSESSMENT.

Hristo A. Desev

***Abstract**: Problems with the protection and safety of society and the environment depends on the quantification of the dangers in which the unit is used to measure risk. Risk is the measure of expected failures in the operations, hazards to humans, adverse effects on the occurrence of which could have a material loss. Kolichesvena risk is characteristic of the actions of the dangers - the product of a particular human activity attributed to a number of people for some time.*

***Key Words**: risk, dangers, measure risk*

Защитата при бедствия за населението и инфраструктурата в страната ни е свързана както с вече явните изменения на някои природни процеси, явяващи се резултат на неизбежно продължаващото природо-технологично взаимовлияние, така и с повишаването уязвимостта на ключови сектори в икономиката ни, като резултат на новите икономически отношения, при които ролята на държавата е минимизирана.

Проблемите със защитата и безопасността на обществото и околната среда зависи от количественото измерване на опасностите, при което за единица се използва мярката на риска. Под термина риск трябва да се разбира многокомпонентна векторна величина с която се характеризират загубите от въздействието на различ-

ните опасни фактори, вероятността от възникване на определен фактор и неопределеността на количеството на загубите.

Рискът е мяра за очакваните неблагополучия в дейностите, опасности за хората, нежелани последствия от настъпването на които може да има материални загуби. Рискът е количесвена характеристика на действията на опасностите - продукт на конкретна човешка дейност отнесена към определен брой жители за определено време. С риска се описват и негативните фактори на производството в качеството на оценка на условията на труд. Термина описва и достоверни събития с вероятност равна на единица, тогава риска е еквивалентен на загубите. Така количествената оценка на риска се явява процес на оценка на числените значения на вероятността и последствията от нежелани събития, явления и процеси. Реалното измерение на риска за хората може дас е раздели в две основни катагории:

- индивидуален риск – вероятността за въздействие предизвикано от собствената дейност ;
- социален риск – като съотношение на пострадалите от аварията и вероятността от нейното сбъдване.

Таблица 1. Сравнителни данни за източниците и нивата на опасност за средноразвитите индустриални държави

Източник	**Причина**	**Средно значение на смъртни случаи $R_{ср}$**
Стихийни бедствия	Земетресения, наводнения, урагани	Rср. 1.10^{-6} 4.10^{-6}, 3.10^{-5}
Техносфера	Транспортни катастрофи, замърсяване на околната среда	Rср. 3.10^{-3}
Професионална дейност	Техногенни катастрофи	10^{-2}>Rср.<10^{-4}
Социална дейност	Бедност, военни действия	$(0,5\text{-}1,5).10^{-4}$

Определянето на приемлив индекс на риска е показател за степента на безопасност, прилага се като оценка на нейното изменение и практическо установяване на диапазон за цялата техносфера.

В най-широк смисъл риска е възможна опасност, породена от съвкупност от фактори за съответни източници. В зависимост от факторите и характерните източници определят разновидности на риска: аналитичен, техногенен, екологичен и др.

Оценката и анализа на риска предполагат избора на оптимални решения за осигуряването на безопасността на дейностите в производството. Те са единствения аналитичен инструмент за определяне на рисковете и определяне приоритетите за тяхното минимизиране.

Независимо от подходите, последователността и етапите на оценката се очертават три направления:

- обобщаване на информацията за събитията и производствата;
- анализ на риска;
- контрол на мерките по безопасността.

Риск - анализа има за цел системно да обобщава наличната информация за явленията и опасностите и честотата на събитията и последствията от тях. Оцен-

ката съчетава анализа на честотата, анализа на последствията и тяхното съчетаване. Анализа се провежда по следната схема:

1. Планиране и организация. Определяне на причините за извършване на риск – анализа, описание на системата подлежаща на анализ. Определяне източниците на информация, изходните данни и ограниченията и целта и степента на приемливия риск.

2. Идентификация на опасностите. Ясно описание на всички опасности и първоначална оценка на същите,

2.1. Храктер на проявления на опасностите.

2.2. Предварителна оценка на характеристиките на опасностите. Целта е задълбочаване на анализа и изработване на препоръки за намаляване на опасностите.

3. Оценка на риска.

3.1. Анализ на честотата. Определя се по статистически данни,експертни оценки от специалисти, логически методи и др.

3.2. Анализ на последствията. Оценка на въздействието върху обществото и околната среда чрез моделиране на авариите, изучаване на поражаващите фактори и критерии за устойчивост на средата.

3.3. Анализ на неопределеността. Възможни отклонения от недостиг на информация, грешки на персонала, слабости на моделите и методите.

4. Разработка на на механизъм на управление на риска. Приемане на съществуващия риск, като приемлив и/или определяне на технически, експлоатационни и организационни мерки за неговото намаляване(третиране).

Количесвеният анализ на риска позволява да се определи вероятността на събитието, количеството нещастни случаи, величината на риска и на последствията. При извършване на анализа основната система се разделя на подсистеми, които се разглеждат като самостоятелни, така можем да разглеждаме вероятността за общото бедствие Е като функция от вероятноста за бедствие в отделни събития Ei. Ако приложим формулния апарат от теорията на вероятностите към пълната група събития:

$\sum P\{Ei\}=1$

За равновъзможните събития $P\{4Ei\}=p,i=1,2,3\ldots n$, вероятността е равна на: $P=1/n$.

Практически се използва обективната вероятност, където:

$P\{E\}=N_E/n$ - като N_E и n са общото число и числото на случаите в които настъпва събитието.

Обикновенно заплахите от екологичен и технологичен характер и техните съставни елементи са свързани с отказ за действие на някои от елементите, ако приемем че елементите са независими помежду си то вероятността има вида:

$P\{E\}=1-(1-p)^{m,}$

където: m – е броят на компонентите.

Формулата показва високо ниво на отказите във сложните системи от което следва, че всяко действие насочено към безопасността може да се счита за паралелно и всяко действие което е необходимо да предотврати обасността може да се счита за последователно. Така числената оценка на риска се характеризира с числените значения на вероятността от събитието (р) и стойноста на последствията (х).

$R=PX$

Когато последствията не са известни то рискът се определя само от вероятностт аза сбъдване на нежеланото събитие.

$R=\sum Pi$

В принципите за управление на риска се залагат стратегически и тактически цели с които се постига максимално ниво на благосъстоянието и паралелно с това бисока степен на безопасност. Общата политика при управление на риска във всички случаи стои в диапазона ограничен от изисквания за непревишаване на въздействия над допустимите за екосистемите и максималните възможности на техническите системи.

Изработването на модел за управление на риска е в основата на ефективността на тази дейност. Предлагат се четири стъпки и етапи в следната последователност:

Първи етап – характеризира се риска, като се извършва сравнителна характеристика на рисковете и се определя техния приоритет. В края на етапа се опрделя степента на вредност.

Втори етап - определяне приемливостта на риска, като се съпоставят редица еколого-икономически фактори (печалба, загуби, възможности за регулиране). Възможните крайни изходи са: риска е приемлив, риска се приема частично и риска не е приемлив. В двата последни изхода се опрделят процедури по третиране на риска.

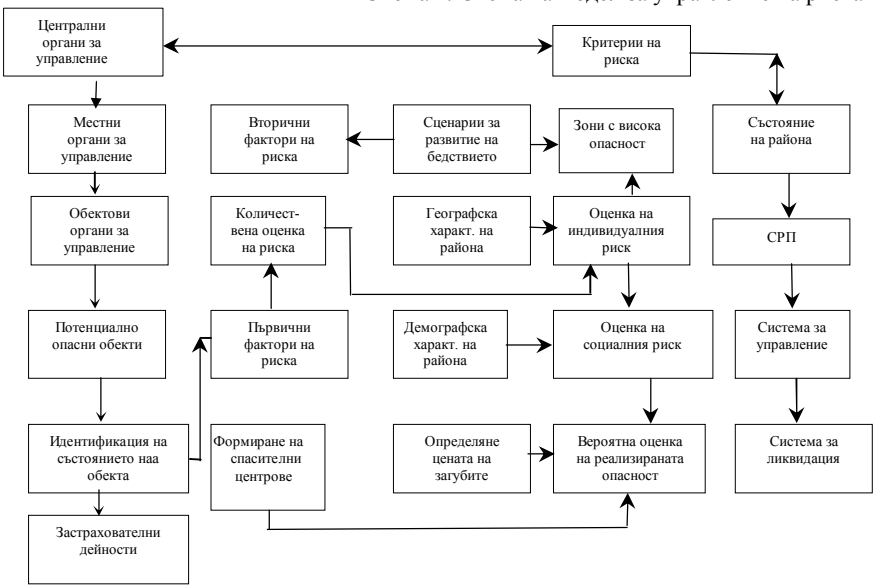
Трети етап – избор на типови мерки за намаляване или отстраняване на риска.

Четвърти етап – приемане на регулиращо решение (нормативен акт, инструкция).

Общ примерен модел на схема за управление на риска е посочен в схема 1.

Общият модел е схематично разделен на три основни зони. В първата зона се включва системата за управление (централно, местно, обектово ниво и актуален списък на обектите). Тук се извършва идентификация на състоянието на обектите, което е и начало на сисртемата за анализ на риска. Смислово обвързано с тази зона е и застраховането на обекти и производства.

Схема 1. Схема на модел за управление на риска



Втората зона е за съществения анализ и обхваща процесите по анализа на първичните фактори и количествена оценка на индивидуалния риск и възможните сценарии на събитието. Сценария е продиктуван от вторичните фактори, които се явяват последствие на инициираните начални събития. Анализа на индивидуалния риск и развитието на събитиети позволява да се определят зони за висок риск. Паралелно се оценява като продукт от демографската оценка на района и индивидуалния риск социалния риск е в основата на реализацията на опасността.

В третата зона се формират стойностите на допустимите рискове. Те са продукт от индивидуалния, социалния и районите свисок риск, при тях се дефинира района по рискови показатели, определят се насоки за системата за защита и системата за ликвидация на явлението.

Ролята на управлението на риска е то да е насочено за неговото предотвратяване или възможно снижаване. Старите детерминиски схващания за нулев риск и абсолютна безопасност днес са несъстоятелни поради несъответствието им на вътрешните закони на техно и биосферата. Нито едно общество не може да продължава да внедрява технически системи за намаляване на риска безкрайно, това са сериозни финансови ресурси. Тази логика насочва вниманието към достигане на ниво на риска, което да наречем „приемливо". Приемливостта трябва да бъде икономически и социално обоснована, като нивото на риска или неговата стойност (вероятност за реализация, възможни загуби) е толкова нищожна, че заради получаваните от това ползи (материални и социални блага) обществото е готово на този риск

Изводи:

Видимо теорията на риска се нуждае от задълбочено разработване на концептуални основи, които да осигуряват възможност за въздействие върху него, което не може да го изключи, но може да го намали до нивото на приемливия. Безконтролната ескалация на рисковете в една ситуация могат да предизвика кризисна ситуация и криза.

Паралелно с това съществуват и рисковете за качеството на управленското решение т.е. постигането на показателя рационалност.

Оценката на риска и намирането на верен подход към неговото управление трябва да е в пълен синхрон с готовността на системите за реагиране при кризи.

Превенцията на кризите от природен, техногенен и екологичен характер, чиято основа е снижаването на риска е процес, който трябва да се прилага в пълния си обем към всички обекти от критичната инфраструктура.

Литература:

1. Салтиров Д. – „Човешкия ресурс като риск за дестабилизация на организацията" – Научна конференция с международно участие ШУ „Еп. К. Преславски" научни трудове 2008.

2. Салтиров Д. – „Критерий за ефективност при вземане на решение" - Научна конференция с международно участие „40 години Шуменски университет 1971-2001г.", Сб. Научни трудове 2001.

3. Шойгу С. К. "От абсолютной безопасности к приемлемому риску", сп. "Экология и жизнь", 2000, №3.

4. Сп. "Проблемь анализа риска". – кн.4 2010.

ПРАВНИ АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В СТРАНИТЕ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ

Велико П. Петров

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

LEGAL ASPECTS OF THE PROTECTION OF PERSONAL DATA IN THE COUNTRIES OF THE EUROPEAN UNION.

Veliko P. Petrov

Abstract: *The report examined legal aspects of the protection of personal data in the countries of the EUROPEAN UNION. The reform of EU data protection aims at establishing a modern, stable, coherent and comprehensive legal framework on data protection to the European Union.*

Keywords: *legal aspects, protection of personal data*

Ежедневно всеки може да стане субект на обработка на лични данни или самите ние да боравим с такива данни. Понятието „Лични данни” по смисъла на правото на ЕС е всяка информация, свързана с конкретно физическо лице, независимо от това дали се отнася до неговия личен, професионален или обществен живот. Това може да бъде име, снимка, адрес на електронна поща, банкови данни, медицинска информация, телефонен номер или IP адрес. Развитието на технологиите и компютъризацията във всеки обществен сектор улеснява още повече получаването на достъп и обработката на данни. Всичко това изисква гаранции за неприкосновеността на личната ни информация и личния ни живот, и същевременно предполага разработването на ясни правила за гарантиране на тази защита. Защитата на личните данни е сравнително нова тема, която се свързва предимно с развитието на информационните технологии, които дават възможност да се обработват бързо огромни бази от данни с лична информация.

В ерата на информацията, правото на защита на личния живот налага поставянето на ограничения върху събирането, разпространяването и използването на лична информация, която се съхранява от правителствени структури, частни фирми и други организации. Тези правила са обикновено известни като „защита на личните данни”. Интересът към това право на защита се увеличава през 60-те и 70-те години на 20 век с развитието на информационните технологии [1].

Развитието на информационните и комуникационни технологии налага необходимостта от специфична правна уредба, която да защити основните човешки права на неприкосновеност на личния живот и свобода и тайна на кореспонденцията, без да се ограничава свободното движение и достъп до информация.

През последните 40 години, се разработват набор от правила, известни като „принципи за коректност към личните данни” (ПКЛД). Тези принципи са предложени за първи път от Американското Министерство на Здравеопазването, образо-

ването и благосъстоянието през 1974 г. и по-късно стават част от законодателствата на много държави.

Може да се посочат следните принципи за коректност към личните данни:

1) Отчетност: Институциите са задължават да опазват личните данни, които съхраняват и да назначат служител, или служители, които са отговорни за изпълнението на следните принципи в институцията.

2) Определяне на целта: Целите, за които се събират лични данни трябва да са определени от институцията преди или по време на събиране на информацията.

3) Съгласие: Знанието и съгласието на лицата са задължителни при събирането, използването, или разкриването на личните им данни, освен когато това е неуместно.

4) Ограничено събиране: Събирането на лични данни трябва да е ограничено само в рамките на необходимото за целите, определени от организацията. Информацията трябва да се събира по законен и обективен начин.

5) Ограничено използване, разкриване и съхранение: Лични данни не могат да се използват или разкриват за цели, различни от тези, за които са били събрани, освен със съгласието на лицето или в случаи, предвидени в закон. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели.

5) Прецизност: Личните данни трябва да са прецизни, пълни и актуални, доколкото това е необходимо за целите, за които се използват.

6) Опазване: Личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

7) Откритост: Институциите трябва да осигуряват свободен достъп до информация за политиките и практиките свързани с управлението на личните данни.

8) Право на достъп: При подаване на заявление, гражданите трябва да бъдат информирани за съществуването, използването и разкриването на техни лични данни и трябва да могат да получат достъп до тях. Гражданите трябва да имат възможността да проверят точността и пълнотата на техните лични данни и да ги поправят, ако е необходимо.

9) Възможност за контрол: Гражданите трябва да имат възможността да проверят дали тези, които използват или събират техни лични данни, спазват горните принципи, като отправят питане към определения служител, или служители.

На основата на тези принципи, през 1981 г. Организацията за икономическо сътрудничество и развитие представя разширени препоръки, които впоследствие се приемат в целия свят.

Първият изчерпателен закон за защита на личните данни е приет в немската провинция Хесен през 1970 г., а впоследствие се приемат подобни закони и в други Европейски страни като Швеция (1973г.), Германия (1977г.) и Франция.

През 1981 г. се приема Конвенция № 108 на Съвета на Европа за автоматизираната обработка на лични данни. Конвенцията дава общата уредба относно защитата на личните данни и по-специално защитата на физическите лица от неправомерно обработване на лични данни. Тази конвенция отразява принципите за коректност към личните данни, като определя правила за трансгранично прехвърляне на лични данни и създава механизми за международно сътрудничество. Много държави в Европа приемат закони след приемането на Конвенцията, ефективно влязла в сила през 1985 г., с което осигуряват безпрепятствено прехвърляне на информация.

В рамките на Съвета на Европа действат и редица препоръки и резолюции на Комитета на министрите, свързани със защита на личните данни в различни области като застраховането, статистиката, медицинските данни, телекомуникации, платежни и други операции, трудова заетост, социално осигуряване и др.

Важна стъпка в развитието на правото на защита на личните данни е приемането на Директива 95/46/ЕО на Европейския парламент и Съвета от 24 октомври 1995 г. за защита на гражданите с оглед на обработването на техните лични данни и свободното движение на такива данни [4]. Целта на тази директива е да хармонизира законите в Европейския Съюз, да осигури надеждна защита на правата на гражданите и да позволи свободен пренос на лични данни между страните на ЕС. Всяка страна-членка на ЕС е задължена да приеме закони осигуряващи прилагането на Директивата.

Основна промяна в Конвенцията на Съвета на Европа е разширяването на правата върху неелектронни носители. Всяка страна от ЕС трябва да създаде Комисия по защита на личните данни или агенция, която да следи за изпълнение на закона. Директивата създава задължение към страните членки да осигури еднакво ниво на защита на личните данни, когато те се прехвърлят или обработват в страни извън ЕС. Това задължение оказва голям натиск върху страните извън Европа да приемат закони за защита на личните данни. Тези държави, които отказват да приемат адекватни закони за защита на личните данни, се оказват в положение на невъзможност да обменят определени видове информация с европейските страни. Това се отнася особено до някои категории чувствителна информация.

Европейският съюз разширява приложението на Директивата за защита на личните данни, като приема Директива за защита на личните данни свързани с телекомуникациите през 1997 г., която урежда конкретна защита при прехвърляне на данни по телефон, дигитална телевизия, мобилни мрежи и други комуникационни системи. Директивата въвежда обширен кръг задължения към носителите и доставчиците на услуги, за да осигури защита на личните данни на потребителите на услуги, свързани с Интернет. След двегодишен дебат, Европейският съюз приема нова Директива 2002/58/ЕО на ЕП и Съвета от 12 юли 2002 г за обработване на лични данни и защита неприкосновеността в електронния съобщителен сектор, както и правилата, свързани с Шенгенското пространство, Европол и Евроюст. Тя по-ясно покрива Интернет комуникациите и слага ограничения върху рекламните e-mail-и (спам). Въпреки това, поради натиска от страна на разузнавателни и правоприлагащи организации от ЕС, директивата отслабва задълженията за събиране на транзакционни данни. Това от своя страна не позволява на държавите да приемат закони, задължаващи комуникационните компании да пазят информация за дейността на техните клиенти.

Правото на защита на личните данни е изрично признато в член 8 от Хартата на основните права на ЕС и в Договора от Лисабон, подписан на 13 декември 2007 г. Договорът дава правното основание за правилата за защита на данните за всички дейности, попадащи в обхвата на правото на ЕС, съгласно член 16 (Договор за функционирането на Европейския съюз). Влизането в сила на Договора от Лисабон и най-вече въвеждането на ново правно основание (член 16) позволяват установяването на цялостна рамка за защита на данните, с която да се гарантира високо ниво на защита на данните на физическите лица, съобразено със специфичното естество на областта на полицейското и съдебното сътрудничество по наказател-

ноправни въпроси. Съществуват и специфични правила за защита на личните данни в полицейското и съдебното сътрудничество по наказателноправни въпроси (Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г.). На това рамково решение обаче приложното поле е ограничено, тъй като се прилага единствено за трансграничното обработване на данни, но не и за дейностите по обработване на данни от страна на полицейските и съдебните органи на чисто национално равнище.

Концепцията за защитата на личните данни е сравнително нова в списъка на основните човешки права. Необходимостта от институционализиране на правото на защита на личните данни е резултат от развитието на технологиите, използвани за обработването на данни през последните 60 години.

Защитата на личните данни на всеки гражданин представлява важен елемент от упражняването на правото на неприкосновеност на личността - едно от основните човешки права и свободи в демократичните общества. Упражняването на правото на защита на личната ни информация осигурява на всеки гражданин демократична защита срещу неправомерна намеса в личната му сфера на живот, и същевременно създават условия за отговорно и прозрачно управление.

В Европейската Конвенция за защита на правата на човека и основните свободи: Право на зачитане на личния и семейния живот (Изм. - ДВ, бр. 137 от 1998 г.) в Член 8 е записано:

- Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище е тайната на неговата кореспонденция;

- Намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

В Хартата за основните права на ЕС (Обн., ОВ, бр. 303 от 14.12.2007г.) в Член 7 (Зачитане на личния и семейния живот) е записано - Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговите съобщения, а в Член 8 (Защита на личните данни) е записано:

- всеки има право на защита на неговите лични данни;

- тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им;

- спазването на тези правила подлежи на контрол от независим орган.

На 4 ноември 2010 г. Комисията изложи стратегия за засилване на правилата на ЕС за защита на данните (IP/10/1462 и MEMO/10/542). Целите на стратегията са да се защитят данните на лицата във всички области на политиката, включително в правоприлагането, като в същото време се намалят административните формалности за бизнеса и се гарантира свободното движение на данни в ЕС. Комисията поиска коментари по своите идеи и проведе също така отделна обществена консултация с оглед на преразглеждането на Директивата на ЕС за защита на данните от 1995 г. (95/46/ЕО).

На 24 февруари 2011 г. Съветът на Европейския съюз прие заключения, в които широко подкрепя намерението на Комисията да реформира рамката за защита на данните и дава съгласието си за много елементи от подхода на Комисията. По

същия начин Европейският икономически и социален комитет подкрепи общия стремеж на Комисията да гарантира по-съгласувано прилагане на разпоредбите на ЕС за защита на данните във всички държави-членки и подходящо преразглеждане на Директива 95/46/ЕО.

Европейският парламент одобри със своята Резолюция от 6 юли 2011 г. относно всеобхватния подход за защита на личните данни в Европейския съюз (2011/2025(INI), доклад в който се подкрепя подходът на Комисията към реформирането на рамката за защита на данните.

Високото ниво на защита на данните е жизнено важно за повишаване на доверието в онлайн услугите и за реализиране на потенциала на цифровата икономика, за което са необходими съвременни съгласувани норми в целия ЕС. С цел осъвременяване на правилата на ЕС за защита на данните, с което се засилва тяхното измерение, свързано с вътрешния пазар, Европейската комисия е изготвила на 25 Януари 2012 г. следните документи:

1) Съобщение на ЕК COM (2012) 9 final - Защитата на правото на личен живот във взаимосвързания свят. Европейска рамка за защита на данните за 21-ви век.

2) Предложение за Регламент относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните);

3) Предложение за Директива на ЕК COM (2012) 10 final относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни;

4) Оценка на въздействието, придружаваща Регламента и Директивата;

5) Оценка на въздействието – обобщение;

6) Доклад на ЕК на основание на член 29, параграф 2 от Рамковото решение на Съвета от 27 ноември 2008 година относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси;

7) Работен документ към Доклада.

С всичките тези документи Европейската комисия предложи цялостна реформа на правилата на ЕС за защита на личните данни от 1995 г., което има за цел да се укрепят правата на личен живот в онлайн пространството и да се даде тласък на развитието на европейската цифрова икономика. Държавите-членки на ЕС прилагат правилата от 1995 г. по различен начин, което води до разминавания в правоприлагането. Еврокомисията предлага един-единствен Закон за личните данни, който ще сложи край на сегашната разпокъсаност и скъпоструваща административна тежест и ще доведе до икономии за бизнеса в размер на близо 2,3 милиарда евро годишно. Актуализират се и се осъвременяват принципите, залегнали в директивата за защита на личните данни от 1995 г., за да се гарантират правата на личен живот в бъдеще. Предложенията се състоят от съобщение относно политиката, в което се излагат целите на Комисията, и две законодателни предложения: регламент, с който се установява обща рамка на ЕС за защита на данните, и директива относно защитата на личните данни, обработвани за целите на предотвратяването, разкриването, разследването или наказателното преследване на престъпления и свързаните с това съдебни дейности.

Основните промени, които въвежда реформата, включват:

- Един-единствен набор от правила за защита на данните, валидни в целия ЕС. Ще бъдат премахнати ненужните административни изисквания, като например изискванията за уведомяване за дружества. Това ще спести на бизнеса около 2,3 милиарда евро годишно.

- Вместо сегашното задължение за всички дружества да уведомяват надзорните органи за защита на данните за всички дейности по защита на данните - изискване, което доведе до ненужни административни формалности и разходи за бизнеса в размер на 130 милиона евро годишно, регламентът предвижда по-голяма отговорност и отчетност за обработващите лични данни.

- Така например, дружествата и организациите трябва да уведомяват националния надзорен орган за сериозни нарушения на сигурността на данните възможно най-бързо (ако е осъществимо, в рамките на 24 часа).

- Организациите ще могат да работят само с един национален орган по защита на данните в държавата от ЕС, в която се намира основното им място на установяване. По същия начин хората ще могат да се обръщат към органа по защита на данните в тяхната страна дори когато техните лични данни се обработват от дружество, установено извън ЕС. Когато се изисква съгласие за обработването на данните, се пояснява, че то трябва да бъде дадено изрично, а не да се предполага.

- Хората ще имат по-лесен достъп до собствените си данни и ще могат по-лесно да предават лични данни от един доставчик на услуги на друг (право на преносимост на данните). Това ще подобри конкуренцията в сектора на услугите.

- „Правото да бъдеш забравен“ ще помогне на хората да управляват по-добре рисковете, свързани със защитата на данните в онлайн пространството: хората ще могат да заличават своите данни, ако няма законни основания за запазването им.

- Правилата на ЕС трябва да се прилагат, когато лични данни се обработват в чужбина от дружества, които осъществяват дейност на пазара на ЕС и предлагат своите услуги на гражданите на ЕС.

- Независимите национални органи по защита на данните ще бъдат укрепени, така че да могат по-добре да прилагат правилата на ЕС в своите страни. Ще им бъде предоставено правомощието да налагат глоби на дружествата, които нарушават правилата на ЕС за защита на данните. Това може да доведе до глоби до 1 милион евро или до 2 % от общия годишен оборот на дружеството.

- Въз основа на нова директива общите принципи и правила за защита на данните ще се прилагат за полицейското и съдебното сътрудничество по наказателноправни въпроси. Правилата ще важат както за вътрешните, така и за презграничните предавания на данни.

Предложенията на Комисията ще бъдат предадени на Европейския парламент и на държавите-членки на ЕС (заседаващи в Съвета на министрите) за обсъждане. Те ще влязат в сила две години след приемането им.

Изводи:

1. Съществуването на изчерпателна правна уредба не гарантира само по себе си правото на защита на личните данни. Съгласно Директива 95/46/ЕО — основният законодателен акт на ЕС в областта на защитата на данните към днешна дата - начините, по които физическите лица могат да упражняват правото си на защита на данните, не са достатъчно хармонизирани в различните държави-членки. Право-

мощията на националните органи, отговорни за защитата на личните данни, също не са хармонизирани достатъчно, за да се гарантира съгласуваното и ефективно прилагане на нормите. Това означава, че действителното упражняване на тези права е по-трудно в някои държави-членки в сравнение с други, особено онлайн.

2. Най-важното, което трябва да се знае в днешно време е това, че не трябва да бъдем безразлични, лекомислени и непредпазливи по отношение на себе си, и да не изключваме възможността, че множеството случаи, на които ежедневно ставаме свидетели за нарушения в областта на информационната неприкосновеност и личните данни, могат да се случат и на нас. Въпросите, свързани с неприкосновеността и защитата на личните данни, често са сред основните теми през последните години. Технологията напредна с огромно темпо, в резултат, на което се извършват големи промени в начина на използване на личните данни при доставката на стоки и услуги.

3. С реформата на ЕС на защитата на данните се цели изграждането на съвременна, стабилна, съгласувана и цялостна правна рамка за защита на данните за Европейския съюз. Укрепва се основното право на физическите лица на защита на личните данни. Реформата ще бъде от полза преди всичко за физическите лица, тъй като чрез нея техните права на защита на личните данни ще бъдат утвърдени, а доверието им в цифровата среда - засилено. Освен това ще се опрости значително правната среда за предприятията и публичния сектор. Очаква се да се стимулира развитието на цифровата икономика в целия единен пазар на ЕС и извън него в съответствие с целите на стратегията „Европа 2020“ и Програмата в областта на цифровите технологии за Европа.

4. С реформата ще се засили доверието между правоприлагащите органи и ще се улесни обменът на данни между тях и сътрудничество в борбата с тежката престъпност, като същевременно ще гарантира високо ниво на защита за физическите лица.

5. Бързите темпове на технологичните промени и глобализацията коренно промениха начина, по който се събират, правят достъпни, използват и предават все по-голям обем от лични данни. В цифровата среда физическите лица имат правото да упражняват ефективен контрол върху своята лична информация. Защитата на личните данни е основно право в Европа и трябва да бъде защитавано по-съответния начин. Новият регламент на ЕС ще осигури силна защита на основното право на защита на личните данни в целия Европейски съюз, ще подобри функционирането на вътрешния пазар и ще сложи край на сегашната разпокъсаност и скъпоструваща административна тежест.

Литература:

1. Дейвид Банисар, „Модели за защита на личните данни”.

2. Габриела Белова, „Някои проблеми във връзка със защитата на личните данни в Европейския съюз”, списание „Икономика и Управление”, ЮЗУ “Неофит Рилски” – Благоевград, год.VI, №3, 2010.

3. Конвенция № 108 на Съветът на Европа от 1981 г., за защитата на индивидите във връзка с автоматичната обработка на лични данни.

4. Директива 95/46/ЕО на Европейския парламент и Съвета от 24 октомври 1995 г. за защита на гражданите с оглед на обработването на техните лични данни и свободното движение на такива данни.

5. Директива 97/66/ЕО на Европейския парламент и Съвета през 1997 г за защита на личните данни свързани с телекомуникациите.

6. Директива 2002/58/ЕО на ЕП и Съвета от 12 юли 2002 г за обработване на лични данни и защита неприкосновеността в електронния съобщителен сектор.

7. Европейската Конвенция за защита на правата на човека и основните свободи (Изм. – ДВ, бр. 137 от 1998 г.).

8. Харта за основните права на ЕС (Обн., ОВ, бр. 303 от 14.12.2007г.).

9. IP/11/102, Брюксел, 28 януари 2011 г., „Ден за защита на личните данни – гарантиране правото на неприкосновеност на личния живот".

10. Рамково решение 2008/977/ПВР относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси.

11. Съобщение на ЕК COM (2012) 9 final (от 25 Януари 2012 г.) - Защитата на правото на личен живот във взаимосвързания свят. Европейска рамка за защита на данните за 21-ви век.

12. Предложение за Директива на ЕК COM (2012) 10 final (от 25 Януари 2012 г.) относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни.

МЕЖДУНАРОДНО ПРАВНО СЪТРУДНИЧЕСТВО МЕЖДУ СТРАНИТЕ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ ЗА ПРОТИВОДЕЙСТВИЕ НА КОРУПЦИОННИТЕ ПРЕСТЪПЛЕНИЯ

Велико П. Петров

Национален военен университет „Васил Левски",
Факултет „Артилерия, ПВО и КИС", гр. Шумен

INTERNATIONAL LEGAL COOPERATION BETWEEN THE COUNTRIES OF EUROPEAN UNION FOR COUNTERACTION OF CORRUPTION OFFENSES.

Veliko P. Petrov

Abstract: *The report examined international legal cooperation between the countries of European Union for counteraction of corruption offenses. The effective anticorruption requires increased, rapid and well-functioning international cooperation in criminal matters.*

Keywords: *Corruption offenses, International cooperation*

Корупцията е явление, познато на човечеството от хилядолетия. Тя разрушава върховенството на закона, подкопава доверието на гражданите в демократичните ценности и възпрепятства гражданското и икономическо развитие. Корупцията е една от най-сериозните заплахи за съвременното демократично общество. Тя е

световно разпространен феномен и нито една държава не е застрахована от пагубното й влияние. Развитието на международното правно сътрудничество ускорява и засилва взаимната връзка и зависимост на националното право и нормите на международното право. Този въпрос придобива особена важност предвид увеличаването на потребностите от наказателно правно сътрудничество, особено между държавите – членки на Европейския съюз (ЕС), налагащо се от съвременните форми на престъпност и най-вече с оглед на нейната транснационалност. Динамиката на престъпността налага все по-често позоваване на международни правни актове.

Нарастването на обществеоопасните прояви в световен мащаб налага създаването на международни инструменти за противодействието им. Ангажираността на държавите и международните организации се проявява в приемането на актове, съдържащи мерки за борба с престъпността. Сътрудничеството между тях се осъществява чрез конвенции, резолюции и препоръки, визиращи различни прояви на обществеоопасно поведение – тероризъм, трафик на наркотици, корупция, компютърни престъпления. Актове в тези области имат ООН, Съветът на Европа, Европейският съюз, Г-8 и други.

Международното правно сътрудничество като понятие и видове сътрудничество включва трансфери на наказателни производства, трансфери на осъдени лица, признаване и изпълнение на присъди на чуждестранни съдилища, екстрадиции, международна правна помощ по наказателни дела, оперативно сътрудничество и обмен на информация. Правната рамка за осъществяване на международно - правно сътрудничество при разследване на престъпления, засягащи корупцията в Общността се определя от редица международни актове, нормативни актове на Европейския съюз и вътрешната нормативна база.

Като най-известен международноправен документ, който регламентира материята относно наказателно-правната взаимопомощ е Европейската конвенция за взаимопомощ по наказателноправни въпроси, приета на 20.04.1959 година в Страсбург (от България е ратифицирана и влиза в сила от 15.09.1994 г). Проблематиката на сътрудничеството и взаимопомощта по наказателноправните въпроси следователно не е отскоро и е нормален ход на развитието на международно - правните отношения. Конвенцията за взаимопомощ от Страсбург е един от първите документи, който дава решение на международните правни проблеми свързани с борбата с организираната престъпност.

Корупционните престъпления се отнасят до всички области на живота, в които е възможна корупция – дейността на държавния апарат, разглеждан в неговия най-широк смисъл, дейността на обществената организация, функционирането на стопанския сектор и спорта. В отделните сфери на живота корупцията има различна степен на обществена опасност. В държавният апарат, тя има отражения във всички сфери на живота – корумпираният държавен служител с поведението си може да засегне не само реда за функциониране на администрацията или на съдебната система, но и да накърни значителни икономически интереси. В професионалните съюзи или в политическите партии, например, често пъти тя е не по-малко опасна от корупцията в държавния апарат. Корупцията в стопанския сектор може да се отрази на цялостния механизъм на функциониране на пазарната икономика.

Корупция има практически навсякъде. Като основнни сфери на разпространение на корупцията се открояват:

- Държавната администрация;

- Политическата корупция;
- Съдебната система и правоохранителните институции;
- Обществените услуги (здравеопазване, образование и т.н.);
- Частния сектор;
- Третия сектор (неправителствени организации и др.).

Досега не е приет универсално приложим закон, отнасящ се до борбата против корупцията. Обаче има многобройни регионални и международни усилия за подпомагане на намаляването и възможното изкореняване на корупцията.

Произходът на понятието корупция е от латински „corruption" и в буквален превод означава „разваленост", „изхабеност", „лошо състояние", а второто й значение е „лъжливост", „разваляне", „подкупване". В Тълковния речник на българския език срещу думата корупция е отбелязано: „покварeност на длъжностно лице"; продажност".

В исторически аспект българското законодателство има нелоши традиции по отношение на регулирането на обществените отношения, свързани с корупционно поведение, които имат комплексен характер. Необходимо е да се отбележат следните по-важни нормативни актове, извън наказателното ни законодателство, които са оказали влияние върху развитието на правната ни система: "Закон за отнемане на имуществото на престъпно забогателите чиновници", "Закон за конфискуване на придобити чрез спекула и по незаконен начин имоти" и други [1].

Терминът „корупция" е широко използван не само в специализираната юридическа литература и средствата за масова информация, но е и легален, законов термин. Проблем е обаче факта, че дефиниция (определение) на това понятие липсва не само в законодателните актове, които го използват, но дори не можа да бъде открито и в доктрината у нас. Това предполага две неща:

Първо, законодателят предполага (предпоставя), че то е известно, ясно по съдържание, поради което не се налага изричното му определяне чрез законова разпоредба.

Второ, че определянето му е твърде затруднено, поради което на този етап опитите това да се направи са изоставени [2].

В българското законодателство няма правна дефиниция на понятието „корупция", а се използва определението на термина „корупция" в изготвената от Съвета на Европа „Наказателна конвенция за корупцията, през 1999 г." и то е следното [14]:

„Искането, предлагането, даването или приемането, пряко или косвено, на подкуп или всяка друга неследваща се облага или обещаването на такава, което засяга надлежното изпълнение на някое задължение или поведението, което се изисква от приемащия подкупа, неполагащата се облага или обещаването на такава".

В приетата от Съвета на Европа Наказателна конвенция за корупцията са посочени и различни категории лица, които тази конвенция визира като субекти на потенциални корупционни действия:

- Национални длъжностни лица и членове на национални публични събрания.
- Чужди длъжностни лица и членове на чужди публични събрания.
- Служители на международни организации и членове на международни парламентарни събрания.
- Съдии и служители на международни съдилища.
- Лица, които изпълняват ръководна работа в частни юридически лица.

Прокуратурата използва работно понятие за „корупция", което включва всички форми на злоупотреба с власт, чрез които се цели или се постига лично или групово облагодетелстване.

В действащото законодателство понятието корупция се среща в 51 нормативни акта от различен порядък. Водещо в практико-приложен аспект остава наказателното ни законодателство. Разпоредбите на Наказателния кодекс (НК) на Република България предвиждат относително изчерпателна система на корупционни престъпления, така както те са предвидени в множество международноправни актове, по които страна е Р. България. Легално в НК на Република България, макар и неизчерпателно, това са престъпленията по чл.чл.201-205, 219, 220, 224, 228, 242, ал.3, 257, 282, 282а, 283, 283а, 289, 301-307а и 387 от НК. Престъплението, което в най-голяма степен съдържа в себе си признаците на корупционно поведение е подкупът (пасивен и активен). В българския НК то е уредено в Раздел IV на Глава Осма от Особената част. НК третира подкупа като престъпление против дейността на държавните органи и обществените организации. Наред с подкупа като корупционно престъпление със същата степен на обществена опасност трябва да се третира и длъжностното присвояване, което е едно от най-характерните престъпления против собствеността. Според НК на Република България престъпления (със съответни наказания) са няколко корупционни деяния [4]:

- престъпленията по служба - общо престъпление по служба – който извърши или не извърши нещо, което му се следва по служба тогава, когато има свой или чужд интерес;

- класическия подкуп - който получи или съответно даде пари или друга имотна облага, за да се извърши нещо, което му се следва по служба.

Измамата в някои правни системи се включва в понятието корупция, както и възпрепятстването на правосъдието, особено в британската система; длъжностните присвоявания; изборните измами.

Много често престъпления, които са свързани с наркотици, в определени системи се третират като корупционни престъпления, доколкото контрабандата твърде често включва и използване на канали, при които се подкупват длъжностни лица.

Корупцията включва в себе си твърде много действия и бездействия.

Могат да се разграничат четири основни категории корупционни действия.

- Първо, корупция за осигуряване на достъп до ограничени ресурси.

- Второ, корупция за получаване на ползи (или намаляване на разходите) които не са ограничени, но достъпът до тях се контролира от лица взимащи решения по лично усмотрение.

- Трето, корупция за извършване на услуга, свързана с получаването на определена полза (или избягването на разходи) например предоставяне на вътрешна информация или ускоряване на взимането на решение.

- Четвърто, корупцията за предоставяне на дадени ресурси или получаването на ползи от други заинтересовани страни (или налагането на допълнителни разходи спрямо тях).

Понятието за корупция включва в себе си някои деяния, които са предвидени в Наказателния кодекс и други, които са предвидени в други нормативни актове.

В кодексите за поведение на държавните служители и правилниците на различни институции, за корупцията пише следното:

- "Неправилно използване на обществен ресурс, неправилно изпълнение на държавна служба за извличане на пряка или последваща полза";

- "Поведение, изразяващо се в нечестно използване на власт или позиция, което има като резултат поставянето на някого в по-добро положение от другиго";

- "Корупцията е дребна и голяма, административна и политическа. Корупцията е разпространена в съдебната и изпълнителната власт. Корупцията създава негативен международен имидж на страната и отблъсква чуждите инвестиции, което има пряко отражение върху икономическото развитие и благосъстоянието на гражданите";

- „Според служебното положение на участващия в корупционната сделка държавен служител корупцията е политическа (голяма) или бюрократична (малка)".

Най-често срещаните възможни форми на корупция могат да бъдат разделени в две основни групи: такива, които вече са квалифицирани като престъпления от наказателното право, и такива, които са свързани с професионална етика, нещо различно от морала.

От гледна точка на наказателното право, като корупционни са квалифицирани общите престъпления по служба. Тогава, когато държавен служител извърши или не извърши нещо, което е задължен да извърши в кръга на служебните си задължения, за извличане на облага за себе си или за другиго. Друг вид корупционни престъпления са длъжностните присвоявания. Много често тези длъжностни присвоявания биха могли да бъдат извършвани в съучастие с други работещи в структурата на съответната администрация – обикновено по-висшестоящи [3].

В Резолюция (97) 24 са залегнали водещи принципи за противодействието на корупцията за [5]:

- криминализация на националната и международната корупция;

- независимост на органите, занимаващи се с превенция, разследване и правораздаване във връзка с извършени корупционни престъпления и възможности за осигуряване необходимите правомощия при събиране на доказателства и при защитата на лицата, оказващи съдействие на властта при противодействие на корупцията;

- разработване на мерки за конфискация и отнемане на имущество във връзка с извършени корупционни престъпления;

- ограничаване имунитета срещу наказателно преследване за извършени корупционни престъпления до минимално необходимия.;

- въвеждане на ефективно финансово законодателство за противодействие на корупцията;

- прозрачност в процеса на вземане на решения от страна на административните органи;

- възможност за обективни финансови и данъчни проверки, включително и на органи в държавната администрация за откриване на корупция в държавната администрация;

- осигуряване на система на отговорност, която да доведе до намаляване на корупционните правонарушения при длъжностните лица;

- мерки, за защита на лицата, претърпели вреди, в резултат на корупционно престъпление;

- предприемане на действия за международно сътрудничество във всички области на противодействието на корупцията.

От 1 януари 2007 г. за България са в сила редица актове на ЕС, които имат непосредствено отношение към противодействието на корупцията. Заедно с някои

конвенции на други международни организации те съставляват правната рамка за противодействие на корупцията в ЕС. В изпълнение на препоръките на Групата държави срещу корупцията (GRECO) към Съвета на Европа и на Работната група по въпросите на корупцията на Организацията за сигурност и сътрудничество в Европа (ОИСР) беше регламентирана отговорност на юридически лица за извършени в тяхна полза престъпления, включително корупционни.

Законодателната рамка в правото на отделните държави при регулирането на противодействието и борбата с корупцията се очертават два подхода:

1) Подробна законодателна уредба в законодателството относно наказателното правораздаване – в Белгия (Централно антикорупционно бюро към федералната полиция и Централно бюро за разследване на корупция в системата на Прокуратурата); Испания (Специализираната прокуратура Антимафия), Великобритания, Германия. Този подход се отличава:

- със стремеж за относително подробно и детайлно уреждане на основните корупционни престъпления и способите за тяхното разкриване и разследване;
- изграждане на специализирани звена в рамките на съдебната система и/или полицията;
- предвиждане на допълнителни мерки в гражданското законодателство за превенция на корупционно поведение и извършване на корупционни престъпления;
- ратифициране на международноправни актове относно корупцията.

2) Самостоятелно законодателно уреждане на противодействието и борбата с корупцията – Румъния, Полша, Казахстан. Този подход се отличава:

- със самостоятелен антикорупционен закон;
- с изграждане на отделна система от специализирани органи с разследващи и превантивни функции;
- липса на „дублиращи" функции с органи от правосъдната система;
- приемане на комплекс от закони, ограничаващи корупцията;
-присъединяване към единни международни стандарти и добри практики в борбата с корупцията;

Законодателната рамка в актовете на ЕС се отличава със следните особености:

1) Могат да се очертаят три групи актове:

- актове, пряко регулиращи обществените отношения във връзка с борбата с корупцията;
- актове, които имат препоръчително - рамкиращ характер по отношение необходимостта от въвеждане на определени правни институти в националните законодателства;
- актове, които имат смесен характер: въвеждат някои основни понятия и/или дават легални дефиниции относно корупцията и свързаните с нея последици и дават препоръки за изграждане на националното законодателство. Много от актовете на Европейския съюз дефинират понятията активна и пасивна корупция, измама, както и лицата, които могат да бъдат субекти на корупционни правонарушения. В някои от случаите тези актове са отворени и към държави, които не са членове на ЕС.

2) Съществуват тенденции към изграждане на единни международни стандарти за разкриване, разследване и доказване на корупционни престъпления.

3) Създава се система от нормативни актове, които не регламентират пряко противодействието на корупцията, но имат пряко отношение към изграждане на

правила, свързани с регулиране на последиците от корупционни действия и поведение. Например извършването на корупционни престъпления се явява препятствие пред осъществяването на различни дейности. Осъждането за корупция с влязла в сила присъда лишаване от свобода е дисквалифициращо основание за участие в процедури за възлагане на обществени поръчки. В други актове се предвижда въвеждането на превантивни мерки, чрез които да се ограничат възможностите за измами и корупция.

4) В структурно отношение повечето международни договори се отличават с типизирана структура, която обхваща: преамбюл, общи разпоредби, в които се дават някои определения, посочват се целите на акта и неговото приложно поле, мерките, които трябва да се осигурят на национално ниво, разпоредби относно международното сътрудничество, разпоредби, уреждащи влизането в сила, изменението и денонсирането на договорите.

5) Прокарва се идеята макар и плахо за създаване на единна система на наказателно правораздаване в рамките на ЕС. Една от стъпките е създаването на CORPUS JURIS, в който се предлага кодификация на наказателното правораздаване. Предвижда се:

- система от престъпления в която са обхванати престъпленията, извършвани от длъжностни лица, като на първо място е посочено престъплението корупция (чл. 5 от CORPUS JURIS);
- създаване на институциите на европейския прокурор и съдия по свободите;
- единна процедура за разглеждане на делата за предвидените в CORPUS JURIS престъпления.

Институционализацията на антикорупционната дейност се подразделя на следните нива:

1) Международно ниво:

- Комисия по превенция на престъпността към ИКОСОС (Икономически и социален съвет) на ООН;
- Работна група на ОИСР (Организация за икономическо сътрудничество и развитие) по въпросите на корупцията;
- Бюрото за борба с измамите (OLAF) към ЕС;
- Група държави срещу корупцията (GRECO) към Съвета на Европа (СЕ);
- Многодисциплинарна група по корупцията (GMC) към СЕ.

2) Национално ниво:

- Комисия за координация на работата по борбата с корупцията към Министерския съвет (МС);
- Държавната административна комисия;
- Главен инспекторат;
- Сметна палата;
- Омбудсман и др.

3) Регионално ниво: областно и общинско:

- Обществен съвет за борба с корупцията;
- Местен омбудсман (обществен посредник, граждански посредник).

4) Ведомствено ниво:

- Съгласно чл. 46 от Закона за администрацията в структурата на всяко министерство и всяка държавна агенция трябва да се създадат инспекторати на пряко подчинение на министъра.

- Комисия за борба с корупцията в съдебната система, която е създадена през 2004 г. към Висшия съдебен съвет (Министерство на правосъдието). Тя има ограничени пълномощия, изготвя анализи и препоръки относно борбата с корупцията и не включва разследване на корупцията в съдебната система.

5) Специализирано ниво:

- Национална разузнавателна служба (НРС);
- Министерство на вътрешните работи (МВР);
- Комисия за борба с корупцията на Народното събрание.
- Държавна агенция национална сигурност (ДАНС);
- Съдебна система (следствие, прокуратура, съд);
- Научни звена и други.

6) Неправителствени структури:

- Трансперанси Интернешънъл (ТІ);
- Асоциация „Прозрачност без граници";
- Групата за антикорупционна инициатива „Коалиция 2000";
- Граждански наблюдател и други.

