НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Катедра “Информационна сигурност”

Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я 2 0 1 3

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2013

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Защитата на личните данни в контекста на националната сигурност", проведена във Факултет "Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Националния военен университет "Васил Левски" - гр. Шумен, на 6 и 7 юни 2013 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 за сигурност на докладите си и носят лична отговорност за публикуване на класифицирана информация в тях.

От редакционната колегия

©НВУ "В. Левски" – Факултет "Артилерия, ПВО и КИС"
Шумен, 2013.
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 госпожи и господа,
Уважаеми офицери, курсанти, студенти, докторанти и специализанти,
Скъпи гости,

Добре дошли на ежегодната конференция по проблемите на информационната сигурност, организирана от Националния военен университет „Васил Левски" - Факултет „Артилерия, ПВО и КИС" в Шумен.

Конференцията представлява част от усилията на ръководството на Университета и Факултета, както и на нашата академична общност да развием, обогатим и интегрираме знания, умения, опит и научни постижения в сектора „Сигурност", канейки на форума представители на водещи институции, държавни структури, органите на държавна и местна власт, висши училища, научни организации, търговски дружества и неправителствени организации.

Вече седем години в Шумен провеждаме обучение на студенти, специализанти и докторанти в професионално направление „Национална сигурност" по специалност „Административна и информационна сигурност". За тези години по тази специалност успешно се дипломираха 75 бакалаври, 60 магистри и 23 специализанти в курс по защита на класифицираната информация.

Към настоящия момент във Военния факултет в Шумен се обучават по специалността „Административна и информационна сигурност" 200 студенти в ОКС „бакалавър", 32 студенти ОКС „магистър" и 5 докторанти в ОНС „доктор". Част от тях присъстват днес на конференцията, други ще изнесат доклади в студентско-докторантската научна секция.

За тези години, смея да твърдя, че натрупахме значителен опит в областта на информационната сигурност, не само в обучението на експерти, но и по отношение участие в научни и образователни проекти, използвайки капацитета си за подготовка на кадри с висше образование по специалности „Компютърни системи и технологии" и „Комуникационна техника и технологии", за което имаме акредитация с най-висока оценка от Националната агенция за оценяване и акредитация още от 1997 г.

Тази година конференцията провеждаме под надслов „Защитата на личните данни в контекста на информационна сигурност". Темата е изключително актуална поради ред причини, свързани с предизвикателствата в съвременния свят пред правото на всеки за защита на личните данни.

Проблематиката, свързана със защитата на личните данни, има много и различни аспекти, започвайки от чисто правния, преминавайки през технологичния, морално-етичния, психологическия до организационно-техническия.

На първо място става дума за новите технологии, които създават възможности за ползване на медицинска, генетична, биометрична, административна и други видове информация за всеки гражданин. Онлайн транзакциите също оставят следи от лични данни. Компютърните и мрежови технологии от своя страна създават нови проблеми, породени от събирането, разпространението и използване на информация, съдържаща лични данни.

В тази връзка в съвременни условия защитата на личните данни се свързва с телекомуникациите, прехвърляне на данни по телефон, цифрова телевизия, мобилни мрежи и други комуникационни системи.

Съществуват редица технологии за повишаване на защитата на личната информация, като кодиране, проксисървъри, препращане на съобщенията, електронни пари и смарткарти.

Важно е обаче да отбележим, че нито една система за защита на правото на личен живот не е достатъчно адекватна поради бързото развитие на технологиите и големия спектър от въпроси, свързани с това право.

Идеята да се опитаме да анализираме всички тези въпроси се породи преди година по време на миналогодишната конференция тук в Шумен по предложение на г-жа Венета Шопова – председател на Комисията за защита на личните данни.

Ето защо днес за мен е чест и удоволствие да обявя, че съорганизатори на настоящата конференция са Комисията за защита на личните данни и Държавната комисия по сигурността на информацията.