Могат да се посочат основните сфери в борбата с корупцията и те са:

1) Създаване на система от превантивни мерки, която да включва:

- осигуряване на добро за длъжността и отговорностите заплащане на длъжностни лица в държавния и частния бизнес;
- изключване или ограничаване на социалния натиск;
- намаляване на монополните права;
- ротация на държавните служители в една система;
- навременна реакция на прояви на корупция и вземане на административни мерки;
- установяване на ефективен текущ контрол от висшестоящите длъжностни лица и органи;
- приемане на правила за поведение;
- създаване на условия за по-лесен достъп до правителствена информация;
- участие в разработване на съвместни мерки за борба с международна корупция;
- прозрачна политика и информация на медиите за нетърпимост към корупция;
- институционализиране на прозрачността чрез създаване на неправителствени организации;

2) Създаване на система от законодателни мерки, която да включва:

- изграждане на система от антикорупционно законодателство – наказателно правна, гражданско правна и административно правна;
- инкриминиране на всички форми на корупция с оглед на обществена опасност;
- инкриминиране на корупционни деяния на чужди длъжностни лица;
- законодателно уреждане издръжката на партиите;
- законодателно лимитиране на банковата и търговската тайна.

3) Национална стратегия за противодействие на престъпността – приета от МС – 01.07.1998 г. Насочена е към: а) провеждане на единна държавна политика за осъществяване на регулативните функции на държавата чрез оптимизиране на държавните структури; б) изграждане на система за административен контрол; в) осъвременяване на нормативната уредба; г) създаване на ясни правила за административно обслужване на граждани; д) разработване на система за координация на

дейностите за противодействието на корупцията; е) създаване на регистър за финансовото и имотното състояние на лицата.

4) Система от мерки за установяване и разследване на прояви на корупция – корупционните престъпления по българското законодателство са тежки, съгл. чл. 93 т. 7 НК –"тежко престъпление" е това, за което по закон е предвидено наказание лишаване от свобода повече от 5 години доживотен затвор или доживотен затвор без замяна.

Изводи:

1) Корупцията не е изкоренена в никоя от развитите европейски страни, но и в нито една от тях тя не съставлява такъв обществен проблем, както у нас. Със сигурност може да се предположи, че с развитието на демократичните процеси в България, с постепенното утвърждаване на гражданския контрол върху държавата, с изграждането на истински независима съдебна власт, с окончателното установяване на истински пазарни принципи в икономиката и най-важното - с окончателното установяване на лична нетърпимост към корупцията от страна на повечето граждани и у нас корупцията ще намалее и ще се сведе до размерите на едно обикновено отрицателно явление.

2) Уредбата на корупцията показва, че в наказателния закон (НК на Р.България) сравнително пълно са обхванати основните форми на корупционно поведение. Основателно в него не са регламентирани по-незначителни с оглед на тяхната обществена опасност прояви, борбата с които остава задача на останалото законодателство.

3) Борбата с корупцията в ЕС придобива все повече общностен характер предимно поради доказаната престъпна симбиоза между нея и организираната престъпност, както и поради разрушителното й въздействие върху мерките, свързани с изграждането на пространството на свобода, сигурност и правосъдие. В приетите от ЕС програми и планове за действие за борба с организираната престъпност, тероризма, измамата, прането на пари и други сериозни престъпления, има включен и специален раздел за борба с корупцията. Основните правни инструменти в които са концентрирани acquis на ЕС за борба с корупцията са:

- Конвенция за защита на финансовите интереси на Европейските общности и протоколите към нея;
- Конвенция за борба срещу корупцията, в която са въвлечени служители от Европейските общности или служители от държавите- членки;
- Конвенция относно изпиране, издирване, изземване и конфискация на облагите от престъпление;
- Конвенция за борба с подкупването на чужди длъжностни лица в международните търговски сделки;
- Наказателна и Гражданска конвенция на Съвета на Европа за корупция;
- Общи позиции и съвместни действия за борба с корупцията;
- Директиви на Съвета на ЕС за предотвратяване изпирането на пари във финансовата система на държавите-членки.

4) Синхронизиране на националната уредба за корупцията със съответната уредба в страните-членки на ЕС, което ще позволи в бъдеще още по-ефективна борба с нея. При тази синхронизация се предпоставя несъмнената необходимост от защита на обществения интерес, значителна по обем нормативна база и многообразна по характер и съдържание практика. Необходими са усилията и на цялото

общество, което трябва да създаде обстановка на непримиримост към това остро антисоциално явление, която е стимул за нравствена борба на присъщият за всеки благороден човек стремеж към законност и морал.

5) Световният опит показа, че дори в страните с развита административна система и контролни механизми корупцията не може да бъде овладяна без съдействието на гражданското общество и независимите средства за масово осведомяване. Практиката в развитите демокрации свидетелства за нарасналото значение на включването на професионалните организации и другите граждански структури в усилията за утвърждаване ценностите на прозрачността, публичността и демокрацията. Особено важен е потенциалът на изграждането на механизми и успешни практики на партньорство между държавните институции, неправителствените организации и частните медии в сфери като обществения контрол върху дейността на администрацията, защитата на правата на гражданите, саморегулирането чрез въвеждане в практиката на ефективни кодекси на поведение, инициирането на независим мониторинг, разгръщането на антикорупционна разяснителна и образователна дейност.

6) Ефективното противодействие на корупционните престъпления изисква разширено, бързо и добре функциониращо международно сътрудничество по наказателните дела. По-голямата част от общите и специалните състави за пряка или косвена борба с този вид престъпления, които българският Наказателен кодекс съдържа са ефективни. Същевременно, някои от новите състави са необосновани и неточни или връщат назад наказателното законодателство, поради което следва да се прецизират и усъвършенстват.

Литература:

1. Резюме на законодателно проучване на тема: „Законодателен опит и нормативна база относно статута на институции и органи за борба с корупцията в страни от ЕС”, . 2007 г.

2. Корупционни практики и превенция на корупцията, Учебно помагало, Център за изследване на демокрацията, София, 2004 г.

3. Икономическата цена на корупцията, Център за изследване на демокрацията, София, 1999 г.

4. Наказателно-правни аспекти в борбата срещу корупцията, Л. Груев, Б. Велчев.

5. Резолюция (97) 24 Относно двадесетте ръководни принципа за борба срещу корупцията (приета от Комитета на министрите на 6 ноември 1997 г. по време на 101-то заседание).

6. Национална стратегия за противодействие на корупцията.

7. Наказателния кодекс.

8. Наказателно процесуалния кодекс.

9. Корупция и антикорупция, Сборник, Център за изследване на демокрацията, София 2003.

10. Резюме на законодателно проучване на тема: „Международни актове и институции за сътрудничество в противодействие на международната престъпност (септември, 2004 г.).

11. Декларация на ООН против корупцията и подкупите от16 декември 1996 г.

12. Европейската конвенция за взаимопомощ по наказателноправни въпроси, приета на 20.04.1959 г. в Страсбург (от Р България е ратифицирана и влиза в сила от 15.09.1994 г.).

13. Конвенция на Европейския съюз за борба срещу корупцията от 1997 г.

14. Наказателна конвенция на Съвета на Европа относно корупцията от 1999 г.

15. Административно процесуален кодекс.

16. Национална стратегия за противодействие на престъпността.

17. Закона за администрацията.

ИДЕНТИФИКАЦИЯ И ТИПИЗАЦИЯ НА ОБЕКТИТЕ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА В ЕЛЕКТРОЕНЕРГИЙНИЯ СЕКТОР

Здравко Ю. Кузманов

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

IDENTIFICATION AND OBJECTS TYPIFICATION OF THE CRITICAL INFRASTRUCTURE IN THE ELECTRICITY SECTOR

Zdravko Y. Kuzmanov

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

ABSTRACT: *The current report presents the main issues related to identification and objects typification of the critical infrastructure in the electricity sector. There are analyzed two main issues. What is the national normative base over identification of items in critical infrastructure in electricity sector? How are the items from critical infrastructure typified in the electricity infrastructure and what does this requires?*

KEY WORDS: *Critical infrastructure, Strategic Infrastructure, Electricity, Electric power system.*

В националното законодателството на Република България определение на термина „критичната инфраструктура” е представен в Закона за отбраната и въоръжените сили и Закона за защита при бедствия, съгласно които се определя, 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”* [4] и *„… система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни после-*

дици за Република България в резултат на невъзможността да се запазят тези функции" [2] .

Едни от най-значимите и важни инфраструктури в съвременния живот са енергийните. Към двете най-важни направления на научно-техническата революция се отнасят замяната на физическата енергия на човека с други видове енергия, преди всичко с електрическа и освобождаването от шаблонни операции с помощта на автоматизация на процесите. Именно затова научно-техническият прогрес се определя от енергетиката и автоматиката на всички отрасли на икономиката.

През последните сто години с особено бързи темпове се развива електроенергетиката. Откриването на електричеството и изграждането на електроенергийни системи (ЕЕС) не само позволиха да се издигне „енерговъоръжеността" на човека, но и предоставят нови, недостъпни преди възможности за регулиране и преобразуване на енергийния поток. В днешните условия е общоизвестно, че от всички видове консумирана енергия електрическата се явява най-съвършен междинен вид, който лесно се преобразува в механична, топлинна, светлинна, химична и др.

Електроенергийната система е елемент (подсистема) на Енергийната (ЕнС) и включва в себе си генераторите и потребителите на електрическа енергия, обединени посредством електрическа мрежа (ЕМ) и работещи съвместно в общ режим [3]. В ЕЕС процесът на производство, пренасяне, разпределение и консумиране е единен и непрекъснат и практически протича мигновено.

Електроиндустрията във всяка страна се състои от множество различни инфраструктурни обекти, собственост на държавата и частни компании, участващи в производството, преноса и разпределението на електрическа енергия. Въпреки това, с цел изпълняване на основните функции и постигне на подходяща ефективност, всички електрически централи, подстанции и електропроводи, формиращи електрическата мрежа, са свързани с диспечерски центрове за контрол и управление, формирайки единна ЕЕС. Тази взаимовръзка, най-силна на национално равнище, формира националната система за електрозахранване.

Към края на първото и началото на второто деситилетие 21-ви век, обектите формиращи ЕЕС са едни от най-критичните инфраструктури, които са жизненоважни за много други, зависещи от надеждна доставка на електроенергия.

Изхождайки от изложеното до тук целата на доклада е да се изследват въпросите свързани с идентификацията и типизацията на обектите от критичната инфраструктура в електроенергийния сектор.

Първият въпрос, който следва да се постави е каква е националната нормативна база относно идентификацията на обектите от критичната инфраструктура в електроенергийния сектор?

Термина „критична инфраструктура" е въведен в националното законодателство през 2005 г., като препокрива частично или напълно значението на още четири: „потенциално опасен обект и потенциално опасна дейност", „стратегически обекти и дейности", „национално стопанство" и „техническа инфраструктура". В последните няколко години започна уеднаквяване на терминологията, главно под влияние на ЕС чрез дефинираните от съюза политики, програми и мерки за защита на обекти от критичната инфраструктура. Въпреки това термините „стратегически обекти и дейности" и „техническа инфраструктура" все още се използват в националното законодателство. Единствената дефиниция на „стратегически обекти и дейности" е представена в Закона за МВР и правилника за прилагането му, съгласно които:

„Стратегическите обекти и дейности са тези с общонационално значение, чието изваждане от строя или нарушаване на нормалния им режим на съществуване и работа би застрашило в изключително висока степен живота, здравето, спокойствието и собствеността на гражданите, както и обществения ред, националната сигурност и управлението на страната" [3, 5].

Определяне на стратегически обекти и дейности в Република България се извършва с приемане на Постановление на Министерски съвет № 181 от 20 юли 2009 г. Чрез него са обособени петнадесет сектора, в които се вклюват четиридесет стратегически дейности и над сто стратегически обекта. В този списък не са включени тези, които са предоставени за управление на Министерството на отбраната, Министерството на вътрешните работи, Националната разузнавателна служба и Държавна агенция „Национална сигурност". Такива обекти се определят със заповед на ръководителя на съответното министерство или ведомство. В това постановление изрично е записано, че стратегическите обекти и дейности, които са от значение за националната сигурност на Република България, ***са част от критичната инфраструктура.*** За сектор енергетика в сферата на електроенергетиката, като стратегически дейности са посочени производството и преноса на електроенергия. Определени са 36 обекта, към които е включена и Националната електрическа компания [6].

С Решение на министерски съвет № 775 от 21 септември 2004 г. са утвърдени стратегическите обекти с национално значение в сферата на енергетиката. Съгласно приложението такива обекти в сектора на електроенергетиката са общо 107. [7] В периода 2005-2011 г. с още пет специализирани подзаконови нормативни акта [8, 9, 10, 11, 12] за стратегически с национално значение са обявени още 11 обекта.

Съгласно разпоредбите на Закона за енергетиката се изготвя *„Списък на стратегическите обекти от национално значение в енергетиката"*, който се обновява ежегодно [1].

От посочените законови и подзаконови актове се налагат следните основни изводи. Първо, че се изготвя „Списък на стратегическите обекти от национално значение в енергетиката", които се обновява ежегодно. Второ, въпреки положените усилия за хармонизиране на терминологията в националната нормативна база, този въпрос продължава да бъде все още не напълно изчистен. Трето, съгласно посочените актове, на територията на Република България се експлоатират и функционират общо 116[1] електроенергийни обекта, определени като стратегически с национално значение, които са част от критичната инфраструктура на страната.

Вторият въпрос е как се типизират идентифицираните обекти от критичната инфраструктура в електроенергийната инфраструктура и какво налага това?

Както вече става ясно от изложеното до тук на територията на страната са разположени 116 обекта от критичната електроенергийна инфраструктура, определени и като стратегически с национално значение.

Една от основните цели на изследването е типизацията на обектите, техното определяне по вид, актуалния брой и събиране на максимално количество данни за активите им.

[1] В общата бройка не се включват дублиращи се обекти от нормативните документи.

За нуждите на изследването най-целесъобразно се явява, обектите от критичната инфраструктура в електроенергийния сектор предназначени за производство и пренос на елекрическа енергия да се класифицират по вид и тип. За територията на страната те са представени в табл. 1.1.

Типизацията се налага по следните причини. Първо с цел да бъдат определени активите на всеки обект, който подлежи на оценка и защита. Второ, да бъде улеснена последваща работа с обекти притежаващи еднаква функционална спецификация. Всички обекти, класифицирани по вид и тип, подлежат на обстойно разглеждане и събиране на максимално количество данни за активите им.

Таблица 1.1.

Класификация по вид и тип на обектите от критичната инфраструктура в електроенергийния сектор – производство и пренос на електроенергия

№	ВИД НА ОБЕКТА	ТИП НА ОБЕКТА	БРОЙ
1. АДМИНИСТРАТИВНИ СГРАДИ И УПРАВЛЕНИЯ			
1.	Диспечерско управление	Централно	1
2.	Диспечерско управление	Териториално	4
		Общо	5
2. ЕЛЕКТРОПРОИЗВОДСТВЕНИ ОБЕКТИ			
1.	Електрическа централа	АЕЦ	2
2.	Електрическа централа	ТЕЦ	6
3.	Електрическа централа	ВЕЦ	3
4.	Електрическа централа	ПАВЕЦ	2
		Общо	13
3. ОБЕКТИ ОТ ЕЛЕКТРОПРЕНОСНАТА МРЕЖА			
1.	Електрическа подстанция	400 kV-възлова	1
		400/220/110 kV	6
		400/110 kV	5
		220/110 kV	3
		Общо	15
2.	Електропровод	400 kV	25
		220 kV	11
		110 kV	47
		Общо	83
		ОБЩО	**116**

Представената типизация следва естествена логическа последователност. На най-високо ниво обектите са групирани според функционалното им предназначение:

1. Административни сгради и управления;
2. Електропроизводствени обекти;
3. Обекти от електропреносната мрежа.

Обектите от всяка група се класифицират по вид и тип както следва:

- За група Административни сгради и управления:
    - По вид на обекта:
        - Диспечерско управление:
    - По тип на обекта:

        - Централно;
        - Териториално.
- За група Електропроизводствени обекти:
    - По вид на обекта:
        - Електрическа централа:
    - По тип на обекта:
        - АЕЦ;
        - ТЕЦ;
        - ВЕЦ;
        - ПАВЕЦ.
- За група Обекти от електропреносната мрежа:
    - По вид на обекта:
        - Електрическа подстанция:
    - По тип на обекта:
        - 400 kV-възлова;
        - 400/220/110 kV;
        - 400/110 kV;
        - 220/110 kV.
        - Електропровод:
        - 400 kV;
        - 220 kV;
        - 110 kV.

Изложената типизация на обектите от критичната инфраструктура в електроенергийния сектор, служи за основа при определяне на активите подлежащи на последваща оценка и защита.

Използвана литература:

1. Закон за енергетиката, Обн. ДВ. бр.107 от 9 Декември 2003 г., изм. ДВ. бр.38 от 18 Май 2012 г.

2. Закон за защита при бедствия, Обн. ДВ. бр.102 от 19 Декември 2006 г., изм. ДВ. бр.80 от 14 Октомври 2011 г.

3. Закон за Министерството на вътрешните работи, Обн. ДВ. бр.17 от 24 Февруари 2006 г., изм. ДВ. бр.81 от 18 Октомври 2011 г., доп. ДВ. бр.38 от 18 Май 2012 г.

4. Закон за отбраната и въоръжените сили на Република България, Обн. ДВ. бр.35 от 12 Май 2009 г., изм. ДВ. бр.33 от 27 Април 2012 г., доп. ДВ. бр.38 от 18 Май 2012 г.

5. Правилник за прилагане на Закона за Министерството на вътрешните работи, Приет с ПМС № 126 от 02.06.2006 г., Обн. ДВ. бр.47 от 9 Юни 2006 г., изм. ДВ. бр.12 от 10 Февруари 2012 г.

6. Постановление на Министерски съвет № 181 от 20 юли 2009 г., За определяне на стратегическите обекти и дейности, които са от значение за националната сигурност, Обн., ДВ, бр. 59 от 28.07.2009 г.

7. Решение на Министерски съвет № 755 от 21 септември 2004 г., За утвърждаване Списък на стратегическите обекти от национално значение в енергетиката.

8. Решение на Министерски съвет № 257 от 8 април 2005 г., За определяне на енергиен обект „Ядрена централа на площадка „Белене" като обект с национално значение.

9. Решение на Министерски съвет № 434 от 22 юни 2007 г., За определяне на топлоелектрическа централа за производство на електрическа енергия от лигнитни въглища от „Мини Марица-изток" ЕАД за обект от национално значение.

10. Решение на Министерски съвет Министерски съвет № 46 от 1 февруари 2008 г., За обявяване на енергийни линейни обекти „ВЛ – 400 kV Карлово-Пловдив", „ВЛ – 110 kV Чернозем-Хисаря" и „ВЛ – 110 kV Пловдив-Чернозем" за обекти с национално значение.

11. Решение на Министерски съвет № 652 от 17 октомври 2008 г., За обявяване на енергийни линейни обекти на територията на община Гълъбово, област Стара Загора, като обекти с национално значение.

12. Решение на Министерски съвет № 35 от 20 януари 2011 г., За определяне на енергийни линейни обекти на територията на общините Несебър, Айтос, Бургас и Поморие, област Бургас и Добрич, Балчик и Каварна, област Добрич, като обекти с национално значение.

СИГУРНОСТ НА ОРГАНИЗАЦИЯ

Генчо Белчев Сандев

ШУ „Епископ Константин Преславски"
Технически факултет. Катедра „Управление на системите за сигурност"

Анотация. *В съответствие с разработените във времето различни парадигми за личната и обществената сигурност и чрез корелация между тях е формирано понятието „сигурност" – безопасност и защитеност на обект от действителността - природна система, общество (организация, човек). Чрез композирането на характеристиките на сигурността със структурата и функциите на организацията са систематизирани основните детерминанти, изграждащи качеството „сигурност" на същата.*

Ключови думи: *общество, организация, човешка сигурност, обществена сигурност, субект и обект на сигурността, сигурност на организация, детерминанти на сигурността.*

1. Дефиниране на сигурността като категория

1.1. Базови постановки

Човекът, обществото и природата са взаимосвързани от сложни процеси, чрез които те си въздействат, взаимно се обуславят, изменят своето състояние и се пораждат един от друг. Взаимодействието между противоположностите е източник, основа и причина за възникването, самодвижението и развитието. Този факт придава особено значение на категорията „взаимодействие" за процеса на познание на природните и обществените явления, като я поставя в основата на системния

подход в изучаване на света и обществената практика. Една от най-сложните и многостранни форми на взаимодействие между елементите на систе-мата „човек - общество - природа" се обозначава с термина „сигурност".

Опитите да се разкрие съдържанието на понятието „сигурност", които не престават от Древността до днес, показват богато разнообразие от непрекъснато обогатяващи се форми и направления на реализация на това взаимодействие. Много изследователи разкриват, че през вековете няколко пъти се променя доми-ниращия смисъл на понятието – от вътрешно усещане на отделния човек, през осъзнаване на сигурността като необходимо условие за индивидуална свобода до състояние на организациите, държавата и международната общност.

Проблемът за личната сигурност възниква с появата на прадедите на съвременния човек. Проявява се като необходимост от всекидневно решаване от отделния индивид на задачата как да оцелее и опази своето поколение.

Американският психолог А. Маслоу поставя потребността от сигурност в групата на първостепенните мотиви, които формират човешкото поведение. Многообразните човешки потребности са групирани от Маслоу в пет категории, подредени в строга йерархична структура (пирамида): физиологични нужди; потребност от сигурност и самосъхранение; социални потребности; потребност от удовлетворение на чувството за собствено достойнство; потребност от само-усъвършенстване. Колкото по-ниско е разположена в пирамидата дадена пот-ребност, толкова тя е по-важна за оцеляването на индивида, толкова по-силно е усещането за нея и приоритетно удовлетворяването ѝ. В този смисъл потребността от сигурност е базова за отделния човек. Тя се постига благодарение на инстинкта или спазването на определени, изработени благодарение на опита, правила на поведение във всекидневния живот (бита), производствената дейност и в различ-ните обществени взаимодействия.

За първи път на най - високо ниво **концепцията за човешката сигурност се появява през 1994 год. в „Доклад за развитието на човека" на ООН.** В него са отбелязани два водещи аспекта на тази концепция:

▪ Защитата от въздействието на трайно появяващи се заплахи като глад, болести и репресии.

▪ Защитата от внезапни и травмиращи сривове в ежедневния начин на живот на хората, в техните домове, на работните им места и в общностите.

Според този доклад най-важните компоненти на човешката сигурност са:

▪ Икономическата сигурност (напр. защита от бедност).

▪ Продоволствената сигурност (напр. достъп до храна).

▪ Здравната сигурност (напр. достъп до здравна помощ и защита от болести).

▪ Екологичната сигурност (напр. защита от опасности като замърсяванията и изтощаването на околната среда).

▪ Личната сигурност (напр. физическата защитеност от явления като войни, криминални нападения, изтезания, семейно насилие, употреба на наркотици, самоубийства и дори пътни инциденти).

▪ Общностната сигурност (напр. оцеляване на традиционните култури и етнически групи, както и на физическата сигурност на тези групи).

▪ Политическата сигурност (напр. зачитане на гражданските и политическите права и свобода от политически гнет).

Други специалисти предлагат дефиниция за „човешка сигурност", включваща само „същностните" елементи, които са „достатъчно важни за хората, така че

те да са готови да се борят за тях или да поставят на значителен риск своя живот или собствеността си" [3, 4]. На базата на тази дефиниция, авторите идентфицират **пет ключови индикатора, свързани с благосъстоянието (качеството на живот):** здраве (липса на опасности от преждевременна смърт, от инвалидиризиране и остри и трудно лечими заболявания; не е на лице преждевременно изчерпване на естествените ресурси); бедност (не са нарушени най-съществените предпоставки за живот; няма разграждане на социалната защита; не е на лице срив на социалния статус); образование (няма ограничения за равен старт, за развитие и реализация); политическа свобода (осигурена е свобода на сдружаването, политически плура-лизъм; няма ограничения за участие в политическия процес); демокрация (уста-новено е разделение на властите, законност, защитени са правата и свободите на гражданите и е осигурено участието им в управлението на различните държавни дела – чрез функциите на гражданското общество, чрез избори или референдуми). Тези индикатори показват границата между човешката сигурност и несигурност. Чрез тях се измерва нивото на човешката сигурност. Посочената граница (праг) на възприемане на опасностите от хората зависи от мирогледа, морала, образованието, социалния статус, степента на информираност, психо-физиологичните и други качества.

По-висша потребност – от обществена сигурност, се появява когато възниква човешкото общество. Основен източник на опасности и рискове, породени от неопределеността, в която съществуват хората, продължава да бъде природата. Оцеляването на човека обаче започва да се свързва с колективните начини на живот. Формите, в които най-напред се орга-низира човешкото общество – племе, род, семейство, удовлетворяват пот-ребността от сигурност, преживявана като усещане за спокойствие, увереност, че опасностите и заплахите ще бъдат по-лесно преодоляни с обединени усилия, както и че ако нещо се случи с индивида, съплеменниците ще неутрализират негативните последици.

След появата на държавата понятието „сигурност" получава полити-ческа украска. Буржоазните революции и конституциите, които се приемат след тях, легитимират либералния модел за обществена сигур-ност. Франция държи приоритет в това отношение – в **Декларацията за правата на човека и гражданина** се съдържа специална дефиниция: „Сигурността се състои в съгласуваната от обществото защита на всеки един от неговите членове за опазване на личността му, правата му и собствеността му" [6].

Защитната функция на държавата се реализира посредством привеж-дане в действие на предвидените в законодателството мерки. Това озна-чава защитата да се разглежда като функционална система от три елемента – превенция; премахване на щети и санкциониране (наказание) на виновния извършител.

В съответствие с разработените във времето различни парадигми за личната и обществената сигурност и чрез корелация между тях може да се формира понятието „сигурност" – безопасност и защитеност на обект от действителността - природна система, общество (организация, човек).

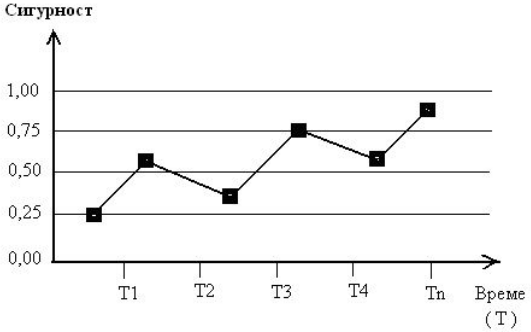
Това разбиране означава, че сигурността е реалистична категория, т.е. има смисъл само ако се отнесе към конкретна система (организация, човек). Казано с други думи, сигурност въобще не съществува, защото тя винаги е нечия сигурност.

Ако се приложи това разбиране към отделна система (организация, човек), то може да се определи че същите притежават качеството „сигурност" когато са в безопасност - в определен отрязък от жизнения им цикъл липсват силни (критични

за реализиране на целите) въздействия или са надеждно защитени от влиянието на определени фактори (опасности). Това означава че сигурността е преходен времеви интервал от развитието на определена система (организация, човек). В такъв случай обективно съществува алтернативно състояние на сигурността – несигурността. Тя е противоположното единство на сигурността, разглеждана като бинарна система в динамично равновесно състояние.

Оценката на всяко от състоянията, може условно да се представи количествено като число със стойности от 0 до 1 (фиг. 1). Промяната на стойностите обикновено във всеки момент от времето представлява сложна крива. Двете крайни състояния са невъзможни. Разрушаването на сигурността обикновено настъпва при критична стойност, намираща се под точка „0".

Трябва да се отчита, че границата между „сигурност" и „несигурност" е трудно определима, тъй като преминаването в едно от двете състояния зависи много често от случайни фактори (често добре прикрити) в системата (организацията, човека) и в средата в която оперират. Това означава, че не съществува абсолютна и непрекъсната сигурност.



Фиг.1

1.2. Субект, обект на сигурността и неопределеност на бъдещето

Проблемите на сигурността, пред които се изправя всяко общество (подсистема, елемент от него) са разнообразни. Въпреки това при всяка свързана с проблема за сигурността ситуация има и елементи, които неизменно се повтарят. Взети в единство, те очертават абстрактния модел на ситуациите свързани със сигурността. Най-общите, неизменно съчетавани елементи са:

- субектът на сигурността;

- обектът на сигурността;

- състоянието на неопределеност на бъдещето, от което зависят както субектът, така и обектът.

Наличието на тези три елемента и връзката между тях са абсолютно необходими за възникването на проблем на сигурността.

Субекти на сигурността могат да бъдат:

- държавата и нейните институции;
- областите и общините;
- различните държавни и частни организации;

- неправителствените организации осъществяващи активност в сферата на обществените отношения;

- други формации (могат да бъдат и със скрито присъствие);

- хората.

Обект на сигурността е онази ценност (материална или нематериална), която в процеса на взаимодействието си субектите се стремят да съхранят, променят или постигнат. В този смисъл това, което не представлява ценност, не е обект и не може да се свърже със сигурност, тъй като съществуването и съдбата му няма да привлекат вниманието на различните субекти. Понятието „ценност" в много отношения е сходно с понятието „интерес". Ценността е онова, с което трайно е свързан интересът на субекта (което той се стреми да получи, увеличи или запази от посегателствата на другите).

За да бъде ценността обект на сигурност е нужно нейното запазване, изменение или придобиване да са в кръга на възможностите на субекта на сигурността. Не може ли да промени обстоятелствата, на субекта не му остава нищо друго, освен примирявайки се за момента, да се приспособи към тях. Тъй като тези възможности също не са постоянни и субектът може да постига тяхното увели-чаване или снижаване, те също се превръщат в ценност, която може да бъде разглеждана и защитавана от него, както и от другите субекти на сигурността.

Отношението на субектите към обектите на тяхната сигурност може да бъде представяно и анализирано от различни гледни точки. Поради разнообразието от интереси един и същ субект може да преценява като обекти на сигурност много и различни такива. От друга страна, със запазването сигурността на един и същ интерес могат да са свързани много страни. Това води до разклонена във всички посоки мрежа от различни преплитащи се и влияещи на сигурността едни на други интереси. Тя остава винаги отворена. Един субект има отношение към множество обекти, към всеки от които насочват вниманието си и други субекти и т.н.

Третият елемент в моделната схема – неопределеността на бъдещето (която засяга интереси, представляващи обект на сигурност) идва от трудностите, свър-зани с направата на точно и прецизно разграничаване и от многовариантността на бъдещето. Тя е характеристика на информационната недостатъчност за промените в текущите ситуации, заплахите и закономерностите на еволюцията на обкръжението.

Неопределеността се състои във възможността да станат събития, които причиняват вреда на субекта и/или обекта или променят връзката между тях. Тези събития могат да бъдат от различно естество: поведение на един или няколко други субекти (участници) във взаимодействията; възникване на неблагоприятна ситуация за реализация на интересите; претенция, насочена против субекта на сигурността; промяна в съотношението на силите, при която се намаляват възмож-ностите да се защити обекта; възникване на висока степен на нестабилност в средата и др.

Неопределеността дали едно събитие ще се случи или не зависи частично от субекта, и отчасти от обстоятелства, които в една или друга степен са неподвластни на неговата воля. Неопределеността става елемент на проблема за сигурността, само когато се отнася за неблагоприятно развитие (т.е. такова, което увреждa определен интерес на даден субект и се преценява от него като опасност или заплаха). От това следва, че съществуването на възможност за някакво негативно, нежелано бъдеще е необходим елемент при всеки модел на сигурност. Неопределеността се отнася и за отношението между субект и обект. **Неопределеността на**

бъдещето въвежда несигурност за възможността на субекта да реализира или да запази онова, което преценява като свой интерес.

От мястото, което този интерес заема в приоритетите на един субект, зависи значението на проблема за сигурността, а от неопределеността зависи величината на самата сигурност (тоест отношението между сигурност и несигурност). По същество усилията на всеки субект целящ да постигне повече сигурност, са насочени към намаляване на състоянието на неопределеност или към подтикване на развитието в благоприятно направление. Неопределеността може да се отнася за различни обекти на анализ, например: възможността да възникне опасност или заплаха; величината на силите, от които биха могли да дойдат заплахите; съотношението между тези сили и възможностите да им се противостои; възможността да се получи външна подкрепа; надеждността на тази подкрепа и много други.

Колкото по-пълна е информацията толкова по-вероятно е да бъде запазена благоприятната за субекта връзка с обекта на сигурност. Пълното сваляне на неопределеността, разбира се, напълно изключва проблема.

Неопределеността на бъдещето може да се изменя с активни действия на субекта, като напр. се въздейства върху ситуацията така, че тя да се стабилизира, или като се достави информация, която да премахне или намали неопределеността. Търсенето на сигурност и нейното поддържане и защита се състоят, от една страна, от дейност, насочена към намаляване неопределеността на бъдещето, и от друга, от въздействия върху обстановката съобразно с възможностите, с които субектът разполага.

Тази теоретична схема не съдържа готови, еднозначни решения. Моделът служи преди всичко за структуриране, организиране и направляване на анали-тичното мислене при ситуационните анализи и при подготвянето на решения. На второ място той помага и за подреждането на информацията, необходима за тези решения, тъй като неточното определяне на субекта или обекта на сигурността и на връзката между тях може да доведе до сериозни грешки.

Съществуването на опасност или на заплаха е част от действителността, но нейното осъществяване е изцяло в сферата на бъдещето. Затова възможността то да се предвиди (т.е. навременното и точно прогнозиране) има огромно значение за обезпечаването на сигурността. Надеждните предвиждания допринасят за снижаването на равнището на неопределеност на бъдещето. Прогнозата е информация, но информация за нещо, което е изцяло напред във времето – може да се осъществи, но все още не съществува и затова не може непосредствено да се наблюдава. Затова тя винаги се определя като вторична информация (такава, която е получена чрез обработване на масиви с данни). Колкото по-мащабни и досто-верни са тези масиви и колкото по-перфектна е тяхната обработка, толкова резул-татите са по-надеждни.

2. Сигурност на система (организация)

На съвременния етап различните анализатори, като използват системния подход, определят понятието „сигурност на система" по следните начини:

- сигурността изразява количествената и качествената определеност на всеки обект (система), на неговото съществуване и развитие в съответствие със същността и собствените му параметри. Това е обективен закон, чието подце-няване или отричане закономерно води до хаос и разпадане на всеки обект (система);

- характеристика на всяка система и тя е в нейната способност да се съхрани при промяна на средата, условията и обстоятелствата, от които зависи, да функционира и се развива оптимално, т.е. при най-малък разход на ресурси да осъществи заложените в нея закономерности и цели; [9]

- динамично състояние, при което за системата (организацията) не съществуват преки опасности, а ако такива се появят, могат да бъдат надеждно отразени, като се гарантира изпълнението на целите и постъпателното развитие.

На основата на различните виждания, могат да се изведат общите, повтарящите се такива за сигурността на системата (организацията):

- количествена и качествена определеност на системата (организацията), основна (екзистенциална) необходимост за съществуване и развитие;
- устойчиво функциониране на системата (организацията);
- състояние на липса на преки опасности (заплахи) за системата (организацията);
- способност на системата (организацията) да се съхрани и развива чрез промени в съответствие с изменението на средата;
- състояние на баланс между заплахи и потенциал за защита.

Съобразно с изложените постановки може да се определи, че с понятието „сигурност" трябва да се описва състоянието на организация, която може да контролира факторите на собственото си присъствие и ефективно функциониране.

Контролирането на факторите на присъствието и функционирането на дадена организация се извършва за намаляване на ентропията (за съхраняване) чрез **реализиране на устойчивост** (запазване на параметрите на функциониране при различни въздействия) и за постоянно **развитие (растеж)**, основано на пулсиращи промени в цялата организация или в отделни нейни подсистеми.

Корелацията между устойчивост и развитие на организацията обезпечава нейната сигурност, която се постига съобразно вътрешния потенциал и условията на средата.

В съответствие с направения анализ, сигурността на организация може да се определи като: „Интегрирана устойчивост на организацията за оцеляване и функциониране (развитие) в сложна (конфликтна) среда".

3. Детерминанти на сигурността на организацията

Композирането на характеристиките на сигурността със структурата и функциите на организацията дава възможност да се систематизират **основните детерминанти**, изграждащи качеството **„сигурност"** на същата:

▪ Изграждане на организационна култура и развитие на организационните ценности. Създаване на благоприятен социалнопсихологически климат.

▪ Обезпечаване на структурно - функционална устойчивост на подсистемите (елементите). Трансформация към по-малко йерархични и повече мрежови структури и овластени групи и индивиди.

Създаване на ефективна специализирана структура за защита.

▪ Изграждане на специфичен комплекс от показатели и регулатори, които да позволят да се следи текущото поведение на организацията и да се привежда същата в съответствие със заложения алгоритъм на функциониране.

▪ Изграждане на система за ранно предупреждение и информираност за външната среда. Наблюдаване на средата и изучаване на различните явления, процеси и действия, които се отразяват неблагоприятно върху функционирането на организа-

цията. Следене на статуса, напрежението в сектора и подготовка на пред-ложения за превенция, намаляване влиянието на заплахите или тяхното неутра-лизиране.

▪ Идентификация и диагностика на вътрешно - системните фактори, които мо-гат да предизвикат критични (екстремни) състояния. Наблюдение, анализ и оценка на риска и прогнозиране развитието на различните ситуации.

▪ Събиране, анализ и съхраняване на информация, необходима за функцио-ниране на организацията и за изпълнението на регламентираните и приоритетните задачи. Администриране и контролиране на експлоатацията на информационната система и осигуряване на нейната защита.

▪ Специализирано формиране на отношението управление - самоуправление с опции за иницииране на съзидателни противоречия, динамизиращи устойчивото развитие.

▪ Реализиране на възможности за ефективно управление на всички нива, чрез осигуряване на творчество, насърчаване на неформалните връзки в звената, автоном-ност и самостоятелност, чувствителност към „слаби сигнали" и др. Пости-гане на рационалност на решенията в условията на висока неопределеност на ситуациите.

▪ Подготовка и реализиране на промени за адаптация и динамично гъвкаво развитие. Активно възпроизвеждане на иновационни идеи.

▪ Осигуряване на ресурси и насочването им към активно противодействие на дестабилизиращите фактори за оцеляване и развитие. Поддържане на необхо-димото ниво от резерви.

Литература:

1. Афанасиев, В. Общество, системност, познание и управление. С., 1991.
2. Бусленко, И. Сложные системи и моделирование. Кибернетика. М., 1992.
3. Величков, И. Сигурност. С., 2002.
4. Георгиев, Р. Делови решения и сигурност на организацията. С., 2007.
5. Давидков, Ц. Избягване на неопределеността. В: „Икономика", 1996.
6. Денчев, Ст. Несигурност, сложност, информация. С., 2004.
7. Добриянов, В. Общество - структура и развитие. С., 1992.
8. Паунов, М. Организационно поведение. С., 1997.
9. Семерджиев, Ц. Стратегическо ръководство и лидерство. С., 2007.
10. Уолтърс, П. Г. Характеристики на успешното организационно развитие. София, 1996.

ТЕХНОЛОГИИ ЗА ГЕНЕРИРАНЕ СИГУРНОСТ НА ОРГАНИЗАЦИЯТА В СРЕДАТА

Генчо Белчев Сандев

ШУ „Епископ Константин Преславски"
Технически факултет. Катедра „Управление на системите за сигурност"

Анотация. *В разработката са заложени следните направления за генериране на сигурност на организацията в средата: избор на стратегическа позиция на организацията в средата, установяване на устойчиво публично присъствие на организацията в средата, мениджмънт на проблеми в средата.*

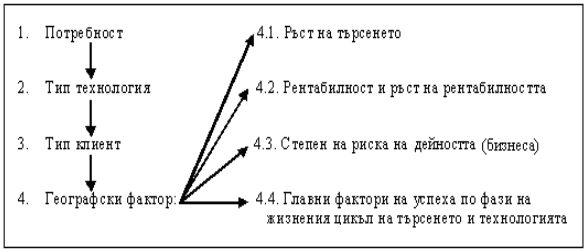
Ключови думи: *организация, среда, стратегическа позиция, стратегически ресурси, технология, устойчиво присъствие, комуникационна тактика, мениджмънт на проблеми.*

1. Избор на стратегическа позиция на организацията в средата

А. Избор на стратегическа позиция

Системата „Избор на стратегическа позиция" се основава върху изследване на възможностите за продуктивна дейност (бизнес), които съществуват вън и независимо от организацията (фирмата). От тези възможности може да се въз-ползва всеки един конкурент. Единица мярка за изследване на възможностите за продуктивна дейност представляват стратегическите бизнес зони.

Как се идентифицират стратегическите бизнес зони? Идентификацията на стратегическите бизнес зони може да се представи чрез фигура 1.



Фиг. 1

Всяка една стратегическа бизнес зона започва идентификацията си със **съответна потребност**. Когато сме открили потребността, отиваме към второ – **типът технология**, с която се задоволява потребността. Трето – от типа технология преминаваме към **типа клиент**. А типът клиент го разшифроваме чрез **географския фактор.** От географския фактор излизат следните четири вектора: ръст на търсенето (платежоспособното търсене) – т.е. да се открие броят на потребителите, които застават зад потребността и освен това са платежоспособни; рентабилността на стратегическата бизнес зона и ръстът на тази рентабилност. Третият вектор се отнася до уязвимостта на дейността в съответната бизнес зона, иначе казано, сте-

пента на риска на дейността в съответната бизнес зона. Чет-въртият вектор включва определянето на жизнения цикъл на търсенето и техно-логията и главните фактори за успех.

Определянето на жизнения цикъл на търсенето и технологията има следните фази [4]:

Първа фаза – усвояване (овладяване) на стратегическата бизнес зона. Тази фаза се характеризира с остра конкурентна борба между организациите (фирмите) коя от тях да овладее (усвои) стратегическата бизнес зона.

Втора фаза – първа фаза на растеж (P_1) **–** нарича се още фаза на победителите, в която същите жънат плодовете на своята победа. Кое я прави такава тази фаза? Отговор: това, че динамиката на търсенето е по-голяма от динамиката на предлагането. В цялата фаза е налице изпреварваща динамика на търсенето пред динамиката на предлагането.

Трета фаза – втора фаза на растеж (P_2). В началото на фазата все още динамиката на търсене е по-голяма от динамиката на предлагане, но ножицата е по-свита, отколкото във фаза P_1. Постепенно тази ножица продължава да се зат-варя. Някъде към средата има изравняване на динамиките и във втората половина на фазата имаме отваряне на ножицата в полза на динамиката на предлагането.

Четвърта и пета фази, съответно – фаза на зрелост и фаза на упадък.

Ако продължителността на срока на живот на една технология съвпада с продължителността на срока на живот на потребността, то в този случай кривата на жизнения цикъл на технологията ще лежи върху кривата на жизнения цикъл на търсенето. Но може да има (и често е така) случаи, когато жизненият цикъл на потребността е по-голям от жизнения цикъл на технологията, с която се задоволява тази потребност. Може да се каже, че най-продължителен жизнен цикъл има потребността, следва жизненият цикъл на технологията и най-кратък е жизненият цикъл на продукта.

Какви тенденции се наблюдават в жизнения цикъл на търсенето и технологията? Налице е тенденция на съкращаване продължителността на жизнения цикъл на търсенето и технологията и на фазите на този жизнен цикъл. Този факт формулира **две съществени детерминанти** за организациите (фирмите). Първо – всяка фирма е длъжна непрекъснато да прибавя нови дейности към своя бизнес портфейл. Ако не прави това, от един момент във времето ще се получи сериозен спад и вакуум в нейната дейност. Втората детерминанта изисква организациите да могат да удължават този жизнен цикъл. Кой е начинът за удължаване на жизнения цикъл на търсенето и технологията? Отговорът е: до края на фаза P_1 организацията действа на националния пазар, а от края на фаза P_2 е добре да излезе на международния пазар. И толкова пъти, колкото може да излезе на външен пазар, ще генерира съответен път на поява изживяване на жизнения цикъл.

Б. Главни фактори за успех

▪ Фактори на успеха свързани с фазите на жизнения цикъл на търсенето и технологията.

В първа фаза главният фактор на успеха е своевременната идентификация и усвояване (овладяване) на стратегическата бизнес зона.

Във втора фаза от жизнения цикъл главният фактор на успеха е производството на масов продукт, недиференциран продукт, с минимални разходи, при желаното от потребителя качество.

В трета фаза главният фактор на успеха е вътрешновидовото развитие на продукта - за всеки купувач съответен продукт, най-малкото със съответна опа-ковка. За да имаме такова вътрешновидово развитие на продукта трябва да имаме изследване на потребителското поведение и сегментиране на пазара като частен случай от стратегическата сегментация.

▪ Фактори на успеха, свързани със зоните на стратегическите ресурси, зоните на стратегическите технологии и групите на обществено влияние.

Зони на стратегически ресурси. Когато се говори за зони на стратегически ресурси се има предвид това, че в турболентна среда са ограничени възможностите на организацията да си осигури безпроблемно ресурси. В такава обстановка се налага да се разработват специални ресурсни стратегии за достъп до зоните на стратегически ресурси.

Зони на стратегически технологии. За достатъчно дълго време е било сигурно обезпечаването на организацията с необходимото й ноу-хау. Но това вече не е така, поради което възниква потребността да се разработват и стратегии за осигуряване на технологии.

Групи на обществено влияние. Най-напред става дума за новия тип потребител, новия тип купувач. Клиентът вече иска да знае всичко за продукта, интересува се освен от самия продукт като средство за задоволяване на негова потребност и от самото съдържание на този продукт. Не стига това, че купувачите стават попретенциозни, претенциозност, граничеща с капризност, но идва и поя-вата на обединения на купувачите, появата на т.нар. движение „консюмеризъм". На трето място стои нарастващата роля на държавата в икономиката, като ката-лизатор на развитието и обслужването на дейностите (бизнеса). На следващо място е появата на нови организирани екодвижения, които все по-често търсят отго-ворност и оспорват съществуването на компании от добивната, химическата промишленост, за това, че увреждат околната среда. И това не са просто забележки на тези организации към фирмите. Тези движения се превръщат в по-кошмарно за организацията явление от данъчните, от одиторските проверки и др. И тази тенденция ще се засилва.

За организациите (фирмите) е дошло време за промяна в тяхната роля. От чисто икономическо явление фирмата все повече се превръща в социално-икономическо организация. За да бъде по-малко притискана организацията трябва да има изпреварващо поведение спрямо обществото и обществените групи. А какво искат обществото и обществените групи? Те искат производството на стоки и услуги за задоволяване на техните потребности, което производство да не причинява вреди и да не бъде антисоциално. Но фирмите трябва да изпълняват това така, че да не се случи задоволяване на една потребност за сметка на други потребности, за сметка на потребностите на други поколения. Обществото иска работни места, където работниците да получават доход, работещите да се трудят при нормални условия на труд, да не е застрашено здравето им и околната среда. При тези условия организацията трябва да промени представата си за своята роля, за своята мисия, за своите функции.

2. Установяване на устойчиво публично присъствие на организацията в средата

Главната задача пред комуникационната тактика е генерирането на доверие спрямо организацията. Наличието на доверие тук означава, че субектът е в състояние

пряко да влияе върху отношението спрямо него, да ревизира процеси, свързани с дейността му и да формира нагласи в полза на организационните си цели и интереси.

Комуникационни средства: PR, реклама, пропаганда, социологически и политологически инструментариум, лобизъм [7].

Комуникационната тактика предполага следното темпорално-пространствено разположение на комуникационните средства:

Първо, PR развива в публичното пространство информационна среда, която да предполага безконфликтно, първосигнално приемане на пожеланата визия за организацията. Тук е важно да се подчертава - всъщност тази пожелана визия е повече от логична по отношение на организационното развитие на субекта, от една страна, и от друга - напълно отговаря на модерността.

Втората стъпка е паралелна на първата и предполага агресивно присъст-вие на рекламни внушения в публичното пространство. Тук се търси ефектът на тотално насищане с информация, въздействаща пряко и директно върху нагласите. Именно агресивността в това отношение постепенно налага мисленето по линия на достоверността и откритостта. Целта е те да започнат да се възприемат като характерни черти на субекта.

Третата стъпка е постигане на убеждение у публиката чрез лансиране на ясни и директни послания за идеите и тезите на организацията, посредством методите на пропагандата. Важно е да се отбележи, че при осъществяването на тази трета стъпка не бива да се прекъсва действието на първите две.

Четвъртата стъпка е да се предприеме инициатива за осъществяване на целенасочено социологическо изследване. Изводите и резултатите от него трябва да се коментират от компетентни и обществено признати специалисти. След което трябва да се осъществят и последващите политологически анализи и коментари. От гледна точка на комуникационната тактика тук е важно да се разбира правилно контролът върху информацията. Не става въпрос за инсинуиране на резултати, а за подход, който да е адекватен на нуждите на субекта. А това се постига, напр. при социологическите изследвания, като внимателно се формулират въпросите и се подредят така логически, че в крайна сметка да се наложи определен начин на мислене.

Петата стъпка е осъществяване на лобистка дейност. Тя няма да е ефективна, ако преди това не е подплатена от резултатите на разгледаното по-горе. Именно резултатът от тази пета стъпка, под формата на взети управленски решения в полза на организационните интереси, представлява фактическата материализация на комуникационната цел.

Оптималността на комуникационната тактика се заключава не само в това да се спазва логиката при използването на комуникационните средства, но и да се постига качествено натрупване, като позитив, от отделните постигнати резултати.

3. Мениджмънт на проблеми в средата - възможности за предотвратяване на конфликти

3.1. Същност и характеристики

Управляването на проблеми се развива като функция на мениджмънта, тясно свързана с обществените дела.

Мениджмънт на проблеми - управленска функция, чрез която се идентифицират потенциални или възникващи проблеми (законодателни, регулативни, политически и социални), които могат да въздействат на организацията и тогава тя

мобилизира и координира организационните ресурси и средства за стратегическо влияние върху тях.

Мениджмънтът на проблеми има за цел да прецени потенциалното въздействие на идентифицираните проблеми и с това да подпомогне стратегическото планиране.

Характеристики на мениджмънта на проблеми [6]:

▪ Да осигури на организацията ранна идентификация на проблемите и техните последствия с оглед на възможността те да повлияят върху ефективността и развитието й.

▪ Да осигури на организацията възможния най-широк спектър алтернативи за решаване на проблемите.

▪ Два елемента: идентификация и влияние образуват същността на мениджмънта на проблеми.

▪ Правилният мениджмънт на проблеми е повече проактивна функция (офанзивен подход), отколкото реактивен (дефанзивен и защитен подход).

▪ Ползата от мениджмънта на проблеми за организацията е да осигури на висшето ръководство начините за едно разумно участие в процеса на формиране на обществената политика.

3.2. Цикличен модел на проблема и въздействие

За ефективността на мениджмънта на проблеми е много важно да се разбере цикличната природа на развитието на даден проблем. **Това развитие като процес протича в четири етапа:**

А. Произход на проблема. Един проблем възниква, когато дадена организация или дадена нейна публика придават значение на доловени състояния на обкръжаващата среда, които са следствия от динамиката на политически, иконо-мически или социални тенденции и развития. Мениджмънтът на проблеми е длъ-жен да улови и идентифицира тези зараждащи се конфликтни точки, като прецени евентуалните вредни последици за организацията.

Ако организацията действа проактивно, тя би могла да прекъсне цикъла още на този етап, като разреши назряващия проблем чрез адекватна комуникационна програма за взаимодействие със засегнатите публики.

Б. Посредничество и разрастване. С активизирането на публиката и очертаването на характеристиките на проблема започва неговото разрастване сред други индивиди и групи по интереси. Включва се посредничеството на медиите, които огласяват проблема и осигуряват публичност за позициите на публиките, споделящи общи ценности и мнения (икономически и социални), както и близки виждания за действия. Посредничеството на медиите стимулира прерастването на проблема в обществен въпрос.

Преди още да се намесят медиите и проблемът да завладее масмедийното пространство, организацията може да упражни ефикасно влияние, като стимулира формиране на обществено мнение посредством активно лансиране на своята позиция и привличане в полза на своята кауза на авторитетни медии. Едновременно с това тя трябва да взаимодейства, доколкото е възможно, по-активно със засегнатите от проблема публични сегменти.

В. Организиране. Масмедийното посредничество и разгръщането на цикъла на общественото мнение подтиква групите в обществото да търсят изход от проблема, така че да се минимизират потенциалните вреди за тях и да се удовлетворят

максимално интересите им. В тази посока се извършва различна степен на взаимодействие и организираност между индивидите, както и различна степен на консолидация на групите (публиките).

Етапът на организиране дава видимост на проблема и го пренася в обществено-политическия процес. Проблемът се превръща в тема на обществения дневен ред, което подтиква и мотивира компетентните държавни институции да обмислят разрешаването му.

Г. Разрешаване. Включването на проблема в политическия процес означава, че компетентните власти ще приложат нормативно решение - закон или подзаконов нормативен акт. Регулативното действие се простира върху всички засегнати и налага ограничения на всяка от страните в конфликта - в тяхна полза или в тяхна вреда.

Окончателното разпределение на ползите и вредите обикновено зависи от ефективността, с която е бил управляван проблемът.

Всеки проблем може да отпадне в някоя от точките на цикъла по различни причини, но може да се разгърне и в пълнота до своето окончателно разрешаване. Важното е същността и механизмите на цикличния модел да се познават, което ще позволи на организацията да участва в процеса по адекватен начин. Това е значима управленска отговорност, защото краят на проблемния обществено - политически цикъл се свежда до разпределяне на ползите и вредите между засегнатите организации.

Мениджмънтът на проблеми функционира по два начина:

Първо, той идентифицира проблеми, върху които организацията не може да упражнява никакъв контрол. Това са случаи, в които общественото мнение неизбежно ще се промени в дадена насока. Ако политиките и практиките на организацията са в противовес на този съзряващ домиращ възглед, тя трябва да ги преосмисли и да ги адаптира в съответствие с него. В противен случай рискува да загуби подкрепата на своите публики и завоюваното обществено доверие.

Просветените в менижмънта на проблеми организации не само се справят с текущите проблеми, но съумяват да прогнозират публичните реакции към назряващи тревоги. На тази основа могат да се заемат лидерски позиции, като организацията своевременно и преди останалите промени своите политики и практики или въведе нови. Такава лидерска позиция не е самоцел. Тя е проява на креативност, на социална мобилност, на потенциал за организационно развитие, съобразено с динамиката на външната среда.

Второ, мениджмънтът на проблеми улавя и проблеми, върху които организацията може да упражни известен контрол, като се включи активно във възникващия публичен дебат. Системата на гражданския диалог е най-ефективният механизъм на социалния контрол. Той дава шанс на засегнатите организации в открита и етична публична комуникация да изложат своите позиции по проблема. По този начин те участват във формирането на общественото мнение и влияят върху институциите, вземащи решения.

Ранната инициатива и поемането на отговорност по управляването на проблема повишава организационния потенциал за оказване на влияние върху понататъшното развитие на проблема. Тази стъпка може да предпази организацията от неблагоприятно ориентиране на цикличния процес, при което да се наложи да се управлява истински конфликт.

Литература:
1. Ангелов, А. Организационно поведение. С., 2002.
2. Бодурова, П. Стратегиите в управлението на фирмите. С., 1999 г.
3. Маринов, Р. Кризисен мениджмънт. С., НБУ, 1997.
4. Павлов, П., Михалева С., Павлова Л. Стратегическо управление в публичния сектор. ВСУ, 2005.
5. Силаги, Е. Мениджмънт - наука, изкуство, практика. В., 1998.
6. Стойков, Л. Фирмена комуникация и култура, С., 1995.
7. Тодоров, К. Стратегическо управление. С., 1997.

РЕАЛИЗИРАНЕ НА СТРУКТУРНА УСТОЙЧИВОСТ НА ОРГАНИЗАЦИЯТА

Генчо Белчев Сандев

ШУ „Епископ Константин Преславски"
Технически факултет. Катедра „Управление на системите за сигурност"

Анотация. *В разработката са заложени основните прийоми за реализиране на структурна устойчивост на организацията: ефективно формиране на звената (групите, екипите) в организацията, коригиране на небалансирана група (екип), управление на междугруповите взаимоотношения, интервенции за устойчиво развитие на групите и устойчивост на човешките ресурси.*

Ключови думи: *организация, группа, човешки ресурси, структурна устойчивост, междугрупови взамоотношения, балансиране на группа, мотивация.*

1. Ефективно формиране на звената (групите, екипите) в организацията
Основни направления:

А. Определяне на предназначението, състава и размера на групата (екипа). Определянето на състава означава да се реши кой е подходящ за целите на групата - като знания, умения и характер. Членовете на групата трябва да си „пасват" и допълват като характери и изпълнявани дейности. Броят на членовете също ще зависи от предназначението/целите на групата.

Б. Подбор на членовете на групата (екипа) - според необходимите компетентности на типажите. Най-добре е в групата да има хора, които изпълняват различни, допълващи се роли. Предварителното проучване и познаване на нагла-сите, ценностите, перцепциите, мотивацията и поведението на всеки член дава възможност на мениджъра да определи ролята, която най-вероятно би изпълнявал индивидът в екипа.

В. Обучение на новосформирана група (екип) - чрез семинари, ролеви игри, насочени към общуването, справянето със задачи, вземането на решения, преговаряне, решаване на конфликти и др. Изграждането на екипен дух е продължителен процес, траещ поне една година.

Г. Определяне на продължителността на съществуване на групата (екипа), подходящите методи на работа и необходимите ресурси.

Д. Определяне на целите и разпределяне на задачите, процедурите, нормите и изискванията.

Е. Развиване на откритост, взаимно доверие, съпричастност и сътрудничество.

Ж. Управление на групата (екипа) - комуникации и информираност; въздействия за сплотеност; привличане в управлението на сътрудниците; индивидуална работа с всеки член; оценяване, поощряване и възнаграждаване; решаване на конфликти и др.

2. Коригиране на небалансирана група (екип)

Неравновесия в групата. За новосформираните екипи са характерни четири вида вакуум, които са заплаха и за вече установените групи. Вакуумът се характеризира с наличие на неясноти и неустановеност в определена област и бива:

- структурен вакуум - кой притежава власт, кой каква роля ще играе, каква роля ще играя аз, мога ли да бъда какъвто искам да бъда;
- вакуум на знанието - кой притежава ключова информация, знания, умения, експертност;
- емоционален вакуум - как се чувствам по отношение на хората в групата, как ме възприемат те, ще бъда ли харесван или не, приет или отхвърлен;
- вакуум на властта - кой контролира групата, кой има най-голямо влияние, кои са потенциалните съюзници/врагове, какви са моите интереси и интересите на другите членове, ще има ли конфликт.

Тези ситуации на неяснота могат да предизвикат нападателно или защитно поведение на някои от членовете на екипа. Субективно/индивидуално възприеманите напрежение, невъзможност за справяне със задачата, кратките срокове или психологическата заплаха (от доминиращ колега) карат някои от индивидите да реагират защитно или нападателно и по този начин изпълнението на задачата се затруднява, а нормалното функционирате на екипа се нарушава.

За балансиране на групата може да бъде приложена комбинация от два или повече от следните подходи:

- разместване - размяна на дейностите, извършвани от членовете на групата;
- увеличаване гъвкавостта на функциите на групата - за всеки сътрудник се проучва кои задачи изпълнява с най-голямо удоволствие и с кои се справя най-добре. На тази основа се разпределят задачите и отговорностите. Понякога може да се окаже, че даден член има желание да изпълни задачата, но му липсва компетентност - в такъв случай трябва да се подходи дипломатично;
- разделяне членовете на групата, които не се разбират помежду си - групата може да се раздели на по-малки групи, които да отговарят за различни части на технологията. При провеждане на групови срещи трябва да има някой миротворец като съекипник или координатор;
- прехвърляне или замяна с друга група - размяна на сътрудници и роли от две различни групи, ако е възможно и полезно, може да се направи;
- набиране на нови членове - ако е необходима нова роля и има възможност (ресурси) да се осигури.

3. Управление на междугруповите взаимоотношения за създаване на устойчивост

Съществуват различни методи за управление на междугруповите отношения. Всички те по същество са методи на координация, основната им цел е да предотв-

ратяват търканията, конфликтите и да създават устойчивост. Най-често използваните между тях са [5]:

▪ Правила и процедури - най-лесният и най-малко костващият метод е предварителното установяване на система от формализирани правила и процедури, които определят точно как членовете на групите трябва да си взаимодействат.

▪ Йерархия - ако правилата и процедурите са неадекватни, използването на организационната йерархия става водещият метод за управление на междугруповите процеси.

▪ Планирането улеснява координацията. Определят се специфичните цели, за които е отговорна всяка група, така че всеки да знае какво трябва да прави. Междугруповите задачи, които създават проблеми, се решават на основата на целите и приносите на всяка група.

▪ Комуникации - определяне на специална роля за връзка на дадени индивиди, които да улесняват комуникациите между взаимозависимите трудови единици.

▪ Целеви групи - създаване на временни групи за решаване на даден проблем, след което участниците в тях се връщат към обичайните си задължения.

▪ Екипи - когато задачите стават по-сложни и започват да възникват допълнително нови задачи в процеса на тяхното изпълнение, се създават постоянни екипи за решаване на възникващите проблеми.

▪ Обединяване на подразделенията в организацията - когато междугруповите отношения станат твърде сложни и горните методи стават недостатъчни.

▪ Предупреждение за назряване на противоречия преди опонентите да са ги осъзнали и да са формирали параметрите на конфликтно поведение;

▪ Предупреждение за последствията от конфликта както за опонентите, така и за организацията.

Тези методи се прилагат и развиват с оглед повишаването на ефикасността на междугруповите взаимодействия, оценявани от гледна точка на организационната ефективност (трансформирането на междугруповите конфликти в съгласувани действия) и качеството (степента, в която получените резултати се проявяват в добре дефинирано и трайно съгласие, благодарение на което методите за координиране улесняват взаимодействието, редуцират дисфункционалния конфликт и създават устойчивост).

4. Интервенции за устойчиво развитие на групите

В практиката на организационното развитие се използват следните модели за устойчивост и групова ефективност: модел за поставяне на цели, ролеви модел, междуличностен модел и решаване на проблеми.

А. Интервенциите за поставяне на цели са насочени към изясняване на общите и конкретните цели на групата. Такива срещи се прилагат обикновено на високите равнища на управление, за да се постигне общо съгласие относно стра-тегическите насоки на развитие на организацията.

В подготовката и провеждането на среща за поставяне на цели трябва да се имат предвид проблемите, които могат да възникнат от поведението на ръководителя и на членовете на групата, свързани със съвместяването на вижданията.

Поради своя характер и високата степен на структурираност интервенциите от този тип подпомагат процеса на целеполагане, планиране и разпределение на задачите и сроковете за изпълнение вътре в групата и не оказват съществено

влияние върху удовлетвореността от групата, климата, комуникацията и взаимоотношенията в нея.

Поставянето на цели е интервенция, която е уместна тогава, когато е необходимо да се определят краткосрочни цели или дълговременни стратегии от изключителна важност, свързани с оцеляването и просперитета на организацията, без да се навлиза в дълбочина във вътрешногруповите проблеми и затруднения. В този смисъл тя е с относителна ниска степен на дълбочина и поради това не носи рисковете, характерни за по-дълбоките интервенции в груповата дейност. Умелото насочване и фасилитиране на срещата е особено ценно поради опасността от изместване на фокуса от поставяне на цели към търсене на причинността за минали проблеми и събития, довели до неуспех на групата.

Б. Ролевият модел за групово развитие е широко приложим в програмите за организационно развитие, особено при новосъздадени групи, в които е нужно изясняване на ролевите очаквания, груповите норми, отговорността и задълженията на всеки член на групата. Този подход съдържа дискусия за ролите и процес на договаряне, в който ролите се приспособяват така, че да удовлетворяват както индивидуалните потребности, така и изискванията на задачата.

Ролята е съвкупност от поведения, които личността в дадена организацион-на позиция е задължена да изпълни и които хората в друга позиция очакват тя да изпълни добре. Ролята е по-широка от длъжностната характеристика. Тя включва не само формалното описание на позицията и задълженията в организационната структура, а и неформалното разбиране, съгласието, очакванията и договорността с другите, които определят начина, по който личността или групата влияе върху ролята.

Съществуват различни методи (техники) за изясняване и договаряне на ролите - анализ на ролите, преговори за ролите, карти за определяне на отговорността и др.

Този метод (техника) може да се използва и при установени постоянни трудови групи, ако възникнат проблеми с ролевата диференциация и се създаде ролева неопределеност, водеща до напрежение и конфликт.

Същността на метода е в това, че всеки споделя перцепцията си за своята роля, отчита очакванията на другите и представя своите очаквания към тях. След като дискутират всички роли, членовете на групата преразглеждат ролите си и ги представят за крайно приемане.

По отношение на договарянето на ролите се въвежда оригинална техника за изграждане на екипи, наречена преговори за ролите. Този подход се основава на презумпцията, че междуличностните проблеми, свързани с властта и влиянието, могат да бъдат преодолени чрез договаряне на желаното поведение. Такъв подход е по-подходящ за реалните условия, при които конкуренцията и властта не позволяват да се преодолеят противоречията чрез открита дискусия. Промяната се постига чрез процес на преговаряне с другите заинтересовани страни. Макар че засяга отношенията на власт и влияние в групата, тази интервенция е така структурирана, че да се избегнат симпатиите и антипатиите на членовете на групата и личните им чувства един спрямо друг.

С помощта на преговорите за ролите се установяват ролевите очаквания и желаното поведение и се разрешават потенциални или действително съществува-щи междуличностни проблеми, без обаче да се навлиза в дълбочина в тяхната същност. По тази причина ролевата техника, основана върху договарянето, е осо-бено

подходяща за организационна среда, в която има опасност от ескалиране на напрежение поради неизяснени въпроси с властта и социалното влияние.

В. Междуличностният модел включва откровени дискусии за взаимоотношенията и конфликтите между членовете на групата. Много често тези интервенции са предназначени да разгледат скрити и необсъждани проблеми, които влошават изпълнението и климата в групата, но до този момент не са се възприемали като достатъчно важни от групата. [8]

Междуличностният подход е осъществим само ако ръководителят и членовете на групата са склонни да споделят взаимните перцепции един за друг, независимо от съдържанието им. Ръководителят на групата трябва както да осъзнава междуличностните проблеми в групата, така и да проявява готовност да изложи своите убеждения и нагласи, да не наказва, да се променя и да се влияе, да е убеден, че членовете на групата разглеждат междуличностните отношения като значими. Този вид интервенции се основава върху допускането, че екипите рабо-тят най-добре в условия на взаимно доверие и открита комуникация и поради това формирането на групова сплотеност е от решаващо значение за ефективността на групата.

Г. Интервенции за решаване на проблеми. Целта им е да се изяснят проблемите, които възникват в процеса на изпълнение на дейността, да се определят възможните варианти за разрешаване на проблема и да се избере най-подходящото решение, като се развие план за действие. Съществена роля в цялостния процес на решаване на проблеми се придава на нагласата за сътрудничество и съвместна работа, която е основополагаща не само за решаване на конкретния проблем, но и за създаване на умения групата да се справя при възникване на проблемни ситуации в перспектива.

5. Реализиране устойчивост на човешките ресурси

Управление на човешките ресурси - процес за определяне на потребностите от човешки ресурси, набиране и подбор на най-подходящите служители, тяхното обучение и мотивация за ефективно изпълнение на стратегическите цели на организацията.

Цели за реализиране на устойчивост

В икономическата траектория управлението на човешките ресурси трябва да осигури:

- работници и служители, които да направят възможното организацията да постигне своите цели;
- най-подходящата работна сила на най-приемлива за организацията цена;
- такива условия на работа, които ще направят възможно пълноценното и ефективно използване на наличната работна сила;
- среда, която ще мотивира работниците и служителите да се ангажират с избраната стратегия и пълноценно да отдадат силите си за нейното постигане.

В социалната траектория управлението на човешките ресурси трябва да осигури:

- приемливи за хората безопасни и здравословни условия на труд;
- възможности за професионално - квалификационно развитие на работни-ците и служителите и за израстването им в кариерата;
- задоволство от изпълняваните трудови задачи и задължения;
- по-добър жизнен стандарт на работниците и служителите.

5.1. Справяне с трудните хора в организацията

А. Идентифициране на трудните хора [4]

В организациите работят хора с различна култура, морал и манталитет. В зависимост от ситуациите някои от тях се отклоняват от общоприетите стандарти за поведение в съвместната дейност. Степента на това отклонение ги определя като трудни, проблемни хора. Тази оценка им се дава от други лица и най-често това са техните мениджъри.

Два са основните критерия за тяхното квалифициране като трудни хора.

Първият се разпростира върху тяхната трудова дейност и поведение. Той се обективира с резултатите от дейността им.

Вторият критерий за идентифициране на трудните хора е от субективен характер. Той се базира върху оценката на едни лица относно характерологичните и други личностни качества на други лица.

Първото изискване към мениджърите е своевременно и точно да идентифицират трудните хора. Това умение мениджърите могат да култивират в своята управленска практика. Улеснени са от обстоятелството, че така наречените трудни хора се разбират по техните постъпки, по поведението им. Те създават нестандартни, обществено неприемливи ситуации. Белезите на тези ситуации са: конфликти, напрежение, влошаване на комуникациите, отчуждаване, пропускане на ползи и други.

Наличните в дадена организация проблемни, трудни хора могат да се групират по признака вреда (щета), която причиняват на организацията. Въз основа на него те могат да бъдат подредени в три групи: сътрудници, работещи незадоволително от гледна точка интересите, изискванията на организацията и създадената в нея култура; сътрудници, които не се сработват със своите колеги, като по този начин затрудняват ефикасното извършване на общата работа; сътрудници, които грубо, постоянно, но във всички случаи недопустимо нарушават наложените и приети от другите сътрудници правила, норми, организация и нравствени принципи.

Следващата стъпка в работата на мениджърите с трудните хора е да установят кои са причините, поради които те демонстрират деструктивно поведение. В основата на деструктивното поведение на някои трудни хора е техният нисък интелект, умствената им непълноценност. Тези хора не могат правилно и точно да преценяват ситуациите, в които са изпаднали или в които постоянно се намират. Причините за деструктивното поведение на друга група трудни хора се коренят в техния мързел. Те са със слабо проявена или напълно липсваща мотивация за труд. Не притежават съзнанието и чувството за дълг и отговорност към организацията, екипа, колегите. Съществена причина за демонстриране на неефективно поведение от някои сътрудници е тяхната незадоволителна квалификация. Някои от тях не притежават необходимите за трудовата им дейност знания.

Б. Целенасочено регулиране поведението на трудните сътрудници

При положение че спрямо някои сътрудници, квалифицирани като трудни, проблемни хора не се действа радикално, е наложително да се предприеме и приложи система от действия за целенасочено регулиране на тяхното поведение.

Основни стъпки:

Първа стъпка - провеждане и поддържане от мениджърите на открита политика при управление на съответните работни групи. На практика това означава да провеждат интензивни и пълноценни комуникации със своите сътрудници,

да идентифицират и оптимизират общуването си с тях. За тази цел мениджърите разчитат много на здравия си разум.

Втора стъпка - насърчаване на груповите дискусии. Те са много добро организационно средство за приучаване на трудните сътрудници открито да обсъждат проблемите си на групови срещи. Те могат да се организират и провеждат целево и за обсъждане и разрешаване на конкретна ситуация, предизвикана изцяло или частично от трудни сътрудници. Груповите срещи могат да бъдат организирани и провеждани регулярно и за обсъждане на текущи проблеми, влияещи върху поведението на трудни хора или предизвикани от него. С груповите дискусии се цели да се премахнат или ограничат различията между нейните трудни и не толкова трудни членове.

Трета стъпка - провеждане на „група – Т" сесии винаги, когато съществуват необходимите условия. Това са сесии за трениране чувствителността на трудните сътрудници, повишаване на техните социални перцепции, увеличаване на възможността им. За тази цел мениджърите създават условия за установяване и поддържане на ефикасни комуникации между хората, участвали в сесията. Събирането е с цел обсъждане на проблеми и вземане на решения. Сесиите се използват за развитието и усъвършенстването на сътрудниците, включително и онези, които се третират като трудни. В същото време се култивира и нагласа за активното им и конструктивно включване в съвместната дейност, осъществявана на групово ниво.

Четвърта стъпка - провеждане от мениджърите на консултации с външни и вътрешни експерти. Те се реализират при настъпване на сериозни затруднения и аномалии в съвместната дейност и във функционирането на отделните структури на организациите, предизвикани от така наречените трудни, проблемни сътрудници. Някои от тях могат да имат силни психични отклонения, затрудняващи и деформиращи общуването и взаимодействието им с колегите. Тези отклонения могат да предизвикат непълноценна трудова изява на индивидуално ниво. Като консултанти мениджърите могат в редица случаи да използват вътрешни експерти. Това са работещите в големите организации специалисти по психология на управлението. Оказваната на мениджърите експертна помощ от външни експерти е висококачествена.

Пета стъпка - приспособяване на трудните хора към груповите цели. Това е решителна стъпка в дейността на мениджърите по регулиране на поведението на техните трудни сътрудници. Най-добрият начин за привличане на трудните сътрудници в преследване на груповите цели е да се въздейства положително върху техни конкретни и незадоволени нужди. Въвличането на трудните сътрудници в преследване на груповите цели изисква от мениджърите да извършат следните действия:

- да се придаде необходимата важност на техния труд и на тяхната роля в дейността на групата като цяло;
- ясно да се изложат на трудните сътрудници груповите цели, тяхната важност и значение за групата, организацията и за всеки неин член;
- да се обещаят значими и впечатляващи за трудните сътрудници награди, ако се включат в постигането на груповите цели;
- мениджърите трябва да направят всичко възможно проблемните им сътрудници да почувстват, че са уважавани и желани от своите колеги и началници;

- мениджърите трябва да възлагат на ръководените от тях работни групи по впечатляващ начин задачи, спрямо които проблемните сътрудници проявяват подчертан интерес.

Шеста стъпка - превръщане на трудните сътрудници в богатство за организацията. Основни начини:

- подменяне на тривиално и неясно поставени задачи пред трудните сътрудници с възлагането на такава работа, която те могат да изпълняват на едно добро ниво;

- евентуално преназначаване на трудни сътрудници на друга, нова работа, в която те са компетентни и за която са мотивирани добре да я изпълняват;

- евентуално променяне на длъжностния статус на трудните хора в хоризон-тална посока, подобряване на условията, при които те се трудят, поощряване и стимулиране на тяхното индивидуално развитие и професионално усъвършенстване;

- съпътстващо упражняване на подходящ надзор и контрол върху поведе-нието на трудните сътрудници с отчитане на всички настъпващи в него промени и посоката на тяхното развитие;

- евентуално освобождаване от работа на определени трудни лица, тези, за които има увереност, че са безнадеждни и непоправими, тяхното заменяне с подходящи нови членове на екипите и на малките групи.

5.2. Мотивиране на персонала

Мотивиране - процес на въздействие върху човека с цел подбуждане към определени действия по пътя на пробуждане на определени мотиви.

Моделът на мотивационния процес се състои от четири основни елемента [3]:

▪ Вътрешни фактори на неравновесие: потребности, желания, подбуди и др. На този етап възниква желание да се постигне равновесие, т.е. удовлетворяване на потребностите и желанията.

▪ Поведение: насочено към възстановяването на равновесието чрез действия.

▪ Резултат: удовлетворяване на потребностите и желанията, които често се разглеждат като възнаграждение.

▪ Обратна връзка - полученото поведение определя и възнаграждението като приемливо и целесъобразно, което ще се повтори и в бъдеще.

Мотивирането е дейност, свързана с изследване на особеностите на организацията, потребностите, интересите и очакванията на сътрудниците, които могат да подбудят мотивите за високоефективна дейност при реализиране на целите на организацията.

Основни мотиватори, реализиращи устойчивост:

Първо - развитие на сътрудниците. Тази възможност може да бъде реализирана, ако в организацията съдържанието на труда се обогатява непрекъснато, той се интелектуализира и става творчески; професиите - широкопрофилни, квалификацията - многофункционална.

Развитието на сътрудниците предполага създаване на условия от организацията за тяхното непрекъснато обучение и самообучение, за творческо, професионално и личностно самоусъвършенстване.

Второ - признание и уважение. Организацията трябва да създаде условия, от една страна, за признаване на постиженията в труда и професионалното развитие на всеки сътрудник от ръководителите и неговите колеги и, от друга страна, самопризнание на собствените успехи и постигане на самоувереност и авторитет на всеки човек.

Трето - социални контакти. Когато човек е приет като част от колектива, част от определена социална група, се удовлетворява неговата потребност за социална принадлежност, за действие. Това е задължително условие както за високоефективна дейност, така и за развитие на личността. В съвременните условия най-удачна форма за организиране на персонала е работата в екип, което утвърждава социалните контакти.

Четвърто - сигурност. Представите за нея значително се промениха с възприемането на концепцията за „гъвкавата работна сила". Днес сигурността в запазването на работното място е свързана с мобилност, гъвкавост и приспособимост към промените. А това означава непрекъснато професионално развитие освен за изпълнение на трудовите задължения и за оцеляване.

Пето - работната заплата. Нейното равнище и динамика определят възможността за задоволяване не само на материалните (физиологически), но и на значителна част от духовните и социалните потребности на личността. Освен това за значителна част (а в някои организации и преобладаващата) от персонала работната заплата все още е основният, главният мотив за активно трудово участие както и за професионално развитие.

Шесто - сътрудничество между ръководителите на организацията и персонала вместо обичайните схеми на йерархично подчинение. Сътрудничеството се изгражда при единство на целите между двете страни при възприета от всички ценностна система на организацията (формализирана в морален кодекс). Това безспорно може да стане при насаждане на отношения на доверие и откритост. От една страна, ръководството дава пълна информация за своите действия, а от друга - получава непрекъснато обратна информация и, което е по-важно, изслушва всички възможни предложения и идеи от сътрудниците.

Седмо - власт за всички, основана на общи възгледи, ценности, доверие и постоянство. Овластяването на специалистите и работниците е основен елемент на сътрудничеството, но има и самостоятелно значение при мотивирането на персонала. Овластяването се разбира и се основава на предположението, че всеки човек е задвижван от вътрешния мотив да върши истинските неща по един правилен начин, независимо от неговата позиция в йерархията или равнището на власт, с която разполага. Подобен мотив се смята за основна човешка позиция, която на базата на оценката на реалната ситуация и способностите и опита на всеки един генерира съответните автономни решения. При това човекът разбира необходимостта от носене на отговорност за своето решение и за последствията от него.

Осмо - оценка на дейността на всички сътрудници. Мотивирането се постига, от една страна, чрез налагане на изисквания посредством ясно формулирани цели, стандарти и очакването, свързано с резултата (положителен или отрицателен) и, от друга страна - чрез обективно, справедливо представяне на резултатите на всеки сътрудник. Важността на оценката се обуславя от обстоятелството, че тя е в основата на изграждане на научнообосновани системи за развитието на сътруд-ниците (обучение, професионална кариера), както и за работната заплата. Така че оценката е мотивиращ фактор както с пряко действие, така и с косвено пос-редством посочените системи, които имат определящо влияние за мотивирането на сътрудниците.

Девето - човешки условия за труд и живот. Човешките ресурси, както бе посочено, се превърнаха в основен стратегически елемент за успеха на органи-зациите и затова следва да се създават условия за осигуряване на трайно развитие на този

ресурс. Осигуряването на справедливи, безопасни и здравословни условия на труд и благоприятни условия за живот на сътрудниците на организацията оказва и голямо мотивиращо въздействие.

Десето - лидерство, основано на компетентността (а не на поста в йерархията), на формиране, поддръжка и управление на взаимоотношенията; на умение за работа с група, зачитане мнението на всеки и признание на неговите резултати; на привличане на сътрудниците в управлението (овластяването им) и създаване на добър социалнопсихологически климат в колектива.

Литература:

1. Армстронг, М. Управление на човешките ресурси. Бургас, Делфин прес, 1993.
2. Джонев, С., Стратегии на ръководителя в междуличностните отношения, С., 2006.
3. Илиев, Й. Мотивация на персонала. С., 1993.
4. Минковски, Р. Социалнопсихологически мениджмънт. С.,1996.
5. Паунов, М. Организационно поведение. С., 1997.
6. Пачев, Т. Икономическа социология. С., 2001.
7. Петровски, А. В. Психологическа теория на колектива. С., 1996.
8. Стоянов, В. Организационна психология. ПСИДО - ЕООД, 2005.
9. Цанков, Ст. Организационни структури и социална дейност. С., 1993

ДЪРЖАВНА СЛУЖБА И ВИДОВЕ ДЪРЖАВНА СЛУЖБА

Димитър С. Димитров

CIVIL SERVICE AND TYPES OF CIVIL SERVICE

Dimitar S. Dimitrov

Abstract: *This report examines the civil service as the primary institution of administrative activities. It carries out in the name of the common goals and objectives pursued by the state to satisfy the interests of all society members. It is connected with the implementation of the government and organizational and functional perspectives.*

Key words: *administration, state powers, public service, civil servant*

Държавните служители заемат различни места в йерархията на държавния апарат, работят в различни отрасли или сфери на дейност, изпълняват различна по характера си работа, имат различно положение в зависимост от начина на заемане на държавната служба. Според отделните критерии могат да се направят многобройни класификации, от които тук ще разгледаме две: основни категории държавни служители и основните системи на държавната служба.

Според характера на функциите, които осъществяват, и в зависимост от характера на служебните им задължения и степента на професионалната им подготовка държавните служители са две основни категории: 1. ръководни служители; 2. експерти /специалисти.

Ръководният служител ръководи административно звено и носи отговорност за неговата работа. Категорията на ръководните служители се състои от държавни служители, които заемат ръководни постове в системата на държавния апарат или общинската администрация при осъществяване на държавната служба. Ръководните служители имат на подчинение определен брой звена и служители, спрямо които те се явяват горестоящи в административната йерархия. Те имат право да издават нареждания, да дават задължителни указания на подчинените им звена и служители, да издават задължителни за изпълнение административни актове. Например: ръководители на ведомства, като председатели и заместник-председатели на държавни агенции, директори на дирекции, началници на отдели и сектори в министерства и общини, главни секретари, административни секретари и други подобни. Към категорията на ръководните служители са предявени по-високи изисквания относно тяхното образователно и квалификационно ниво, напр. висше образование и научна степен, или квалификационна степен над висше образование по публична администрация.

Експертът изпълнява служба, подпомагаща осъществяването на функции на държавната власт. Категорията на експертите /специалистите/ се отличава с конкретния, непосредствено изпълнителен характер на тяхното участие в осъществяването на държавната служба. Към тях може да се предявяват изисквания за квалификационен ценз, свързан със специалността, по която работят и характера на работата, която изпълняват. Тук спадат такива служители, като държавни експерти, инспектори, специалисти - счетоводители, архитекти, плановици, и др. Конкретната категоризация на държавния служител зависи най-вече от длъжностната характеристика на мястото, което заема, и правомощията, които му се предоставят.

Според типовете системи на държавни служители:

В съответствие с начина и предназначението на назначаването съществуват четири основни типа на системи на държавни служители. Тези четири основни типа системи на държавните служители са :

- политическа система за назначаване на държавни служители;
- система на общата държавна служба;
- система на професионалната кариера;
- колективна система.

Политическа система за назначаване. „Политически административни служители" са тези държавни служители, които идват да работят като екипи в администрацията на определена политическа сила или политически и държавен деец, и си отиват когато политическата сила или дееца се оттегли от поста си. Към този тип у нас би трябвало да спадат държавни служители като съветниците на президента, секретаря на Министерския съвет, непосредствения административен екип на министър председателя и т.н. Тези държавни служители обикновено се назначават в службата без срок, понякога те имат властнически правомощия за определяне на насоките на държавните дейности в сферата, в която работят. Те са извън системата на общата държавна служба. Те изпълняват различни функции на различни нива на управление, свързани са и работят за различни органи на държавната власт.

Характерни за тях са липсата на сигурност за работа и високият служебен риск. В САЩ например съществуват около 7,000 такива щатни бройки на федерално ниво и заемащите ги служители се наричат „същинската връзка между политиците и администрацията".

„Политическите административни служители" като група показват някои общи тенденции, характерни за тази система на държавната служба. Най-забележителното може би е нарастващото значение на интелекта, като политическият опит и политическите им изяви в партиите са от решаващо значение в подбора им.

Втора тенденция в системата на политическите назначавания е нарастващото значение на общата подготовка за разлика от специалната подготовка на администраторите. Образованието в областта на обществените науки е все повече застъпено сред политическата администрация. Във Франция например на такива длъжности се назначават лица, завършили специалните висши училища по администрация.

Третата тенденция изразява значението на съществуващия вече опит в правителствената администрация. Много голямо предимство се отдава на предишен опит в правителството или поне в администрацията на друго отговорно ниво.

Политическата система за назначаване на държавни служители е неизбежна в една модерна администрация. При тази категория служители не може да се изисква аполитичност и политическо безпристрастие, защото то не може реално да се гарантира. Не може да се наложи на новия премиер да задържи на работа и да се доверява на секретаря на Министерския съвет, който е бил назначен и е работил преди за напусналия и минал в опозиция бивш министър председател. В интерес на работата е политическият и държавен деец да може да подбира непосредствения си екип. На по-ниските нива и на местно ниво политическите назначения могат понякога да означават по-скоро разплащане на политически дългове и отблагодаряване на политически услуги, отколкото професионално осигуряване на съответното административно управление. Системата на политическите назначавания на държавните служители трябва да се прилага ограничено. У нас към този тип спадат членовете на политическите кабинети (заместник-министрите, началниците на политическите кабинети, парламентарните секретари, началниците на звената за връзки с обществеността), заместник областните управители и заместник-кметовете на общините. Широкият кръг държавни служители и техният статут не би трябвало да се влияе от политическите промени, настъпили в държавното управление или в конкретното учреждение, даже и ако това е Министерския съвет или Народното събрание. Техните права са защитени най-вече чрез системата на общата държавна служба.

Система на общата държавна служба. Системата на общата държавна служба или общата система на държавните служители обхваща чиновническия персонал, който по принцип не включва професионалните специалисти и чието назначаване и носене на службата се извършва съобразно традиционната практика на държавната служба. Отличителна черта на тази е, че акцентът се поставя върху длъжността - длъжностна характеристика с описание на задълженията, изискванията, квалификацията, точно определяне на отговорностите и т. н. Това е и причина тази система да се нарича още и „система на длъжностите" или „система на назначенията". Докато проблемите на държавната служба при политическата система за назначаване са повече проблеми, свързани с хората, които са или ще бъдат политически административни служители, то при общата система това са проблеми на постове-

те или длъжностите в държавната администрация. Общата система на държавните служители е резултат на историческото развитие на концепциите и принципите на публичната администрация. В тази система могат да се наблюдават традиционните елементи на статута на държавните служители, възприет и от европейските законодателства. При тази система значение се отдава на характеристики като „деполитизация", „ неутралитет", „назначаване по професионални качества", „назначаване с конкурс", „стабилност", „защита на правата на държавните служители". У нас това са държавните служители, които заемат щат за държавен служител и попадат под режима на Закона за държавния служител.

Система (или по-точно системи) на професионалната кариера. Системите на професионалните кариери съществуват в различни отрасли на публичната администрация и се отнасят до точно определени професии и тяхната изява при осъществяването на държавни функции. Те обхващат държавни служители, по принцип професионални специалисти, които заемат дадена длъжност, в резултат на тяхното професионално и служебно израстване. Системата на професионалната кариера е комбинация от няколко елемента: ранно назначаване в живота с оглед на преследване и постигане на кариера в определена публична администрация; йерархическо израстване на успешни етапи и нормативно регламентирани условия за напредък; приемането, че служителят ще заема серия от последователни постове през периода на неговата кариера. Към заемането на определена длъжност от професионалната кариера не могат да се ориентират всички кандидати, притежаващи качествата за предварително поставени изисквания за заемането на тази длъжност. На такава длъжност се назначава определеният служител, който показва всички съвкупни качества да бъде назначен на такава длъжност. Основната характеристика на системата на професионалната кариера за разлика от общата система на държавните служители е, че акцентът е поставен повече върху личността, отколкото върху длъжността, но за разлика от политическата система тук личността се преценява не толкова от страна на личните й качества, колкото от съответни нейни качества, проявени в предишната й длъжност. Според системата на професионалната кариера индивидуалната професионална кариера, служебното израстване на конкретен специалист се осъществява планово, служителят очаква да напредне последователно посредством няколко йерархически длъжностни постове, които отговарят на неговия професионален опит и развитие. Добър пример за спецификата на служителите по тази система са служителите в дипломацията и ранговете в тяхната дипломатическа кариера. Тук спада и кариерата във военната служба, а с някои уговорки може да се приобщи и академичната кариера в държавни институции (капитанът става майор; асистентът - главен асистент и т.н.).

Колективната система. Тази система обхваща преди всичко служителите, които извършват материално-техническа дейност и работниците-специалисти, работещи в администрацията. Техните трудови отношения се уреждат с договори между ръководителя на учреждението или органа и работника. Колективната „система" е по-скоро категория персонал в държавната администрация, отколкото вид система различаваща се от останалите. Тя обхваща предимно материално-техническите лица и обслужващия персонал. Тук влизат технически сътрудници, изпълнители, секретарки, и компютърни оператори, шофьори, техници по поддръжката и т.н. У нас това са служителите в администрацията, които работят по трудов договор и се намират под режима на Кодекса на труда.

ДЪРЖАВЕН СЛУЖИТЕЛ

В Закона за държавния служител се урежда възникването, съдържанието и прекратяването на служебните правоотношения между държавата и държавния служител при и по повод изпълнението на държавната служба, доколкото друго не е предвидено в специален закон.

Държавен служител

Държавен служител е лице, което по силата на административен акт за назначаване заема платена щатна длъжност в държавната администрация и подпомага орган на държавната власт при осъществяване на неговите правомощия. Държавни служители са и лицата, на които специален закон предоставя статут на държавен служител при спазване изискванията на този закон.

Длъжностите, които се заемат от държавни служители, се определят в Класификатора на длъжностите в администрацията, който се приема от Министерския съвет и се обнародва в "Държавен вестник".

Не са държавни служители по смисъла на този закон лицата, които:

- са еднолични органи или техни заместници;
- са членове на колегиални органи;
- са членове на политически кабинети или съветници и експерти към тях, с изключение на ръководителя на звеното за връзки с обществеността;
- изпълняват технически функции в администрацията.

Изисквания при изпълнение на държавната служба. Държавният служител при изпълнение на своята служба се ръководи от:

- закона и законосъобразните актове на органите на държавната власт;
- спазването и защитата на правата, законните интереси и свободите на гражданите;
- интересите на държавата.
- Държавният служител при изпълнение на своята служба трябва да бъде политически неутрален.

Видове държавни служители

В зависимост от характера на служебните си задължения и степента на професионалната си подготовка държавните служители са ръководни служители и експерти. Ръководните служители, които заемат длъжностите главен секретар, секретар на община, главен директор на главна дирекция, директор на дирекция и ръководител на инспекторат, са висши държавни служители. Експертът изпълнява служба, подпомагаща осъществяването на функции на държавната власт.

Възникване на служебното правоотношение

Изпълнение на държавна служба. Държавният служител изпълнява държавната служба въз основа на назначаване от компетентен орган на държавна власт. За държавен служител може да бъде назначено лице, което:

- е български гражданин, гражданин на друга държава - членка на Европейския съюз, на друга държава - страна по Споразумението за Европейското икономическо пространство, или на Конфедерация Швейцария;
- е навършило пълнолетие;
- не е поставено под запрещение;
- не е осъждано за умишлено престъпление от общ характер на лишаване от свобода;
- не е лишено по съответен ред от правото да заема определена длъжност;

– отговаря на специфичните изисквания, предвидени в нормативните актове за заемане на съответната длъжност.

Не може да бъде назначавано за държавен служител лице, което:

– би се оказало в йерархическа връзка на ръководство и контрол със съпруг или съпруга, с лице, с което е във фактическо съжителство, роднина по права линия без ограничения, по съребрена линия до четвърта степен включително или по сватовство до четвърта степен включително;

– е едноличен търговец, неограничено отговорен съдружник в търговско дружество, управител, търговски пълномощник, търговски представител, прокурист, търговски посредник, ликвидатор или синдик, член на орган на управление или контрол на търговско дружество или кооперация;

– е народен представител;

– е съветник в общински съвет - само за съответната общинска администрация;

– заема ръководна или контролна длъжност в политическа партия;

– работи по трудово правоотношение, освен като преподавател във висше училище.

За висши държавни служители, както и на длъжности, свързани с изпълнението на функции в областта на отбраната, обществения ред, външната политика, националната сигурност и опазването на държавната тайна, могат да се назначават само български граждани.

На ръководни длъжности могат да бъдат назначавани само лица с висше образование.

При заемане на държавна служба не се допускат дискриминация, привилегии или ограничения, основани на раса, народност, етническа принадлежност, пол, произход, религия, убеждения, членуване в политически, синдикални и други обществени организации или движения, лично, обществено и имуществено положение или на наличие на увреждане.

Постъпването на държавна служба в съответната администрация задължително се предхожда от конкурс, т.е. назначаването на всяка длъжност на държавен служител се извършва чрез конкуренция, основана на професионални качества.

Конкурсната комисия се състои от трима до седем членове. Поименният състав на комисията се определя със заповед на органа по назначаването. В състава на комисията задължително се включват непосредственият ръководител на свободната длъжност, служител или лице с юридическо образование и представител на звеното "Човешки ресурси".

Конкурсната комисия провежда конкурса по обявения начин, като преценява професионалните и деловите качества на кандидатите и класира от първо до трето място най-успешно издържалите конкурса.

Когато кандидатът се назначава за първи път на държавна служба, в едногодишен срок, считано от датата на встъпване в длъжност, *органът по назначаването може да прекрати служебното правоотношение без предизвестие*.

Статут на държавния служител

Изпълнението на държавната служба се основава на принципите на законност, лоялност, отговорност, стабилитет, политическа неутралност и йерархична подчиненост. Държавата създава необходимите условия за изпълнението на задълженията на държавния служител, като го защитава при законосъобразното изпълнение на

служебните задължения и обезщетява него и семейството му за вреди, причинени при и по повод на изпълнение на държавната служба.

Задължения на държавния служител

Задължения към гражданите

Държавният служител е длъжен да се произнася без забава по искането на гражданите. Той трябва да удовлетворява точно и своевременно тези от тях, които са законосъобразни, и да съдейства за признаването на техните права и законни интереси. Държавният служител е длъжен да не проявява грубост, невъзпитание и неуважение към гражданите, които обслужва.

Задължение за подпомагане и съдействие на органите на държавната власт

Държавният служител е длъжен активно да подпомага и съдейства на органите на държавната власт при осъществяване на техните правомощия.

Задължение за спазване на работното време

Държавният служител е длъжен да спазва установеното работно време и да го използва за изпълнение на възложените му задължения.

Йерархична подчиненост

Държавният служител е длъжен да изпълнява законосъобразните актове и заповеди на по-горестоящите органи и държавни служители, но не е длъжен да изпълни неправомерна заповед, издадена по установения ред, когато тя съдържа очевидно за него правонарушение или да изпълни нареждане, насочено срещу него, неговата съпруга или съпруг, роднини по права линия без ограничения, по съребрена линия до четвърта степен и по сватовство до втора степен включително. В такъв случай той е длъжен незабавно да уведоми органа, от когото е получил нареждането, който от своя страна трябва да възложи изпълнението на друг служител или да го извърши сам.

Защита на класифицираната информация, представляваща държавна или служебна тайна

Държавният служител е длъжен да защитава класифицираната информация, представляваща държавна или служебна тайна, станала му известна при или по повод изпълнение на служебните му задължения. Класифицираната информация, представляваща държавна или служебна тайна, както и редът за работа с нея се определят със закон.

Задължение за опазване престижа на държавната служба

При изпълнение на служебните си задължения и в обществения си живот държавният служител е длъжен да има поведение, което да не уронва престижа на държавната служба и да съответства на Кодекса за поведение на служителите в държавната администрация, като последния се приема от Министерския съвет и се обнародва в "Държавен вестник".

Задължение за деклариране на имотното състояние

При встъпването си в длъжност държавният служител е длъжен да декларира своето имотно състояние пред органа по назначаването. Всяка година до 30 април държавният служител е длъжен да декларира пред органа по назначаването своето имотно състояние, както и получените през предходната календарна година възнаграждения, свързани с полагане на труд извън служебното правоотношение, основанията за тяхното получаване, както и възложителя/работодателя, който ги е изплатил.

Права на държавния служител

Право на заплата.

За изпълнение на държавната служба държавният служител има право на брутна заплата, която включва основна заплата и допълнителни възнаграждения.

Право на почивка.

При изпълнение на държавната служба държавният служител има право на почивки по време на работния ден, на междуседмична и междудневна почивка и на обявени официални празници.

Право на отпуск. Държавният служител има право на редовен платен годишен отпуск. Държавният служител има право и на допълнителен отпуск, на служебен отпуск, на отпуск за изпълнение на обществени задължения, на отпуск по социалното осигуряване и на неплатен отпуск.

Професионална квалификация. Органът по назначаването осигурява условия за повишаване на професионалната квалификация и преквалификация на държавния служител. Когато нуждите на службата налагат, разходите за повишаване на професионалната квалификация и преквалификация на държавния служител са за сметка на съответната администрация.

Повишаване в държавна служба. Повишаването в държавна служба се осъществява чрез последователно преминаване в по-висок ранг или длъжност.

Социално и здравно осигуряване. Държавният служител има право на задължително социално и здравно осигуряване като то става за сметка на съответните бюджети.

Безопасни и здравословни условия на труд. Държавният служител има право на безопасни и здравословни условия на труд съгласно Закона за здравословни и безопасни условия на труд и нормативните актове за неговото прилагане.

Свобода на мнението. При изпълнение на служебните си задължения държавният служител има право свободно да изказва мнения относно законосъобразността и целесъобразността на дадените му нареждания и да предлага по-удачни решения. Изказаните мнения и предложения не могат да засягат служебното положение на държавния служител.