В научния форум участват и представители на Дирекция „Сигурност на информацията" - МО, Дирекция „Комуникационни и информационни системи" – МО, Държавна агенция „Национална сигурност", Министерството на вътрешните работи, Комисията за регулиране на съобщенията, Изпълнителната агенция „Електронни съобщителни мрежи и информационни системи" към Министерството на транспорта, информационните технологии и съобщенията, Административен съд – Шумен, Фондация „Право и интернет". В конференцията участват колеги от другите факултети на НВУ „В. Левски", преподаватели и изследователи от Шуменския университет „Епископ Константин Преславски", Великотърновския университет „Кирил и Методи", Бургаския свободен университет.

Госпожи и господа, за мен е чест да обявя нашите гости:

- Изпълняващият длъжността областен управител – г-н Ивайло Илиев;
- г-жа Венета Шопова – председател на Комисията за защита на личните данни;
- г-н Цанко Цолов – началник на отдел „Регистър и архив" в Комисията за защита на личните данни;
- г-н Стайко Христов - директор на Дирекция „Защита на класифицираната информация" в Държавната комисия по сигурността на информацията;
- д-р Румен Гюров – главен експерт в Дирекция „Защита на класифицираната информация" в Държавната комисия по сигурността на информацията;
- полк. Йосиф Атанасов – началник на отдел в Дирекция „Сигурност на информацията" – МО;
- подп. Митко Димитров - дирекция „Сигурност на информацията" – МО;
- подп. Васил Стайков – главен експерт в Дирекция „Комуникационни и информационни системи" – МО;
- г-н Стоян Тонев – директор на Териториална дирекция „Национална сигурност";

- комисар Здравко Захариев – директор на Областна дирекция на МВР;
- г-н Иван Капралов – обществен посредник на Община Шумен;
- съдия Снежина Чолакова – Административен съд – Шумен;
- доц. д-р Георги Димитров – председател на Фондация „Право и интернет";
- адвокат Десислава Кръстева - старши експерт във Фондация „Право и интернет";
- г-н Степан Химук – старши юрисконсулт в Комисията за регулиране на съобщенията;
- г-н Николай Николов – началник на отдел „Регионална поддръжка" в Дирекция „Дунав" на Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" към Министерството на транспорта, информационните технологии и съобщенията;
- г-н Неделчо Неделчев - главен експерт ОМП и служител по сигурността на информацията в Областна администрация Шумен;
- г-н Дилян Узунски – главен експерт ОМП и служител по сигурността на информацията в Община Шумен.

Благодаря на всички гости, че уважиха нашата покана и се включиха в работата на конференцията.

Госпожи и господа,

По време на пленарната сесия на форума ще имате възможността да се запознаете с актуалните постановки, свързани с държавната политика в сферата на защитата на личните данни, техническите и организационни изисквания за защита на същите. Ще бъдат анализирани правните проблеми, свързани с прилагането на отделните нормативни актове, регламентиращи защитата на данните на различните видове потребители на услуги. Ще бъде предложен модел за изграждане на система за киберсигурност.

След пленарния панел работата на конференцията ще продължи в три научни секции – „Държава и сигурност" с модератор доц. д.и.н. Красимир Марков, „Информационна сигурност" с модератор проф. д.в.н. Манол Млеченков и студентско-докторантска секция с модератор подп. доц. д-р Чавдар Минчев.

В отделните научни секции има депозирани интересни доклади и презентации, свързани с използване на стеганографски методи за защита на информацията и анализ на конкретни стеганографски алгоритми, анализ на злонамерени уеббазирани атаки, модел на интегрирана система за физическа сигурност, изследване на сигурността при сесиите с т.нар. „бисквитки" в интернет браузърите, анализ на сигурността в социалните мрежи и други.

За нас е много важно, че в работата на конференцията се включват с доклади и съобщения курсанти, студенти и докторанти. Това е традиция, която се стремим да утвърждаваме и задълбочаваме.

Благодаря на организаторите и съорганизаторите на настоящата конференция.

Желая на всички участници и гости на конференцията успешна и ползотворна работа.

Откривам научната конференция „Защитата на личните данни в контекста на информационната сигурност" – Шумен 2013-та.