Членство в политическа партия. Държавният служител има право да членува в политически партии, доколкото не съществува забрана, установена в специален закон, но при осъществяване на службата си държавният служител не може да се ръководи и да защитава интересите и волята на политическата партия, в която членува.

Право на изявления. Държавният служител може да прави изявления от името на органа по назначаването или администрацията със съгласието на органа по назначаването или на определен от него служител.

Право на неприкосновеност на личната кореспонденция и съобщения. Държавният служител се ползва с неприкосновеност на личната си кореспонденция и съобщения, но кореспонденцията и съобщенията, адресирани до държавен служител в това му качество, не се считат за лични.

Рангове и повишаване в длъжност

Рангове. Рангът е израз на професионалната квалификация на държавния служител като съвкупност от знания и умения, необходими за качествено изпълнение на длъжността. Ранговете на държавните служители се разделят в две групи: "младши ранг" и "старши ранг". Младшият и старшият ранг имат по пет степени.

Повишаване в ранг. Повишаването в ранг се извършва въз основа на годишната оценка на изпълнението на длъжността на държавния служител: при две или три

последователни годишни оценки - за младшите рангове, и при три или четири последователни годишни оценки. Държавният служител се повишава в следващия по-висок ранг преди минималните срокове, при условие че е получил най-високата годишна оценка на изпълнението на длъжността.

Оценяване на изпълнението на длъжността. Държавният служител ежегодно се оценява за изпълнението на длъжността. Оценяването на изпълнението на длъжността обхваща периода от 1 януари до 31 декември на съответната година. Всеки служител, който има действително отработени най-малко 6 месеца за една календарна година, подлежи на оценяване. Оценяването на изпълнението на длъжността на служителя се извършва от оценяващ ръководител, на когото служителят е непосредствено подчинен. Оценяването на изпълнението на длъжността се извършва въз основа на:

– постигането на предварително определени цели или изпълнението на преките задължения и поставените задачи;
– показаните компетентности.

Изменение на служебното правоотношение

Стабилитет. Служебното правоотношение на държавния служител не може да бъде едностранно изменяно, освен в случаите и по реда, предвидени в този закон.

Преминаване на държавна служба в друга администрация. Държавен служител, който работи в една администрация и едногодишният срок за изпитване е изтекъл, може да бъде назначен на длъжност в друга администрация, ако отговаря на условията за нейното заемане и след сключване на писмено споразумение между него и органите по назначаване на двете администрации.

Временно преместване в друга администрация. Държавен служител може да изпълнява длъжност в друга администрация за срок до 4 години, ако отговаря на условията за нейното заемане, едногодишният срок за изпитване е изтекъл и служебното му правоотношение е безсрочно.

Когато временното преместване в друга администрация е свързано със смяна на населено място, органът по назначаването в тази администрация е длъжен да изплати на държавния служител:

– пътните разноски за него и за членовете на семейството му;
– разноските по пренасяне на покъщнината му;
– заплатата за дните на пътуване и за още два дни.

Изпълняване на длъжност в институция на Европейския съюз. Държавен служител може да бъде изпратен да изпълнява длъжност в институция на Европейския съюз за срок до 4 години. За срока на изпълнението на длъжност в институция на Европейския съюз държавният служител запазва служебното си правоотношение и продължава да получава от органа по назначаването основната си месечна заплата.

Отличия и служебна отговорност .

Отличия. За образцово изпълнение на служебните си задължения държавният служител може да бъде награждаван с отличия със заповед на органа по назначаването или на лицето по чл. 6, ал. 2 от ЗДС, която се оповестява по подходящ начин от органа по назначаването. Отличията са:

– грамота;
– сребърен почетен знак на съответната администрация;
– златен почетен знак на съответната администрация.

Литература:
1. Балабанова, Хр.; "Администрация на изпълнителната власт в "Законодателството на Република България"; "Албатрос"; 2000
2. Величков И., Бенев Б., Държавна администрация, част втора, ЕкоПринт, С., 2004
3. Димитров Д., Административно право. Обща част, Сиела, С., 2006
4. Димитров Д., Държавнослужебно право на Република България, Сиела, С., 2010
5. Друмева Е., Конституционно право, Сиела софт енд паблишинг, С., 2008
6. Казанджиева М., Правен режим на държавната служба, С., 2007
7. ЗАКОН ЗА АДМИНИСТРАЦИЯТА, Обн. ДВ. бр.130 от 5 Ноември 1998г., изм. и доп. ДВ. бр.15 от 21 Февруари 2012г.
8. ЗАКОН ЗА ДИПЛОМАТИЧЕСКАТА СЛУЖБА, Обн. ДВ. бр.78 от 28 Септември 2007г, изм. ДВ. бр.38 от 18 Май 2012г.
9. ЗАКОН ЗА ДОСТЪП ДО ОБЩЕСТВЕНА ИНФОРМАЦИЯ, Обн. ДВ. бр.55 от 7 Юли 2000г., изм. ДВ. бр.39 от 20 Май 2011г.
10. ЗАКОН ЗА ДЪРЖАВНИЯ СЛУЖИТЕЛ, Обн. ДВ. бр.67 от 27 Юли 1999г., изм. и доп. ДВ. бр.38 от 18 Май 2012г.

ОТГОВОРНОСТ НА ДЪРЖАВНИЯ СЛУЖИТЕЛ ПРИ ИЗПЪЛНЕНИЕ НА СЛУЖЕБНИТЕ МУ ЗАДЪЛЖЕНИЯ

Димитър С. Димитров

RESPONSIBILITY OF THE CIVIL SERVANT IN THE PERFORMANCE OF HIS DUTIES

Dimitar S. Dimitrov

Abstract: *This report deals the achievement of organizational efficiency by using various forms of control which in certain cases has a sanctioning character. Determination of deviations from the norm is combined with the implementation of various policies against violators. Therefore, the law provides disciplinary responsibility for the administrative staff.*
Key words: *organizational efficiency, control, disciplinary responsibility, sanctions*

Дисциплинарната отговорност на държавния служител е само една от правните отговорности, които той съгласно действащото законодателство носи за своето противоправно поведение в това му качество. Законът за държавния служител подробно регламентира дисциплинарната отговорност и реда за нейното реализиране, като в отделни текстове той съдържа и останалите правни отговорности, чието търсене и реализиране подробно са уредени в действащото административно, гражданско и

наказателно процесуално законодателство. Този факт обаче не е основание да се счита, че само дисциплинарното наказание на държавните служители е част от правната проблематика относно държавната служба и „те също следва да бъдат отбелязани"[1].

Дисциплинарната отговорност на държавния служител се различава и от дисциплинарната отговорност на работниците и служители, работещи в държавната администрация по трудово правоотношение. Дисциплинарната отговорност на държавните служители е заради неспазване на служебни задължения, докато тези на служителите в държавната администрация по трудово правоотношение - заради неспазване на трудови задължения, за нарушаване на трудовата дисциплина. Редът за правна защита при незаконно дисциплинарно наказание също е различен. Работещите по трудово правоотношение използват общия гражданскоправен път за правна защита, а държавните служители - административните съдилища.

Проблемът за политическата отговорност на държавните служители не съществува, доколкото Законът за държавния служител и специалните закони са въвели принципа за политическата неутралност при изпълнение на държавната служба. За някои категории държавни служители дори има забрана за членуване в политически партии. Нарушаването на принципа за политическа неутралност ще влече съответната **юридическа отговорност.**

Всички видове юридическа отговорност, които държавният служител носи, имат своята служебна характеристика, доколкото нейни адресати са държавни служители, допуснали съответните правни нарушения в това им качество. Такава характеристика има и дисциплинарната отговорност на държавния служител.

Какви са основанията за търсене и реализиране на дисциплинарна отговорност на държавния служител

Безспорно най-авторитетният специалист по въпросите на чиновническото право у нас акад. Петко Стайнов още през тридесетте години на двадесетия век е писал: „Правилното и полезно функциониране на една служба изисква спазване на установен вътрешен ред: определен час за започване и завършване на работата, йерархическо подчинение, прилични обноски с началството и публиката, експедитивност, редовност, добро поведение, пазене на служебната тайна и т.н. Всяко нарушение на този ред съставлява дисциплинарно нарушение и се свързва със съответно наказание".

Основанията за търсене и реализиране на дисциплинарна отговорност на държавния служител са най-доброто средство за даване отговор на въпроса за същността на този вид правна отговорност.

Тези основания са посочени в Закона за държав**ния служител и в специалните закони. В настоящото изложение се имат пред вид само разпоредбите, съдържащи се в Закона за държавния служител. От посочените в Закона за държавния служител основания би могло да се обособи едно обобщаващо основание - неизпълнено служебно задължение във вид на дисциплинарно нарушение.** То обуславя в частност служебния характер на дисциплинарната отговорност на държавния служител. Този служебен характер на дисциплинарната отговорност на дър-

[1] М. Казанджиева. Правен режим на държавната служба. С., 2007 г., с. 184.

жавния служител е присъщ на работника и служителя, работещ по трудово правоотношение.

Неизпълнението на служебните задължения, като основание за дисциплинарна отговорност на държавния служител, следва да се изрази в извършено дисциплинарно нарушение.

Като всяко правно нарушение и дисциплинарното нарушение трябва да де човешко деяние (действие или бездействие), то да е обществеоопасно, противоправно, да е извършено виновно, да е довело до неблагоприятни резулт, т.е. неблагоприятните резултати да са в причинна връзка с правонарушението.

Особеност при дисциплинарното нарушение е, че неблагоприятните резултати от него засягат държавнослужебното правоотношение, нормалното и ефективно осъществяване на държавната служба в държавната администрация[2].

Конкретните основания, т.е. дисциплинарните нарушения за търсене и реализиране на дисциплинарна отговорност на държавния служител, посочени в Закона за държавния служител, са [3]:

– дейност, която е извън длъжностната характеристика на заеманата длъжноет или не следва от нейния характер;

– не осъществяване на служебна дейност, която е включена в длъжностната характеристика на заеманата длъжност;

– неспазване установеното работно време;

– неизползвано работно време за изпълнение на възложените задължения;

– неизпълнение на законосъобразните заповеди на органа по назначаването или на по-високостоящи държавни служители;

– забавено изпълнение на служебните задължения, т.е. след установени срокове за дължимо изпълнение;

– неспазване на кръга на служебните правомощия на държавния служител с което чрез превишаване на власт е осъществил чужди правомощия - на по-вис- стоящите по длъжност и ранг държавни служители, на органа по назначаване- или на друг по-горестоящ държавен орган. При условие когато в самата длъжностна характеристика на заеманата длъжност ясно са указани служебните му правомощия.

– нарушение на задълженията на държавния служител спрямо гражданите, които са указани в чл. 20 на ЗДС;

– неспазване на правилата на Кодекса за поведение на служителите в държавната администрация;

– неизпълнение на задълженията за точно, добросъвестно и безпристрастно в съответствие със законите на страната и устройствените правилници на съответната администрация;

– необръщане внимание на оплаквания на гражданите от страна на държавен служител на служител, заемащ ръководна длъжност (е „ръководител") за извършени дисциплинарни нарушения от подчинени му държавни служители (чл. 89, ал. 3ДС). В случая дисциплинарната отговорност се носи не от всеки държавен служител, а само от този, който е в положение на „ръководител";

---

[2] Димитров Д,. Държавнослужебно административно право, Сиела, С., 2010

[3] ЗАКОН ЗА ДЪРЖАВНИЯ СЛУЖИТЕЛ, В сила от 27.08.1999 г., изм. и доп. ДВ. бр.38 от 18 Май 2012.

– основание за дисциплинарна отговорност е и неизпълнението на удължението за уведомяване за наличие на някое от основанията за недопустимост;

– не е спазил изискването за йерархическа подчиненост - да изпълнява законосъобразните заповеди на по-горестоящите органи и държавни служители (чл. 24, ал. 1 ЗДС);

– не е защитил класифицирана информация, представляваща държавна или служебна тайна, станала му известна при или по повод изпълнение на служебните му задължения (чл. 25, ал. 1 ЗДС);

– не е изпълнил задълженията си за уведомяване за наличие на някое от основанията за недопустимост (чл. 24 ЗДС);

– не е опазил, уронил е престижа на държавната служба (чл. 28, ал. 1 ЗДС);

– недекларирane на имотното си състояние (чл. 29 ЗДС);

– не е изпълнил задължението си за разкриване и за избягване на конфликт на интереси (чл. 29а, ал. 1 ЗДС);

– не е изпълнил задължението си да уведоми, да не участва в обсъждането, подготовката и вземането на решения, които той или свързани с него лица са заинтересовани от съответното решение или когато има със заинтересованите лица отношения, пораждащи основателни съмнения в неговата безпристрастност (чл. 29а, ал. 2 ЗДС);

– не е изпълнил задължението си до 31 март ежегодно да декларира писмено пред органа по назначаването всеки търговски, финансови или други делови интереси, които той или свързани с него лица имат във връзка с функциите на администрацията, в която работи (чл. 29а ЗДС).

Не всяко неизпълнение на служебно задължение е основание за дисциплинарна отговорност. Самият Закон за държавния служител посочва хипотези, при които такава отговорност не се търси. Така съгласно разпоредбата на ал. 2 на чл. 24 ЗДС държавният служител не е длъжен да изпълни неправомерна заповед, издадена по установения ред, когато тя съдържа очевидно за него правонарушение. Държавният служител може да поиска писмено потвърждение на служебния акт, когато в отправената до него устна заповед съдържа очевидно за него правонарушение (ал. 3 на чл. 24 ЗДС). Държавният служител не е длъжен да изпълни нареждане, насочено срещу него, неговите съпруг, или съпруга, роднини по права линия без ограничения, по съребрена линия до четвърта степен включително и по сватовство до втора степен включително. В такъв случай той е длъжен незабавно да уведоми органа по назначаването, от когото е приел нареждането, който от своя страна трябва да възложи изпълнението на друг държавен служител или да го извърши сам (ал. 4 на чл. 24 ЗДС).

Дисциплинарно наказващи органи

По този въпрос законодателят е категоричен - това са преди всичко органите по назначаване в съответната администрация. Дисциплинарните им правомощия се основават на присъщата им дисциплинарна власт спрямо всички държавни служители в конкретните администрации, и които са пасивната страна на отделните държавнослужебни правоотношения. Тези правни отношения са възникнали въз основа на техни правни актове - заповед за назначаване.

Органите по назначаване са основните дисциплинарно наказващи органи. Това е принципът. Разпоредбата на чл. 92, ал. 1 на ЗДС гласи: „Дисциплинарните наказания се налагат от органа по назначаването...".

Но законодателят допуска и изключение от принципа. Това изключение се съдържа в същата разпоредба, която завършва с думите „с изключение на случаите по чл. 6, ал. 2 и 3".

А случаите по чл. 6, ал. 2 и 3 показват, че законодателят, макар и под условие, е предоставил ролята на дисциплинарно наказващи и на други субекти, извън органа по назначаването. Такива са главният секретар, ръководителите на териториални звена или на териториални поделения, създадени с нормативен акт. Тези субекти могат да бъдат дисциплинарно наказващи само при изрично възлагане на дисциплинарно наказващи правомощия от органа по назначаването. Освен това тяхната дисциплинарно наказателна отговорност е ограничена до налагането на по-леките дисциплинарни наказания - забележка и порицание.

Подлежащи на дисциплинарна отговорност лица

Подлежащите на дисциплинарна отговорност лица по Закона за държавния служител са преди всичко държавните служители. Те са такива едва след фактическото им встъпване в длъжност, предхождано от назначаване и полагане на клетва, чрез подписване на клетвен лист. Това се отнася за държавните служители, които встъпват в държавно служебно правоотношение чрез конкурс.

Освен тях, подлежащи на дисциплинарна отговорност са и държавните служители, които по изключение заемат длъжността за държавен служител без проведен конкурс. Сред тази категория са и лицата, чиито заемани по-рано длъжности в държавната администрация са обявени за заемане по държавно служебно правоотношение и те по съответния ред и изпълнени условия са заели длъжността по държавно служебно правоотношение.

На дисциплинарна отговорност са подложени и стажантите по смисъла на Закона за държавния служител, независимо че не са държавни служители и стажантската им дейност не съставлява изпълнение на държавна служба по смисъла на Закона за държавния служител. Те носят на общо основание дисциплинарна отговорност при извършено от тяхна страна дисциплинарно нарушение при и по повод изпълнението на стажантските им задължения.

На дисциплинарна отговорност подлежат всички държавни служители, без оглед дали тяхното държавно служебно правоотношение е безсрочно или срочно и дали то е първо по ред или е в резултат на повишаване в държавна служба.

Само служебно дееспособни лица подлежат на дисциплинарна отговорност.

Дисциплинарното наказание - начин за реализиране на дисциплинарната отговорност

Дисциплинарната отговорност на държавните служители и стажантите на практика се реализира чрез налагането на предвидените в ЗДС дисциплинарни наказания. В това отношение Законът за държавния служител не препраща към аналогични разпоредби в Кодекса на труда.

Дисциплинарното наказание е неблагоприятна правна последица от извършено дисциплинарно нарушение. Чрез него се осъществява държавната дисциплинарна репресия по отношение на извършилите дисциплинарни нарушения държавни служители и стажанти в държавната администрация по Закона за държавния служител.

Дисциплинарното наказание по време на налагането му е винаги след факта на извършеното дисциплинарно нарушение. Но за да постигне комплекса от своите цели, дисциплинарното наказание следва да се осъществява в кратки срокове.

Едно дисциплинарно нарушение се открива с факта на узнаване от дисциплинарно наказващия орган на самото дисциплинарно нарушение, неговия извършител, времето и мястото на извършване.

Видове дисциплинарни наказания по ЗДС

Законът за държавния служител посочва изчерпателно видовете дисциплинарни наказания за извършени дисциплинарни нарушения от държавни служители и стажанти по смисъла на Закона за държавния служител.

Тези наказания са:

- забележка;
- порицание;
- отлагане повишението в ранг е една година;
- понижение в по-долен ранг за срок от шест месеца до една година;
- уволнение.

Първите две нарушения имат ярко изразено морално съдържание, но запазват юридическата си същност и правни последици, с оглед бъдещи оценки на поведението на наказания.

Друго е със следващите две наказания - те се очертават като специфични само за държавно служебното право, тъй като засягат качество, присъщо само на държавен служител - неговия ранг, с оглед отлагане на повишаване в по-висок ранг, респ. понижаване в по-долен ранг за указаните срокове.

Производства за реализиране на дисциплинарна отговорност на държавния служител по специални закони

Производство за реализиране на дисциплинарна отговорност на държавния служител по Закона за Министерството на вътрешните работи [4]

Проблемът с дисциплинарната отговорност на държавните служители в МВР е регламентиран с разпоредбите на Глава шестнадесета на Закона за Министерството на вътрешните работи.

Съгласно тези разпоредби дисциплинарните наказания на държавните служители и в МВР се налагат при извършени дисциплинарни нарушения по смисъла на Закона за Министерството на вътрешните работи. Те са правното основание за реализирането на дисциплинарната отговорност спрямо държавните служители в МВР. Основанието - нарушена служебна дисциплина.

Дисциплинарните нарушения, заради които се носи дисциплинарна отговорност държавните служители, са посочени в разпоредбата на ал. 2 на чл. 224 на Закона за МВР[5].

Държавните служители в МВР носят дисциплинарна отговорност, независимо че деянията им могат да са основание за търсене и на друг вид правна отговорност.

Дисциплинарните наказания се налагат не по-късно от два месеца от откриване на нарушението и не по-късно от една година от извършването му.

Когато дисциплинарното нарушение е и престъпление или административно нарушение, посочените срокове за налагане на наказанието започват да текат от влизане в сила на присъдата или на наказателното постановление. Тези спорове не текат,

[4] Законът за МВР е обнародван в ДВ, бр. 17/2006 г

[5] ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ, В сила от 01.05.2006 г., доп. ДВ. бр.38 от 18 Май 2012г.

когато държавният служител е в законоустановен отпуск или му е наложена мярка за неотклонение задържане под стража или домашен арест.

За едно и също дисциплинарно нарушение може да се наложи само едно дисциплинарно наказание.

Наказанията се налагат със заповеди, както следва:

от министъра на вътрешните работи - за всички наказания, предвидени в Закона за МВР за стажантите и служителите от категории А, Б, В, и Г, без наказанието „уволнение", ако служителят е назначен с указ на президента на Република България;

– от директорите на главните дирекции, на областните дирекции, на специализираната дирекция „Оперативни технически операции", на дирекция „Вътрешна сигурност", на специализираните административни дирекции, на Медицинския институт, на научноизследователските и научно-приложните институти и ректорът на Академията та МВР - наказанията мъмрене, писмено предупреждение и порицание;

– от служителите на длъжност „началник на сектор", приравнените на нея и повисока - за наказанията мъмрене, писмено предупреждение и порицание;

– от служители на длъжност „началник на група" и приравнените на нея за наказанията мъмрене и писмено предупреждение.

Дисциплинарнонаказващият орган е длъжен преди налагане на дисциплинарното наказание да изслуша държавния служител или да приеме писмените му обяснения, освен когато по зависещи от държавния служител причини той не може да бъде изслушан или да даде писмено обяснение.

При определяне вида и размера на дисциплинарните наказания се взема: предвид тежестта на нарушението и настъпилите от него последици, обстоятелствата при които е извършено, формата на вината и цялостното поведение на държавния служител по време на службата.

За разкриване на обективната истина могат да се използват всички налични средства, допустими от закона.

Производство за реализиране на дисциплинарна отговорност на държавния служител по Закона за отбраната и въоръжените сили на Република България

Дисциплинарната отговорност на военнослужещите - държавни служители, е регламентирана в Глава седма, раздел XI на Закона за отбраната и въоръжените сили на Република България[6], а редът за налагане, изпълнение и заличаване на дисциплинарните наказания се уреждат в Правилника за приложение на закона за отбраната и въоръжените сили на Република България.

Виновното неизпълнение на служебните задължения от военнослужещите е нарушение на военната дисциплина.

Нарушителят на военната дисциплина се наказва с дисциплинарните наказания по ЗОВС РБ независимо от предвидената имуществена, административнонаказателна или наказателна отговорност.

За едно и също нарушение на военната дисциплина може да се наложи само едно дисциплинарно наказание.

Дисциплинарното наказание уволнение се налага задължително в следите случаи:

- осъждане за умишлено престъпление от общ характер или лишаване от право да заема държавна длъжност или да упражнява професията или дейността;

[6] ЗАКОН ЗА ОТБРАНАТА И ВЪОРЪЖЕНИТЕ СИЛИ НА РЕПУБЛИКА БЪЛГАРИЯ, В сила от 12.05.2009 г., доп. ДВ. бр.38 от 18 Май 2012 г.

- нарушаване забраните по чл. 182 и 184;
- неподаване на декларация по чл. 188, ал. 5;
- нарушаване на правилата за защита на класифицираната информация, довело до нерегламентиран достъп;
- неявяване на работа без уважителни причини в два последователни работни дни;
- злоупотреба със служебното положение;
- увреждане на имущество - държавна собственост, разпиляване на материали, суровини, енергия и други средства, когато са причинени значителни вреди на държавата;
- явяване на военнослужещия в състояние, което не му позволява да изпълнява служебните си задължения, причинено от употреба на алкохол или от злоупотреба с наркотични вещества;
- когато по вина на военнослужещия настъпи смърт или тежка телесна повреда на негов подчинен военнослужещ.

В случаите на временно отстраняване от длъжност по реда на Наказателно-процесуалния кодекс, когато военнослужещият **е** осъден за извършено умишлено престъпление от общ характер, дисциплинарното наказание уволнение се налага от датата на отстраняването.

Дисциплинарните нарушения се установяват от преките командири и или началници на нарушителите.

Когато на военнослужещия се налага дисциплинарно наказание уволнение съответният командир или началник назначава извършване на служебна проверка за събиране на доказателства за извършеното нарушение, изслушва нарушителя или приема писмените му обяснения. Материалите от служебната проверка се изпращат на наказващия орган.

Извършването на служебна проверка не е задължително, ако нарушението е установено с финансова *ревизия, с* вътрешноведомствена проверка или с влязла в сила осъдителна присъда.

Производство за реализиране на дисциплинарна отговорност на държавния служител по Закона за дипломатическата служба[7]

Законът за дипломатическата служба предвижда разпоредби, които да осигурят дисциплинарната отговорност на държавните служителите в дипломатическата служба на Министерството на външните работи.

Прави впечатление, че този закон предвижда като видове дисциплинарни нарушения:

- посочените в Закона за държавния служител;
- посочените в Закона за дипломатическата служба.

Органът по назначаването има възможност да се позове на двете групи нарушения предвидени в общия и специалния закон.

По същия начин законът подхожда и относно видовете дисциплинарни наказания. Органът по назначаването има на разположение предвидените в Закона за държавния служител дисциплинарни наказания, а така също и указаните в Закона за дипломатическата служба.

Указаните в Закона за дипломатическата служба дисциплинарни наказания са:

[7] Вж. чл. 58-60 на Закона за дипломатическата служба

- временно понижаване с един предходен дипломатически ранг на по-ниска с едно ниво длъжност за срок до една година;

- предсрочно прекратяване на задграничния мандат.

Производство за реализиране на дисциплинарна отговорност по Закона за Държавна агенция „Национална сигурност"[8].

Основанията за дисциплинарна отговорност по този закон, видовете дисциплинарни наказания и производството за реализиране на отговорността, се регламентират с разпоредбите на Раздел седми на закона, членове 88-99.

Обобщеното основание за търсене и реализиране на дисциплинарната отговорност от държавните служители в агенцията е виновното нарушаване на служебните задължения, чрез конкретно извършени дисциплинарни нарушения.

Тази отговорност се носи независимо от гражданската, наказателната или административнонаказателнатаотговорност, ако такава се предвижда.

Когато дисциплинарното нарушение е и престъпление или административно нарушение, сроковете за налагане на дисциплинарното наказание започват да текат от влизане в сила на съдебния акт или на наказателното постановление. Сроковете не текат, когато държавният служител е в законоустановен отпуск или по отношение на него е взета мярка за неотклонение задържане под стража или домашен арест.

Дисциплинарните наказания се налагат не по-късно от два месеца от откриване НЕ нарушението и не по-късно от една година от извършването му. За едно и също дисциплинарно нарушение може да се наложи само едно дисциплинарно наказание.

Производство за реализиране на имуществената отговорност за вреди по закона за държавния служител и специални закони

Производство за реализиране на имуществената отговорност за вреди по Закона за държавния служител

Имуществената отговорност на държавата за вреди, причинени на граждани от незаконосъобразни актове, действия и бездействия на държавни органи и длъжностни лица е принципно положение в Конституцията от 1971г. и Конституцията на Република България от 1991г.

Законът за отговорността на държавата и общините[9] за вреди в своя чл. 3 изисква от органа, който е отменил незаконния акт да разясни на увредения от акта реда, по който може да защити имуществените си права. Този закон установява принципа за пълна имуществена отговорност: „Държавата дължи обезщетение за всички имуществени и неимуществени вреди, които са пряка и непосредствена последица от увреждането, независимо от това, дали са причинени виновно от длъжностното лице".

Всички видове юридическа отговорност на държавния служител могат да се възприемат и като видове служебна отговорност, тъй като те са отговорности заради неправомерно служебно поведение, имащи съответната степен на обществена опасност, извършени при или по повод осъществяването на държавната служба в администрацията на държавния апарат. Тази отговорност е лична, субективна. Когато обаче при един от видовете правни отговорности - имуществената, се носи от държа-

[8] ЗАКОН ЗА ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ", В сила от 01.01.2008 г., доп. ДВ. бр.38 от 18 Май 2012г.

[9] ЗАКОН ЗА ОТГОВОРНОСТТА НА ДЪРЖАВАТА И ОБЩИНИТЕ ЗА ВРЕДИ (ЗАГЛ. ИЗМ. - ДВ, БР. 30 ОТ 11.04.2006 Г., В СИЛА ОТ 12.07.2006 Г.), изм. и доп. ДВ. бр.38 от 18 Май 2012г.

вата спрямо гражданите, то тази отговорност е обективна и цели да обезщети претърпените вреди на ощетените от действия и бездействия на техни държавни служители като страни на държавно служебното правоотношение.

Обективната отговорност изключва личната отговорност за противоправно поведение.

При другите видове юридическа отговорност държавата по принцип не носи юридическа отговорност. Такава носят само извършителите на съответните престъпления, дисциплинарни нарушения и административни нарушения. При тези правни нарушения се прилага принципа за личната отговорност на лицата, които виновно са ги допуснали. Едно изключение законодателят е допуснал само при административно наказателната отговорност, като е предвидил такава, под формата на имуществена санкция на юридически лица и еднолични търговци (чл. 83 Закон за административните нарушения и наказания).

Законът за държавния служител предвижда имуществената отговорност на държавните служители и на държавата като неизбежна, щом са налице законовите предпоставки за нейното осъществяване. Тя е една необходимост, за да се постигне желаната компенсация на ощетените граждани или държава от поведението на държавните служители.

Що се отнася до отговорността на държавата, то тя се основава на идеята за риска, която тя носи за поведението на своите държавни служители, които при осъществяване на държавната служба действат от име и за сметка на държавата, като империум, като публична власт. **Държавата притежава възможно най-солидните финансови възможности (парични средства) за обезщетяване нанесените на гражданите вреди от незаконосъобразните действия и бездействия на нейните държавни служители.**

Солидарното обезщетяване на претърпелите вреди в по-голяма степен осигурява своевременно и реално обезщетяване, и в същото време чрез институцията на регреса спрямо виновните държавни служители, утвърждава принципа за личната отговорност за неправомерното им поведение.

Понятие за имуществена отговорност за вреди по Закона за държавния служител

Имуществената отговорност е вид правна отговорност. Тя е гражданска отговорност. Тя е имуществена, защото има нанесени вреди - материални или морални, и които следва да бъдат парично, т.е. имуществено компенсирани. Увреденият трябва да получи равностойно парично (имуществено) обезщетение. Основната характеристика на имуществените спорове е, че те могат да бъдат оценени в пари, т.е. че те имат парична равностойност. Такива искове могат да се предявяват само относно имуществени права.

В Закона за държавния служител на имуществената отговорност са заделени само текста - членове 101, 102и 125, уреждайки съответно обхвата на отговорността и реда за нейното осъществяване.

Субекти, които носят имуществена отговорност за вреди

Законът за държавния служител предвижда два вида субекти които носят имуществена отговорност по него. Това са държавните служители и държавата.

Държавният служител носи имуществена отговорност спрямо ощетените граждани или спрямо държавата и в двата случая отговорността му е заради нанесени им

вреди при и по повод осъществяването на държавната служба. Неговата отговорност е лична и се свързва с виновност в поведението му.

Отговорността на държавата е обективна, т.е. не се основава на нейна вина. Въпросът за вината идва впоследствие - след като обезщетението е осъществено и по пътя на регреса тя търси от държавния служител връщане на изплатеното от нея.

Държавата носи имуществена отговорност спрямо гражданина само в качеството ú на солидарен длъжник, получила го посредством изрична законова норма: „За вреди, причинени на гражданите, държавата отговаря солидарно с причинилия ги държавен служител" (чл. 101, ал. 2 ЗДС).

Принципът за пълна имуществена отговорност на държавния служител за вредите, които е причинил умишлено или при груба небрежност на държавата или на гражданите не е защитен при регресния иск на държавата или общината спрямо виновния държавен служител. Това е случаят, при който при условията на солидарност, държавата, респ. общината, е обезвредила в пълен размер ощетения гражданин, след което предявява регресен иск срещу виновния държавен служител. Тук държавният служител носи имуществена отговорност спрямо държавата, респ. общината в пълен размер, но при условията и по реда, предвиден в Кодекса на труда. Тоест, пълната отговорност може да се окаже реалност само когато нанесената вреда е под размера на предвидената в Кодекса на труда ограничена имуществена отговорност. Ограничената имуществена, отговорност по Кодекса на труда е уредена в разпоредбите на чл. 206. Разпоредбата на ал. 1 на чл. 206 гласи: „За изпълнението на трудовите задължения работникът или служителят отговаря в размер на вредата, но не повече от уговореното месечно трудово възнаграждение."

Производство за реализиране на имуществената отговорност за вреди по Закона за Министерството на вътрешните работи

По силата на Закона за МВР, държавите служители в МВР отговарят единствено но за вредите, които са причинили на държавата по непредпазливост при или по повод изпълнение на служебните си задължения.

За вреди, причинени на граждани при или по повод изпълнение на служебните си задължения, те носят имуществена отговорност към увредения. В тези случаи държавата е длъжна да обезщети увредения за всички имуществени и неимуществени вреди, съобразно общите правила на гражданското право. За вредите, причинени умишлено или в резултат на престъпление или причинени не при или но повод на изпълнение на служебните задължения, отговорността се определя в съответствие с гражданския закон.

Държавните служители в МВР не отговарят имуществено за вредите, които са възникнали от рискова дейност, свързана с изпълнението на служебните им задължения. Държавата и държавните служители в МВР не отговарят за вреди на трети лица когато са причинени в условията на извънредни обстоятелства при осъществяване на действия, свързани със защита на националната сигурност и обществения ред и при извършване на пожарогасителна или аварийно спасителна дейност.

За изплатените от МВР обезщетения за вреди, причинени на граждани от незаконосъобразни актове, действия и бездействия на органи и длъжностни лица. Министерството на вътрешните работи има право на иск срещу служителите, които са ги причинили виновно по непредпазливост при или по повод изпълнение на служебните си задължения.

Държавата има право на иск срещу служителите, виновно причинили вреди но непредпазливост при или по повод изпълнение на служебните задължения, за обезпечението, изплатено на увредения (за всички имуществени и неимуществени вреди), съобразно общите правила на гражданското право.

Когато служителят е изпълнявал служебните си задължения точно, държавата отговаря за всички имуществени и неимуществени вреди, причинени от него на граждани, без да има право да търси от причинителя на вредата възстановяване на платеното от нея.

Държавните служители в МВР отговарят за причинените вреди, но не и за пропуснатите ползи. Размерът на вредата се определя към деня на настъпването им, а ако това не може да се установи - към деня на откриването им.

За вреди, причинени на държавата по непредпазливост при или по повод изпълнение на служебни задължения, държавните служители в МВР отговарят в размера на вредата, но не повече от едно брутно месечно възнаграждение, но ако те са висши ръководни служители - отговорността е в размера на вредата, но не повече от три брутни месечни възнаграждения.

Производство за реализиране на имуществена отговорност за вреди по Закона за отбраната и въоръжените сили на Република България.

Разпоредбите на Закона за отбраната и въоръжените сили, включени в Глава седма, Раздел XII са посветени на имуществената отговорност на военнослужещите, а тези на Раздел XIII от същата глава - на имуществената отговорност на държавата за вреди причинени на военнослужещи.

Съгласно чл. 253 на ЗОВС РБ, военнослужещите отговарят имуществено за вредите, които са причинили на държавата по непредпазливост при или по повод на изпълнение на служебните си задължения.

За вреди, причинени умишлено или в резултат на престъпление при или по повод изпълнение на служебните задължения, отговорността се определя в съответствие с гражданския закон.

Имуществената отговорност на военнослужещите се прилага независимо от дисциплинарната, административно наказателната и наказателната отговорност за същото деяние.

Военнослужещият не отговаря имуществено за вредите, които са настъпили в резултат на военна или друга рискова дейност, свързана с изпълнението на служебните му задължения.

За изплатеното обезщетение за вреди, причинени на граждани от умишлени актове при действия или бездействия на военнослужещи, Министерството на отбраната има право на иск срещу виновно причинилите вредите военнослужещи.

Военнослужещият отговаря за претърпените вреди, но не и за пропуснатите ползи.

Размерът на вредите се определя към деня на настъпването им, а ако това не може да се установи - към деня на откриването им.

За вреди, причинени по непредпазливост при или по повод изпълнение на служебните задължения, военнослужещият отговаря в размера на вредите, но не повече от три брутни месечни възнаграждения, изчислени към размера на възнаграждението получено към датата на установяване на вредата.

Имуществената отговорност по ал. 1 не може да се търси, когато от датата на причиняване на вредите са изтекли повече от три години.

Исковете за пълна имуществена отговорност по ал. 1 се погасяват с 10-годишен давностен срок, който започва да тече от деня на причиняването на вредата.

Производство за реализиране на имуществена отговорност за вреди по Закона за Държавна агенция „Национална сигурност".

Законът за Държавна агенция „Национална сигурност" твърде подробно регламентира материята относно имуществената отговорност на държавните служители в агенцията за вредите, които те са причинили на държавата. Уредена е и отговорността (имуществена) за вредите, които те са причинили на гражданите.

Имуществената отговорност на държавните служители в агенцията за вредите, които те са нанесли на държавата има основанието си в допусната от тях непредпазливост при или по повод изпълнение на служебните им задължения.

Що се отнася за вредите, които те са причинили на граждани при и по повод изпълнение на служебните задължения, в състояние на непредпазливост, имуществена отговорност те самите не носят. В тези случаи отговорността спрямо увредения се поема от държавата. Държавата е длъжна да обезщети увредения за всички имуществени и неимуществени вреди съобразно общите правила на гражданското право.

За вредите, причинени умишлено или в резултат на престъпление или причинени при или по повод изпълнение на служебните задължения, отговорността на държавните служители в агенцията се определя в съответствие с гражданския закон.

Законът изрично указва, че имуществената отговорност на държавните служители в агенцията се носи независимо от дисциплинарната, административно наказателната наказателната отговорност, ако такава се предвижда.

Държавните служители в агенцията не отговарят имуществено за вредите, които възникнали от рискова дейност, свързана с изпълнението на служебните им задължения.

Държавата и държавните служители в агенцията не отговарят за вреди на трети лица, когато са причинени в условията на извънредни обстоятелства, свързани със защитата на националната сигурност.

В случаите на ограничена имуществена отговорност, председателят на агенцията или оправомощено от него длъжностно лице издава заповед за основанието и размера на отговорността на служителя.

Заповедта се издава в едномесечен срок от откриването на вредата, но не по - късно от една година от причиняването й, а когато е причинена от ръководен служител в тримесечен срок от откриването й, но не по-късно от 5 години от нейното причиняване. Тези срокове не текат, ако е образувано производство за осъществяване на пълна имуществена отговорност, докато производството е висящо.

В заключение може да се отбележи, че освен специалните права, осигурени от ЗДС, всички държавни служители носят и съответните отговорности.

Литература:

1. Димитров Д., Държавнослужебно право на Република България, Сиела, С., 2010

2. Казанджиева М., Правен режим на държавната служба, С., 2007

3. Стоилова А., Актове на администрацията с гражданскоправни последици, Автореферат, ЮЗУ, Бл.гр., 2011

4. ЗАКОН ЗА ДЪРЖАВНИЯ СЛУЖИТЕЛ, В сила от 27.08.1999 г., изм. и доп. ДВ. бр.38 от 18 Май 2012г.

5. ЗАКОН ЗА ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ", В сила от 01.01.2008 г., доп. ДВ. бр.38 от 18 Май 2012г.
6. ЗАКОН ЗА ОТГОВОРНОСТТА НА ДЪРЖАВАТА И ОБЩИНИТЕ ЗА ВРЕДИ (ЗАГЛ. ИЗМ. - ДВ, БР. 30 ОТ 11.04.2006 Г., В СИЛА ОТ 12.07.2006 Г.), изм. и доп. ДВ. бр.38 от 18 Май 2012г.
7. ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ, В сила от 01.05.2006 г., доп. ДВ. бр.38 от 18 Май 2012г.
8. ЗАКОН ЗА ОТБРАНАТА И ВЪОРЪЖЕНИТЕ СИЛИ НА РЕПУБЛИКА БЪЛГАРИЯ, В сила от 12.05.2009 г., доп. ДВ. бр.38 от 18 Май 2012г.

КМЕТСКАТА ИНСТИТУЦИЯ КАТО ГАРАНТ НА ОБЩЕСТВЕНИЯ РЕД

Димитър САЛТИРОВ

MAYOR'S AUTHORITY AS A GUARANTOR OF PUBLIC ORDER

Dimitar SALTIROV

Abstract: *This report examines the administrative law aspects of certain powers within the competence of the mayors in the public order ensuring.*

Key words: *public order, administrative powers, properties of the mayor's orders to the police chief*

В съвременните демократични държави общинските дейности не могат да бъдат изцяло ръководени и осъществени от гражданите като общност. Поемането на отговорностите, произтичащи от автономния статут на общинската власт, поставя проблема за ангажирането на висококвалифицирани специалисти във всички области на местното самоуправление. Затова гражданите делегират правото си да управляват общината на свои представители в местната власт. Делегирането на права става посредством демократични общински избори, които са свободни, тайни, равни, преки и общи. Демократичността се гарантира от всеобщото избирателно право. Това на практика означава, че могат да бъдат избирани представители на всички законно регистрирани политически партии, както и отделни независими граждани, а право да избират имат всички български граждани, навършили 18 години и живеещи на територията на дадена община.

Демократичният характер на местната власт се гарантира от прилагането на принципа на разделение на властите, на законодателна, съсредоточена в дейността на общинския съвет и на изпълнителна, осъществявана от кмета и общинската администрация.

България е единна държава с местно самоуправление. Чл. 2 от Конституцията отразява и двата принципа - единство на държавната власт и местно самоуправление. Местното самоуправление е създадено да изпълни няколко основни функции.

1) На първо място трябва да се задоволяват по-ефикасно местните интереси.

2) Те обаче не трябва да се противопоставят на общодържавните - необходима е хармония между тях.

По-голямата част от органите на местно управление се създават на демократична основа чрез избори без всякакво назначение. Обхватът на управлението по места има тази специфичност, че не засяга всички области на държавно управление - осъществява се цялостното държавно управление с изключение на външната политика и на отбраната.

Орган на местното самоуправление в общината е общинският съвет. Кметът на общината е само орган на изпълнителната власт, но не и орган на местно самоуправление. От друга страна пък, измежду изброените органи на изпълнителна власт общинският съвет не фигурира, т.е. той е орган на местното самоуправление, но не е орган на изпълнителната власт. Общинският съвет може да се определи като т.нар. съвещателен орган.

Общинският съвет е орган на местното самоуправление и се избира от жителите на общината при условия и ред, определени от закона. Като главно управително тяло на общината, общинският съвет е отговорен за всички права, които са му предоставени, както и за прилагането на всички задължения, определени от закона. Само съветът има законодателни права и той не може да упражни властта си като ги предостави на комисия, съставена от членове на съвета.

Общинският съвет е постоянно управляващ орган. Неговите функции са свързани с:

- определяне на политиката на общината по изграждането и развитието;
- решаване на местните проблеми, свързани с икономиката, опазването на околната среда, здравната, социалната, образователната, културната и комунално-битовата дейност;
- териториално-селищното устройство;
- общинската собственост;
- безопасността на движението и обществения ред.

Той решава и проблеми от местно значение, които не са от изключителна компетентност на други органи. В случаите, определени от закона, изпълнява и функции, възложени му от централните държавни органи.

Независимо, че основните законодателни и изпълнителни органи в общината са регламентирани от Закона за местното самоуправление и местната администрация ((ЗМСМА), то в процеса на свободното изграждане на общинските структури на управление следва да се има предвид, че на основата на едни и същи структурни елементи, може да се постигне различно въздействие върху управлението, чрез промени в съотношенията, в пропорциите им. И ако при законодателните функции тези възможности са все пак ограничени, тъй като те са приоритет единствено на общинския съвет, то при административните могат да възникнат различни форми, в зависимост от пълномощията на кмета, общинския съвет и общинския секретар.

Съгласно разпоредбите на действащото българско законодателство, общината е основната административно-териториална единица, в която се осъществява местното самоуправление. Орган на изпълнителната власт в общината е кметът.

Следва да се отбележи обстоятелството, че кметът на общината е определен от закона като орган на изпълнителната власт в общината. Въпреки това неговите правомощия са уредени не в Закона за администрацията, където са уредени основните правомощия на другите органи на изпълнителната власт, а в Закона за местното самоуправление и местната администрация. Това обстоятелство поставя въпроса за

природата на кметската институция – дали той принадлежи към системата на изпълнителната власт, или към органите на местно самоуправление.

За да бъде даден точен отговор на този въпрос, трябва да се направи внимателно изследване на нормативната уредба, уреждаща правомощията и статута на кметовете на общини. Съгласно разпоредбата на чл. 139, ал. 1 от Конституцията на Република България, орган на изпълнителната власт в общината е кметът, а съгласно чл. 138 от КРБ, орган на местното самоуправление в общината е общинският съвет. Чл. 139, ал. 2 от КРБ определя, че в своята дейност кметът на общината се ръководи от закона, актовете на общинския съвет и решенията на населението. Именно в тази конституционна разпоредба се проявява двойствената природа на кмета на общината. От една страна, той се ръководи и изпълнява закона, т.е. той действа като типичен орган на изпълнителната власт. От друга страна, той се ръководи и изпълнява и актовете на общинския съвет и решенията на населението, т.е. той изпълнява и решенията на органите на местно самоуправление. Тази конституционна разпоредба дава основание да се направи извода, че кметът на общината притежава двойствена природа. Когато изпълнява законите, актовете на Министерския съвет и когато осъществява функции, възложени му от централните държавни органи (чл. 44, ал. 5 от ЗМСМА), кметът на общината действа в качеството си на териториален орган на централната изпълнителна власт. Следователно в тези случаи се проявява природата му на ***деконцентриран*** орган на централната изпълнителна власт. Когато действа в изпълнение на актовете на общинския съвет и решенията на населението, обаче, кметът на общината действа в качеството си на част от ***системата за местно самоуправление***, като орган на местното самоуправление или както го определя проф. Д. Димитров като „изпълнителен орган на самоуправлението”.[1]

Като институция в системата на местното самоуправление кметът произлиза от общинския съвет като изборен орган на населението и е неразделна част от него. „Същевременно кметът организира провеждането на общинската политика и в това си качество оглавява изпълнителните структури на общината. Той е основната връзка между общинския съвет и общинската администрация, която внася единство между целите, които общината си поставя и процесите на тяхната реализация”[2].

Имайки предвид двойствената природа на кмета на общината, трябва да се направи уточнение кои точно от предоставените му правомощия той упражнява като орган на централната изпълнителна власт и кои – като изпълнителен орган на самоуправлението.

Като изпълнителен орган на самоуправлението, т.е. като децентрализиран орган на местното самоуправление, кметът на общината:

- ръководи цялата изпълнителна дейност на общината;
- организира изпълнението на общинския бюджет;
- организира изпълнението на дългосрочни програми;
- организира изпълнението на актовете на общинския съвет;
- поддържа връзки с политическите партии, обществените организации и движения, както и с други органи на местното самоуправление в страната и в чужбина;
- представлява общината пред физически и юридически лица и пред съда;

[1] Димитров, Д., Основи на публичното право. Лекционен курс, С., 2007
[2] Миланов, Ж., Местното самоуправление,С., 2001

– осигурява организационно-техническото обслужване на общинския съвет и участва в заседанията му с право на съвещателен глас;

– утвърждава устройствения правилник на общинската администрация;

– изпраща на общинския съвет административните актове, както и договорите и техните изменения и допълнения, издадени в изпълнение на актовете, приети от съвета, в тридневен срок от издаването или подписването им.

Като териториален орган на централната изпълнителна власт на територията на общината, т.е. като деконцентриран орган на централната изпълнителна власт, кметът на общината притежава следните правомощия:

– насочва и координира дейността на специализираните изпълнителни органи;

– назначава и освобождава от длъжност заместник-кметовете на общината, кметските наместници, ръководителите на звената на издръжка от общинския бюджет, началниците и служителите в общинската администрация, с изключение на тези по чл. 46, ал. 1, т. 4 (тези, които се назначават от кмета на район или кметство), налага предвидените от закона дисциплинарни наказания;

– ***отговаря за опазването на обществения ред, като за осигуряването му издава писмени заповеди, задължителни за началниците на съответните полицейски служби***;

– организира изпълнението на задачите, които произтичат от законите, от актовете на президента на републиката и на Министерския съвет;

– възлага изпълнението на свои функции на кметовете ма кметствата и районите, координира и осъществява контрол за целесъобразността и законосъобразността при тяхното изпълнение. Осъществява контрол по законосъобразността на актовете и действията на кметовете при изпълнение на техните правомощия и налага предвидените административни наказания;

– ***председателства съвета по сигурност***;

– възлага или разрешава изработването на устройствени планове и техни изменения за територията на общината или за части от нея и одобрява определени устройствени планове при условията и по реда на Закона за устройство на територията, както и организира изпълнението им;

– изпълнява функциите на длъжностно лице по гражданско състояние. Той може да възлага тази функция с писмена заповед на кметовете на кметствата, в които се поддържат регистри за гражданското състояние, кметските наместници и на други длъжностни лица от общинската администрация;

– оказва съдействие на етажните собственици и техните управителни органи при условията и по реда на Закона за управление на етажната собственост.