ДЪРЖАВНАТА ПОЛИТИКА В СФЕРАТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Венета Л. Шопова

Комисия за защита на личните данни
kzld@cpdp.bg

THE STATE POLICY IN THE FIELD OF PERSONAL DATA PROTECTION

Veneta L. Shopova

ABSTRACT: The independent and well equipped supervisory authority, assessing public attitudes towards issues related to data protection, adequate prevention, and enhanced supervision are the buildings blocks of the state policy in the data protection field. The state policy on data protection is of dynamic nature. We have to look at the notion of data protection in a broader cross-border context, and especially how it relates to other fundamental rights, social norms and technological developments.

KEY WORDS: institute of the data protection authority, risk analysis, prevention, supervision, risk-based approach

Интердисциплинарният характер на защитата на личните данни е основният фактор, който обуславя провеждането на държавната политика в тази област. Той предопределя съдържанието на политиката не само на национално ниво, но и тенденциите за развитие в международен план. Провеждането на държавната политика в областта на защитата на личните данни е постоянен процес, който включва ефективно функциониране на институцията на надзорния орган на национално ниво, оценка на обществените нагласи, прилагане на адекватна превенция и упражняване на засилен контрол.

Важен елемент от политиката също така е предприемането на действия, насочени към осъзнаване на собствената отговорност на всички участващи в процеса страни: физическо лице - администратор - надзорен орган. Предмет на този доклад са именно тези теми.

Основополагащ елемент на държавната политика в сферата на защитата на личните данни е институцията на **надзорния орган**. Неговият статут и правомощия в държавата са от решаващо значение за ефективното провеждане на националната политика. Действащата европейска Директива 95/46/ЕО разписва важни условия относно функционирането на надзорния орган по защита на данните – гарантиране на неговата пълна независимост, компетенции за консултиране и намеса в операциите по обработването на данни, правомощие по разследване, разглеждане на жалби, налагане на административни санкции.

В национален план, тези генерални правомощия, въведени в Закона за защита на личните данни, са фундамента, върху който се гради държавната политика.

Независимият статут, дистанцирането от външно влияние, указания и натиск, **легитимира дейността на надзорния орган** като самостоятелна в рамките на

общата национална политика и като пряко насочена към конкретните потребности на обществото (администратори и физически лица) по отношение правото за защита на личните данни. Това обстоятелство прави Комисията за защита на личните данни лесно разпознаваема за отделния гражданин и гарантира валидност на взетите от надзорния орган решения.

Правомощието за консултиране и намеса има за цел да наложи унифицирано правоприлагане и работи в посока създаване на национален стандарт за защита на данните и постигане на високо ниво на осъзнатост по отношение на рисковете, правата и задълженията.

Правомощието за разследване и разглеждане на жалби е ключово за реалното упражняване на надзор, каквото е предназначението на органа по защита на данните и без което не може да се гарантира законосъобразност на обработването на лични данни.

Редица специфични правомощия, установени в резултат на добрата национална практика, способстват провеждането на отговорна държавна политика в областта на защитата на личните данни и поради това, че надхвърлят правомощията на надзорния орган по Директива 95/46/ЕО, имат уникален характер. Тези правомощия са издаването на подзаконови нормативни актове, участието в преговори и сключването на двустранни или многостранни споразумения в областта на защита на личните данни. Те дават възможност за бъдещо развитие на държавната политика и извеждат българският надзорен орган сред малцината в Европейския съюз, на които държавата е делегирала подобни правомощия. Друго специфично национално правомощие от 2011 г. с все по-широко приложение е провеждането на обучение на национално ниво от страна на Комисията за защита на личните данни.

Към специфичните правомощия може да бъде посочено обстоятелството, че Комисията за защита на личните данни е **наблюдаващ орган** относно сигурността на трафичните данни, съхранявани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.

Изпълнението на така заложените по закон правомощия на надзорния орган е немислимо без наличието на адекватна финансова, ресурсна и техническа обезпеченост. Комплексният характер на защитата на личните данни налага ангажирането на добре подготвени експерти в тази област и специализирането им по ключови направления.

Въвеждането на ефикасна система за електронно управление на процесите по регистрация на администратори на лични данни, подаване на жалби, консултиране на лицата, както и на вътрешно-организационната дейност на Комисията също са предпоставка за изпълнение на политиката.

След този общ обзор на институцията на надзорния орган, по-нататък в изложението ще се спрем по-подробно на компонентите, съставляващи държавната политика.