Внимание заслужава разпоредбата на чл. 44, ал. 1, т. 4 от ЗМСМА. Съгласно нея, ***кметът на общината отговаря за опазването на обществения ред на територията на общината***. За целта законодателят му е предоставил правомощието да издава заповеди, които са задължителни за началниците на съответните полицейски служби. Въпросът в случая е дали кметът на общината разполага с необходимите организационни предпоставки и правомощия, за да реализира предоставената му от законодателя функция по опазване на обществения ред на територията на общината. Следва да се отбележи, че в България все още няма създадена и действаща общинска полиция. Полицията е централизирана и правомощията на кмета на общината да поставя задачи на териториалните звена на Министерство на вътрешните работи са ограничени.

Функциите и правомощията на кмета като орган на изпълнителната власт ***могат да се очертаят в две направления***.

Първото включва неговите правомощия и отговорности относно изпълнението на решенията на общинския съвет. Например общинският съвет приема наредби за опазване на обществения ред, чието нарушаване обосновава административно-наказателна отговорност. Контролът по изпълнение на наредбите е възложен на кмета.

Към ***второто*** направление се отнасят функциите и правомощията на кмета, които са му възложени на специално основание със закон. Например осигуряването на обществения ред е изпълнително-разпоредителна дейност, при осъществяване на която кметът на специално основание действа като орган на държавната администрация. Следователно осигуряването на обществения ред е проблематика както от ***компетентността на местното самоуправление, така и на централната държавна администрация***.

Като учредява един или друг държавен орган, правната норма определя и функциите, които той трябва да изпълни. Със закон например на кмета на общината е възложена отговорността за осигуряване на обществения ред, а на кмета на район или на кметство е възложена функцията за осигуряване на спазването на обществения ред.

Правомощията на кмета във връзка с обществения ред се прилагат по ред, установен от закона. Прилагането на административните правомощия е част от административния процес. Особеност на административното правоприлагане са максималната опростеност и процесуалната икономия. Например проверката за установяване на самоличността, проверката на превозно средство, личният обиск или административното задържане не са свързани със сложни процесуални правила. Практическото съображение за това е необходимостта от бързина, оперативност и ефективност при осъществяване на административните задачи.

Административните правомощия на кмета понякога са обусловени от упражнени преди това контролно-надзорни функции. Въпросът е дали административните правомощия не са част от контролната, респективно надзорната дейност? В практиката този въпрос е разрешен по два начина:

– административните правомощия ще бъдат приложени от онзи орган, който е осъществил контролно-надзорните функции. В тази хипотеза те са част от неговата компетентност. Например в дейността си по осигуряване на спазването на обществения ред кметът при условията на чл. 46, ал. 1, т. 8 от ЗМСМА е установил нарушение на обществения ред от лице, което показва тежки психични отклонения. Това е основание кметът да задържи лицето, а ако е необходимо, според чл. 70, ал. 1, т. 3 от Закона на МВР може дори да го настани в специално помещение. Следователно в конкретния пример органът на държавното управление е проконтролирал спазването на обществения ред, а заедно с това е бил компетентен и е упражнил предоставеното от закона административно правомощие за преустановяване на противоправното деяние.

– административните правомощия на кмета се прилагат за опазване или спазване на обществения ред.

Какво следва да разбираме под обществен ред?

На понятието "обществен ред" са посветени множество разработки. Независимо от това то си остава дискусионно. Обикновено се приема, че това понятие следва да ***се разглежда в широк и тесен смисъл на думата***.

В широк смисъл общественият ред се определя като система от всичките обществени отношения в обществото, които са предмет на регулиране от цялата съвкупност

на социални норми (правни, морални, политически, обичайни и пр.). В това широко значение общественият ред включва производствения ред, политическия ред, правовия ред, държавния ред и пр. Следователно общественият ред в тесен смисъл е част от обществения ред в широкото значение на това понятие.

В тесен смисъл, или общественият ред като правна категория, се използва за определяне както на сферата на дейност на държавните органи, така и на родовия и непосредствения обект на конкретните видове престъпления и административни нарушения.

Средствата за регулиране на обществения ред могат да бъдат само правните норми, т.е. понятието "обществен ред" включва само тези обществени отношения, които се регулират с правни норми.

Кметът като орган на власт в изпълнение на своите правомощия прилага наредбата за обществения ред известна в практиката като Наредба № 1. По тази наредба се установява, че полицейските правомощия на кмета са 15 и не са никак маловажни[3].

Видовете нарушения, по които могат да бъдат налагани глоби, са:

1. Управление на МПС в паркове, алеи и др.
2. Извършване на ремонтни дейности извън определеното време.
3. Провеждане на тържества извън определеното време.
4. Ремонт на МПС извън определените места.
5. Разхождане на кучета без нашийник и повод.
6. Разхождане на кучета извън определените места.
7. Паша на селскостопански животни извън определените места.
8. Изхвърляне на строителни отпадъци извън определените места.
9. Незаконна търговска дейност.
10. Незаконна търговска дейност в заведения.
11. Поставяне на търговски обекти без разрешение.
12. Малолетни и непълнолетни без придружител в заведение.
13. Продажба на алкохол и цигари в училища и здравни заведения.
14. Звуковъзпроизвеждане на открито.
15. Други.

От което е видно, че кметът като орган на власт със силите и средствата на общинската администрация е в състояние да въведе ред на територията, където той е избран.

Обществото иска решаване на комплекс от въпроси, свързани с осигуряването на обществен ред и сигурност. Тези въпроси понастоящем се решават приоритетно от органите на Националната полиция, въпреки че редица централни и регионални институции имат законоустановени правомощия, свързани с осигуряване сигурността и безопасността на гражданите. Съществува необходимост да се подобри координацията между тях и да се установят механизми за партньорство, които да доведат до успешното постигане на общата цел. Особено внимание следва да се обърне на оптимизиране на работата на районните и младшите районни инспектори, чиито преки задължения са свързани с непосредствена работа сред населението.

Необходимо е да отбележим, че такива правомощия са присъщи за полицейските органи от МВР. Кметът в тези случаи не е полицейски орган, но по волята на закона той е оправомощен да действа като такъв до пристигане на полицейските органи.

[3] Костов Е., Правомощия на кмета за осигуряване на обществения ред, Албатрос, С., 2000

Съгласно чл. 44, ал. 1, т. 4 от ЗМСМА кметът на общината отговаря за обществения ред, като за осигуряването му издава писмени заповеди, задължителни за началниците на съответните полицейски служби.

ЗМСМА изрично и специално е натоварил кмета на общината да отговаря за спазване на обществения ред, като за осигуряването му го е овластил да издава писмени заповеди, задължителни за началниците на съответните полицейски служби. Въпросът е може ли кметът на общината да делегира (да възложи) на други органи упражняването на предоставените му от закона права?

Изключение от това правило може да има, ако текст изрично предвижда това. Освен това то трябва да отговаря и на някои допълнителни условия: компетентности могат да се делегират поначало само на органи от съответното ведомство; делегирането трябва да бъде изрично и писмено; приема се също, че делегираните органи не могат от своя страна да пределегират възложената им власт. Според чл. 44, ал. 1, т. 9 от ЗМСМА кметът на общината може да възлага на кметовете на кметства или райони да изпълняват негови функции, като същевременно осъществява контрол за целесъобразността и законосъобразността при тяхното изпълнение. Кметовете на райони и кметства при делегирането на права по осигуряването и спазването на обществения ред имат правомощията по чл. 61, 63, 68, 69, 71, 72 и 74 от Закона за Министерството на вътрешните работи, на съответната територия до пристигане на полицейския орган и може да:

- извършва проверки за установяване на самоличността;
- задържа лица;
- извършва личен обиск;
- проверява личните вещи;
- извършва проверки в помещения без съгласието на собственика или обитателя или в тяхно отсъствие;
- използва физическа сила и помощни средства при изпълнение на служебните си функции, когато те не могат да се осъществят по друг начин;
- използва оръжие като крайна мярка;
- организира и ръководи защитата на населението при бедствия и аварии.

Освен това отношение към опазване на обществения ред имат и разработените планове в общините и утвърдени от кмета за :

1. План за управление на риска от ядрена или радиационна авария, трансграничен пренос на радиоактивни вещества и аварии с радиоактивни източници и материали на територията на общината.

При изготвянето и изпълнението му задължително се спазват изискванията на:

- Закона за безопасно използване на ядрената енергия;
- Наредбата за аварийно планиране и аварийна готовност при ядрена и радиационна авария;
- Наредбата за основните норми за радиационна защита;
- Наредбата за безопасност при управление на радиоактивните отпадъци;
- Наредбата за радиационна защита при дейности с източници на йонизиращи лъчения и др.

2. План за управление на риска от наводнения на територията на общината;

Плана се разработва на основа на Директива на Европейския съюз 2000/60/ЕО, в която се формулират определенията, видовете наводнения и необходимите мерки за намаляване на неблагоприятните последици от настъпването им.

3. План за управление на риска при свлачища, снегонавявания и обледявания на територията на общината.

Целта на разработения план е:

– създаване на необходимата организация за действия при бедствия и в тежки зимни условия;

– поддържане на оперативно дежурство в общинската администрация и формированията на юридическите лица;

– осигуряване и поддържане на информационната система;

– разработване на варианти за временна организация на движението и снегопочистването;

– организация на транспорт за нуждаещи се и снабдяване с основни продукти;

– дейности по възстановяването на нормалния ритъм на живот.

4. План за управление на риска при земетресения на територията на общината.

В плана се прави анализ на сеизмичния риск, характеристиките на земетресенията и възможните последици според използваните сеизмични скали. Набелязват се изисквания за сеизмичното осигуряване на сградите и съоръженията. Разработват се стратегии за намаляване на сеизмичния риск и задачите по защита на населението.

За първите четири плана мероприятията задължително се съгласуват с областните дирекции на "Пожарна безопасност и защита на населението" по изискванията визирани в чл.52г, ал.1, 2 и 3. на Закона за МВР.

5. Договор между областната дирекция на МВР и общината за охрана на специализирани обекти от отбранително-мобилизационната подготовка и управление при кризи.

В договора се визира предмета, срока, цената на охраната на съответните обекти, предмет на договора. Посочват се правата и задълженията на страните, условията за прекратяване на договора и допълнителните условия, ако има такива. Най-често обектите и цените на охрана се оформят в приложения към договора.

От всичко изброено е видно, че проблемите на обществения ред в една община са многообразни и понякога дискусионни. Избирателите изискват осигуряването на обществен ред и сигурност. Това предава и специфичността и отговорността на кмета при тяхното решаване. Въпросът в случая не е дали кметът на общината разполага с необходимите организационни предпоставки и правомощия, за да реализира предоставената му от законодателя функция по опазване на обществения ред на територията на общината, а как ги използва. Работи ли съвместно с намиращите се на територията на общината специализирани ведомства за осигуряване на обществения ред, съдейства ли за подобряване на координацията между тях и установяване на механизми за партньорство, които да доведат до успешното постигане на общата цел.

Литература:

1. Димитров, Д., Основи на публичното право. Лекционен курс, С., 2007

2. Костов Е., Правомощия на кмета за осигуряване на обществения ред, Албатрос, С., 2000

3. Миланов, Ж., Местното самоуправление,С., 2001

4. Стоилов Я., Държавната власт, Сиби, С., 2001
5. Стоилова А., Актове на администрацията с гражданскоправни последици, Автореферат, ЮЗУ, Бл.гр., 2011
6. ЗАКОН ЗА МЕСТНОТО САМОУПРАВЛЕНИЕ И МЕСТНАТА АДМИНИСТРАЦИЯ, Обн. ДВ. бр.77 от 17 Септември 1991г., изм. ДВ. бр.38 от 18 Май 2012.
7. ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ, В сила от 01.05.2006 г., доп. ДВ. бр.38 от 18 Май 2012.
8. КОНСТИТУЦИЯ НА РЕПУБЛИКА БЪЛГАРИЯ, Обн. ДВ. бр.56 от 13 Юли 1991г., изм. ДВ. бр.12 от 6 Февруари 2007.
9. ЗАКОН ЗА АДМИНИСТРАТИВНО-ТЕРИТОРИАЛНОТО УСТРОЙСТВО НА РЕПУБЛИКА БЪЛГАРИЯ, Обн. ДВ. бр.63 от 14 Юли 1995г., изм. ДВ. бр.95 от 2 Декември 2011.
10. ЗАКОН ЗА АДМИНИСТРАТИВНИТЕ НАРУШЕНИЯ И НАКАЗАНИЯ, Обн. ДВ. бр.92 от 28 Ноември 1969г., изм. ДВ. бр.19 от 6 Март 2012.

ИНФОРМАЦИОННА СИГУРНОСТ

НОВИТЕ РЕАЛНОСТИ В СЕКТОРА „ИНФОРМАЦИОННА БЕЗОПАСНОСТ И СИГУРНОСТ" И ВЛИЯНИЕ НА ЧУВСТВИТЕЛНАТА ИНФОРМАЦИЯ ВЪРХУ НАЦИОНАЛНАТА СИГУРНОСТ НА Р. БЪЛГАРИЯ

Стоян Г. Тонев

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ - СОФИЯ
ИНСТИТУТ ЗА НАУЧНИ ИЗСЛЕДВАНИЯ И ОБУЧЕНИЯ НА ДОКТОРАНТИ

NEW ACTUALITIES' IN SECTOR "INFORMATION SAFETY AND SECURITY" AND INFLUENCE TO SENSITIVE INFORMATION OVER NATIONAL SECURITY TO REPUBLIC OF BULGARIA

Stoyan G. Tonev

Abstract: The management of the sensitive information are contemporary approach whose application in the sphere of the security allow realization to complex counteraction to multiform and interdependence and interlinks sources to risk and threat, which are factor for reliability prevention to negative influence toward National security to Republic of Bulgaria.

***Key words*:** Information security; Politics safety; Sensitive information

Информационната сигурност, както и защитата на информацията, е комплексна задача, като пътищата да бъде реализирана е чрез единни правила за безопасно използване на информацията в Р. България. Проблемът за защита на информацията се явява сложен многопланов и комплексен процес обхващащ редица важни задачи. Информационната сигурност непрестанно се комплецира и прониква във всички сфери на обществения и социален живот, както при обработка, така и при предаването и съхранението на информацията.

Към момента се определят три базови принципа, които задължително осигуряват информационната безопасност:

- цялоста на данните - защита от пропадания, водещи до загуба на информация, както и защита от неоторизиран /несанкциониран/ достъп по създаване и унищожаване на данни;
- конфиденциалност на информацията;
- достъп до информацията само до упълномощените ползватели.

Средствата за защита на информацията не следва да се проектират, закупуват или инсталират преди провеждането на задълбочен анализ на средата за сигурност от съответните експертни нива и финансова обосновка за това.

При анализа на информационната безопастност следва да се отчита мястото и в системата за национална сигурност, определяне на жизнено важните интереси в информационната сфера и заплахите за тях. Необходимо е да се разгледат въпросите за информационната война, информационните оръжия, принципи ,

основни задачи и функции по осигуряване на информационната сигурност и безопасност. Да се изучават и прилагат, държавните, чужди и международни стандарти в областта на информационната сигурност и безопасност. Ключов елемент в анализа на сигурността следва да се отдели и законована и подзаконова нормативна база по въпросите на информационната сигурност и безопасност на информацията по каналите по които протича и крайните устройства.

Необходимо е да се отчетат общите въпроси за защита на информацията в автоматизираните информационни системи -АИС за обработка на данни, предмет и обект на защита на информацията, задачи за защита на информацията в системите за обработка на данни.

Необходимо е да бъдат разгледани и типовите преднамерени заплахи за безопасността и методите на защита на информацията.

Задължителна е задълбочена оценка на значението на методите и средства за оторизиран достъп на ползвателите, деференциране на достъпа до информационните ресурси и контрол на достъпа до апаратурата.

Основните задачи при контрола по защита на информацията се свеждат до:

- събиране, обобщаване и анализ на информацията за състояние системата за защита конфиденциалната информация за организационната система;
- анализ на състоянието в структурните подразделяния, а така също и във филиалите и представителствата на организационната система;
- проверка наличието на носителите на конфиденциална информация.
- проверка за спазване на горните правила от всички сътрудници в организационната система работещи с различни носители.
- прояви на заплахи по защитата на информацията и разработването на мерки за тяхното неутрализиране.
- анализ, пълнота и качество на изпълненение на планираните мероприятия по защита на информацията в хода на дейността на организационната система;
- оказване на методическа помощ на длъжностните лица при отстраняване на нарушенията съгласно изискванията към нормативно-методическите документи.
- прилагане на мерки за административни и дисциплинарна отговорност към лицата нарушаващи изискванията към изградената система за работа с конфиденциална информация.
- проверка ефективността на прилаганите мерките по защита на конфединциална /чувствителна / информация, прилагани от длъжностните лица и ръководителите на структурните звена.

Изборът на методи за контрол, зависи от конкретните цели, задачи и обекти на контрол, а също така и от съвкупните сили и средства, които се предполага, че ще се използват.

Основните методи за контрол състоянието на защита на информацията включват, проверка, анализ, наблюдение и сравнение.

Управлението на инциденти в информационна сигурност, в съответствие с разпоредбите на Международния стандарт ISO / IEC 27001:2005, както и много други стандарти основен компонент за управлението е контрол, който е необходим за всяка информация и система за сигурност.

Управлението на сигурността е едно от нивата на практическо управление на информационното съдържание – безопасна среда за работа. Управлението на информационната сигурност е непрекъснат процес на изучаване на опита на

водещи специалисти по изграждането и сертифицирането на система за управление на информационната сигурност и нейното адекватно прилагане в реалната среда за сигурност.

Управлението на информационната сигурност - е цикличен процес, който включва, осъзнаване на необходимостта от защита на информация и задачи по събиране и анализ на данни за състоянието на информационната безопастност и сигурност в организационите системи, оценка на информационните рискове, планиране за работа с рискове; реализация и изпълнение на подходящи и адекватни механизми за контрол, правилно разпределение на роли и отговорности, обучение и мотивация на персонала, оперативната работа за прилагането на защитни мерки, мониторинг на функционирането на механизмите за контрол, оценка на тяхната ефективност и адекватни коригиращи подходи.

Разработването и прилагането на ефективни политики за информационна безопасност и сигурност се фокусирани върху съвременните подходи за развитието на ефективна политика по безопасност на информацията и са необходими за създаването на всеобхватна система за осигуряване на сигурност на структурното звено. Както се планира, изгражда, реализирана и представя ефективността на политиката по безопасност, така ще се оценя качеството на сигурност на самите документи, които отговарят на действителното-реално състояние на организацията и вземат под внимание основните принципи по прилагане на информационната сигурност.

Горното трябва да бъде съобразено с пълнота на досегашен опит иновации и законодателство. Международния опит в управлението на информационната сигурност за организационните звена в Р. България, и световните търговска организация се определя от спешността на новата ни серия от международни стандарти ISO / IEC, включително в областта на управление на информационната сигурност, въз основа на известен стандарт BS 7799. Балансиран подход към изграждане на корпоративни системи за управление на информационната сигурност, касаеща еволюцията на компютърни технологии, която непрекъснато се ускорява. Бизнес лидерите трябва да следят новите тенденции и решения, свързани с осъвременяване на инфраструктурата на информационните технологии. Това са и новите технологии и начини за организиране на бъдещата работа и служещи като източник на нова uslug.Sistema за сигурността на управление.

Наблюдава се една нова тенценция към налагане на прости решения и повече пристрастие по отношение на политиките по защитата на данните на всички нива на управление. Кото извода от проведените работни срещи и задълбочени дебати за сигурността на информацията на първо място се имат предвид защитата на вируси и хакери. Все по актуални стават и въпросите по сигурността свързани с загриженост от дейността на "вътрешни" (служители) в организациите, което е потвърдено и в годишен доклад на ФБР за Компютърни престъпление и проучване за сигурността. Последните се базират на направени глобални проучванния на информационната сигурност през 2004 г. от компанията Ernst & Young, и изследване, озаглавено "Вътрешен ИТ-заплахите в Русия 2004", проведено от Info Watch.

Обобщавайки опита се достига до основния въпрос. Какво трябва да се направи, че нивото на сигурността на информацията в структурните звена без

значение частни или държавни, национални или чуждеустранни да е на добро ниво и в оптимално съотношение с разходите които трябва да се направят за това ?

Изследователските и учебни възможности за автоматизация на процедурите за анализ на уязвимостта на информационна сигурност, налага необходимостта от въвеждането на единна класификация на сигурността и заплахите. Изграждането на единна европейска общност на базата на "общи критерии" позволяващи да се постигне съвместима с текущото състояние на ИТ и международни стандарти за информационната сигурност, както и способността да използва резултатите от оценките на сигурността.

Какво е положението в страната?

Р. България като страна членка на ЕС и НАТО е предприела мерки и е синхронизирала нормативните и поднормативните документи касаещи работата с класифицирана информация. Към момента липсва нормативна база касаеща **чувствителната информация**, която все по ясно се материализира и се явява основен ресурс за управление и развитие на обществото.

В редица източници се налага представянето на релацията „чувствителна информация - национална сигурност в процеса на информационна сигурност и глобализация".

Новите предизвикателства и заплахи за сигурността на социалните организации са с висока степен на неопределеност, проявяват се в сложна взаимозависимост и са трудно предвидими, което определя невъзможността за ефективно противодействие с традиционни сили и средства.

Необходимо е извършване на трансформация в политиката за сигурност свързана със социалните организации, с цел създаване на благоприятни условия за изпълнение на мисията им и гарантиране устойчивото развитие на обществото. Трансформацията в политиката, стратегиите и подходите е свързана с коренна промяна от реагиране на промените в средата за сигурност към формиране на способности за гарантиране на сигурността, основани на целесъобразно проактивно противодействие на съвременните асиметрични заплахи или тяхното превантивно отстраняване.

Управлението на **чувствителната информация /ЧИ/** е съвременен подход, чието приложение в сферата на сигурността позволява осъществяването на комплексно противодействие на многообразните и взаимно зависими източници на заплаха и надеждно предотвратяване на негативното им въздействие спрямо социалните организации в публичния сектор. Управлението на **ЧИ** като фактор за националната сигурността позволява извършването на приоритизиране на целите и задачите на социалните организация и оптимално използване на ограничените им ресурси, с цел създаване на условия за реализация на ефективно стратегическо ръководство.

Службите за сигурност, като едни от основните подсистеми на системата за национална сигурност на Република България са в процес на мащабна трансформация насочена към изграждане на оперативни способности за изпълнение на мисията и задачите й в национален и международен аспект съобразно новите динамични реалности.

В процеса на утвърждаване на международната кооперативна система за сигурност, като компонент в глобализиращия се свят, службите за сигурност са обект на въздействие на многообразни и сложни съвременни заплахи – международен тероризъм; разпространение на оръжие за масово унищожение; незаконна търговия с оръжие и стоки и технологии с двойна употреба; корупция; деструктивни въз-

действия върху комуникационните и информационни системи и мрежи; международна организирана престъпност, неосъзнат трансфер на технологии и др..

Една от тези заплахи е свързана с **ЧИ** ефективното и управление е показател за надеждността на системата за сигурност на обществото. Атаките върху **ЧИ** като **явление** е с изключително висока степен на опасност не само поради деструктивното въздействие върху личността, икономиката, финансите, но и за културата и морала на обществото и прекия негативен ефект върху националното стопанство, но и поради сложната взаимозависимост с останалите глобални заплахи и проявата й както като обособено посегателство, така и като основна характеристика, мотив или цел на другите заплахи за сигурността.

В условията на преход, службите за сигурност са в повишена уязвимост на посегателства към ЧИ и въпреки, че текущото състояние на посегателство може да бъде определено в диапазона "ниска" – "средна" степен, то тенденцията за нарастване на финансовите и материални ресурси, необходими за преструктуриране и модернизация, са основа за прогноза за повишена активност на субекти на интерес към ЧИ и нарастване на заплахата от ЧИ за организациите.

Актуалността и значимостта на задачата за формулиране, приемане и овладяване на ЧИ, като фактор за националната сигурност в условията на преход налага да се направи критичен обзор на съвременните методики, методи и механизми за управление на ЧИ. Анализа ще позволи да се формулират целта, конкретните задачи и ограниченията на изследването. Публикуваните в последните години концепции и модели, потвърждават известните схващания за рисковете и заплахите за ЧИ и нейното неефективно управление.

Необходимо е да се дефинират критериите за рамката на ЧИ, нейните характеристики, основните заплахи, което ще позволи успешната трансформация на службите за сигурност и развитие на обществото в глобализиращия се свят. Налага се оценка и анализ на социалната и правна среда за развитие на **явлението** ЧИ и на тази основа да бъде интерпретирана нова платформа на противодействие по защита на ЧИ.

Към момента липсва на методика /метод / за управление на ЧИ в сферата на сигурността и конкретно технологията за управление на риска в управление на ЧИ в определена среда.

Въз основа на критичния анализ на събраните емпирични данни за ЧИ в определени организации са в процес на трансформация са формулирани: възможностите, формите и съдържанието на ЧИ; отрицателните ефекти и границите на появата им; стратегията за управление на ЧИ и предотвратяване на негативните последици от неправомерното и управление.

Особената значимост на методиката ще се определя от възможностите, които ще предложи подхода на управление на ЧИ за противодействие на сложни и динамично развиващи се предизвикателства и заплахи и изграждане на гъвкава и надеждна система за сигурност във социалните организации.

Разработването на модел за управление на риска в сферата на сигурността в национален аспект, който не само съдържа основните принципи на проектодокументи, но и ги развива в комплексна технология би допринесло за прилагане на адекватен подход за противодействие на съвременните глобални заплахи, една от които е заплахата към ЧИ.

Налага се необходимостта от поставяне на **цел относно:**

- оптимизиране и усъвършенстване процеса на **индивидуализиране** на ЧИ на национално и съюзническо ниво, извеждане на основните параметри и особености на ЧИ в период на трансформация на социалните организации, на база на което да се разработи технологична схема за избор и изпълнение на стратегия за управление на ЧИ в социалните организации;
- готовност за определяне на проблеми при управление на ЧИ и готовност за изпълнения на съвместни задачи на между институционално и международно ниво.

За постигане на целите е необходимо да бъдат решени следните **задачи**:

- определяне на критериите за обхвата на рамката на ЧИ, нейните характеристики в сферата на информационната сигурност;
- изучаване на теорията за управление на ЧИ като фактор за националната сигурност в социалната организация;
- изучаване и систематизиране на нашия и чуждестранен опит за изграждане на ефективни системи за сигурност за защита на ЧИ на социалните организации;
- изучаване на нормативната база, отразяващи състоянието и системата за управление на ЧИ в социалните организации в РБ;
- изследване на тенденциите за нарастване на заплахата за сигурността на средата от неефективно управление на ЧИ;
- разработване на методика /модел/ за управление на ЧИ.

Необходимо е изследване на дейността по управление на ЧИ в социална организация като фактор за националната сигурността, като изследването да обхваща всички аспекти на сигурността, определени от проявата на многообразни, взаимозависими и динамично променящи се източници на заплаха за организацията.

Ефективно управление на ЧИ, като фактор за НС в период на трансформация налага определяне на:

- Държавната политика по защита на информацията в началото на 21век.
- Какво представлява информационна сигурност /наличност, интегритет и конфиденциалност/.
- Национални стратегии по защита на чувствителната информацията /структури, ангажирани с процеса/.
- Международни стратегии по защита на информацията. Структури на стратегическо ниво.

ИЗВОДИ:

1. Управлението на риска от заплаха на ЧИ в социалните организации е комплексна технология за ефективен контрол на явлението, основана на целесъобразни проактивни действия за предотвратяване на заплахи и изграждане на функционираща сигурна среда.
2. Ефективното управление на ЧИ в Р.България, може да бъде реализирано само след детайлно изследване и комплексни, синхронизирани действия на съответните органи на изпълнителната, законодателната и съдебна власти.

Литература:

1. Стратегия за национална сигурност на Р. България - 2011 г.
2. Сариев, Ив. Мениджмънт на информацията, Класика и стил, 2007.
3. Семерджиев, Ц. Информационна война, Софттрейд, С., 2000.

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ОПЕРАТИВНОТО ПРОТИВОДЕЙСТВИЕ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ В СОЦИАЛНАТА ОРГАНИЗАЦИЯ

Христо Атанасов Христов

Университет по библиотекознание и информационни технологии – София,
hristov63@abv.bg

ORGANIZATION AND MANAGEMENT OF OPERATIONAL ENCROACHMENT TO HAVE UNREGULATED ACCESS TO SENSIBLE INFORMATION IN SOCIAL ORGANIZATION

Hristo A. Hristov

***Abstract*:** *This paper deals with management of operational encroachment as a complex method. The same approach should be applied successfully in the field of company security in order to create effective reaction against contemporary global threats and encroachments and also to build up flexible dynamic system of security which have to guarantee mission accomplishment of each social organization. Management of operational reaction against encroachment upon company security is mainly related to complex neutralization of various and interdependent sources of threats and also to effective prevention of their negative influence upon social organizations. The discussed security approach will contribute to adequate prioritization of tasks and goals which should be taken in security organizations, along with planned use of their limited resources which will provide the right conditions for effective realization of strategy management. The applied nature of research is strictly defined by concrete specifics of social organization that has been considered as the main subsystem of the system of national security in The Republic of Bulgaria.*

***Key words*:** management encroachment, information security, national security, information, security policy, social organizations.

Развитите страни през XXI век се характеризират с глобализираща се икономика. Във формиралия се нов световен пазар, съвременната глобална среда за сигурност се характеризира с висока сложност и хаотична динамика на промените, нарушаваща стабилността и устойчивостта на развитието на обществото.

Новите предизвикателства и заплахи за сигурността на социалните организации /търговски дружества, корпорации, компании, фирми и др./ са с висока степен на неопределеност, проявяват се в сложна взаимозависимост и са трудно предвидими, което определя невъзможността за ефективно противодействие с традиционни сили и средства.

Необходимо е извършване на трансформация в политиката за сигурност на социалните организации, с цел създаване на благоприятни условия за изпълнение на мисията им и гарантиране устойчивото развитие на обществото. Трансформацията в политиката, стратегиите и подходите е свързана с коренна промяна от реагиране на промените в средата за сигурност към формиране на способности за гарантира-

не на сигурността, основани на целесъобразно проактивно противодействие на съвременните заплахи и посегателства.

Управлението на противодействието на посегателства срещу фирмената сигурност е съвременен подход, чието приложение в сферата на сигурността позволява осъществяването на комплексно неутрализиране на многообразните и взаимозависими източници на заплаха и надеждно предотвратяване на негативното им въздействие спрямо социалните организации. Разглежданият подход в сферата на сигурността позволява извършването на адекватно приоритизиране на целите и задачите на социалната организация, съчетано с планирано използване на ограничените им ресурси, позволяващо създаване на условия за реализация на ефективно стратегическо ръководство.

Във демократичните общества с развита пазарна икономика естествен процес е разширяването на недържавната система за защита на сигурността. Държавата отстъпва част от своите правомощия и функции на собственика, които е най-заинтересован да се гарантира неговия живот, имущество и интереси. В тази връзка фирмените служби за сигурност стават един от елементите на системата за национална сигурност.

Възприето е схващането, че фирмената сигурност в условията на пазарна икономика е част от националната сигурност и съответно защитата на фирмената сигурност е тясно свързана с националната сигурност.

В процеса на утвърждаване като компонент на националната система за сигурност, социалната организация е обект на въздействие на многообразни и сложни съвременни заплахи и посегателства: – шпионаж, -нерегламентиран достъп до чувствителна информация, -фирмената тайна, -международен тероризъм; -корупция; -деструктивни въздействия върху комуникационните и информационни системи и мрежи; -организирана престъпност, -изнудване, -подкупи, кражби в корпоративния сектор и др. Всички тези дейности са свързани с неетични и незаконни действия, които не следва да бъдат подценявани и пренебрегвани.

Една от тези диференцирани заплахи и посегателство е нерегламентирания достъп до чувствителна информация в социалната организация и ефективното и противодействие е показател за надеждността на системата за сигурност на организацията. Нерегламентиран достъп до чувствителна информация като деяние е с изключително висока степен на опасност, поради прекия негативен ефект върху националното стопанство,.

Актуалността и значимостта на задачата за опазване на чувствителна информация във фирмата налалага да се направи критичен обзор на съвременните методи и механизми за управление на противодействието на посегателства срещу фирмената сигурност, което да позволи формулиране на целта и конкретните задачи.

Анализът на публикуваните в последните години концепции и модели, потвърждава известните схващания за противодействието на заплахите и ефективното функциониране на фирмите. Нерегламентирания достъп до чуствителна информация, е разгледан като една от основните заплахи и посегателство за успешния проспиритет на фирмата.

Моделът за организация и управление на оперативното противодействие на посегателства в сферата на фирмената сигурност /специфичната дейност на органите на фирмената сигурност, която има за основна цел да разкрива, неутрализира и подпо-

мага откритото пресичане на посегателства, чрез прилагане на специфични средства и методи/ е необходимо да бъде разработен в теоретичен и практически план.

За всяка социална организация въз основа на анализ на събраните емпирични данни за посегателства срещу фирмената сигурност е необходимо да бъдат формулирани: възможностите, формите и съдържанието на нерегламентиран достъп до чувствителна информация; негативните ефекти и границите на появата им; стратегия за управление на противодействието и минимизиране последиците от явлението.

Спецификата на предложената технология се определя от възможностите, които предлага подхода на управление на оперативното противодействие на сложни и динамично развиващи се предизвикателства и заплахи, изграждане на ефективна система за сигурност на социалната организация.

Разработването на модел за организация и управление на противодействието на посегателства в сферата на сигурността на фирмата в национален аспект, би допринесло за прилагане на адекватен на предизвикателствата подход за противодействие на съвременните глобални заплахи, една от които е нерегламентиран достъп до чуствителна информация.

Моделът следва да бъде разработен на база изучаване и проучване "Процедурите за управление на противодействието в сферата на сигурността" и принципите за защита сигурността на информацията и активите на организацията.

Системно в областта на фирмената сигурност акцента е поставен върху инструментите за защита, в контекста на изследване насочено към стратегията и концепцията за използване на тези инструменти.

Преди създаване на структура за сигурност в социалната организация е необходимо органите на управление да си поставят за цел изследване и определяне на концепция на контраразузнавателния цикъл -/КРЦ/ на оперативното противодействие срещу посегателства на фирмената сигурност. Концепцията обединява и определя пътя за изграждане и реализиране на КРЦ с цел развитие на фирмата /защита на секрети, неутрализиране на заплахи, понижаване на риска и предотвратяване на посегателства/, при ясното разграничаване на контраразузнавтеланата и разузнавателна проблематика на сигурността

Изследването цели и извеждане на ключови параметри и особености на нерегламентиран достъп до чувствителна информация, на база на което да се разработи стратегия за управление на оперативното противодействие.

Постигането на дефинираните цели в организацията налага решаването на следните задачи:

1. Изучаване на теорията за организация и управление на оперативното противодействие на посегателства срещу фирмената сигурност.

2. Обобщаване и систематизиране на нашия и чуждестранен опит за изграждане на ефективни системи за сигурност на социалната организация -фирмата.

3. Систематизиране на явните литературни източници и документи, отразяващи състоянието и системата за противодействие на нерегламентиран достъп до чувствителна информация във фирмата.

4. Анализ на тенденциите за нарастване на заплахата за сигурността на корпорацията от нерегламентиран достъп до чуствителна информация.

5. Разработване на модел за организация и управление на оперативното противодействие на посегателства срещу фирмената сигурност.

Обект на изследване е дейността по организация и управление на оперативното противодействие в сферата на сигурността за дадена социална организация, в аспекта "Процедури за управление на противодействието в сферата на фирмената сигурност" и принципи за защита сигурността на информацията и активите на фирмата. Обектът на изследване комплексно оценява всички аспекти на сигурността, дефинирани от проявата на многообразни, взаимозависими и динамично променящи се източници на заплаха и посегателства срещу организацията.

Предмет на изследването е дейността по управление на оперативното противодействие, вследствие нерегламентиран достъп до чувствителна информация във фирмата.

За постигане на целите на изследването в организацията могат да бъдат формулирани следните генерална и частни хипотези:

Генерална хипотеза – управлението на оперативното противодействие е комплексен подход, който може успешно да бъде приложен в сферата на фирмената сигурност, за надеждно противодействие на съвременните глобални заплахи и посегателства, елемент от които е и нерегламентиран достъп до чувствителна информация, за изграждане на гъвкава динамична система за сигурност - гарантираща изпълнението на мисията на социалната организация.

Тази постановка се конкретизира в следните частни хипотези:

1. Нерегламентираният достъп до чувствителна информация е една от основните заплахи за изпълнение мисията на корпорацията, поради тясната взаимозависимост на деянието с останалите глобални съвременни заплахи и проявата й, като основна характеристика, мотив или цел на другите посегателства за сигурността.

2. Управлението на противодействието на нерегламентиран достъп до чувствителна информация във фирмата е комплексна технология за ефективно противодействие на деянието, основана на целесъобразни проактивни действия за предотвратяване на нерегламентиран достъп и изграждане на функционираща среда за сигурност.

3. Ефективното управление на противодействието на посегателства срещу фирмената сигурност. може да бъде реализирано само при комплексни, синхронизирани действия на органите за фирмената сигурност, съответните органи на изпълнителната, законодателната и съдебна власти, като основна тежест и отговорност за реално противодействие имат органите за сигурност на съответната социална организация.

За постигане на по-висока ефективност в процеса на изследване е необходимо да бъде разработен модел на изследването, включващ:

1. Установяване на комплекса от причини и условията за развитие на деянието нерегламентиран достъп до чувствителна информация.

2. Диференциране на различните категории субекти на нерегламентиран достъп до чувствителна информация.

3. Определяне на основните характеристики на нерегламентиран достъп до чувствителна информация.

4. Анализ на прилаганите схеми за реализация на нерегламентиран достъп до чувствителна информация.

5. Систематизиране на форми, средства и индикатори за осъществяване на нерегламентиран достъп до чувствителна информация.

6. Планиране и организация на дейността по противодействие на нерегламентиран достъп до чуствителна информация – нормативна база, предотвратяване на нерегламентиран достъп до чуствителна информация, разкриване, неутрализиране и

подпомагане откритото пресичане на посегателства, разследване на нерегламентиран достъп до чуствителна информация, административни и дисциплинарни санкции за нерегламентиран достъп до чуствителна информация във социалната организация.

Значимостта и приложният характер на изследването се определя от конкретната специфика на социалната организация, разглеждана, като една от основните подсистеми на системата за национална сигурност на Р. България.

Литература:

1. Проф. д.н. инж. Йордан Начев - „Конкурентно разузнаване", -Сиела –Софт ЕНД Публишинг.
2. Тодор Бояджиев „Шпионажът като занаят" –Издателство „Захарий Стоянов" –София 12002год.
3. Бончо Асенов, Александър Кипров -„Теория на контраразузнането" – Издателска къща „Труд" –София 2000год. .
4. *от Мариан Lawlor,* -„Корпоративно контраразузнаване" - Публикувано от AFCEA International, Copyright © 2007 AFCEA International.
5. Стив Уайтхед –„Корпоративно контраразузнаване" - 1 юли 2003 г.
6. Желев, Ст. и др. Computer vision - simulation modules for a moving object selection 7 international conference, Liapaja affiliate, Latvia, May 2010.

ИНФОРМАЦИОННА СИГУРНОСТ И ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

ПЛАМЕН В. ГЕОРГИЕВ

PAPI2010@ABV.BG

INFORMATION SECURITY AND POLICY OF INFORMATION SECURITY

PLAMEN V. GEORGIEV

ABSTRACT*: The paper presents a definition, functions of the system of guaranteeing information security, methods of guaranteeing information security, possible attacks against information systems and policy of information security.*

Key words*: information security and policy of information security.*

Информацията все по-ясно се възприема като универсален и ключов ресурс за развитие на държавата и обществото. Нещо повече - толкова голяма част от живота ни "протича" в информационното пространство, че не случайно все по-често се говори за информационна ера и информационно общество.

Управлението, събирането, натрупването, обработването и достъпът до информация в съвременните държавни структури, правителствени и неправителствени

организации и фирми 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.

Важността на информацията и информационните процеси предизвикват все по-голям интерес и изискват все по-голямо внимание във всяка една организационна структура.

Силата на информацията е във влиянието й върху процесите, а ефектът й пряко зависи от създадените условия за достъп до нея и за нейната защита. Последното произтича от уязвимостта на информацията и информационните системи от различни злонамерени (хакерски) атаки. Това налага анализ и определяне на заплахите за информационната инфраструктура, дефиниране и провеждане на последователни мерки за всестранната й защита. Информационната инфраструктура от своя страна е в основата на други критични инфраструктури за страната като отбраната и сигурността, банково-финансовата система, службите за критични услуги (бърза помощ, полиция, противопожарна защита, спасителните служби) и др. Уязвимостта на информационната инфраструктура много лесно може да се превърне в уязвимост на зависещите от нея критични за обществото системи.

В този смисъл гарантирането на информацията, разбирано като осигуряване на постоянна наличност, интегритет, автентичност и конфиденциалност, е основа за гарантиране на развитието и сигурността.

С навлизането на информационните технологии, непрекъснато се увеличават и компютърните престъпления. Ежедневно се осъществява активен нерегламентиран достъп до държавни и фирмени бази данни и пароли. Според някои сведения, на всеки 3 сек. се появява по една заплаха в интернет, което прави около 5 млн. за три месеца. Кражбите във виртуалния свят стават все по-голям проблем, а щетите от тях - все по-осезаеми. Днес, вероятността да станем жертва на компютърно престъпление е много по-голяма, отколкото на физическо.

Сигурността на държавната и корпоративна информация онлайн е не по-малко важна дейност от останалите, но за съжаление, много ръководители разбират това едва след като са загубили част от нея или това е рефлектирало негативно върху дейността им.

В действителност не съществува 100%-а сигурност за информацията, но това не означава, че не трябва да се полагат грижи за нея. Въвеждането на ефективен процес за мениджмънт на информационната сигурност минимизира вероятността с 90% тя да бъде успешно атакувана и да бъдат загубени не само репутация, но и финансови средства.

На настоящия етап, в световен мащаб липсва единно определение на понятието „**информационна сигурност**". Исторически този термин се употребява за да изрази комбинацията между "компютърна сигурност" (COMPUSEC) и "комуникационна сигурност" (COMSEC). В най-общ план, същият може да бъде разглеждан като противодействие на всички възможни рискове за информационната сигурност и потенциални заплахи в киберпространството, разработването на злонамерен софтуер за извличане или умишлено унищожаване на информация, преднамерена подмяна на данни, дезинформация, унищожаване на информационни системи или на част от тях.

Обобщавайки казаното, може да се въведе работно определение според което, **информационната сигурност е състояние на защитеност на личностните, обществените и държавните интереси в информационната сфера от преднамерени или непреднамерени зловредни (хакерски) въздействия и недопускане на загуба на информационно превъзходство в националното информационно пространство [1].**

От своя страна, **националните интереси** в информационното пространство се формират като балансирана съвкупност от интересите на **личността, обществото и държавата**.

Интересите на личността се свеждат до реализиране на конституционните права и свободи на човека и гражданина за:

- свободен достъп до информация;
- използването на тази информация за осъществяване на незабранена от закона дейност;
- физическо, духовно и интелектуално развитие;
- защита на информацията, гарантираща сигурността на личността.

Интересите на обществото се заключават в:

- утвърждаване на националните идеали, интереси, ценности и демократични принципи;
- усъвършенстване и спазване на законите;
- постигане и поддържане на обществен консенсус за начините и средствата за постигане (гарантиране) на научно-технологичното, образователното и духовното развитие на обществото.

Интересите на държавата са насочени към:

- гарантиране на суверенитета;
- създаване на условия за политическа и социална стабилност;
- хармонично развитие;
- безусловно спазване на законността и правовия ред и утвърждаване на равноправното и взаимноизгодно международно сътрудничество в това пространство.

Информационната сигурност може да бъде разглеждана и като свойство на информационните продукти и системи, демонстриращо степента на достигнато преди всичко състояние на: **поверителност, отчетност, цялостност, достъпност и увереност**. [7]

Поверителност означава, че в определена степен данните в паметта, както и обработваните и предаваните не подлежат на неправомерен или случаен достъп и възпроизвеждане.

Отчетност означава, че действията на дадена единица могат да бъдат осъществявани единствено от нея, за което съществува определен каталог.

Цялостност означава, че техническите средства, технологиите и данните са защитени в достатъчна степен срещу непозволен достъп и изменение.

Достъпност означава, че за конкретно приложение са удовлетворени изискванията за защита срещу непозволен достъп.

Увереност означава убеденост, че са постигнати останалите четири цели на сигурността.

Всяка една система много внимателно се изследва за възможни **уязвимости**[1] и потенциални **заплахи**, с цел намиране на възможно най-рационалната й защита [4].

Информационната сигурност, се интересува от **идентифицирането на уязвимостите в системите и намирането на ефективна защита срещу потенциалните заплахи [4, 5].**

Всяка компютърна система е уязвима за атака. Политиката и продуктите на сигурността могат да намалят вероятността дадена атака да бъде в състояние да разбие защитите на системата, като накарат даден хакер да вложи толкова много време и ресурси, че това да не си заслужава разходите. Един основен принцип обаче гласи, че не съществува изцяло сигурна система.

Уязвимостите, в зависимост от мястото на податливост на системата на атака, могат да се разделят на:

- физически;
- природни;
- бедствия;
- хардуерни и софтуерни;
- в периферията;
- от излъчване;
- комуникационни;
- човешки;
- експлоатационни.

Физическите уязвимости се свеждат основно до сградите и компютърните зали. Злоумишленик може да влезе с взлом в компютърните приложения така, както и във всеки дом.

Природни уязвимости - компютрите са много уязвими на природни бедствия и на заплахи от околната среда.

Бедствия като пожар, наводнение и земетресение и др. могат да разрушат компютърните системи и база-данните.

Хардуерните и софтуерни уязвимости се определят от факта, че някои видове хардуерни повреди могат да компрометират сигурността на цялата компютърна система.

Уязвимости в **периферията** - дисковите пакети, ленти и печатащи устройства могат да бъдат откраднати или повредени от прах и химикали. Повечето дискови и лентови операции предизвикват презапис на файловите описатели, а не изтриват действително целия диск или лента и затова важни данни могат да бъдат възстановени от магнитен носител.

Уязвимости **от излъчване** - цялото електронно оборудване предизвиква електрическо и електромагнитно излъчване. Електронните подслушвачи могат да засекат сигналите, излъчвани от компютърните системи и мрежи и след това да ги възстановят. По такъв начин, информацията, съхранявана и предавана от системите и мрежите, става уязвима.

Комуникационните уязвимости се определят от факта, че при свързване на компютъра в мрежа, съществува възможност за проникване в цялата компютърна система. Съобщенията могат да бъдат засичани и подправяни. Комуникационните

[1] Уязвимостта е точка (място), където дадена система е податлива на външно въздействие (атака).

линии, свързващи компютрите един с друг или свързващи терминали с централен компютър, могат да бъдат прекъснати или физически повредени.

Човешки уязвимости - бивши служители, които искат да си отмъстят на работодателя или слабо подготвени администратори, представляват най-голямата от всички уязвимости и са най-честата причина за кражбата на фирмена информация. Сигурността на цялата система е често в ръцете на системния администратор. Обикновените компютърни потребители, оператори и други хора от експлоатиращия екип могат също да бъдат подкупени или принудени да предадат пароли, да "отворят врати" или по друг начин да изложат на опасност сигурността на системата.

Експлоатационни уязвимости - могат да се дискутират много варианти за лесно използване на различни типове уязвимости. Например подслушването на телефонен кабел или на клетъчен преносим телефон изисква само един скенер. Включването в система, която няма защита с пароли или е с минимален контрол, е почти толкова лесно. Подслушването на криптирана оптична комуникационна връзка, от друга страна, или прихващането на излъчвания от специално защитено оборудване е много трудно.

Заплахата е възможна опасност за системата, която може да бъде човек (системен хакер или шпионин), предмет (дефектна част от оборудването) или събитие (пожар или наводнение). Заплахите попадат в три основни категории:·**природни, случайни и преднамерени**.

Природни и физически заплахи са тези, които излагат на опасност всяко физическо лице и част от оборудването: пожари, наводнения, повреди в захранването и други бедствия. Не е възможно винаги да се предотвратят такива бедствия, но е възможно да се разберат бързо, ако някое от тях възникне (с противопожарни аларми, термометри и др.). Може да се минимизира шансът повредата да бъде сериозна. Може да се учредят органи, които да наблюдават за случаи, представляващи опасност за компютрите (като пушене). Може да се предпазят системите от бедствия (чрез пазене на резервни копия на важните данни в друга сграда или чрез организиране на система за резервни копия, която да се използва при опасна ситуация).

Случайни заплахи са тези които са породени от невежество - например някой потребител или системен администратор, който не е обучен както трябва, който не е чел документацията и който не разбира важността на правилното прилагане на защитните процедури. Някой потребител може да изпусне диск или може да се опита да актуализира неправомерно база данни и по невнимание да изтрие някой файл. Някой системен администратор може да стане супер-потребител и да промени защитата на файла с пароли или на важен системен софтуер. Много повече информация е компрометирана и загубена поради невежество, отколкото поради злонамереност.

Заплахите също така могат да бъдат определени като: **вътрешни** и **външни**. [7]

Най-опасните **вътрешни заплахи** мога да бъдат сведени до:

- нарушаване на установения регламент за събиране, обработване, съхраняване и предаване на информацията в сферата на отбранителния комплекс;

- преднамерени действия, както и грешки на персонала на информационни и телекомуникационни системи със специално предназначение; надеждно функциониране на информационни и телекомуникационни системи със специално предназначение; възможна информационно- пропагандна дейност, която подрива престижа на въоръжените сили и тяхната бойна готовност;

- нерешеност на въпросите за защита на интелектуалната собственост на предприятията от отбранителния комплекс, което води до изтичане в чужбина на изключително ценни държавни информационни ресурси; нерешеност на въпросите за социалната защита на военнослужещите и техните семейства. Тези заплахи да особено опасни в условията на изостряне на военнополитическата обстановка.

Външните заплахи, които заслужават голяма доза внимание са:

- всички видове разузнавателна дейност на чужди държави;

- информационно - техническите въздействия (включително радиоелектронната борба, проникването в компютърни мрежи) от страна на вероятни противници;

- диверсионно-подривната дейност на специални служби на чужди държави, осъществявана чрез методите за информационно- психологическо въздействие; дейност на чуждестранни политически, икономически и военни структури, насочена срещу националните интереси в отбраната.

От своя страна, външните заплахи могат да бъдат сведени в следните категории:

- агенти на чуждо разузнаване - те не се срещат навсякъде, но в действителност съществуват. Продуктите, използващи технологията TEMPEST (за специална защита) или криптиращите устройства, са най-подходящи за инсталиране там, където атаките върху определена информация са реалистична заплаха;

- терористи - реалното им присъствие са компютърните вируси. Съществуват и примери на целенасочени атаки срещу университетски компютърни центрове, военно-ремонтни центрове, съдебни сгради и др.;

- престъпници - компютърното престъпление е прикриваемо за разлика от много други типове престъпления. Целта може да бъде незаконна кражба или някакъв вид изнудване;

- корпоративни нарушители - корпоративните записи, памети и неформални съобщения стават понякога по-уязвими за атаките на конкуренцията;

- разрушители - когато хората говорят за разрушители или хакери, те обикновено имат предвид хакери, които са по-заинтересувани от предизвикателството да разбиват, отколкото от резултатите. Тези хакери могат да надничат в интересни данни и програми, но те обикновено не вършат това за пари или за политически дивиденти.

Атаките срещу информационните системи могат да бъдат обобщени в следните категории: [6]

- **кражба на пароли** - методи за получаване на други потребителски пароли;

- **социален инженерин**г - придобиване на информация, до която достъпът е забранен;

- **грешки и черни врати** - получаване (използуване) на преимущества посредством използуване на системни грешки;

- **възможностите за автентификация** - използване на дефектите (противоречивост и непълнота) на механизмите за автентификация;

- **грешки** (провали) **в някои протоколи** - протоколи с грешки в проектирането и реализацията;

- **изтичане на информация** - използване на системи като системата за подписване или системата за именуване за информация необходима на администратора или необходима за функционирането на мрежата, но която може да се използува за мрежови атаки;

- **отказ от обслужване** - опити за лишаване на потребителите от услугите на тяхната компютърна система.

Има много различни **типове на противодействие** в зависимост от уязвимостите и заплахите. Противодействията могат да се разгледат в следните измерения: **компютърна, комуникационна и физическа сигурност**.

Компютърна сигурност- означава защита на информацията, съхранявана в компютърните системи (за разлика от защитата при предаване или защитата на физическото оборудване). Съсредоточава вниманието върху възможностите на системния софтуер за контрол на достъпа до системата и до съхраняваните данни.

Комуникационна сигурност - означава защита на информацията по време на предаването и по различните възможни начини. Съсредоточава вниманието върху възможностите за мрежов достъп до компютърната система и върху технологиите, увеличаващи сигурността на системи, допускащи връзки с външния свят.

Физическа сигурност - означава защитата на компютърното оборудване от повреди, предизвикани от природни бедствия и злоумишленици. Включва всички възможни средства - от обикновени ключалки и ключове до смарт карти и биометрични устройства.

Защитата на системните ресурси на информационни системи на административните органи също е процес за противодействие, при който използването на системните ресурси се регулира в съответствие с политиката в областта на мрежовата и информационна сигурност и е позволено само за упълномощени лица чрез използваните от тях информационни системи. Това включва **предотвратяването на нерегламентиран достъп до ресурсите**.

Управлението на защитата от нерегламентиран достъп се категоризира на няколко степени в зависимост от оценките на потенциалните последствия за администрацията при нарушаване на конфиденциалността, интегритета и/или достъпността, както следва:

- **ограничено**, когато организацията продължава да изпълнява функциите си, но с понижена ефективност, на информационните активи са причинени незначителни вреди и финансовите загуби са незначителни;

- **умерено**, когато ефективността на основните функции на администрацията е съществено понижена, на информационните активи са причинени значителни вреди и финансовите загуби са значителни;

- **високо**, когато загубата на конфиденциалност, интегритет и/или достъпност оказва тежко или непоправимо въздействие на администрацията, при която тя загубва способност да изпълнява основните си функции, на информационните активи са причинени тежки вреди и финансовите загуби са много големи.

Политиката за информационна сигурност може да бъде разглеждана като съвкупност от правила и практики, чрез които една организация или държавата управлява, защитава и разпределя наличния информационен поток. Същата представлява своеобразна рамката, в която определена система осигурява своята защита и се изразява в описание на средствата за защита, обектите на защита, службите и механизмите и основни практически принципи.

Политиката за информационна сигурност може да бъде интерпретирана по няколко начина:

- **първата** интерпретация включва средствата за атака. Например атакуващият може да използува компютърни програми от типа на „вируси”, „червеи” и др., или

да използува стартирането на скриптове използващи грешки в използвания софтуер за да получи контрол над един процес;

- **втората** интерпретация е по отношение на резултатите. Компютърът трябва да бъде защитен срещу безусловните резултати на една атака;

- **третата** интерпретация предполага защита от четене, модифициране и изтриване на файловете и данните, предавани по мрежата.

На основата на националните интереси в информационното пространство се формират стратегическите и текущите задачи на **вътрешната и външната политика по проблемите на информационната сигурност на държавата**.

В контекста на определението за информационна сигурност, политиката за информационна сигурност може да бъде разглеждана като система (комплекс) от знания и технологии за рационално използване на ресурсите на държавата, с цел гарантиране на стратегическите й интереси, чрез защита на жизненоважните интереси на личността, обществото и държавата от заплахи в информационното пространство.

Структурата на политиката за информационна сигурност включва **четири основни компонента**, които се дефинират при отчитане на националните интереси:

- спазване на конституционните права на гражданина в областта на духовния живот, информационната дейност и духовното възраждане на нацията;

- информационното осигуряване на вътрешната и външната държавна политика;

- развитие на националната информационна инфраструктура и на националните информационни ресурси;

- защита на информационните и телекомуникационните средства и системи на територията на страната.

Политиката за информационна сигурност се основава на редица **принципи**, по–важните от които са:

- съответствие с Конституцията, действащото законодателство и международните закони, по които държавата е страна;

- съгласуване с националните интереси;

- отчитане на изискванията на националната сигурност;

- осигуряване на равен достъп до информация на гражданите и обществените групи, независимо от техния политически, икономически и социален статус;

- откритост;

- предимство на националните участници в създаването на информационните системи, технологии и инфраструктура и върховенство на националния интерес при предоставянето на информационни ресурси на чуждестранни оператори.

Държавните органи, осъществяващи политиката за информационна сигурност, носят отговорност за неутрализиране на различните външни и вътрешни въздействия върху националната информационна система за стратегическо ръководство.

Държавната политика в областта на информационната сигурност почива върху следните основни принципи:

- спазване на конституцията, законодателството, общопризнатите принципи и норми на международното право при дейността в тази област;

- правно равенство на всички участници в процеса на информационното взаимодействие, независимо от техния политически, социален и икономически статут,

основаващо се на конституционното право на гражданите за свободно търсене, предаване и получаване на информация по всички законни начини;

- приоритетно развитие на националните информационни инфраструктури и ресурси с цел гарантиране на жизненоважните национални интереси в информационната сфера и безпрепятственото свързване с международните информационни инфраструктурни ресурси.

В процеса на осъществяване на функциите и гарантиране на информационна сигурност държавата:

- провежда обективен и всестранен анализ и прогнозиране на заплахите в областта на информационната сигурност и разработва мерки за нейното гарантирани;

- организира дейността законодателните и изпълнителните органи на държавната власт за реализиране на комплекс от мерки, насочени към предотвратяване на, отблъскване и неутрализиране на заплахите за информационна сигурност;

- поддържа на обществените обединения, насочена към обективно информиране на населението за социално значими явления в обществения живот, към предпазване на обществото от изопачаване и недостоверна информация;

- осъществява контрол над разработването, създаването, развитието, използването, износа и вноса на средства за защита на информацията чрез тяхното сертифициране и лицензиране.

Първостепенните мероприятия за осъществяване на държавната политика за гарантиране на информационната сигурност са:

- разработване и внедряване на механизми за правните норми, регулиращи отношенията в информационната сфера, както и подготвяне на Програма за правно осигуряване на информационната сигурност;

- разработване и реализиране на стратегията "електронно правителство" за повишаване на ефективността на държавното ръководство и на дейността на държавните средства за масово осведомяване за осъществяване на държавната информационна политика.

Решаващ фактор за успешното реализиране на стратегията за „**електронно правителство**" е гарантирането на информационната сигурност на всички етапи на нейната реализация. Това изисква използването на необходимите инструменти за оценяване на ситуациите, заплахите и риска в реално време. За целта в плановете за нейното изпълнение се осигуряват и разпределят необходимите за тази цел ресурси.

Международното сътрудничество в областта на гарантирането на информационната сигурност също е неотменима съставна част на политическото, военното, икономическото, културното и другите видове взаимодействия на страните от международната общност. То трябва да съдейства за повишаване на европейската и евроатлантическата информационна сигурност и да допринася за сигурността в световното информационно пространство. Особеността на международното сътрудничество в областта на гарантирането на информация е, че се осъществява в условията на изостряне на международната конкуренция за притежавани на технологични и информационни ресурси, за доминиране на пазарите, както и на увеличаване на възможностите за създаване на "информационни оръжия". Едновременно нараства заплахата от агентурно и оперативно-техническо проникване на чужди разузнавания, включително с използване на глобалната информационна инфраструктура.

Посочените по-горе мероприятия за осъществяване на държавната политика за гарантиране на информационната сигурност са свързани с:

- приемането на държавни програми, повишаване на правната култура и компютърната грамотност на гражданите;
- развиване инфраструктурата на единното информационно пространство срещу заплахите на информационна война;
- създаване на безопасни информационни технологии за осъществяване на жизненоважните функции на обществото и държавата;
- пресичане на компютърната престъпност;
- създаване на информационно-телекомуникационни системи със специално предназначение в интерес на държавните органи и органите на местното самоуправление;
- гарантиране на технологична независимост на страната в областта на създаване на и експлоатация на информационно-телекомуникационни системи с отбранително предназначение.

Необходимо е да се развива система за подготовка на кадри, използване в областта на информационната сигурност както и да се хармонизират националните стандарти в областта на информационната сигурност с тези на международните общност.

Системата за гарантиране на информационна сигурност на Р България е част от цялостната система за национална сигурност. Основните й функции са:

- разбиране влиянието на природни, икономически и идеологически фактори върху ежедневния живот;
- определяне и поддържане на баланса между потребностите на гражданите, обществото и държавата за свободен обмен на информация и необходимите ограничения за разпространяването й;
- оценяване на състоянието на информационна сигурност, откриване източниците на външните и вътрешните заплахи, определяне приоритетните направления за предотвратяване, отблъскване и неутрализиране на тези заплахи;
- контролиране на дейността на държавните органи и органите на местното самоуправление, държавните и междуведомствените комисии, участващи в решаването на задачите за гарантиране на информационна сигурност;
- провеждане на единна техническа политика за гарантиране на информационната сигурност;
- защитаване на държавните информационни ресурси - преди всичко на държавните органи, органите на местното самоуправление и в предприятията на отбранителния комплекс;
- усъвършенстване и развитие на системата за подготовка на кадри, използвани в областта на информационна сигурност;
- осъществяване на ефикасно международно сътрудничество за гарантиране на информационната сигурност с отчитане на националните приоритети и защитата на националните интереси в международните организации.

Системата за гарантиране на информационна сигурност се изгражда в съответствие с Конституцията и законите на страната, които определят правомощията в сферата на информационната сигурност. Основните елементи на организационната система за гарантиране информационната сигурност на Р България са Народното събрание, президентът, Консултативният съвет за национална сигурност, Минис-

терският съвет, Съветът по сигурността към Министерският съвет, органите на изпълнителната и съдебната власт, междуведомствените комисии, органите за органите на местното самоуправление, недържавните обществени организации и граждани, които в съответствие със законодателството участват в решаването на всички задачи в тази област.

Народното събрание изгражда законодателната база на системата за информационната сигурност; определя приоритетните направления за работа по изграждане и развиване на системата за информационна сигурност. В рамките на парламентарния контрол и чрез своята постоянна Комисия по външната политика, отбрана и сигурност оценява законосъобразността на работата на изпълнителната власт и ефективността на използването но ресурсите за гарантиране информационната сигурност на страната; чрез Комисията по външна политика , отбрана и сигурност и/ или Комисията по европейска интеграция контролира изпълнителната власт в областта на външните аспекти на информационната сигурност.

Президентът на Р. България като върховен главнокомандващ на въоръжените сили в рамките на своите конституционни правомощия утвърждава стратегическите планове за действие на въоръжените сили в условия на информационни конфликти, кризи и война; оглавява Консултативния съвет за национална сигурност, в който се дискутират въпросите на гарантирането на информационната сигурност на страната, изискващи широк политически консенсус. [4]

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, 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 правонарушения 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.

Специфичните направления за усъвършенстване на системата за гарантиране на информационната сигурност в областта на отбраната са:

- систематичното разкриване на заплахите и техните източници, структуриране на целите за гарантиране на информационна сигурност в областта на отбраната и определяне на съответните практически задачи;

- сертифициране на общото и специалното програмно осигуряване, на пакетите приложни програми и средствата за защита на информацията в съществуващите и създаваните автоматизирани системи за управление с военно предназначение и в системите за връзки, които имат елементи на изчислителна техника;

- постоянно усъвършенстване на средствата за защита на информацията от несанкциониран достъп, развиване на защитени системи за връзки и управление на войските и оръжието, повишаване надеждността на специалното програмно осигуряване;

- усъвършенстване на структурата на функционалните органи на системата за гарантирането на информационната сигурност в областта на отбраната и координирането но взаимодействието им, усъвършенстване на похватите и способите за стратегическа и оперативна маскировка, разузнаване и радиоелектронна борба, на методите и средствата за активно противодействие на информационно- пропагандни и психологически операции на вероятния противник; подготовка на специалисти в областта на гарантиране на информационна сигурност за отбраната.

Посочените 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. Пенев П., Основи на националната сигурност. Учебно пособие, 2008.

2. Семерджиев Цв., Информационна сигурност. Софтрейд, 2004.

3. Шаламанов, В. Тагарев, Т. Информационни аспекти на сигурността. С. ПРО-КОН, 1996.

4. http://www.helpos.com/archive/preview-web/02_013_01_index.html

5. http://it-consalting.net/zashchita-ot-zakladok.php

6. http://www.help-antivirus.ru/protectioninformation/2/Index1.php

7. http://209.85.129.132/search?q=cache:mVHX3lIeV1sJ:www.daits.government.bg/dox/NIS-Ann5%D0%90.doc+%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%B8+%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%B8%2B%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B8&hl=bg&ct=clnk&cd=1&gl=bg

СЪВРЕМЕННИТЕ МЕДИИ МЕЖДУ СВОБОДАТА НА СЛОВОТО И ОТГОВОРНОСТТА ПРИ ОТРАЗЯВАНЕ НА ИНФОРМАЦИЯТА

Милена Д. Френкева
mdfole@abv.bg

MODERN MASS MEDIA BETWEEN THE FREEDOM OF SPEECH AND THE RESPONSIBILITY IN REPORTING THE INFORMATION

Milena D. Frenkeva
mdfole@abv.bg

Abstract: *Modern mass media is a factor of information influence and at the same time under pressure from a number of influential political and economic groups in society. On the one hand, the media has to balance between preserving the freedom of speech and, on the other hand, it has to take responsibility when covering topical events and news. This is difficult to achieve in view of the media contexts and the aspiration of the media itself for presenting sensations and news retaining the attention of the audience.*

Key words*: mass medias, society, information*

Въпросът за баланса между свободата на словото в съвременните медии и отговорността при отразяване на информацията присъства непрекъснато в дневния ред на СМК. Докъде се простира свободата на словото и къде медиите навлизат в опасни територии на манипулация и дезинформация на общественото мнение са теми, които вълнуват, както обществото, така и медиите.

В съвременното общество медиите играят важна и безспорна роля. Дори съществуват теории, според които именно средствата за масова информация са индикатор за наличието на демокрация и демократични ценности в дадено общество.

Добре известна е че събитие, което е станало, но не е отразено в медиите, все едно не се е случило за обществото. Вероятно го има и обратното - нещо да не е станало, но в резултат на медийна кампания на обществото да му изглежда, че се е случило. Светът става все по-медиен и от тази гледна точка отговорността на медиите ще става все по-голяма.

Един от основните концепти за изучаване на медиите е структурата на комуникацията. Тя се илюстрира най-често с класическия модел на Ласуел, наричан още формулата на петте К [2]. Моделът включва основните елементи, необходими за протичане на процеса на медийната комуникация:“кой” е комуникатора. “какво казва,” или медийното послание, “на кого” е реципиента или аудиторията, медийният канал (телевизия, радио, преса, интернет), ”с какъв ефект”е свързан с въздействието на медийната информация върху реципиента и неговите действия, продиктувани от взаимодействието с нея. Всеки елемент от модела на Ласуел е потенциален източник на определено влияние върху аудиторията.

Като представители на четвъртата власт, медиите осъществяват най-вече информационно социално влияние. Медиите влияят главно чрез предоставяне на

нова информация, която рамкират по начин, продиктуван от медийния контекст. Като основни разпределители на многобройните информационните потоци, СМК, играят важна роля в селектирането на информацията, подреждането на темите по важност, подчертаването на едни или други нейни аспекти [3,4]. Липсата или наличието на голямо количество информация по даден проблем, начинът, по който той се формулира, представя и анализира, оказва влияние върху начина му на разискване в обществото. Това поставя редица въпроси за отговорността на медиите пред обществото и определяне правилата на медийната етика, която би въпрепятствала възможните злоупотреби с медийната власт.

Според Тофлър медиите прилагат различни тактики за манипулиране на информацията, които той нарича образно "масажиране на съобщението". Чрез тях медиите прилагат различни стратегии за рамкирне и представяне на събитията [5]. Такива са тактиката на премълчаване, тактиката на общите приказки, тактика на игра с времето, тактика на раздробяването, тактика на заливането, тактика на димната завеса, тактика на ехото, тактика на "голямата лъжа" и "тактиката на преобръщане с главата надолу".

Медиите осъществяват информационна власт, произтича от това, че влияещият притежава ценна информация, която предоставя на обекта на влиянието, за да го убеди в наложителността на промяната. Информационната власт на медиите понякога се надценява, но и често се схваща като незначителна.

Информационната власт, която упражняват медиите произтича от това, че влияещият притежава ценна информация, която предоставя на обекта на влиянието, за да го убеди в наложителността на промяната. СМК са основен източник на информация за формиране на редица понятия, мнения и нагласи. Новата информация се натрупва в съзнанието на индивидите. Чрез честото представяне на подобни апели те се затвърждават в паметта и при многократно активиране стават лесно достъпни в паметта.

Социалното влияние и убеждаващите стратегии на медиите не могат да се разглеждат изолирано от социалния контекст на медийната комуникация, който оказва влияние върху дейността на медиите. Той включва в себе си различни субекти като държавата и законовата система, комерсиални влияния, медийна технология, организационна и професионална експертиза, конкурентни организации, собственици и контрол, реалният свят и пр. Всеки елемент от социаното обкръжение на СМК им оказва влияние в една или друга степен [4].

Информацията предоставена в медиите не се покрива напълно с реалната, а е нейно субективно отражение. Информацията се формира в значителна степен от интересите и представите на своя производител, и в този смисъл не съществува свободна от мнение и несвързана с определени интереси информация. Тя е едностранчива и субективна. Индивидуалното "преживяване" на ставащото, преминаването на съобщенията през личностната стойностна система в процеса на селекция, персонифицират всеки текст, имащ информационна стойност, т. е. нормират неговата индивидуална различност. Допълнителната намеса на редактори, режисьори и т.н. в оформянето на писмени, устни и визуални послания, предназначени за масов информационен обмен, предполага многостепенна, наслагваща се субективност.

Медиите оказват различни по сила и посока влияния върху аудиторията. Те използват разнообразни техники за манипулиране на информацията, които оказват

влияние върху начина, по който тя се възприема и интерпретира от аудиторията. В медийната психология са известни три основни медийни техники на влияние. върху постъпващата информация [2]. Те са свързани с начина, по който се подбира, оформя и поднася информацията. Най-важните от тях са: определяне на дневен ред (agenda setting), ефект на активиране (priming effect) и ефект на рамкиране (issue-framing effect).

Първата техника се свързва със способноста на медиите да отразяват определен проблем или тема като важни за деня. Поради липса на други ориентири в претоварения от информация свят, хората са склонни да се доверят на преценката на медиите.

Активирането се свързва с подготовка на аудиторията да оценява определено събитие въз основа на текущите новини. То се отнася до факта, че част от медийната информация може да повлияе на процеса на интерпретиране на следващите части от информация чрез настройване на определени зони на мислене.

Същността на тези два подхода е, че темите, подбрани от медиите влияят върху оценката на аудиторията чрез активиране на определени системи от знания [2].

Третият подход представя, че медийното рамкиране показва способността на медиите да формират обществено мнение и промяната на гледната точка. Той също може да бъде обяснен като следствие на схематичното мислене. Задълбочен анализ на особеностите на рамките е направен от Канеман и Тверски, в теорията за вземане на решение [2]. Според изследователите, повечето хора вземат решение в зависимост от влиянието на ситуационните фактори, а не на основата на обективните факти. Начинът, по който медиите представят възможните алтернативи на даден проблем пред аудиторията, оказва влияние върху избора на водеща алтернатива. В областта на рамкирането са и изследванията, посветени на приписването на отговорност за случващото се около нас. Ингар разглежда ефектите на атрибутиране на отговорността, основно като резултат от склонността към достъпност (accessability bias). Когато новините представят дадена тема в епизодични схеми, то аудиторията разполага с информация, засягаща хора и събития, и в същото време разполага с малко информация, която се отнася до системната или институционалната отговорност [2].

Гамсон също представя подобна гледна точка относно рамките на новините. Той разглежда конструкцията на разбирането по дадена тема като резултат от съчетанието на медийния дискурс, популярната мъдрост на обществото (popular wisdom) и личния опит. В неговия модел хората приписват знак на наблюдаваното събитие [2]. Рамката на разбиране по дадена тема от страна на отделния човек се формира извън посочените три фактора. Веднъж конструирана, тази рамка действа като гид за разбиране на проблемите и формиране на реакция спрямо събитията. Гамсон допуска, че влиянието на медийното послание се отнася до възприетото съдържание на проблема, модифицирано от културалния контекст [2].

Съвременни изследвания показват, че историите, които се представят в медиите често се избират от комерсиални, а не релевантни цели [9]. В много случаи, селекцията на новините може да се обясни с влиянието на фактори като организации на новинарски агенции, финансова зависимост от източници и нарастваща конкуренция между медиите. Медиите не могат да включат истории, които не подхождат на съществуващия формат или не се отнасят до съществуващата тема. СМК дефинират новинарската ценност на историята в зависимост от това дали носи белезите на самосбъдващо се пророчество. Медиите

предпочитат емоционални персонализирани истории, които са подходящи за политическия дневен ред на обществото. Социалните проблеми, свързани със заплахи, страхове и опасности, са много атрактивни за СМК и често заемат важна част от медийните истории [6, 7]. Те се нуждаят от реални събития и реални хора, които да придадат на медийната история човешко, атрактивно звучене. В някои случаи се преувеличават минимални рискове, а в други се пренебрегват сериозни опасности [8]. Между отделните медии съществува силна конкуренция относно отразяването на тези събития. Различни групи по интереси, политици и експерти се опитват да наложат своят дневен ред за тях. Медиите неизбежно играят ключова роля в този конфликт, защото изборът им на конкретен, експертен източник на информация, оказва влияние върху формирането на схващането за дадено социално явление или събитие. Медийното решение относно това, на кого е позволено да спомене или да дефинира даден проблем не е контролирано по демократичен начин [8; 7].

Медиите в постмодерната епоха

В изследвания на Gronbeck и Lucas от 2000 г.се установява, че развитието на масмедиите в постмодерната ера наложи промяна в схващанията за тяхната природа и роля в обществото. Оказва се, че в наши дни, не е в сила принципът за едностранно провеждане на информацията от комуникатора към реципиентите, независимо от аудиторията [4].

В постмодерната епоха аудиторията играе важна и значима роля в процеса на комуникация. Тя избира това, което е близко до възгледите й, а комуникаторът се опитва да влияе чрез проява на толерантност и гъвкавост по отношение на тях. Индивидите подкрепят силно нещата, в които и те вземат участие. Всичко е комуникация, комуникаторът е съобщението (т.е. всички личностни черти и външни характеристики на комуникатора въздействат на аудиторията). Съобщението е не това, което е изпратеното, а това, което е получено. Индивидите преработват информацията в зависимост от когнитивния си стил. Целта на комуникацията е установяване на доверие, което удовлетворява очакванията на аудиторията. Успешните комуникативни умения се свързват с усъвършенстване в получаването на обратна връзка от реципиента [4]. Всички тези особености на новите медии показват засилване ролята на аудиторията в определяне на водещите медийни теми. Това показва, че в съвременната епоха част от отговорността за достоверността на информацията се прехвърля върху аудиторията, която се информира от различни източници на СМК. По този начин тя засилва критичността си към медиите, а от там ги предизвиква да проявяват по-голяма коректност и точност при предоставяне на медийната информация.

Заключение

Медиите като носители на четвъртата власт в обществото е необходимо да предоставят достоверна информация за събитията, които се случват. От друга страна те носят отговорност за начина, по който рамкират и подреждат новините. Тяхната посредническа роля на медиатори между различни обществени групи в обществото и обществото като цяло изисква от тях умело да балансират между истината и справедливостта от една страна и толерантността и разбирането от друга.

Библиография
1. Ласуел, Х., С, 1992.
2. Русинова -Христова, А. (2003). Политическото говорене. Психологични механизми. София, Интерпрес.
3. Петев, Т. (2004). Теории за масовата комуникация. С. Изд. Св. Климент Охридски, ФЖМК.
4. Стоицова, Т. (2004). Лице в лице с медиите, С., Просвета.
5. Тофлър, А. (1992). Шокът от бъдещето. Народна култура, С.
6. Altheide, D. L. (1997). "The News Media, The Problem Frame, and the Production of Fear.", The Sociological Quarterly, 38, 646—668.
7. Altheide, D. L. 2002. Creating Fear: News and the Construction of Crisis. New York: Aldine de Gruyter.
8. Kitzinger J., Reilly J. (1997).The Rise and Fall of Risk Reporting: Media Coverage of Human Genetics Research, "False Memory Syndrome" and "Mad Cow Disease",. European Journal of Communication, 12, 319-350.
9. Shoemaker, P.J., & Reese, S. (1996). Mediating the message: Theories of influences on mass media content (2nd ed.).White Plains, NY: Longman.

ЗАПЛАХИТЕ И ДЕЙСТВИЯТА НА ХАКЕРСКАТА ГРУПА „АНОНИМНИТЕ", ОТРАЗЕНИ ВЪВ В. „24 ЧАСА"

Милена Д. Френкева
mdfole@abv.bg

THE THREATS AND ACTIONS OF THE ANONYMOUS HACKER GROUP AS REPORTED BY 24 CHASA NEWSPAPER

Milena D. Frenkeva

Abstract: *The article deals with analisis of the materials reporing the threats and the acts of Anonimus group in the 24 chasa newspaper during the period januari, 2010 – may, 2011. It establishes patern of distribution of the articles throughout the period as well as the characteristic features of media language. It also outlines the scoup of media topics. The words used in naming the Anonimus group and spesified as well as the synonyms signifying the Anonimus group. The article analyses the parallels with historical events from the present and the past year.*

Key words*: hacker attacks, group " Anonimius", content analisis, neuspapers, threats*

Увод

Интернет пространството разширява възможностите за комуникация и споделяне, и развива особен вид интернет комуникация. От друга страна улеснява активността на различни активиски групи, които преследвайки свои цели и идеи.

С атаките от типа на компютърния вирус "Стъкснет" (Stuxnet) или на тези, съпътствали аферата “Уикилийкс”, през 2010 г. интернет стана свидетел на появата на нов вид престъпници - т.нар. хактивисти, които са идеологически мотивирани, и кибервоините, които целят да предизвикат интернет хаос.

Според Катя Долмаджан от Франс прес хакерите, мотивирани от идеологически и политически причини, са новото лице на престъпността в интернет (2).

При анализа си Евгений Касперски, президент на фирмата за информационна сигурност Касперски се установява, че “в наши дни сме свидетели на бум на нови заплахи под формата на кибертероризъм” [2].

Според Жан-Филип Бишар, анализатор в “Касперски Лаб” целта, която преследват създателите на програми за злонамерено проникване в компютрите и организаторите на кибератаки, е достъп до информация и борба за влияние” [2].

Според Лоран Хело от фирмата за информационна сигурност “Симантек$ “в бъдеще независимо дали ще говорим за кибервойна, киберпартизани или кибертероризъм, целта ще бъде винаги политическа. Действията на киберпиратите няма да бъдат само обикновено жестикулиране с цел привличане на вниманието, а атаки срещу важни инфраструктури, които могат да доведат до хаос” [2].

Подобна дейност извършва хакерската група “Анонимните”, чиито действия и заплахи са обект на изследване в настоящата статия. Групата “Анонимните” са международна група от хакактивисти, които атакуват сайтове на редица компании, държави пр. Групата принадлежи към т.нар „хактивисти“, атакуващи предимно сайтове на компании, които по тяхно мнение, действат във вреда на сайта Wikileaks, на свободата в интернет и в живота, както и на върли врагове на копирайта. Характерно за групата “Анонимните” е, че няма ясно определена организация с йерархична структура, лидер или централизирано ръководство. При нея се наблюдава т.нар групово лидерство и географски разпръсната мрежова структура. В собствен смисъл това не е групировка, тъй като липсва закритост и постоянно членство: по-голяма част от членовете й са посетители на анонимни имиджбордове, действията се организират по схемата пост за предстояща атака — сбор на желаещите да вземат желание за участие — атака — дискънект.

“Анонимните” се формират през 2003 г. като малка група в имиджборда (вид интернет форум) 4chan. Като активна група с влияние се изявяват за първи път през 2008 г. Тогава провеждат първата си значима акция. Целта им е дружеството на сциентолозите, което се опитва да им наложи цензура. Хакерите блокират сайта на сциентолозите и организират демонстрации пред техните черкви.

Голяма популярност “Анонимните” получават в края на 2010 г. във връзка с ареста на Джулиан Асанж, основателя на “Уикилийкс”. Тогава групата предприема серия кибератаки срещу банките и компаниите, които са спрели паричните преводи за скандалния сайт. Сред жертвите на хакерите са “Виза” и “Мастъркард”.

Под ударите им попадат им най-яростните критици и противници на Асанж. Блокиран е сайтът на американския сенатор Джо Либърман. Той лобира за закон, по който Асанж би могъл да бъде съден за шпионаж. “Анонимните” атакуват личната страница и електронната поща на бившата губернаторка на Аляска Сара Пейлин, която призовава за физическото отстраняване на основателя на “Уикилийкс”.

През 2011 г. “Анонимните” започват атаки срещу правителството на Египет. Жертви на действията им са министерството на информацията в Кайро, както и

управляващата партия на тогавашния президент Хосни Мубарак. По подобен начин по-рано атакуват и властите в Тунис.

През юли същата година групата атакува американската консултантска компания "Бууз Алън Хамилтън".

В началото на 2012 се закрива "МегаЪплауд" - един от най-големите сайтове, предоставящ свободен достъп до различна музика и филми. Това предизвиква наймасираната атака от страна на "Анонимните". Минути след ареста на Ким Шмиц, собственик на сайта, и неговите сътрудници в Нова Зеландия групата започва наказателна акция срещу тези, които смята за инициатори на арестите.

Смята се, че групата сътрудничи с други по-малко известни хакерски групи по света. Филиали на "Анонимните" действат на територията на цял свят. Най-активни са представителите им в САЩ, Великобритания, Германия, Полша и Русия.

"Анонимните" използват маски, станали прочути от комикса на Алън Мур "V - като вендета", филмиран през 2006 г. В него главният герой V се опълчва срещу фиктивен тоталитарен режим в Англия. Той мъсти за сторените злини, при акциите си носи маската на легендарния Гай Фокс. Фокс е английски католик, който участва в т.нар. *Барутен заговор* срещу краля на Англия Джеймс I през 1605 г., хванат е, а по-късно екзекутиран.

Метод

Обект на настоящия анализ са статии, отразяващи заплахи и действия на хакерската група "Анонимните" във 24 часа и проследени в периода януари, 2011 – май, 2012 г. Основният метод, който е използван в изследването, е контент анализ. Статиите са подбрани по ключова дума *Анонимните* и са подложени на експертна оценка [1].

Анализът на изследването включва проучване на особеностите на медийния език и установяване на модела на разпределение на статиите през изследвания период. Следващата стъпка в анализа включва определяне на думите и словосъчетанията, използвани за етикетиране на действията и заплахите на Анонимните. Изследвани са също и синонимите за етикетиране на „Анонимните" на страниците на в. „24 часа".

Установени са особеностите на посланията на групата "Анонимните", съпровождащи техните действия и отговор на конкретни мерки от страна на правителства и други организации.

Обект на анализ са и метафоричните изрази, използвани за отразяване на действията на групата на "Анонимните".

Друга стъпка в анализа е свързана с определяне на водещите медийни теми и откриването на позоваванията на исторически събития – от настоящето и от миналото.

Резултати и дискусия

Модел на разпределение на статиите

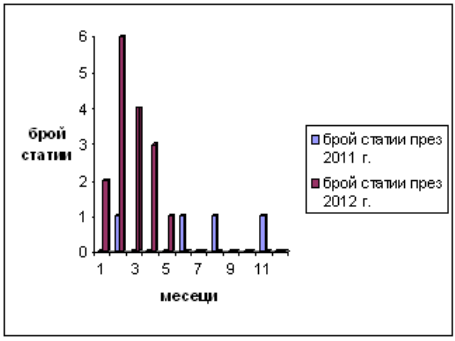
Резултатите от изследването показаха, че в в периода януари - декември, 2011 г. във в. „24 часа" са публикувани 4 статии, свързани с действията на групата "Анонимните", а в периода януари –май, 2012 г. - 16 статии. В тях са отразени различни заплахи и действия на групата "Анонимните", засягащи сайтове на различни институции по света и др. Моделът на разпределение на статиите за периода януари, 2011 г. – май, 2012 г. може да се проследи на графика № 1. На хистограмата ясно се

вижда увеличаване на броя на статиите за групата "Анонимните" през 2012 г. в сравнение с 2011 г. Най-много статии има през м. февруари, следван от месец март и април. Това е свързано с по-голямата активност на групата през 2012 г.

Медиен език и стил

Медийният стил е формален и информативен. Отразяването се характеризира се с честа употреба на компютърна терминология, кратки изречения и липса на емоционални апели. Статиите съдържат обикновено кратки, стегнати медийни послания, които се придържат до действителната фактология и използване на много компютърни термини. Наблюдава се известна сухота на изказа, което не е характерно за медийния език на „24 часа", чийто език е предимно разговорен и експресивен, но съответства но спецификата в дейността на изследваната група.

Графика № 1. модел на разпределение на статиите за групата „Анонимните" в периода януари – декември, 2011 г. и януари – май, 2012 г.



В хода на изследването се установи широка употреба на думи и словосъчетания за означаване на действията на (таблица № 1). Те са предимно с метафоричен характер и използват термини като атака, удар, които се свързват с военни и терористични действия. В случая те се употребяват, за да обяснят агресивния характер на действията на групата "Анонимните" върху компютърни сайтове. Наблюдава се пренос на терминология от една област – военно дело в друга област – компютърни технологии и по-специално компютърно пиратство.

Те се подразделят в следните основни групи:

- групирани около думи от военната терминология
- групирани около думи, съчетаващи думи от военната терминология и компютърни термини
- използване на компютърна терминология
- подчертаващи заплашителния характер на действията

Към първата група думи и словосъчетания спадат такива като: удар, атака, кординирана атака, акция и други. Те са директно заимствани от терминологията на военното дело и са пренесени в друга област на знанието за обяснение на действията на групата "Анонимните".

Към втората група, съчетаваща термини от военното дело и компютърните науки спадат думи и словосъчетания като кибератаки, кибернападения, хакерска

атака и др. При тях се вижда, че се създава нова терминология на границата между две науки за обяснение на действията на групата.

Третата група обхваща типична компютърна терминология, която обяснява спецификата в действията на групата "Анонимните". Тук се употребяват изрази като срив на сайт, Dos атаки, обезличаване (defacement) на интернет-сайтове и др. Тази група от думи и словосъчетания е с най-висока специфичност.

Синонимите за етикетиране на групата „Анонимните" са разнообразни (таблица № 2).

Таблица № 2. Част от синонимите за етикетиране на групата "Анонимните"

	Синоними
в. „24 часа"	хакерска група, хакерска група "Анонимните", хакери от "Анонимните", хакери от групата "Анонимните" , групата "Анонимните", "Анонимните", компютърни гении, "Анонимните", руския клон на организацията, група "Лулсек", клон на най-известния представител на хактивистите, групата "Анонимните", борци за справедливост, активисти от група "Анонимните" - храбрите воини на мишката, международната организация Anonymous

Те се разпределят в няколко основни групи (таблица № 3):

1. идетифициране на групата по нейното нейното наименование
2. идентифициране на групата на базата на занимаване на членовете й с хакерска дейност
3. идентифициране на групата на базата на компютърните умения на членовете
4. идентифициране на групата на базата на занимаване с хакактивиска дейност
5. идентифициране на групата на базата на занимания с компютърно пиратство
6. идентифициране на групата на геогравски и регионален принцип
7. смесени синоними
8. дусмислени синоними

Най-много синоними съдържат в себе си информация за наименованието на групата, което е обяснимо с факта, че то носи най-голяма информационна стойност и идентификационна сила за разпознаване на групата "Анонимните" от други сходни организации.

При анализа е установена честа употреба на така нар. "смесени" синоними, които идентифицират групата на базата на поне два характерни нейни особености: например - информация за името на групата и информация заниманието й с хакерска дейност (хакерската група, хакерската група "Анонимните") или информация за името на групата и информация за нейна региионална структура (група "Лулсек", клон на "Анонимните"). Употребата на тези синоними носи по-голяма информативност и показва стремежа на в. „24 часа" към по-прецизно и детайлно описание на групата за постигане на по-голяма яснота.

Интересни са двусмислените синоними, които според Даниел Пайпс се използват за действията на различни терористични групи и терористи. Тук групата е

свързана със синоними, които идентифицират представителите й със синоними като борци за справедливост, храбри войни на мишката и др. Тези синоними не показват каква е действителната дейност на групата и разрушителния характер на нейните действия върху сайтове на редица важни институции, организации и цели държави. Употребата на тези синоними в „24 часа“ е рядка.

Таблица № 3. Класификация на основните групи синоними за етикетиране на групата “Анонимните“

Групи	Синоними
идентифициране на групата по нейното име	„Анонимните" , групата "Анонимните", Членове на “Анонимните”
идентифициране на групата на базата на занимаване на членовете й с хакерска дейност	хакерската група, хакерската група “Анонимните”, Хакерите от "Анонимните", хакери от групата „Анонимните", хакерската организация „Анонимните"
идентифициране на групата на базата на компютърните умения на членовете й	компютърни гении
идентифициране на групата на базата на занимаване с акактивиска дейност	известния представител на хактивистите клон на ,най-известният представител на хактивистите
идентифициране на групата на базата на географско местоположение на членовете й	международната организация Anonymous, група “Лулсек”, клон на “Анонимните, местният филиал на групата
идентифициране на групата на базата на занимания с компютърно пиратство	виртуалните пирати
“смесени” синоними	хакерската група “Анонимните”, Хакерите от "Анонимните", хакери от групата „Анонимните",
дусмислени синоними	борци за справедливост, активисти от група, “Анонимните” - храбрите воини на мишката, романтични разбойници

Употреба на метафори при отразяване на действията на групата “Анонимните”

При отразяването на действия на групата “Анонимните” се използват най-често изречения, които съдържат като ключови думи като хакери, удари, удариха и сайтове. Подобни изрази са с метафоричен характер, в които акцентират на думата удар. Такива са фразите като “Хакери удариха сайта на Елисейския дворец”, “Хакери от “Анонимните” удариха ЦРУ”, “Анонимните” удариха много правителствени сайтове.

По подобен начин са изградени и метафоричните изрази, описващи действия на властите, насочени срещу дейността на “Анонимните”. Например: “Интерпол удари “Анонимните” и др.

Друг група метафорични изрази са “Анонимните” - храбрите воини на мишката”, “Анонимните се прочуха с успешните си пробиви на официални сайтове на властите в САЩ и други страни, сред които бе и сайтът на ЦРУ” и др.

Особеностите на посланията на групата "Анонимните"

Ще разгледаме особеностите на посланията на "Анонимните", които са представени във в.24 часа. Характерните им черти съдържат следните основни елементи:

- съдържат елемент на изненада
- появяват се паралелно по време на осъществен хакерски удар
- имат провокативен и пропаганден характер
- насочени са към конкретен обект на атака
- имат конкретна и специфична аргументация насочена към конкретна публика
- изразяват конкретна протестна позиция срещу предстоящи мерки или действия
- съдържат заплашителни апели към конкретен обект или институция
- съдържат апели за получаване на подкрепа от обикновеното население
- съдържат апели, насочени към промяна в обществото, изразяват мисията на групата, свързана със запазване на свободата.

Тематичен анализ

В статиите на „24 часа" се разглеждат редица акции на групата "Анонимните" в периода януари, 2011 - май, 2012 г. Основните медийни теми включват "Заплахи и действия на групата "Анонимните", Акции срещу групата "Анонимните", "Мястото на групата "Анонимните" в съвременния свят".

Най-много статии се групират в първата тема " Заплахи и удари на групата "Анонимните" - 12 статии (2 през 2011 г. и 10 през 2012 г.).

В темата " Акции срещу групата "Анонимните " са включени 4 статии (1 през 2011 г. и 3 през 2012 г.).

В третата тема "Мястото на групата "Анонимните" в съвременния свят" се включват 4 статии (1 през 2011 г. и 3 през 2012 г.)

Исторически позовавания

Наблюдават се исторически позовавания от настоящата история, тази тенденция е свързана с малката история на групата и спецификата на нейните действия, характерни за епохата на Интернет.

Историческите позовавания от настоящата история свързват групата "Анонимните" с най-влиятелните фигури на 2012 г според в. "Тайм", цитиран от в. 24 часа. Вестникът се е опитал да открои хората, чието въздействие е дълготрайно и запомнящо се през настоящата година. Въпреки, че включването в списъка да се приема за голяма чест, редакцията на в."Тайм" подчертава, че избраниците попадат в него, ако са повлияли за променянето на света за добро или за лошо. Водещите личности са разделени в пет категории - пробиви, пионери, магнати, лидери и икони. Тук са включени хакери (блогъри от Русия и Грузия), политически фигури (американския президент Барак Обама, кандидата за президент от републиканците Мит Ромни, държавния секретар Хилари Клинтън, президента на Бразилия Дилма Русеф и др.), хора от бизнеса (милиардера Уорън Бъфет, изпълнителният директор на "Епъл" Тим Кук и на Ай Би Ем Вирджиния Ромъти и др.), медийни звезди (съпругата на принц Уилям - Кейт Мидълтън, и сестра й Пипа, певицата Адел, много артисти и медийни звезди от САЩ), учени(Елинор Остръм, статистикът Ханс Рослинг и вирусологът Рон Фуше) спортисти (футболиста Леонел Меси , баскетболистът от Ню Йорк Джеръми Лин, Отличени са също тенисистът Новак Джокович, амери-

канският футболист Миа Хам, южноафриканският бегач с протези Оскар Писториус и китайската шампионка по голф Яни Цан).

Действията на групата "Анонимните" се свързват основно и с протестите срещу Акта и аферата Укиликс, личността на Джулиан Асанж., както и вълненията в Египет, Тунис и др.

Литературните препратки свързват анонимните с романтичните герои от литературата и киното Зоро и Робин Худ.

Заключение

В резултат на анализа беше установена широка употреба на думи и словосъчетания за означаване на действията и заплахите на групата "Анонимните". Използвани са разнообразни синоними за етикетиране на отделни представители или групата като цяло. Интерес представляват смесените синоними, съчетаващи термини от военното дело и компютърните технологии, както и двусмислените синоними, които не дават ясна представа за дейността на групата.

Медийният език на статиите е формален и информативен с придържане до фактологията на събитията и широка употреба на компютърна терминология. Точно и ясно се съобщават обектите на кибератаките и последствията от техните действия.

Наблюдава се широка употреба на метафори при отразяване на действията на групата Анонимните, както и при контрадействия от страна на властите срещу тях.

Историческите позовавания са свързани основно с настоящата история. Това е свързано с малката история на групата и специфичността на нейните действия, характерни за интернетната епоха.

Библиография

1. Стоицова, Т., Полио, Х. (2004). Ръководство за идентифициране на фигуративен език, Психологически изследвания, кн.3, 17 - 33.

2. Хактивисти поведоха войните в интернет, www.vesti.bg, , 7.01.2011 - http://www.vesti.bg/index.phtml?tid=40&oid=3524391

ЗАПЛАХИТЕ И ДЕЙСТВИЯТА НА ХАКЕРСКАТА ГРУПА "АНОНИМНИТЕ", ОТРАЗЕНИ В ИНТЕРНЕТ МЕДИЯТА WWW.VESTI.BG

Милена Д. Френкева

mdfole@abv.bg

THE THREATS AND ACTIONS OF THE HACKER GROUP "ANONYMOUS", REPORTING IN THE INTERNET MEDIA WWW.VESTI.BG

Milena D. Frenkeva

Absract: *The article deals with analisis of the materials reporing the threats and the acts of Anonimus group in the www.vesti.bg during the period januari, 2011 – may, 2012. It establishes patern of distribution of the articles throughout the period as well as the characteristic features of media language. It also outlines the scoup of media topics. The words used in naming the Anonimus group and spesified as well as the synonyms signifying the Anonimus group. The article analyses the parallels with historical events from the present and the past year.*

***Key words**: hacker attacks, group " Anonimius", content analisis, neuspapers, threats*

Увод

Интернет пространството разширява възможностите за комуникация и споделяне и развива особен вид интернет комуникация. От друга страна улеснява действията на различни активиски групи, които използват мрежата за постигане на злонамерени свои цели.

С атаките от типа на компютърния вирус "Стъкснет" (Stuxnet) или на тези, съпътствали аферата "Уикилийкс", през 2010 г. Интернет стана сцена за появата на нов вид престъпници - т.нар. *хактивисти*, които са идеологически мотивирани, и кибервоините, които целят да предизвикат интернет хаос.

Според Катя Долмаджан от Франс прес хакерите, мотивирани от идеологически и политически причини, са новото лице на престъпността в интернет [2].

При анализът на Евгений Касперски, президент на фирмата за информационна сигурност Касперски се установява, че "в наши дни сме свидетели на бум на нови заплахи под формата на кибертероризъм" [2].

Според Жан-Филип Бишар, анализатор в "Касперски Лаб целта, която преследват създателите на програми за злонамерено проникване в компютрите и организаторите на кибератаки през 2011 г., е свързана с осигуряване на достъп до информация и борба за влияние [2].

Лоран Хело от фирмата за информационна сигурност "Симантек" пояснява, че "В бъдеще независимо дали ще говорим за кибервойна, киберпартизани или кибертероризъм, целта ще бъде винаги политическа. Действията на киберпиратите няма да бъдат само обикновено жестикулиране с цел привличане на вниманието, а атаки срещу важни инфраструктури, които могат да доведат до хаос" [2].

Подобна дейност извършва хакерската група “Анонимните”, чиито действия и заплахи са обект на изследване в настоящата статия.

Групата принадлежи към т.нар „хактивисти“, атакуващи предимно сайтове на компании, които по тяхно мнение, действат във вреда на сайта Wikileaks, на свободата в интернет и в живота. Характерно за групата “Анонимните” е, че няма ясно определена организация с йерархична структура, лидер или централизирано ръководство. При нея се наблюдава нар групово лидерство и географски разпръсната мрежова структура. В собствен смисъл това не е групировка, тъй като липсва закритост и постоянно членство: по-голяма част от членовете ѝ са посетители на анонимни имиджбордове, действията се организират по схемата пост за предстояща атака — сбор на желаещите да вземат желание за участие — атака — дискънект.

Смята се, че тя сътрудничи с други по-малко известни хакерски групи. Филиали на “Анонимните” действат на практика по цял свят. Най-активните са в САЩ, Великобритания, Германия, Полша, Русия.

Членовете на тази група стават активни в края на 2010 г. и началото на 2011 г., когато бяха извършени серия политически мотивирани компютърни атаки срещу църквата на сциентолозите, фирмите за електронна търговия и банките. Сродна на тях група, наречена “Лулз Секюрити”, предприе собствени нападения в мрежата, след което отново потъна в анонимност.

“Анонимните” използват маски, станали прочути от комикса на Алън Мур “V - като вендета”, филмиран през 2006 г. В него главният герой V се опълчва срещу фиктивен тоталитарен режим в Англия. Той мъсти за сторените злини, при акциите си носи маската на легендарния Гай Фокс. Фокс е английски католик, който участва в т.нар. Барутен заговор срещу краля на Англия Джеймс I през 1605 г.

Метод

Обект на настоящия анализ са статии, отразяващи заплахи и действия на хакерската група “Анонимните” във www.vesti.bg и проследени в периода януари – май, 2012 г.. Основният метод, който е използван в изследването, е контент анализ. Статиите са подбрани по ключова дума *Анонимните* и са подложени на експертна оценка [1].

Анализът на изследването включва проучване на особеностите на медийния език и установяване на модела на разпределение на статиите през изследвания период.

Анализирани са послания на групата “Анонимните”, съпровождащи техните действия и отговор на конкретни мерки от страна на парвителства и други организации.

Следващата стъпка в анализа включва определяне на думите и словосъчетанията, използвани за етикетиране на действията и заплахите на Анонимните. Изследвани са също и синонимите за етикетиране на Анонимните на страниците на в. „24 часа“.

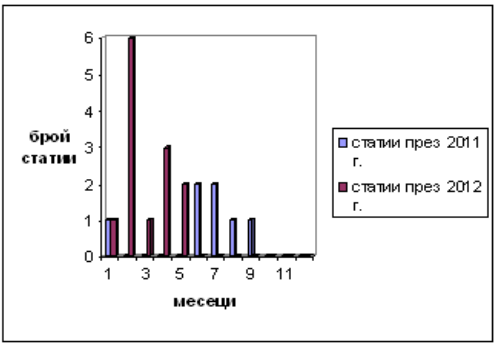
Друга стъпка в анализа е свързана с определяне на водещите медийни теми и откриването на позоваванията на исторически събития – от настоящето и от миналото.

Резултати и дискусия

Резултатите от изследването показаха, че в периода януари – май, 2012 г. действията на групата Анонимните са отразени в 7 статии през 2011 г и 13 статии през 2012 г. В тях са представени различни заплахи и действия на групата “Анонимните”, свързани с пробив на сайтове на редица важни институции по света и др.

Модел на разпределение на статиите

Моделът на разпределение на статиите за периода януари, 2011 г. – май, 2012 г. може да се проследи на графика № 1.



Графика № 1. модел на разпределение на статиите за групата „Анонимните“ в периода януари – декември, 2011 г. и януари – май 2012 г.

От хистограмата ясно се вижда увеличаване на броя на статиите за групата “Анонимните” през 2012 г. в сравнение с 2011 г. Това е свързано с по-голямата активност на групата “Анонимните” през 2012 г. Най-големият пик през 2012 г. се наблюдава през месец февруари, с 6 статии, следван от месец април с 3 статии.

Медиен език и стил

Медийният стил е формален и информативен, характеризира се с честа употреба на компютърна терминология, кратки изречения и липса на емоционални апели. Статиите съдържат обикновено кратки, стегнати медийни послания, които се придържат до действителната фактология и използване на много компютърни термини. Наблюдава се известна сухота на изказа, което не е характерно за медийния език на 24 часа, чийто език е разговорен и експресивен.

В хода на изследването се установи широка употреба на думи и словосъчетания за означаване на действията (таблица № 1). Те са предимно с метафоричен характер и използват термини като атака, удар, които се свързват с военни и терористични действия.

Таблица № 1. Широка потреба на думи и словосъчетания за означаване на действията на групата “Анонимните” във www.vesti.bg

	Думи и словосъчетания
www.vesti.bg	акт, атаки, кибератаките срещу уебсайтовете, хакерска атака срещу сайтове, атаките от типа "отказ на услугата" (DOS), , технологии за хакване, нападение, масирано нападение, кибернападения, кражба, война, координирани кибератаки, координирани кибернападения, киберпрестъпления., различни пунктове в конспирация и умишлено повреждане на защитен компютър, нарушения, , кибпрестъпност, хактивизъм, кибератаки, кибертероризъм, по-скоро политически театър, отколкото война в интернет, войната в мрежата, кибервойна, хакерска война, война в Интернет, повече демонстрация и политическа агитация, отколкото истинска интернет война, атаки хактивизъм

Използваните думи и словосъчетания за означаване на действията и заплахите на групата "Анонимните" се подразделят в следните основни групи:

- групирани около думи от военната терминология
- групирани около думи, съчетаващи термини от военното дело и компютърни термини
- използване на компютърна терминология
- подчертаващи заплашителния характер на действията
- подчертаващи престъпния характер на действията

Към първата група думи и словосъчетания спадат такива като удар, атака, кординирана атака, акция и други. Те са директно заимствани от терминологията на военното дело и са пренесени в друга област на знанието за обяснение на действията на групата "Анонимните".

Към втората група, съчетаваща термини от военното дело и компютърните науки спадат думи и словосъчетания като кибератаки, кибернападения, хакерска атака и др. При тях се вижда, че се създава нова терминология на границата между две науки за обяснение на действията на групата.

Третата група обхваща типична компютърна терминология, която обяснява спецификата в действията на групата "Анонимните". Тук се употребяват изрази като срив на сайт, Dos атаки, обезличаване (defacement) на интернет-сайтове и др. Тази група от думи и словосъчетания е с най-висока специфичност.

В последните две групи се подчертава заплашителния и престъпен характер на действия на групата.

Синонимите за етикетиране на групата "Анонимните" са разнообразни (Таблица № 3). Те се разпределят в следните основни групи:

1. идетифициране на групата по нейното наименование
2. идентифициране на групата на базата на занимаване на членовете й с хакерска дейност
3. идентифициране на групата на базата на компютърните умения на членовете
4. идентифициране на групата на базата на занимаване с активиска дейност
5. идентифициране на групата на базата на занимаване с компютърно пиратство
6. идентифициране на база на занимаване с престъпна дейност
7. идентифициране на групата на геогравски и регионален принцип
8. смесени синоними
9. дусмислени синоними

Таблица № 3. Класификация на основните групи синоними за етикетиране на групата "Анонимните"

Групи	Синоними
идетифициране на групата по нейното име	"Анонимните", добре (не)познатите ни Anonymous, Anonymous, движение
идентифициране на групата на базата на занимаване на членовете й с хакерска дейност	хакери, хакерите от Anonymous, хакерска група, хакерската група "Анонимните", Хакерите "Анонимните", хакери от групата", хакерската организация", хакерско движение, хакерското движение "Анонимните" (Anonymous), хакерски кръг "Анонимните"

Групи	Синоними
идентифициране на групата на базата на компютърните умения на членовете	компютърни гении
идентифициране на групата на базата на занимаване с хакактивиска дейност	известния представител на хактивистите, клон на ,най-известният представител на хактивистите, активисти на движението “Анонимните”, хактивистката организация Anonymous,
идентифициране на база на занимаване с престъпна дейност	новите престъпници
идентифициране на групата на базата на географско местоположение на членовете й	руското крило на "Анонимните", гръцки хакери, германска хакерска организация “Анонимните”, членове на прословутия хакерски кръг “Анонимните”, членове на “Анонимните”, италианските “Анонимни”, италиански хакери, членове на полския клон на международната група “Анонимните” (Anonymous)
идентифициране на групата на базата на занимания с компютърно пиратство	кибер пирати, интернет пирати, пирати, пирати от групата “Анонимните”
“смесени” синоними	хакерската група “Анонимните”, , хакери от групата “Анонимните”, хакерско движение, хакерска група, активисти на движението “Анонимните”, международната хакерска мрежа “Анонимните”
дусмислени синоними	киберпартизани

Най-честа употреба имат синонимите на групата, които съдържат в себе си информация за името на групата, и тези, които са свързани с извършваната от нея хакерска дейност.

При анализа е установена употреба на така нар. “смесени” синоними, които идентифицират групата на базата на поне два характерни нейни особености: например - информация за името на групата и информация заниманието й с хакерска дейност (хакерска група “Анонимните”, хакерите от “Анонимните”) или информация за името на групата и информация за нейна региионална структура (руското крило на “Анонимните”, гръцки хакери и др.). Употребата на тези синоними носи по-голяма информативност и показва стремежа на www.vesti.bg към по-прецизно и детайлно описание на групата за постигане на по-голяма яснотав отразяването.

Интересни са двусмислените синоними, които не показват каква е действителната дейност на групата и разрушителния характер на техните действия.

Тук представителите на “Анонинимните” са представени като киберпатизани. Употребата на тези синоними в www.vesti.bg е рядка.

Употреба на метафори при отразяване на действията на групата

При отразяването на действия на групата “Анонимните” се използват най-често изречения, които съдържат като ключови думи атакуват, атака, пробив и др. Такива са фразите “Кибератаки извадиха временно от строя и над 40 правителствени сайта в Малайзия “, ”, Анонимните опитаха да саботират наградите "Гоя” и др.

По подобен начин са изградени и метафоричните изрази, описващи действия на властите, насочени срещу дейността на "Анонимните". Например: "ФБР подгони хакерите от "Анонимните " и др**.**

Друг група метафорични изрази са "Хактивисти поведоха войните в интернет", Хакерските атаки - по-скоро политически театър, отколкото война в интернет и др.

Особеностите на посланията на групата "Анонимните"

Основните характеристики на посланията на групата "Анонимните" съдържат следните компоненти: елемент на изненада; появяват се паралелно по време на осъществен хакерски удар; имат провокативен, пропаганден и наказателен характер; насочени са към конкретен обект на атака; имат конкретна и специфична аргументация насочена към конкретна публика; изразяват конкретна протестна позиция срещу предстоящи мерки или действия; съдържат заплашителни апели към конкретен обект или институция; съдържат апели за получаване на подкрепа от обикновеното население; съдържат апели насочени към промяна в обществото; изразяват мисията на групата, свързана със запазване на свободата на личността, свободата на словото и информацията в интернет.

Често пъти в края на своите послания групата "Анонимните" поставя своя девиз: "Ние сме "Анонимните". Броят ни е безчет. Ние не прощаваме. Ние не забравяме. Чакайте ни."

Вижда се ясно изразеният заплашителен характер на девиза, употребата на кратки апели – изградени от прости изречения, съдържащи информация за силата на организацията, изградена от много хора (обичайното назоваване на групата в редица послания с фразата "Името ни е легион"), както и нейните намерения за нови атаки в бъдеще време.

Ето част от посланията на групата, отразени във www.vesti.bg по повод различни акции на групата:

"Бихме искали да привлечем вашето внимание, надявайки се да се вслушате в предупрежденията ни. Вашето средство за комуникация, което всички така обожавате, ще бъде унищожено. Ако сте активист или просто човек, който иска да защити свободата на информация, тогава присъединете се към каузата. Убийте "Фейсбук", за да запазите неприкосновеността на личния си живот"(при заплахата на "Анонимните " за спиране на Фейсбук)

"Анонимните" реши днес да обсади сайта ви в отговор на доктрината, на литургиите и на абсурдните и анахронични концепции, които вашата организация със стопанска цел (Римската апостолическа църква) разпространява в цял свят." (при удара на "Анонимните" срещу сайта на Католическата църква).

Тематичен анализ

В статиите на www.vesti.bg се разглеждат редица акции на групата "Анонимните" в периода януари, 2011 - май, 2012 г.

Статиите се разпределят в следните основни теми: Заплахи и действия на групата "Анонимните", Акции срещу групата "Анонимните", Мястото на групата "Анонимните" в съвременния свят".

Най-много на брой статии са включени в първата тема - 14 статии (5 - 2011 г., 9 през 2012 г.). Тук са отразени редица акции на групата като нападението срещу системата за електронни разплащания "ПейПал"**,** блокирането на сайта на ЦРУ и сайта на американския Сенат, заплахата за спиране на Фейсбук, атаките срещу правителствени сайтове в Полша, атаката срещу сайта на българската организация

за авторски права Профон, заплахата за спиране на Интернет, блокирането на сайта на католическата църква във Ватиката и др.

Във втората тема са групирани три статии (1 през 2011 г 2 през 2012 г.) В третата тема са включени три статии (1 през 20111 , 2 през 2012 г.).

Исторически позовавания

Наблюдават се главноо исторически позовавания от настоящата световна история, което е свързано с малката история на групата и спорадичния характер на нейните действия. Позоваванията са свързани с личността на Джулиан Асандж и "Уикиликс", споразумението АСТА , хакерските атаки в Грузия през 2007 г. и Русия през 2008 г., кибератаката с вируса "Стъкснет", който поразява чувствителни инфраструктури, главно в Иран, кибератаката срещу Гугъл, кризата в Гърция и др.

Заключение

В резултат на анализа беше установена широка употреба на думи и словосъчетания за означаване на действията и заплахите на групата "Анонимните". Използвани са разнообразни синоними за етикетиране на отделни представители или групата като цяло. Интерес представляват смесените синоними, съчетаващи термини от военното дело и компютърните технологии, както и двусмислените синоними, които не дават ясна представа за дейността на групата..

Медийният език на статиите е формален и информативен, с широка употреба на компютърна терминология. Точно и ясно се съобщават обектите на кибератаките и последствията от техните действия.

Наблюдава се широка употреба на метафори при отразяване на действията на групата "Анонимните", както и при контрадействия от страна на властите срещу тях.

Историческите позовавания са от настоящата история и рядко от минала история. Това е свързано с малката история на групата и специфичността на нейните действия, характерни за интернетната епоха.

Библиография

1. Стоицова, Т., Полио, Х. (2004). Ръководство за идентифициране на фигуративен език, Психологически изследвания, кн.3, 17 - 33.
2. Хактивисти поведоха войните в интернет , www.vesi.bg, 7.01.2011 - http://www.vesti.bg/index.phtml?tid=40&oid=3524391

РАЗВИТИЕ НА АНОНИМНИТЕ МРЕЖИ И АСПЕКТИ НА СИГУРНОСТТА В БЪДЕЩИТЕ МРЕЖИ

Красимир О. Славянов, Линко Г. Николов

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

k.o.slavyanov@gmail.com linkonikolov@mail.bg

EVOLUTION OF THE ANONYMOUS NETWORKS AND SECURITY ISSUES IN THE FUTURE NETWORKS

Krasimir O. Slavyanov, Linko G. Nikolov

ABSTRACT: *Today the speed and anonymity of cyber-attacks makes distinguishing the actions of terrorists and criminals very difficult. Therefore, anonymity and privacy are increasingly important issues. A variety of existing or proposed anonymous networks achieve diverse levels of anonymity against a variety of adversarial attacks. Key anonymity and privacy components in the future networks are: anonymity property, adversary capability, virtualization and network type.*

KEYWORDS*: Future networks, routing, anonymous networks, MANET, pseudonyms, public key, onion routing, cyber warfare, encryption*

1. Бъдещи мрежи

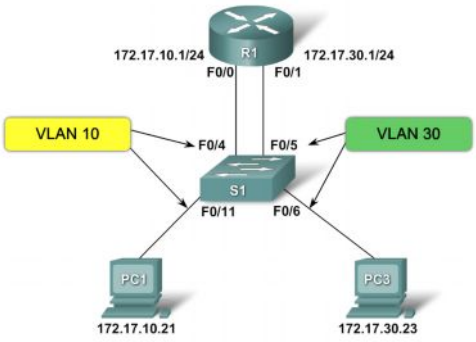
Към момента в Интеренет няма полета за име при идентификацията на хоста. Вместо това се използват IP адресите, които на практика указват местоположението на възела. Тази двойна роля създава проблеми за мобилността, мултихоуминга (технология за повишаване на мрежовите връзки с помощта на допълнителни алтернативни мрежови интерфейси и IP адреси), защитата и маршрутизирането в Интернет. За да се решат тези проблеми са започнали изследвания на архитектури за разделянето на идентификатор (име на хост) и локатор (IP адрес).

Бъдещите мрежи носят със себе си проблеми, свързани с адресното пространство. ITU-T е установил Въпрос 21, който касае изискванията към бъдещите мрежи и степенувано стандартизира техните функционални архитектури. Тези дейности са подкрепени от огромния обем проучвания и експерименти върху бъдещите мрежи – проект AKARI в Япония (http://akari-project.nict.go.jp), Future Internet Forum (http://fif.kr) в Корея, FIRE (http://cordis.europa.eu/fp7/ict/fire/) в Европа, както и FIND (www.nets-find.net) и GENI (www.geni.net) в САЩ [1].

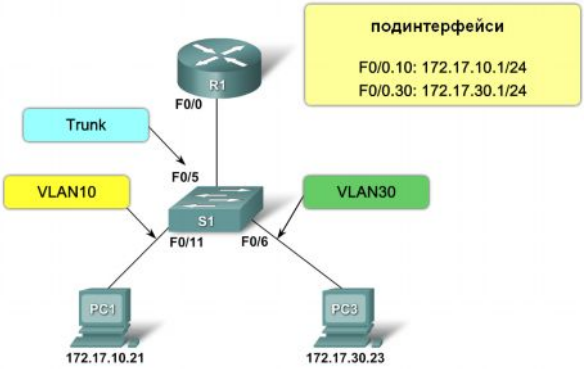
Вследствие на проекта FIND, Националната Научна Фондация наскоро стартира програма Бъдеща Интернет Архитектура под която са избрани четири проекта (Named Data Networking, MobilityFirst, NEBULA, и eXpressive Internet Architecture). Тези предложения целят главно да реализират съдържателно-ориентирани мрежови архитектури, които включват надеждни характеристики по сигурността и мо-

билността. Другото широко коментирано предложение касае възможността множество виртуални Интернет мрежи на съществуват по една физическа платформа. Организирането на виртуални мрежи допринася за повишаване на сигурността между различните LAN мрежи.

Фиг. 1. Настройване на нормално маршрутзиране между VLAN мрежи



Нормалното маршрутизиране отнема голямо количество портове от рутера, което е нерентабилно. Като по-подходящ метод се използва маршрутизиране чрез рутер на един порт и подинтерфейси:



Фиг. 2. Настройване на VLAN маршрутзиране чрез рутер на един порт

На базата на изходен документ от Фокус-групата за Бъдещи Мрежи (FG-FN), основана преди две години от ITU-T, е представена Препоръка Y.3001 [2], която описва целите и насоките при проектиране. Тя разграничава четири раздела (услуги, данни, околна среда и социално и икономическо осъзнаване), които ще отличават бъдещите мрежи от сегашните. Идентифицирани са 12 насоки, за да се реализират тези идеи: разнообразие на услугите; функционална гъвкавост; виртуализация на ресурсите; достъп до данни; разход на енергия; универсалност; икономически стимули; управление на мрежата; мобилност; оптимизация на мрежата; идентификация; **сигурност и надеждност.** Сегашните пакетни преносни мрежи –

Интернет и Мрежи от ново поколение (NGN) са базирани на два вида адресни пространства:

- имена на домейни;
- IP адреси.

Интернет приложенията преобразуват буквеното име на домейна в цифров интернет адрес чрез справка в системата DNS. Новите реалности с нарастващото потребление на IP терминали и обединяването на Интернет като основополагаща платформа за все повече и повече приложения, допринесоха за появяването на проблеми с използването на органиченото пространство от IP адреси. Проблеми възникват и в семантиката на мрежовия протоколен стек – един и същ IP адрес се използва както за идентификатор на хост в транспортния слой при инициализирането на завършването на сесия или услуга, така и за локализиране на хоста местоназначение в мрежовия слой. Този адрес се използва и от рутерите, които преглеждат заглавната част на IP пакета, за да определят маршрута. Многостепенната роля на един и същ IP адрес прави трудна работата по проектирането на ефективни решения за мобилност, сигурност и маршрутизиране. Новият стандарт за Интернет адресиране IPv6 предвижда рисковете и усилията са насочени към повишаването на сигурността.

2. Кабелни Интернет анонимни мрежи

Желанието да се запази сигурността и тайната в киберпространството подтиква изследването в областта на анонимните мрежи. Всяка единица, работеща в киберпространството е податлива на кибер атаки. Интернет днес е невероятно ефективно и неконтролирано оръжие за подслушване и шпиониране. С кибер атаките, целящи да получат разузнавателна информация и да прекъсват комуникацията, се задава нова ера на война. Ето защо, тайната и анонимността са въпроси с нарастваща важност. Предложени са анонимни мрежи, които постигат нива на поверителност срещу различни атаки [3, 8].

Този раздел представя огромния брой внедрени или предложени анонимни мрежи. Всеки протокол е обобщен и са подчертани главните предимства и недостатъци.

2.1. Анонимник [4] – това е HTTP прокси, който филтрира идентифициращата заглавна част и адреса на изпращача от Web-браузъра. Анонимникът предлага на потребителите бърз начин за анонимно сърфиране без да се разкрива тяхната идентичност. Смесената топология и маршрут се състои от единствен възел – Анонимизиращ сървър. Силните страни са ниско закъснение, лесно внедряване и повишаване на анонимността. Слабите страни са невъзможност за криптиране, защита на влизането и скритост на пренасочването.

2.2. Java Anon Proxy – е работеща анонимна мрежа за сърфиране в уеб-пространството. При тази мрежа единствен адрес е споделен между много потребители така, че подателя и комуникационната анонимност са защитени от противниците и получателя (уеб-сайта). Клиентът взаимодейства паралелно, като използва предварително определена последователност на смесването. Силна страна е трудното осъществяване на трафик анализ, поради големия брой потребители, използващи един и същ микс.

2.3. PipeNet – това е прост теоретичен модел за сърфиране през Интернет. Той е протокол от 3-ти слой с ниско закъснение подобен на Mixmaster с допълнителен трафик като защита срещу синхронизиращи атаки. Всички потребители изпращат

истински или фалшиви съобщения във всеки времеви слот, идентичен с каскадния микс, като използват криптиране. Каскадния микс се състои от предварително установени и фиксирани 3 до 4 маршрута. Качествата като силна анонимност и защита от трафик анализ са в противотежест с непрактичността на модела, уязвимост от DoS атаки и ниска ефективност. Проблема с ниската ефективност идва от постоянните криптирани линии с дълго времетраене, заемащи честотна лента и ресурс и водещи до високи разходи.

2.4. Onion Routing (Tor) – [5, 6] добре изследвана анонимна комуникационна мрежа за интерактивен Интернет трафик като Web, Internet Relay Chat (IRC) and Secure Shell (SSH). Onion Routing установява вериги със асиметрични ключове и скрива адресите на подателя и получателя. Този модел е вграден на приложно ниво или транспортния слой и предлага анонимност на подателя, получателя и комуникационната мрежа. Основни предимства са, че осъществяваните връзки са независими от приложенията и са криптирани по слоеве. С това се постига възпиране на атаки с трафик анализ. Слабост е липсата на защита от глобален активен противник. От тук идва уязвимостта на атаки, които могат да управляват (или следят) много различни елементи от мрежата едновременно.

2.5. Freedom Network – [6] вградена е в 3-ти слой и е подобна на Onion Routing. Тази мрежа използва слоеве на криптиране и позволява голямо разнообразие от псевдоанонимни действия. Анонимността се осъществява чрез заместването на различните поддържани протоколи и изпращането на пакети през частни мрежи преди доставянето им до Интернет. Основен компонент в тази система са AIPs (анонимни Интернет прокси сървъри). Това са мрежови прокси демони, които пропускат капсулирани пакети помежду си, преди да се изпратят към Интернет. Топологията е ациклична, каскаден микс и с определена дължина на маршрута. Подателят може произволно да избере пътят без завръщане, но дължината е фиксирана в 3 междинни възела. Положителни страни на тази мрежа са ефективността и значителна (но не максимална) защита срещу DoS атаки. Недостатъците са зависимостта от използваните приложения и уязвимостта към трафик атаки. Например, ако се използват блокове-отговори за e-mail, глобален неприятел като правна агенция, законодател, разузнавателна агенция, организирана престъпност или хакери, могат да разобличат истинския e-mail адрес на подателя и да го използват за собствени цели.

2.6 Cyberpunk – [7] Киберпънк е „тип I" компютърна e-mail услуга която препредава текста на съобщенията без да разкрива информация за постигане на анонимност с ключ без да смесва съобщенията. Този метод осигурява само комуникационна анонимност. Маршрутът се избира следствие на поредица от податели. Силна страна на този метод е осигуряването на силна анонимност, като се има предвид липсата на псевдоними и липсата на секретни идентификационни таблици. Друго предимство се основава на факта, че редицата от податели получават криптирани и-мейли, декриптират ги и подават наново полученото писмо. Това допринася за предпазването от подслушване на зложелатели, които се свързват с входящите и изходящите съобщения.

3. Безжични анонимни мрежи

Динамичната топология на безжичните мрежи, поради мобилността, грешки при маршрутизиране и влизане и излизане от възли прави опита за активното под-

държане на топологията много скъп. Това разкрива познаването на отделните възли за недоброжелателите. Безжичният стандарт IEEE 802.11 определя конкретните топологии, за да позволи мобилността на възлите да бъде прозрачна за по-високите слоеве на протокола [9]. Тези топологии включват мрежи с основен пакет услуги (Basic Service Set (BSS) networks), мрежи с разширен пакет от услуги (Extended Service Set (ESS)), както и мрежи с независим основен пакет услуги (Independent Basic Service Set (IBSS)). На фигура 4 са показани двете основни мрежи [8].

Фиг. 4. Мрежи BSS и IBSS

Мрежа BSS притежава мобилни възли в една и съща зона, които комуникират през една точка на достъп. Всеки мобилен възел предава всички пакети до точката за достъп, която ги препраща в рамките на същата зона или по централната система за дистрибуция. Мрежата с разширен пакет услуги се състои от една или повече BSS мрежи, в които всяка точка за достъп действа като Ethernet бридж и комуникира по системата за дистрибуция.[32] Тези топологии могат да постигнат анонимност както при кабелният тип мрежа.

За разлика от тях, мрежата IBSS или „ad-hoc" възлите на мрежата комуникират директно един с дуг. Точковата линия показва,че един или повече възли все още могат да имат достъп до централната система за дистрибуция. IBSS изисква различен подход за постигането на анонимност. „ad-hoc" мрежите се самоорганизират, изграждат се бързо и с не толкова добра инфраструктура. Възлите и могат да бъдат високо мобилни или стационарни и имат широка гама функционалности[8,10].

Изследователите предлагат направления за мобилните IP мрежи [11], Ipv6 базирани на onion рутиране [12], мобилните IPv6 [63, 64], подвижни мобилни агенти [15], индивидуални мрежи (personal areas networks (PAN)) и безжичните градски преплетени мрежи (mesh networks) [16]. Много протоколи са насочени към решаване на възникналите проблеми с рутирането. Въпреки че активните протоколи (reactive protocols) са по подходящи за мобилните безжични мрежи, всеки подхожда към рутирането от различна перспектива и с различни предположения. Нито един протокол не е универсално приложим и употребата им зависи от типа на „ad hoc" мрежата. Следва кратък преглед на всеки протокол за безжично анонимно споделяне.

3.1. SDAR

Анонимно рутиране със защитена дистрибуция (Secure Distributed Anonymous Routing - SDAR) [17] е както динамична смесена мрежа, така и анонимен рутиращ протокол с разкриване по заявки за мобилна ad hoc мрежа (MANET), изградена във

враждебна среда. Той позволява възелът на изпращача да посочи маршрута за установяване чрез разпространяване на съобщение за откриване на маршрута със специфични изисквания за надеждност към съседните възли. Целта е да се осигури маршрутизиране само по одобрените от гледна точка на сигурността маршрути за запазване на анонимността. Използва се криптографна „задна врата" (trapdoor) с публичен ключ. Тук имаме „задна врата", мащабност и сигурност [18]. Дългият частен дескрипторен ключ води до много висока изчислителна сложност, когато множеството пакети от заявки за маршрут (route request -RREQ) станат големи за междинните възли. Дългият частен ключ предизвиква високата сложност на изчисленията по време на маршрутизацията., защото междинните възли създават определяне на маршрута със съобщения с криптиран подпис. Накрая част от маршрутизиращите съобщения може да бъдат изтрити или модифицирани от междинните възли или противник.

3.2. AnonDSR

Анонимно рутиране с динамичен източник (Anonymous Dynamic Source Routing - AnonDSR) [18] е протокол по заявка за смесена onion мрежа, без разкриване на съседните възли, с крипто защита за получателя [19]. Съставен е от установяване на маршрута в защитен периметър, анонимно маршрутизиране до получателя и анонимни криптографски протоколи за onion трансфер на данни за MANET. При протокола за изграждане на маршрута не могат да бъдат успешни неприятелски активни модификации, атаки с повторение или изпълнение на атака с пасивно подслушване. При протокола за откриване на маршрута противника не може да модифицира публичния ключ, задната врата или onion, а атаката с повторение се детектира. В протокола за трансфера на информацията onion технологията защитава всички комуникации с данните. AnonDSR се мащабира по-добре от SDAR особено за анонимно изграждане на маршрут при нарастване на дистанцията.

3.3. MASK

MASK [11] е протокол с активно детектиране на съседни възли с виртуален схематичен обмен на данни без разкриване на съседни елементи и повредени примници [19]. Съвместим е с MAC слоя и мрежовия слой на комуникации и предлага анонимност на изпращача, на получателя и на комуникацията при пасивна неприятелска структура за широка гама, широкозонални комуникации (множество MANET) или тактически комуникации на ниско ниво при военни операции в градски условия. Изгражда виртуални схеми изпращач-получател и използва динамични псевдоними за представяне на маршрута [20]. Устойчив е за кодирани съобщения, разпознаване на потоци, повтарящи и времеви атаки и предлага висока рутираща ефективност в сравнение с класическата AODV [21]. За разлика от ANODR, MASK не е високо чувствителен за мобилността на възлите и позволява анонимни комуникации на MAC слоя. Съществуват и слабости: последния приемник се съдържа във всяко RREQ съобщение в прав текст, нарушавайки по този начин анонимността и зависимостта от строгата синхронизация на съседните ключове и псевдонимите [22].

3.4. PUZZLE /пъзел/

PUZZLE [23] е протокол с мащабираща споделена анонимност базирана на споделяне на тайни. Той позволява анонимно запитване и изтегляне на файлове за мобилни P2P мрежи в среда ad hoc. Главните предимства включват анонимни запитване и зареждане на файлове, надеждно доставяне на съобщения, висока

степен на анонимност и ниско ниво на криптографско натоварване в сравнение с APFS, P5, ANODR, MASK, смесени типове мрежи и други onion рутиращи подходи като Freedom, Tarzan, и Tor. Той използва AODV рутиращата таблица за доставяне на частите от заявката и използва комбиниран засекретяващ алгоритъм за информационна дисперсия (SIDA) за да осигури защита на информацията от комплексни атаки. Схемата за споделяне на защитени данни на Шамир постига анонимност на изпращача, а криптографските механизми RSA и AES постигат анонимността на комуникацията за пренасяните данни.

Допълнително, протокола позволява изпращача и получателя анонимно да отговарят и потвърждават съобщения чрез onion рутиране за постигане на взаимна анонимност. Степента на анонимност обаче зависи от броя връзки и броя връзки, получаващи дялове, а изпращача може да регулира вероятността от препълване или задните врати SIDA ако е необходимо.

3.5. ARM

Анонимно рутиране за MANET (ARM) [22] е анонимен рутиращ протокол по заявка за MANET мрежи, които са защитени срещу два предполагаеми противника: сътрудничащи възли в мрежата и външен, глобален пасивен противник извършващ мониторинг на целия трафик по мрежата. Предлага анонимност на изпращач, получател и комуникацията между тях както в статични, така и в динамични мрежи. Предполага, че всеки възел има постоянна информация за идентичността на другите възли, а изпращач и получател споделят секретен ключ и псевдоним. Всеки възел изгражда ключ за разпространение в най близко съседство, както и симетрични безжични връзки. Както произволното уплътнение, така стойностите на времената на живот са приложени за RREQ и RREP съобщенията. Основните предимства тук са по-високата ефективност в сравнение с ASR, ANODR и SDAR, както и подобрена анонимност на получателя спрямо SDAR и MASK и защитена комунукационна анонимност срещу силен противник за разлика от ANDOR, ASR, SDAR и MASK [22].

3.6. ASRPAKE

Анонимен протокол за защитено рутиране с размяна на автентичен ключ (ASRPAKE) [24] за спешни случаи и възстановяване след природни бедствия, военен конфликт, както и с комерсиално приложение за MANET. Осигурява анонимност за изпращач, получател и комуникация както и анонимност за всички междинни трансферни възли. Така осигурява стриктна анонимност по целия път на трансфер при условие всички междинни възли са в тази система. Той също интегрира ефективна схема базирана на елиптична криптосистема за постигане на анонимно удостоверяване постигано с увеличаване на групата подписи. Механизъм DECOY защитава срещу идентификации на нови атаки от противника.

3.7. ANODR

Анонимно рутиране по заявка (ANODR) [25] е протокол, базиран на „рапространение с информация за задни врати" концепцията за постигане на непроследяем и устойчив на атаки протокол за MANET, изградени във враждебна среда. Работи по заявка,използва опознавателни потоци при първи контакт, виртуална схема за обмен на данни, без разкриване на съседите, както и криптозащитен анонимен протокол за приемника [19]. Използва се псевдонимен рутиращ метод и симетричен ключ от тип бумерангов onion, слойна криптографска структура, в която добавянето и премахването на защитни слоеве се осъществява от самите възли по тра-

сето. Протокола е устойчив на силни атаки от обратно проследяващи потоци до изпращач и получател (комуникационна анонимност) и осигурява невъзможността на противниците да идентифицират трансферни възли за локални съобщения (локална защита). Поддържа задни врати и задаване на анонимност [18]. Непрактично е това че всеки възел в маршрута трябва да изпробва всеки познат споделен ключ за бумеранг onion задната врата. Втори проблем е как да се изградят споделени ключове за сесия, докато RREQ и отговор за маршрут (RREP) фазите не са регламентирани.

3.8. SDDR

Защитено рутиране с динамична дистрибуция (SDDR) [26] е протокол базиран на алгоритъм за разпределено рутиране, използван за изграждане на анонимни маршрути в ad hoc мрежи като безжични бойни полета, конференции във въздуха или спешни спасителни операции. Целта е да се разреши на междинните възли да изграждат пътища без да поставят на риск анонимната комуникация. SDDR не изисква глобален поглед над мрежовата топология и е гъвкав на отвличане на пакети. Има доказана устойчивост на повтарящи и модифициращи атаки. Ограниченията му са невъзможност да се промени маршрута в момент на атака, ограничена дължина на линията, както и липса на минимални изисквания за възлите по отношение на изчислителна мощ и обем памет. Оттук идва и уязвимостта му на DoS атаки. Тук също така се пренебрегва анонимността на кореспондентите и не се осигурява силна защита на данните за локацията [27].

3.9. ASR

ASR [28] е на основата на асиметрични криптосистеми. Конструиран е да осигури сигурност на откритите маршрути, защита на анонимността за локацията, кореспондентите и комуникацията срещу познатите пасивни и активни атаки. За разлика от SDDR предлага междинни възли, усилена анонимност за локация и комуникация. За разлика от ANDOR тук се предлагат анонимност както за кореспондентите, така и за локацията. Недостатъци са бавните изчисления, размера на ключа, както и консумираната мощност и невъзможността за динамично поправяне на пропаднали маршрути. Разликата е че всеки направляващ възел трябва да генерира нова двойка публични или секретни ключове. За всяко RREQ съобщение се изпраща и разкодира всяко RREP със всеки частен ключ във възловата рутираща таблица [22].

3.10. ZAP

Зоновият анонимен рутиращ протокол (ZAP) [29] е конструиран да постига k-анонимност за получателя в позиционните рутиращи алгоритми. Притежава групов подход и използва безжична среда за да даде “грешни” позиции близо до потребителя. Базиран е на „тълпа” от възли така, че анонимността на практика зависи от размера на тази група. Необходими са официални възли за разпространение, силно насищане, винаги наличен GPS и публични ключове, симетрични радиоканали, равна вероятност за вид възел (изпращач или получател) както и глобални, пасивни и адаптивни противници. K-анонимността е осигурена с първоначално избиране на голяма фиксирана зона или динамично поддържана зона с размер k, базирана на плътността на възлите и тяхната мобилност.

3.11. AO2P

Ad hoc протоколът на основа на позиционно защитено ad hoc рутиране (AO2P) [30] използва асиметрични криптосистеми. Използва се схема за рутиране със

съревнование между получателите (независм подход) със псевдоними и временни MAC адреси за доставка на данни. Създаден е за мрежи с висока плътност и предлага анонимност за изпращача, възлите по трасето, комуникацията и локацията, но не и анонимност на получателя. Модифицираният протокол RAO2P [31] подобрява анонимността на получателя. Тук отново са налице недостатъците по отношение на: бавни изчисления, размер на ключа и консумирана мощност. Оттук и вероятността да не се мащабира добре за големи мрежи.

4. Заключение

Подбирайки подходящи хост идентификатори, става възможно различните изисквания за услугите да се предадат като функционалности на мрежата. Съществува свързваща функция в подслоя за идентификация на протоколния стек, която определя връзката между идентификатора и съответния локатор в асоциация с изискванията към мрежовите услуги.

В състояние на постоянна кибервойна, анонимността може да намали уязвимостта като цяло и да защити собствеността чрез осуетяване на неприятелските способности за събиране на информацията и разстройване на комуникацията.

Съществуват широка гама кабелни и безжични анонимни протоколи. В тези протоколи уязвимостите и защитите са важни качества в дизайна и приложението на анонимните мрежи. Свързването на изискванията за анонимност с конкретни съществуващи и нови протоколи подобрява възможността за количествено сравнение между съответните типове протоколи.

ЛИТЕРАТУРА

[1]. Ved P. Kafle and Masugi Inoue, National Institute of Information and Communications Technology “Introducing Multi-ID and Multi-Locator Into Network Architecture”

[2] ITU-T Recommendation Y.3001 “Future Networks: Objectives and Design Goals,” May 2011.

[3] M. J. Freedman and R. Morris, "Tarzan: A Peer-to-Peer Anonymizing Network Layer" in 9th ACM Conference on Computer and Communi-cations Security (CCS), Washington DC, USA, 2002.

[4] J. Boyan, "The Anonymizer," in CMC Magazine, 1997

[5] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second Generation Onion Router," in 13th USENIXSecurity Symposium, 2004.

[6] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Sel. Areas Commun., vol. 16, 1998.

[7] A. E. Pascual, "Anonymous and Untraceable Communications," 21 June 2000.

[8]. Douglas Kelly, Richard Raines, Rusty Baldwin, Michael Grimaila, and Barry Mullins „Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics“ IEEE communications surveys & tutorials, vol. 14, no. 2, second quarter 2012

[9]. N. A. Fraser, "Mitigating Distributed Denial of Service Attacks in an Anonymous Routing Environment: Client Puzzles and Tor," in Computer and Electrical Engineering. vol. Master Wright-Patterson Air Force Base: Air Force Institute of Technology, p. 122, 2006.

[10]. Y. Ko and N. Vaidva, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," in *4th International Conference on Mobile Computing and Networking*, Dallas, USA,. pp. 66-75, 1998.

[11] L. Dang, W. Kou, H. Li, J.. Zhang, X. Cao, B. Zhao, and K.Fan, "Efficient ID-based Registration Protocol Featured with User Anonymity in Mobile IP Networks," *IEEE Trans. Wireless Commun.*, Vol. 9, Issue 2, pp. 594-604, 2010.

[12] Z. Jia, D. Haixin, L. Wu, and W. Jianping, "A light-weighted extension of anonymous communications in IPv6 Network," *International Conference on Green Circuits and Systems (ICGCS)*, pp. 404-408, 2010.

[13] H. Hartenstein, K. Jonas, M. Liebsch, M. Stiemerling, R. Schmitz,and D. Westhoff, "Scalable Anonymous Connections in the Context of MIP and AAA," in *10th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 217 - 222, 2001.

[14] Q. He, D. Wu, and P. Khosla, "Quest for Personal Control over Mobile Location Privacy," in *IEEE Commun. Mag.*. vol. 45, pp. 130-136, 2004.

[15] L. Korba, R. Song, and G. Yee "Anonymous Communications for Mobile Agents," *Proc. 4th International Workshop on Mobile Agents for Telecommunication Applications*, pp. 171-181, 2002.

[16] Z. Wan, K.. Ren, B. Zhu, B. Preneel, and M.. Gu, "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Network," *IEEE Trans. Vehicular Technology*, Vol. 59, Issue 2, pp. 519-532, 2010.

[17] C. Bowen and T. Martin, "A Survey of Location Privacy and an Approach for Solitary Users," in *40th Annual Hawaii International Conference on System Sciences* Hawaii, 2007.

[18] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-hoc Networks," in *3rd ACM Workshop on Security of Ad hoc and Sensor Networks* Alexandria VA, USA, pp. 33-42, 2005.

[19] J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing,* vol. 6, pp. 888-902, 2007.

[20] Z. Yanchao, L. Wei, and L. Wenjing, "Anonymous Communications in Mobile Ad Hoc Networks," in *24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pp. 1940-1951 vol. 3, 2005.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing," RFC w2561July 2003.

[22] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," in *20th International Conference on Advanced Information Networking and Applications (AINA)*, Vienna, AU, pp. 133-137, 2006.

[23] J. Han, Y. Liu "Mutual Anonymity for Mobile P2P Systems," *IEEE Trans. Parallel and Distributed Systems*, Vol. 19, pp. 1009-1019, 2008.

[24] X. Lin, R. Lu, H. Zhu, P. Ho, and Z. Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," in *IEEE International Conference on Communications (ICC)*, Glasgow, pp. 1247-1253, 2007.

[25] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks," in *4th ACM International Symposium*

on Mobile Ad-hoc Networking & Computing (MobiHoc), Annapolis MD, USA, pp. 291-302, 2003.

[26] K. Il-Khatib, L. Korba, R. Song, and G. Yee, "Secure Dynamic Distributed Routing Algorithm for Ad hoc Wireless Networks," in *International Conference on Parallel Processing Workshops (ICPPW)*, pp. 359-366, 2003.

[27] M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," in *International Symposium on Applications and the Internet (SAINT)*, p. 7, 2006.

[28] B. Zhu, Z. Wna, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," *29th Annual IEEE International Conference on Local Computer Networks* pp. 102-108, 2004.

[29] X. Wu and E. Bertino, "Achieving K-anonymity in Mobile Ad Hoc Networks," in *1st IEEE ICNP Workshop on Secure Network Protocols (NPSec)*, pp. 37-42, 2005.

[30] X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," *IEEE Trans. Mobile Computing,* vol. 4, pp. 335-348, 2005.

[31] X. Wu and B. Bhargava, "AO2P: Ad hoc On-demand Position-based Private Routing Protocol," in *IEEE Trans. Mobile Computing.* vol. 4, pp. 335-348, 2005.

[32] Фефтов О.,"Източници на уязвимост на информацията в безжичните комуникационни мрежи", Годишник на НВУ "В. Левски", 2005/06.

ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Величка Д. Станчева

Шуменски университет „Еп. К. Преславски"
veli4ka_stan4eva@abv.bg

INFORMATION SECURITY POLICIES

Velichka D. Stancheva

ABSTRACT: *Security policy includes sections relating to risk assessment, allocation of liability classification of vulnerabilities. Adequate security policy provides adequate protection of the system, while minimizing losses to acceptable levels.*

KEYWORD: *Information, information security, secret, integrity, availability, security policies, three-layer model of security policy.*

Информацията, заедно с техническите и програмни средства, инфраструктурата и средата, имащи отношения към нея, са ценни активи и трябва да бъдат защитавани.

Под *"информация"* трябва да се разбира многообразието от форми и носители, в които тя съществува - напечатана или написана на хартия, на технически носител, пусната по пощата - обикновена или електронна, текст, диаграми,

таблици, графики, снимки, филми, предадена/приета в телефонен или в пряк разговор и още много други форми и носители.

Информационна сигурност

Информационната сигурност е защитата на информацията от различни видове заплахи, с цел гарантиране непрекъсваемостта на работните процеси. Информационната сигурност означава опазване на поверителността, целостта и достъпността на информацията.

По своята същност, схващането за информационна сигурност е стратегически възглед за интересите на личността, обществото и държавата в информационната сфера, заплахите за тези интереси и пътищата и средствата за тяхната защита. В този контекст се анализират стратегическата среда, видовете и източниците на заплахи, състоянието, задачите и методите за гарантиране на сигурността, основните положения на държавната политика и на системата за гарантиране на информационна сигурност.

Информационната сигурност се дефинира като: защитеност на държавата на стратегическо, оперативно и тактическо равнище от всякакви опити:

- Да се наруши неприкосновеността, достоверността, конфиденциалността, селективността и отказоустойчивостта на достъпа до информационните ѝ ресурси (сигнали, данни, знания, култура) и инфраструктури;
- Несанкционирано да се ползват, манипулират или разрушат информационните ѝ ресурси;
- Каквато и да е степен да се отслабят или премахнат възможностите за създаване, събиране, разпространение, обработка, съхранение и ползване на информация от граждани, организации и органи на държавно управление;
- Несанкционирано да се ползва, манипулира или да се разруши информационната ѝ структура ;
- Целенасочено да се дезинформира обществото или вземащите решение лица и структури.

Основни цели на информационната сигурност:

- Да осигури непрекъснато функциониране на бизнес процесите
- Да минимизира пораженията върху бизнеса чрез предотвратяване или минимизиране на инциденти свързани със информационната сигурност
- Да осигури запазването на конфиденциалноста, целостта и наличността на информацията

Исторически терминът *информационна сигурност* се употребява да изрази комбинацията между "компютърната сигурност" (COMPUSEC) и "комуникационната сигурност" (COMSEC).

Информационната сигурност осигурява: тайна, цялостност и наличност.

Тайна означава, че една защитената компютърна система не трябва да допуска разкриването на информация от потребител, който не е упълномощен (няма автентификация и авторизация за достъп до нея).

Authentication - това е процес на верифициране на достъпа на партньора до даден процес, а Authorization е разрешаването на достъпа до процеса

Цялостност е такова свойство на компютърна система което гарантира поддържането на цялостта на информацията, съхранявана в нея.

Наличността е качество на компютърната система с което се осигурява наличност на информацията за потребителите. Наличност означава, че хардуерът и софтуерът на компютърната система работят ефикасно и че системата има възможност да се възстанови бързо и цялостно, ако възникне някое бедствие.

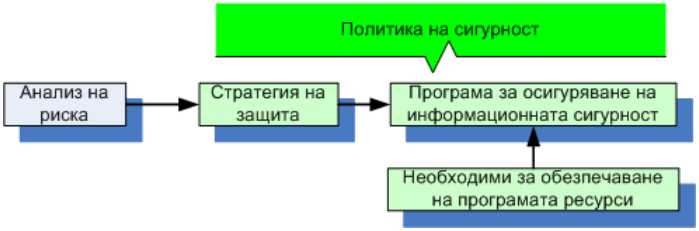
Политика за информационна сигурност

Политиката по информационна сигурност е съвкупност от закони, принципи, правила и норми на поведение, определящи методите и средствата за вземане на решения за защитата на информацията в процесите на нейното създаване, обработка, съхранение, ползване и обмен, в границите на дадената система.

Политиката по сигурността включва раздели, свързани с оценка на риска, разпределение на отговорността, класификация на уязвимите места.

Описание на политиката за сигурност

Политиката на сигурност се изгражда на база анализ на рисковете, които са реални за информационната система. След анализ на риска се разработва стратегия на защита и съответна програма за осигуряване на информационната сигурност. За тази програма се заделят ресурси, определят се отговорници, редът за контрол, времето за изпълнение и т.н.



Фиг. 1

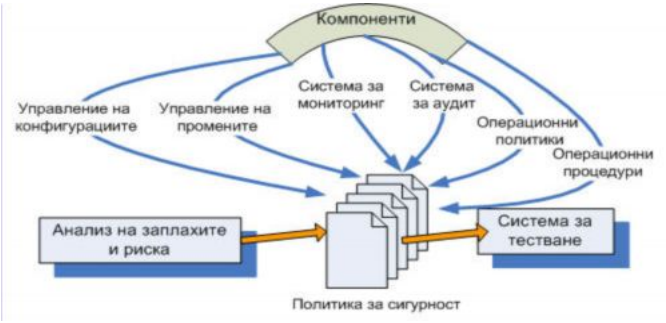
Политика на сигурност (security policy) – съвкупност от документирани решения, приети от ръководството на организацията и насочени към защита на информацията и асоциираните с нея ресурси.

Политика на сигурност на организацията (organizational security policies) — съвкупност от ръководящи принципи, правила и процедури в областта на сигурността, които регулират управлението, защитата и разпределението на ценната информация.

Адекватна политика на сигурност – осигурява достатъчно ниво на защита на системата, като минимизира загубите до допустими нива.

Политиката на сигурност зависи от:

- Конкретната технология за обработка на информация.
- Използваните технически и програмни средства;
- Организационната култура на организацията;
- Разположението на организацията.



Фиг. 2. Обхват на политиката за сигурност

Цел на политиката за сигурност - да формулира и обезпечи поддръжка на подходи и средства в областта на информационната сигурност от страна на ръководството на организацията.

Основни характеристики:

- Дефинира мястото на политиката за сигурност по отношение на мисията и целите на организацията.
- Установява в организацията общи правила за поведение, съобразени с необходимото ниво на сигурност.
- Предоставя рамка за разработка и внедряване на процедури.
- Определя общи правила за действие при нарушаване на сигурността.

Изисквания към политиката:

- Да има ясен ангажимент от страна на висшето ръководство.
- Целите и дейностите по сигурността трябва да бъдат базирани на бизнес цели и изисквания.
- Да има ясно виждане относно рисковете за сигурността на активите и нивото на сигурност в организацията.
- Да мотивира всички мениджъри и служители да спазват изискванията за сигурност.
- Да дава насоки за прилагане на политиката за сигурност на всички служители и външни изпълнители.

Критични фактори за успех:

- Ръководещите за организацията принципи.
- Съотношението на поставените цели.
- Наличните ресурси.

Политиката включва:

- Общи принципи - определят подхода към сигурността.
- Конкретни правила за работа - определят това, което е разрешено и това което е забранено. Правилата могат да се допълнят с конкретни процедури и различни ръководства.
- Технически подход - анализ, който подпомага изпълнението на принципите и правилата.

Ефективността на политиката зависи от това доколко разработчиците на политиката са разбрали смисъла на компромисите, които трябва да направят.

Процес на реализиране политиката за сигурност:

- Разработка на политиката за сигурност.
- Внедряване политиката за сигурност.
- Мониторинг на системата.
- Тестване.
- Актуализиране и промени в политиката.

Извод:

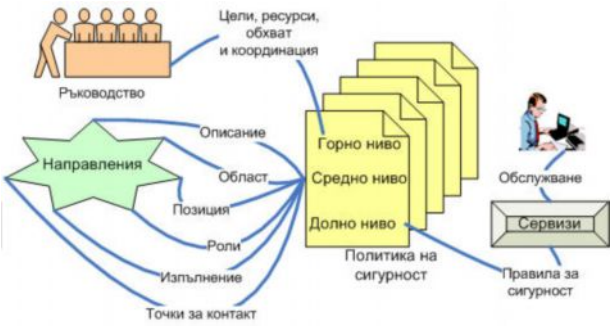
От направения обхват на политиката за сигурност и нивата могат да се направят следните изводи относно необходимостта от политиката за сигурност:

Необходимост от политика за сигурност:

- Определя какво може и какво не може.
- Помага за определяне на средствата и процедурите за осигуряване сигурността на системата.
- Предоставя основата за реализиране защитата на системата.
- Позволява достигане договореност между служителите, приемащи ключови решения, както и за описване областите на отговорност между потребителите и администраторите.
- Определя регламент са носене на отговорност при нарушаване на зададените правила или допускане на грешки.
- Създава основа за предприемане на юридически действия.

Трислоен модел на политиката

Политиката за сигурност обикновено се разглежда на три нива – горно, средно и долно ниво.



Фиг. 3

Горно ниво

1) Характеристики:

* Разглежда организацията като цяло;
* Има общ характер;
* Изготвя се от ръководството на организацията.

2) Елементи

* Решение за създаване или актуализация на комплексната програма за информационно сигурност;

* Формулиране на целите, които преследва организацията в областта на сигурността;

* Осигуряване на ресурси и база за спазване на съответните закони и стандарти.

3) Дейности:

* Управление и координация на ресурсите за защита;

* Определяне на персонал за защита на критически важни системи;

* Взаимодействие с други организации, имащи отношение към политиката.

4) Обхват (варианти):

* Само най-важните системи;

* Всички компютърни системи на организацията;

* Системите на организацията и домашните компютри на сътрудниците.

5) Задължения на ръководството:

* Да следи организацията да съблюдава съответните закони;

* Да контролира действията на отговорните за реализиране на политиката лица;

* Да осигури реализация на политиката, като разработи система за поощрения и наказания.

Средно ниво

На това ниво се определят въпросите, касаещи отделни направления от дейността по осигуряване на информационна сигурност. За всяко направление трябва да се изяснят следните въпроси:

1) Описание на направлението – физическа защита, ползване на неофициално програмно осигуряване, достъп до ресурси и т.н;

2) Област на използване – къде, кога, как по отношение на кого и защо се прилага тази политика на сигурност;

3) Позиция на организацията – цели на организацията в даденото направление и регламенти за реализирането им;

4) Роли и задължения – информация за длъжностните лица, отговорни за реализация на политиката и за решаване на възникнали проблеми (разяснения, разрешения, забрани и т.н.);

5) Изпълнение – общо описание на забранените действия и наказанията при нарушения;

6) Точки за контакт – длъжностни лица, които трябва да оказват помощ, да разясняват и да дават допълнителна информация.

Долно ниво

1) Характеристики:

* Отнася се за конкретни информационни сервизи;

* Подробно описание на политиката;

* Включва два аспекта – цели и правила за изпълнението им.

2) Отговаря на въпросите:

*Кой има право на достъп до обектите, поддържани от сервизите?

*При какви условия могат да се четат и модифицират данните?

*Как е организиран отдалечения достъп до сервизите?

3) Формулировка на целите:

Фиг. 4

Изхожда се от съображения за **конфиденциалност, цялостност и достъпност,** като целите трябва да бъдат много конкретни и да свързват обектите на конкретния сервиз и действията с тях.

На база целите, се формулират правилата за сигурност, описващи кой, какво и при какви условия може да работи със съответните информационни ресурси.

Колкото по-подробни и формализирани са правилата за сигурност, толкова по-лесно може да се осъществи поддръжката им с програмно–технически средства.

Използвани източници

1. Annual Report 2005, Federal Office for Information Security (BSI) www.bsi.bund.de
2. INFOSEC ASSURED PRODUCTS
3. Establishing the European Network and Information Security Agency, COMMISSION OF THE EUROPEAN COMMUNITIES, 2005

КИБЕРВОЙНИЦИ И КИБЕРВОЙСКИ

Иван М. Михалев

Щаб на Командването на Военноморските сили на Република България

CYBER WARRIORS AND CYBER MILITARY FORCES

Ivan M. Mihalev

***ABSTRACT**: This article describes an offensive view to the problem with the cyber war, the cyber crime and the cyber terrorism. As one of possible ways to resolve the problem is shown the process of building of Cyber Military Forces manned with Cyber Warriors.*

***KEY WORDS**: Cyber warriors, Cyber Military Forces, Cyber Offense, Cyber Defense, Computer Network Attack*

В съвременния свят информацията придобива все по-голяма стойност, често пъти неизмерима в парични знаци. Този който притежава и умее да управлява по подходящ начин дадена информация, владее, управлява или използва в определена степен заобикалящата го среда. Колкотокибер по-голямо е количеството информация и по-добри уменията за управление или използване, толкова по-големи са възможностите за владеене и управление на средата, а от там като следствие и властта която се придобива.

Съвременните информационни технологии дават нови възможности, които драстично намаляват или елиминират пространствения фактор и разширяват границите на владеене и управление отвъд тези на заобикалящия ни физически свят, което от своя страна води и до определена степен на виртуализация на средата, в която живеем.

Информационните технологии променят основите на съвременната икономика, превръщайки информацията в своеобразен, особен и без аналог вид стока.

Следвайки този ред на мисли, трябва все пак да упоменем, че само факта на владеене на информацията не носи ползи, ако тази информация не се използва по подходящ начин.

Изхождайки от горните разсъждения, може да се каже, че в нашето съвремие, а с голяма доза увереност и в нашето бъдеще, победата в един конфликт ще принадлежи на този от опонентите, който разполага с повече информация и умее да я използва по по-подходящ начин или казано с други думи, на този, който успее да завоюва информационно превъзходство. Тук може да се разгледат два основни варианта, при които се постига победа в даден конфликт:

- при еднакви възможности за управление или използване на информацията, печели този, който разполага с по-голямо количество от нея;
- при равно количество информация, печели този, който умее да я управлява или използва по-добре.

Тук следва да отбележим, че информацията, с която разполага единия от опонентите, може да способства за компенсиране на технологичното или количествено превъзходство на другия опонент.

Разглеждайки горните варианти, можем да посочим четири основни пътя за постигане на победа:

1. Увеличаване количеството на информацията с която единия от опонентите разполага.
2. Намаляване или ограничаване на количеството на информацията с която другия опонент разполага.
3. Повишаване на възможностите за управление или използване на информацията на единия от опонентите.
4. Намаляване възможностите на другия опонент, за управление или използване на информацията.

При един прост анализ, се вижда, че за постигане на победа е по-подходящо, ако не и наложително, да се използват офанзивни действия.

Подхождайки по-прагматично към горните проблеми, може да кажем, че киберпространството ни предлага редица дилеми, които изискват подходящи пътища за разрешаването им. Например, какво ще направим, ако получим информация за готвена кибератака срещу наша информационна система?

Изхождайки от смисъла на широко налаганото понятие киберзащита (Cyber Defense), за да се предпазим от атаката, следва да имаме активирани защитни стени, антивирусни системи, системи за откриване на проникване (IDS), обучен персонал, инсталирани последни пачове (кръпки) и редица други елементи, които да създадат наша собствена, образно казано киберкрепост.

За жалост обаче, от древността до наши дни, историята помни много паднали "непревземаеми" крепости. Киберпространството не прави изключение, тъй като то се явява един вид виртуален образ на реалността.

Много показателен пример от не толкова далечната история е Одринската крепост. Считана за непревземаема на времето си, тя пада за няколко месеца, не без помощта разбира се, на някои нововъведения във военното изкуство.

Разсъждавайки в този дух, следва да посочим, че без да знаем от какво да се защитаваме, ние сме обречени да паднем жертва на някоя неизвестна за нас слабост в собствената ни киберзащита. Или казано по-кратко, не съществува универсална защита, още повече кибер такава.

Да се върнем все пак на въпроса - какво да правим, ако разполагаме с информация за готвена срещу наша система кибератака?

Всъщност има два, много прости отговора - можем да чакаме да ни атакуват и да разчитаме, че нашата система ще устои на атаката или ние да атакуваме първи, като постигнем ефекта на изненадата или предимството да местим първи пешката на бойното поле на кибервойната.

Един умен военоначалник е казал, че най-добрата защита е нападението.

Това виждане явно се споделя от САЩ, Русия, Китай, Израел и редица други държави, които дали официално или не, са създали и поддържат организационни структури за въздействие върху киберсистемите или киберсегментите на държави или структури, считани за евентуални или настоящи опоненти.

В отговор на така поставения по-горе въпрос, може да приемем, че използвайки организационни структури с подобни възможности, ще успеем ако не да елимини-

раме опасността, то поне да отслабим силата на провежданата срещу нашата система кибератака.

С развитието на информационните системи се появи нов тип война – мрежова или кибер война. Основно оръжие в този нов тип война са компютърните вируси, програмирани да повредят софтуера, логическите бомби, които да се задействат в определено време и да унищожат данните и HERF (high-energy radio frequency) оръжия (електро-магнитни бомби), които унищожават електронните устройства чрез мощен електромагнитен импулс.

Количеството на потенциалните цели е безкрайно и може да включва финансови пазари, електрически мрежи, контрола на въздушния трафик, авиониката на самолети, сателити и др.

Информационната война в неиното ново въплащение (мрежова война - netwar или кибервойна - cyberwar) може да се проведе на няколко нива: персонално, институционално и национално. Всяко от тези нива има свои собствени нива на заплахи, потенциални разрушения и др.

Бойното поле на кибервойната включва всички аспекти на Internet, от гръбнака на уеб пространството, до доставчиците на Internet услуги и до различни типове преносна среда и мрежови устройства. То не свършва в нивата, на върха на планината или на брега на морето. Вместо това, то обхваща градове, общности и света в който ние живеем. Бойното поле на 21-ви век е съставено от много компоненти, които включват Internet и всичко което е свързано към него, като уеб сървъри, корпоративни информационни системи, системи клиент-сървър, комуникационни връзки, мрежово оборудване, десктоп и лаптоп компютри на работните места и у дома. В него също така се включват информационни системи, като тези на електрическата мрежа, телекомуникациите и различни корпоративни и военни роботизирани системи.

Основен субект в кибервойната е т. нар. кибервоин.

Кибервоин ("cyber warrior") е лице, което притежава висока квалификация в изкуството на кибервойната (Cyber Warfare). Правителства, техните ВС, правоналагащи органи, частен сектор и престъпници (самостоятелни и групи) по целия свят, предприемат действия за да обучат собствени хора в полето на кибер войната. Уменията, които кибервоинът притежава, могат да варират като големина и обхват, но най-важните от тях включват: информационна сигурност, хакване, шпионаж и разследване на компютърни престъпления.

Специалистът по информацинни войни Мохамед Шариф, в своята статия „Information Warfare Tactics", дефинира следните типове атаки, които се използват в този вид война:

- Пасивни атаки:
  - атакуващия само наблюдава изходящия трафик, за да научи тайните;
  - пасивните атаки се откриват най-трудно
  - да предположим какви ще са последствията, ако някой подслушва системата;
- Активни атаки:
  - атакуващия се опитва да премине през нашите защити
    - криптографски атаки
    - измама (Spoofing)
    - опити за достъп до системата

От своя страна, полевият устав 3-13 (FM 3-13 / FM 100-6), Информационни операции: Доктрина, Тактики, Техники и Процедури на ВС на САЩ, дефинира няколко метода за атака:

- неоторизиран достъп
- зловреден софтуер
- електромагнитна заблуда / измама
- електронна атака
- физическо унищожаване
- манипулиране на възприятията

Според устава, опонентът може да използва няколко от горните методи за да атакува нашата система за командване и контрол и другите ни информационни системи или за да моделира информационната среда по собствен вкус. Същността на информационната среда прави тези атаки трудни за откриване.

Списъкът с възможни видове кибератаки, обобщен на база на различни източници включва още:

- Internet социално инженерство
- подслушване на мрежи (Network sniffers)
- подмяна на пакети (Packet spoofing)
- отнемане на сесии (Hijacking sessions)
- автоматизирани проверки за наличие на хостове и сканиране на мрежи
- графични помощни средства за проникване в системи
- автоматизирани широкоразпростиращи се атаки
- широко разпростиращи се атаки за предизвикване отказ на услуги (Widespread DoS)
- атакуване на изпълним код
- техники за анализ на кода за уязвимости, без да се разполага с изходния код
- широко разпростиращи се атаки на DNS инфраструктурата
- широко разпростиращи си атаки, използващи NNTP за разпространение на атаката
- "Stealth" и други напредничиви техники за сканиране
- Windows базирани дистанционно контролирани троянски коне (Back Orifice)
- разпространение на зловреден код чрез E-mail
- широкомащабно разпространение на троянски коне
- помощни средства за разпределени атаки
- разпределни атаки за предизвикване отказ на услуги (DDoS)
- прицелване в специфични потребители
- техники за заличаване на доказателства
- широкомащабно използване на червеи
- специализирани атаки срещу системи за командване и контрол

Целта на едно кибератака включва четири области: загуба на целостта, загуба на наличността, загуба на поверителността и физическо унищожаване.

Едно от основните проявления на кибервойната е компютърната атака. Тя може да се дефинира като, действия, насочени срещу компютърните системи, с цел нарушаване работоспособността на оборудването, промяна начина на обработка или

нарушаване целостта на съхраняваните данни. Различните методи за атака са насочени към различни уязвимости и включват различни типове оръжия. Понастоящем са идентифицирани три различни метода за атака, но с напредването на технологиите, границата между тях все повече ще се размива:

- физическа атака – включва конвенционални оръжия, насочени към компютърните съоръжения или преносните линии;
- електронна атака – включва използване на силата на електромагнитната енергия, за да се претоварят захранващите вериги на компютърните системи и „по-мека" форма, чрез която се внасят смущения в линиите за радиокомуникация;
- компютърна мрежова атака (computer network attack - CNA) - обикновено включва злонамерен код, използван като оръжие, който инфектира компютрите на противника, така, че да може да се използват слабости в софтуера, компютърните конфигурации или в процедурите за сигурност на организацията или потребителите. Друга форма на CNA е, когато атакуващият използва придобита информация за да влезе в компютърни системи с ограничен достъп.

Националната военна стратегия за операции в киберпространството на САЩ дефинира по следния начин процеса на прилагане на тактиките на кибервойната:

- идентифицирай целта;
- идентифицирай информационните й интерфейси;
- търси правителствени системи;
- събирай разузнавателна информация;
- идентифицирай критичните елементи;
- идентифицирай мрежовите уязвимости;
- опитвай тайно да проникнеш в ситемата или мрежата и документирай резултатите;
- след като веднъж проникнеш, провери за други системи;
- след като веднъж проникнеш, търси и предавай чуствителна информация;
- след като веднъж проникнеш, заложи логически бомби, троянски коне и тайни вратички;
- заличи доказателствата за проникването;
- търси други системи, особено правителствени такива.

Типовете военни компютърни мрежови операции (Computer Network Operations (CNO)) според Joint Pub 3-13 включват:

- Computer Network Attack (CNA): включва действия, осъществявани чрез компютърните мрежи, за нарушаване, подмяна, разрушаване или унищожаване на информацията в компютрите или мрежите и/или на самите компютри или мрежи.
- Computer Network Defense (CND): включва действия, осъществени чрез компютърни мрежи за защита, наблюдения, анализиране, откриване и отговор на мрежови атаки, проникивания, разрушения или други неоторизирани действия, които могат да компрометират или парализират отбранителните информационни системи и мрежи. Joint Pub 6.0 освен това представя CND като аспект на NetOps
- Computer Network Exploitation (CNE): включва различни действия и разузнаване чрез компютърни мрежи, които позволяват използване на данните от информационните системи или мрежи на целта или врага.

Кибервойната поставя няколко предизвикателства пред съвременния свят [1]:

1. Няма физически граници. Световната мрежа, наричан от мнозина "киберпространството", няма физически граници. Нападателят вече не определена държава или нация, а само група от съмишленици, които са свързани чрез Интернет. Нарастващата ни свързаност през киберпространството увеличава експозицията ни към противниците. Кибератаките могат да допълнят или заменят традиционните военни атаки, което значително усложнява и разширява уязвимостите, които ние трябва да предвидим и на които да се противопоставим. На риск е изложена не само информацията ни, но и всички компоненти на нашата национална инфраструктура, която зависи от информационните технологии и навременното предоставяне на точни данни. Тук се включват далекосъобщителната инфраструктура; банковата и финансовата системи, електрическата и други енергийни системи.

2. Няма фронтова линия и обща бойно поле. Фронтовата линия може да бъде навсякъде, където сателитите и Интернет работят. Кибервойната пренесе бойното поле в домовете на хорат. Поради факта, че икономиките стават все по-зависима от комплекс, взаимосвързани компютърни системи, кибервоините ще имат потенциал за нарушаване на обществения ред чрез причиняване на тежка повреда на компютърна система, което може да доведе например, до спиране на електроцентрали, загуба на съзнание или смърт на тежко болни пациенти, железопътни катастрофи, хаос на фондовите борси и др.

3. Няма физическо представяне. В кибервойната атакуващите не трябва непременно да разрушат една системи, а е достатъчно просто да нарушат работата й. Не е необходимо физически да влязат в организацията или да пресекат държавната граница. Вместо това те просто имат достъп до системите. За да се води кибервойната не е необходима голяма ударна сила.

4. Трудно се открива и проследява. При една атака ние може никога да не разберем кой е нашия нападател, поради големите възможности за дезинформация. Ако атаката е добре планирана и координирана ще е много трудно да се разбере от къде идва и кой е отговорен за нея. Дори само един човек би могъл да бъде в състояние да осъществява саботаж, причинявайки по този начин много вреди, като в същото време неможе да бъде открит и елиминиран. Това е абсолютна илюстрация на истинските предизвикателства и възможности, които дава информационната война. Ние може да започнем атака, която да изглежда така, сякаш идва от някъде много далеч от действителната точка на произход. По подобен начин, когато атаката е срещу нас, ще е много трудно да се открие от къде идва тя. Дори и да открием източника, ще бъде много трудно да отговорим на тази атака.

5. Лесно се организира и е евтино. Използвайки инструменти, които са безплатни и лесни за работа, притежавайки известен опит и ноу-хау, и няколко компютъра с достъп до интернет, всеки един човек може да организира и да започне кибервойната. По тези причини е далеч по-лесно да се финансира кибервойната, вместо конвенционалната такава. Недоволни програмисти, които са готови да продадат способностите си на всеки купувач могат да бъдат намерени лесно навсякъде.

---

1 "Information Warfare: Cyber Warfare is the future warfare"; SANS Institute 2004

6. 24 часа в денонощието и 7 дни в седмицата. Във физическия свят, ние обикновено работим от 9 ч. до 5 ч. В киберпространството няма работно време, поради което атаката може да се води във всяко едно време, което нападателя си избере. В резултат на това е трудно да се предскаже или предвиди една кибератака.

Освен кибервойната, в света се появиха още две явления, свързани с развитието на компютърните мрежи.

Компютърната ера откри възможности пред терористите и неприятелските правителства, които не съществуваха преди. Точно така както предизвика революция във военното планиране и подготовка, така и даде живот на първото явление, което е информационния тероризъм или още кибертероризъм и роди заплахата от информационната война [2]. За първи път, терминът кибертероризъм (Cyber terrorism) е използван през 80-те години на миналия век от Бари Колин [3] от Института за сигурност и разузнаване в Калифорния.

Кибертероризмът има две форми: базирана на ефект (effects-based) и Internet базирана (internet-based). При първата форма като резултат от атака над компютърна система се генерира страх, както при традиционния тероризъм. При втората форма, целта е да се предизвика загуба, която обикновено е икономическа.

Традиционните оръжия на кибертерориста включват компютърни вируси (логически бомби, червеи, троянски коне), крakване (неоторизиран достъп до компютърни системи), подслушване (sniffing) на трафика за пароли, номера на кредитни карти и други данни, социално инженерство и ровене в боклука (dumpster diving).

Второто явление е киберпрестъпността. На X-я конгрес на Обединените нации за предотвратяване на престъпността и третиране на правонарушителите, киберпрестъпността е разделен на две категории:

- киберпрестъпност в тесен смисъл (компютърни престъпления): всяко незаконно поведение, осъществено с помощта на електронни средства, чиято цел е сигурността на компютърните системи и данните обработвани от тях;
- киберпрестъпност в по-широк смисъл (свързани с компютрите престъпления): всяко незаконно поведение, извършено с помощта на, или във връзка с, компютърна система или мрежа, включително такива престъпления като незаконно притежание и/или предлагането или разпространяване на информация с помощта на компютърна система или мрежа.

Връщайки се към началото на настоящия труд, освен отговор на въпроса "Какво?", следва да посочим и "Кой" ще реализира всички преждеизброени действия.

Един естествен отговор на този въпрос би могъл да бъде, че това следва да бъдат кибервойски, включващи в състава си кибервойници. По своята същност кибервойските представляват организационна структура, специално изградена и притежаваща способности за въздействие върху киберсистеми или киберсегменти на опонентите си. Въздействието би могло да се осъществява в рамките на информационни операции, чиято основна цел е постигане на информационно превъзходство.

Съгласно Концепцията за информационна стартегия на МО, информационното превъзходство и информационните операции се дефинират като:

- Информационно превъзходство - по-добрата способност спрямо противника за събиране, обработка, анализ и разпространение на информация, като в същото

2 Helen Nissenbaum, "Hackers and the Battle for Cyberspace", Dissent, New York, Fall 2002, pp. 50 – 57.

3 Barry C. Collin, Cyber terrorism From Virtual Darkness: New Weapons in a Timeless Battle, http://www.counterterrorism.org

то време той се възпрепятства да прави същото.

- Информационни операции - въздействия над информацията и информационните системи на противника, при което се осигурява защитата на собствените такива, които се провеждат през всички фази на военните действия и по време на всички типове военни операции.

Приемайки изследванията и опита на САЩ, отразени в US Joint Publication 3-13.1, "Electronic Warfare", в личния състав на кибервойските трябва да включим: дипломати, експерти, журналисти, писатели, публицисти, преводачи, оператори, комуникационни специалисти, уеб дизайнери, хакери и др.

Извършвайки анализ на процеса на изграждането на кибервойските, може да откроим два основни проблема: юридическа легитимност на действията и осигуряване на подходящ личен състав.

Проблемът с юридическото легитимиране на кибервойските е свързан с факта, че действия, свързани с умишлено увреждане на чужда информация или нерегламентиран достъп до нея, се считат за противозаконни както от българското законодателство, така и от международното и това на други държави. За декриминализиране на извършването им следва да се приемат специални законови разпоредби. Това разбира се не се отнася за случаите, когато официално е обявена война.

Не трябва да се пренебрегва факта, че въздействието върху информационна система на чужда държава или организация, най-вероятно ще се възприеме като акт на агресия и разкриването на източника на въздействие, в най-лошия случай може да доведе до избухване на реален, конвенционален военен конфликт. Това налага много внимателно да се преценява кога, къде и как да се използват кибервойските.

Вторият основен проблем, свързан с изграждането и функционирането на кибервойските е намирането и задържането на подходящ личен състав. Реализацията в цивилни агенции или фирми на едно лице с достатъчни познания в тази областта, ще му донесе като минимум няколкократно по-големи финансови облаги, отколкото реализацията му в държавния сектор и в частност в Българската армия.

Трябва да се отбележи, че обучението на едно лице за достигане на познанията и уменията му до едно приемливо ниво е дълъг и сложен ресурсо, трудо и времеемък процес, с неясен изход. Народната поговорка „От всяко дърво свирка не става" важи с пълна сила в тази област от познанието. По същество, този вид офанзивни действия може да се разглеждат като род военно изкуство и там нямат място лаици и дилетанти. Поради горните причини, подбора на подходящ персонал и стимулирането му са особено важни процеси.

Към настоящия момент в България, а може би и в света, не се преподава и изучава материя, еднаква или близка по съдържание с „въздействие върху кибер-системи или киберсегменти". Отделни университети и преподаватели водят лекции или дори дисциплини в някои от разделите на тази област, но специалност, която да осигури на изхода си готов специалист, не съществува.

Заучаването на някои техники и методи за въздействие, не прави от заучилия ги кибервойник, така както и придобиването на умения за маршировка и боравене с оръжие не правят от военнослужещия войник. Само продължителните тренировки, учения, а най-добре и реални действия, под ръководството на много добре подготвени инструктори, водещи до натрупването на достатъчно опит и рутина,

превръщат боеца в истински войник (познат в англоезичния свят като warrior, за разлика от soldier).

За да дадем представа за сложността на процеса на обучение на киберсилите, ще се позовем на информация, публикувана от групата Монтерей [4], за нивата на обучение на кибертерористите, без разбира се да поставяме знак за равенство между последните и собствените ни сили. Групата дефинира три нива на способност за кибертерор:

- Просто – неструктурирано (Simple-Unstructured): способност за използване на базови хакерски техники срещу отделни системи, чрез използване на помощни средства, създадени от друг (ламери). Организацията притежава много малки способности за анализ на целите, за командване и контрол и за обучение;
- Напреднало – Структурирано (Advanced-Structured): способност за провеждане на по-сложни атаки срещу многобройни системи или мрежи и създаване на елементарни хакерски помощни средства. Организацията притежава основни способности за анализ на целите, за командване и контрол и за обучение.
- Комплексано – Координирано (Complex-Coordinated): способности за провеждане на координирани атаки, предизвикващи масови поражения, срещу интегрирани, хетрогенни защити (включително криптографски). Способност за създаване на сложни помощни хакерски средства. Организацията притежава големи способности за анализ на целите, за командване и контрол и за обучение.

Групата Монтерей твърди, че на една организация, стартираща от възможно най-ниското ниво, ще и отнеме от две до пет години за да достигне ниво „advanced-structured" и шест до десет години за да достигне ниво „complex-coordinated".

В заключение може да посочим, че изграждането на кибервойски, които да водят бойни действия в киберпространството, на съвременния етап от развитието на информационните технологии, не е безсмислена прищявка, а по скоро крайна необходимост. Уменията за поразяване на елементи от киберпространството, развивани от структури на държавно ниво, криминални и терористични организации, все повече се повишават и изоставането от тази тенденция може да доведе до значителни щети за националните интереси.

Идеята за настоящия труд води началото си от друга, по-глобална идея, свързана със създаването на войски за информационно поразяване, като автор на последната е професор Павел Демиров от В. А. "Г. С. Раковски".

4 The Monterey Group is a think tank situated in California. The organisation's web site is at http://cns.miis.edu

ЕДИН ПОДХОД ЗА ИНТЕГРИРАНЕ НА АВТОМАТИЗИРАНАТА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ЧОВЕШКИТЕ РЕСУРСИ В МИНИСТЕРСТВОТО НА ОТБРАНАТА И ПОЛЕВАТА ИНТЕГРИРАНА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА СИСТЕМА

Александър А. Колев **Милена Х. Ламбева** **Иван С. Христозов**

Институт по отбрана, София 1606, бул. „Тотлебен" № 34, тел. 21841
НВУ "Васил Левски", Факултет „Артилерия, ПВО и КИС"
Институт по отбрана, София 1606, бул. „Тотлебен" № 34, тел. 21832

AN APPROACH FOR INTEGRATION OF HUMAN RESOURCES AUTOMATED CONTROL SYSTEM AND FIELD INTEGRATED COMMUNICATION-INFORMATION SYSTEM

Alexander A. Kolev **Milena H. Lambeva** **Ivan S. Hristozov**

ABSTRACT: The analyses of data base structures for personal data handling of Human resources in MoD automated control system and Field integrated communication and information system is proposed. An approach for integration between this systems is proposed, based on exporting data from Human resources in MoD automated control system and their automated input in FICIS.

KEY WORDS: command and control information systems, integration

В Българската армия са внедрени и функционират различни информационни системи. Такива са например мирновременните системи – Автоматизирана система за управление на човешките ресурси в Министерството на отбраната (АСУ ЧР) [ ], информационната система „Заплати", информационната система „Логистика", системите за моделиране и симулации от рода на Joint Conflict and tactical simulations (JCATS), полевата комуникационно-информационна система (ПИКИС) [1, 2] и др. Те изпълняват различни функции за нуждите на командването и управлението. Разработени са и функционират независимо една от друга. Базите от данни, които една система създава и поддържа често пъти включват информация, която се дублира с аналогична в другата система. Типичен пример за това са персоналните данни за личния състав като единен граждански номер (ЕГН), име, презиме, фамилия, звание, длъжност и др., които се въвеждат независимо в три от съществуващите системи, а именно АСУ на ЧР, ИС „Заплати" и ПИКИС. При това поради грешки, ненавременно актуализиране или пропуски се получават несъвпадения при извеждане на едни и същи справки от тези системи.

Базите от данни на разглежданите системи са структурирани по различен начин: АСУ на ЧР ползва собствен модел на базата от данни, докато ПИКИС ползва базата данни на общия концентратор (Army Tactical Command and Control Interoperability Specifications (ATCCIS) [1, 2, 3]. Това прави невъзможно използване на механизма за репликация на данните на базата на общия концентратор или

автоматизиран механизъм за репликация (Automated Replication mechanism (ARM), характерен за база от данни, разработена на основата на Multilateral Interoperability Program (MIP) [4]. Необходимо е разработване на специализирано приложение – шлюз за прехвърляне на данните от едната система към другата.

Цел на настоящата работа е създаване на подход за прехвърляне на информация за личния състав между АСУ на ЧР и ПИКИС.

Полева комуникационно-информационна система

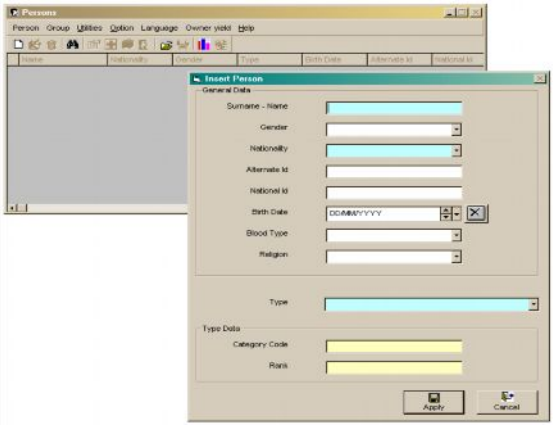
Както бе споменато по-горе, основата на информационното осигуряване на Полевата интегрирана комуникационно-информационна система на БА е модел базата данни на общия концентратор (Army Tactical Command and Control Interoperability Specifications (ATCCIS)) [3], доразвит като Land Command & Control Information Exchange Data Model (LC2IEDM), публикуван в съюзната публикация (ADatP-32) [5]. В модела са специфицирани изискванията към данните и структурата под форма на обекти, атрибути и връзки и е дефинирана физическа схема на метаданните.

Модулът за обслужване на данни за личен състав на комуникационно-информационната система е ”Personal data handler”. Той осигурява работата на длъжностните лица, в чиито задължения влиза поддръжката на данните за личния състав от батальона (B1), бригадата (G1) или съвместно командване (J1). Поддържа данните за организационните единици, тяхната подчиненост и йерархия, данни за личния състав, окомплектоването на подразделенията с личен състав, мобилизация, загуби и др.

Основната форма за въвеждане на персоналните данни е дадена на фиг. 1.

Както е видно от формата, основните данни, които се въвеждат за даден човек са: име, фамилия, пол, националност, персонален номер, национален идентификатор (за България това е единния граждански номер (ЕГН)), рожденна дата, кръвна група, религия. Всички тези данни се поддържат и в АСУ на ЧР в МО.

Допълнително модулът за личните данни позволява въвеждане и изобразяване на информация за тип на съответното лице, който се определя в зависимост от две други полета, а именно категория (category) и звание (rank).



Фиг. 1. Форма за въвеждане на персоналните данни

Полето категория може да взема следните стойности:

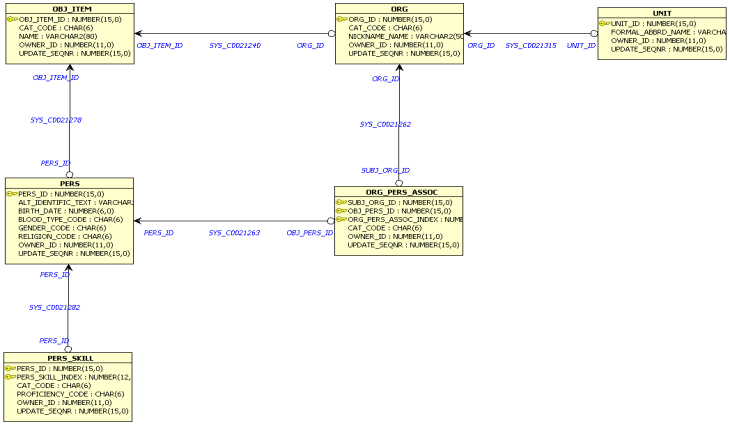
- ALM-Allied Military;
- CIV-Civilian;
- MIL-Military;
- NKN-Not Known;
- PAR-Paramilitary;
- POW-Prisoner of War;
- REF-Refugee)

Званията се задават в съответствие с тези, описани в STANAG 2116 [6]:

- EPTE - Enlisted Private
- NCO - NCO, Not Otherwise Specified
- NKN-Not Known
- OF1/OF10
- OFFR-
- OR1/OR9
- OTHR-Other Ranks, други звания.

Лицето се въвежда в определена група (команда).

Допълнителните данни не съответстват на възприетите значения за звание в АСУ на ЧР. На Фиг. 2 са представени структурите от информационния модел, които имат отношение към въвеждане и поддържане на данните за личния състав.



Фиг. 2. Физическия модел на базата данни от ПИКИС в частта, касаеща персоналните данни на личния състав

Таблица **OBJ_ITEM** – основна информационна единица за въвежданите елементи. Полетата в нея са следните:

- CAT_CODE – обозначава същността на даден елемент. Може да приема следните стойности:

  - PERSON (PE) – лични данни за човек;
  - ORGANIZATION (OR) – данни за административна или функционална структура;

- FACILITY (FA) – данни относно способности;
- FEATURE (FE) – данни относно характеристики;
- MATERIEL (MA) – данни за материали от логистично осигуряване.

- NAME – наименование на даден елемент от данните. В случая на данни за човек това е неговото име.

Таблица **PERS** – съдържа допълнителни данни за човек. Полетата в нея са както следва:

- ALT_IDENTIFIC_TEXT – допълнителни идентификационни данни. При използване в условията на БА това е ЕГН на човека;
- BIRTH_DATE – рождена дата на човека;
- BLOOD_TYPE_KODE – код на кръвната група на човека;
- GENDER_CODE – обозначава пола на човека;
- RELIGION_CODE – обозначава религиозна принадлежност.

Таблица **PERS_SKILL** – съдържа данни за подготовката на човека и има следните полета:

- CAT_CODE – описва категория способности;
- PROFICIENSY-CODE – представя нивото на владеене на дадената способност. Може да съдържа следните стойности: slightly(слабо), moderately(средно), very(добро), extremely(много добро).

Таблица **ORG** – описва административна или функционална стуктура. Полетата в нея имат следното значение:

Поле CAT_CODE – код на описваната структура;

Поле NICKNAME_NAME – наименование на структурата

Таблица **UNIT** – описва формация като част от организация. Поле FORMAL_ABBRD_NAME съдържа съкратено обозначение на формацията;

За поддържане на целостта на даните са въведени следните **правила**:

PERS.PERS_ID->OBJ_ITEM.OBJ_ITEM_ID – осигурява връзка 1:n (едно към много) между таблиците PERS и OBJ_ITEM;

PERS_SKILL.PERS_ID->PERS.PERS.ID – осигурява връзка 1:n (едно към много) между таблиците PERS_SKILL и PERS;

ORG.ORG_ID->OBJ_ITEM.OBJ_ITEM_ID – осигурява връзка 1:n (едно към много) между таблиците ORG и OBJ_ITEM;

UNIT.UNIT.ID->ORG.ORG_ID – осигурява връзка 1:n (едно към много) между таблиците UNIT и ORG;

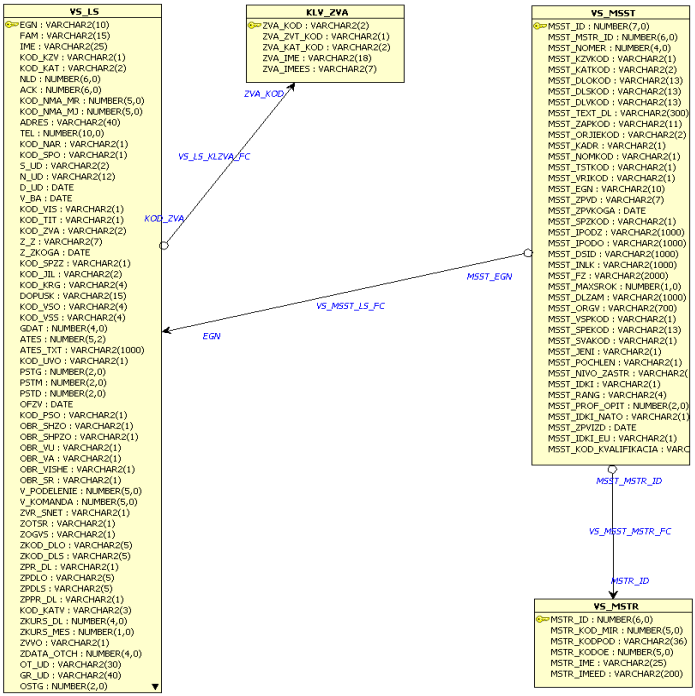
ORG_PERS_ASSOC.OBJ_PERS_ID->PERS.PERS_ID и ORG_PERS_ASSOC.SUBJ_ORG_ID->ORG.ORG_ID – осигурява връзка m:n (много към много) между таблиците ORG и PERS с използване на служебна таблица ORG_PERS_ASSOC. Последното позволява групи от хора да бъдат присъединявани към различни административни и функционални структури.

Автоматизирана система за управление на човешките ресурси в Министерството на отбраната

Автоматизирана система за управление на човешките ресурси в МО създава, съхранява и поддържа в актуално състояние единен информационен ресурс за човешките ресурси на министерството на отбраната.

Една от основните и подсистеми е “Персонални данни за служителите” . Тя е предназначена за създаване, поддържане и разпространение в нужния обем на електронна картотека с персонални данни на всички категории служители в МО,

включително обучаемите във военните учебни заведения и подлежащите на отчет във военните окръжия офицери, сержанти и войници от резерва. От нея могат да се извлекат персоналните данни на личния състав, които да се ползват от ПИКИС. На фиг. 3 е представен физическият модел на базата данни от АСУ на ЧР в МО в частта, касаеща персоналните данни за личния състав.



Фиг. 3. Физическия модел на базата данни от АСУ на ЧР в МО в частта, касаеща персоналните данни на личния състав, които могат да се ползват от ПИКИС

Основна таблица с персоналните данни е **VS_LS.** Полетата с информация необходима за ПИКИС са както следва:

- ЕГН – дава единния граждански код на лицето;
- FAM – фамилия;
- IME – име;
- KOD_KRG – кръвна група;
- KOD_NAR – народност;
- KOD_KZV – код на званието;
- V_PODELENIE – номер на поделението;

По кода на званието, от таблица KLV_ZVA се определя самото звание. Допълнителни данни за поделението се извличат от таблица VS_MSST, а за военновре-

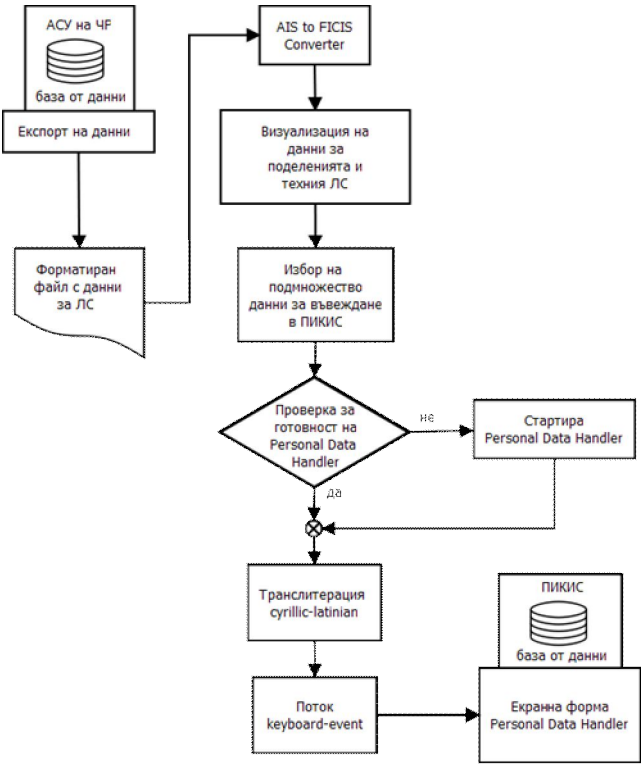
менната команда – от таблица **VS_MSTR**. Организационната йерархия на поделенията се определя в допълнителна таблица.

Подсистемата "Персонални данни за служителите" може да експортира определени персоналните данни в текстов файл.

Модул (шлюз) за автоматизирано прехвърляне на данни от Автоматизирана система за управление на човешките ресурси в Министерството на отбраната в ПИКИС

Един успешен опит за автоматизирано прехвърляне на данни за личния състав от АСУ на ЧР в МО и въвеждане в модула "Personal Data Handler" на ПИКИС е реализиран като специализирано програмно осигуряване, наречено "AIS to FICIS converter".

Функционална диаграма на приложението е представена на фиг. 4.



Фиг. 4. Функционална диаграма на "AIS to FICIS converter"

Програмата "AIS to FICIS converter", екран от която е показан на Фиг. **5**, притежава следните функционални особености:

- Със средствата на АСУ на ЧР се експортират данни за личен състав като форматиран текстов файл.
- Операторът избира и подава към ПИКИС конкретен файл с актуални данни за личен състав.

- В програмата е реализирана процедура за визуализация на административни и функционални структури на единиците личен състав, спадащи към отделните структури в йерархичен вид и от тази структура операторът избира подмножество от данни за автоматизирано въвеждане в ПИКИС. За прехвърляне към ПИКИС могат да бъдат избрани данни за отделен човек, или цяла група от организационна структура;

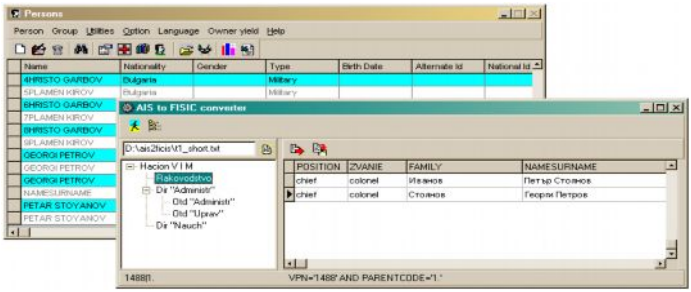
- Операторът стартира процедурата за прехвърляне на данни.

- Програмното осигуряване проверява дали е зареден модула ”Personal Data Handler” и ако не е го зарежда.

- Тъй като в ПИКИС се работи само с латиница се извършва прекодиране (транслитерация) на символите кирилица към съответните на латиница с използване на общовъзприетия в България метод.

- Програмното осигуряване определя като цел на изходящия поток екранната форма „Personal Data Handler” на ПИКИС и генерира изходящ поток събития тип ”keyboard event”, съдържащ исканите данни за личен състав.

- Модулът ”Personal Data Handler” възприема генерираните командни последователности и визуализира новопостъпилите данни за личен състав.



Фиг. 5. Екран от програмата за прехвърляне на данни от АСУ на ЧР в МО към ПИКИС

Изводи:

1. С интегрирането на различните информационни системи за командване и управление се създава възможност за създаване на единна система с обща база от данни, избягва се необходимостта от многократно въвеждане и поддържане на една и съща информация и се повишава достоверността на извежданите справки и отчети.

2. Интеграцията на новоразработвани системи за командване и управление в съвременни условия се осъществява на основата на общ модел на данните C2IEDM/JC3IEDM и ADatP-3 интерфейси за форматирани съобщения, съгласно изискванията на MIP (Multilateral Interoperability Programme).

3. Възможните подходи за интегриране на съществуващи системи за командване и управление се състоят в създаване на специализирани приложения (шлюзове), които хармонизират описанията на данните на различните системи или както е предложено в настоящата работа, като се ползват функционалните възможности за експортиране на данни от едната система и автоматизираното им въвеждането им чрез съответния потребителски интерфейс в другата система.

4. Приложението на предложения подход е препоръчително, когато алгоритмите за обработка на информацията не са известни точно и липсва сорс кода на програмната реализация на информационната система за командване и

управление, какъвто е случаят с ПИКИС. Възпремането на този подход ще доведе до значително съкращаване на времето за въвеждане в ПИКИС на съществуваща информация от мирновременните системи за командване и управление и ще премахне възможността за допускане на операторски грешки.

ЛИТЕРАТУРА:

1. Система ПИКИС. Проектиране на системата (4ie-tt000047-e, rev.C), Октомври 2001 г., стр. 60-72
2. Система ПИКИС. Проектиране на системата (C&C-FICIS (Cod. 149-6731/00E-Rel. 1.0), 2001
3. Army Tactical Command and Control Interoperability Specifications (ATCCIS), Working Papers 14-X series (2000)
4. http://www.mip-site.org
5. Land Command & Control Information Exchange Data Model, Edition 2.0, 31 March 2000
6. NATO rank codes, Stanag 2116, http://en.wikipedia.org/wiki/STANAG_2116
7. Желев, Ст. Опит за съставяне на емпиричен модел на компетенции по КИС за студенти на ФТН. Московский городской педагогический университет, Самарский филиал, Сборник научных статей, 2012.

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

ЗАЩИТАТА НА ИНФОРМАЦИЯТА - СЪСТОЯНИЕ И ПЕРСПЕКТИВИ

СБОРНИК НАУЧНИ ТРУДОВЕ

Б ъ л г а р с к а . И з д а н и е п ъ р в о . Т и р а ж 5 0

Предпечатна подготовка във Факултет „Артилерия, ПВО и КИС“ - Шумен