А**нализ на проблемите** е първата стъпка, която предопределя всички по-нататъшни действия в процеса по защита на данните. Чрез проучване на потребностите и нагласите сред обществото, Комисията набелязва целевите групи и проблемните области. Резултатите от проучването осигуряват навременна информираност на надзорния орган и отварят пътя за прилагане на един от следните два подхода: тематичен - по проблеми или секторен - по категории администратори.

Тематичният подход включва анализ на въпроси от широк обществен интерес и формулиране на ясни препоръки и указания от страна на Комисията за защита на личните данни. Като пример можем да посочим обработки на данни с възможно негативни последици за лицата, каквото е нерегламентираното видео-наблюдение, обработването на лична информация в големи (често трансгранични) бази данни, копирането на лични документи, рисковете пред неприкосновеността в интернет пространството.

Секторният подход се фокусира върху проблемите и очакванията на група от администратори със сходен предмет на дейност. Като чувствителни за обществото групи можем да посочим телекомуникационния, банковия, образователния сектор, както и компаниите, предоставящи комунални услуги. Обект на постоянна оценка са и някои социални групи, характеризиращи се с повишен риск от нарушаване правото на защита, каквито са децата в контекста на информационното общество. Действията, които Комисията предприема в тази връзка, включват провеждането на специализирани обучения, проучване на потребностите в даден сектор и извършването на секторни проверки. Прилагането на секторната политика води до много по-лесно идентифициране на конкретните трудности за обработката на данни, при отчитане спецификата на дейността и възможните неблагоприятни последствия върху защитата на личните данни. В резултатът се предписват *действия по мярка*.

Адекватната превенция е ядрото на държавната политика в сферата на защитата на личните данни. Тя влиза в действие веднага след анализа на проблемите и потребностите. На базата на подход, основан на управление на риска, се предприемат конкретни превантивни действия. Значимостта на този подход наложи Комисията да установи нови правила за техническите и организационни изисквания, който администраторите са длъжни да предприемат, основани на предварителна оценка на въздействието.

Превантивната дейност има широкоспектърно действие. Обхваща образователната и информационна дейност на надзорния орган, политика за съгласуваност с други държавни институции, налагането на единни стандарти за защита. Осъществява се координирано с добрите общоевропейски практики и включва голям набор от направления, сред които:

- Издаването на становища и съгласуването на проекти на нормативни актове, целящи унифицирано правоприлагане в сферата на неприкосновеността. Тази мярка следва да се възприема в контекста на комплексния и интердисциплинарен характер на защитата на личните данни. Трябва да се знае много добре къде е точно място на защитата на личните данни в различните сфери на обществените отношения и как най-ефикасно тя следва да се прилага в съотношение с други норми и права.
- Издаването на задължителни указания е също съществен елемент от налагането на унифицирана практика. Комисията вече се възползвала от този инструмент във връзка с контролните си функции по Закона за електронните съобщения. Издадените от Комисията през 2012 г. задължителни указания съдържат параметрите, които налагат уеднаквяване в практиката на всички ангажирани субекти - предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги, компетентни органи, съдилища, прокуратура.
- Поощряване на администраторите да създават кодекси за поведение и политики по неприкосновеността, както и готовност за тяхното консултиране и съг-

ласуване. Насърчаването на този подход е изключително важен за оправдаване на доверието и очакването на потребителите, и създаване на правна сигурност чрез канализиране на процесите по обработка и защита на данните.

- Насърчаване въвеждането на технологии за подобряване на неприкосновеността. Това е особено актуална тема в контекста на законодателната реформа на ниво Европейски съюз и въвеждането на механизми, като „защита по подразбиране" (privacy by default) и „защита при проектиране" (privacy by design).
- Непрекъснат обмен на информация и добри практики с други национални органи по защита на данните от европейските държави. Тази практика позволява формулирането на общ подход за превенция и реакция в единния вътрешен пазар.
- Практиката на Комисията да публикува предварително „План за годишните проверки на администраторите на лични данни" е с доказан дисциплиниращ ефект.
- Предвижданите в Закона за защита на личните данни високи санкции също са с превантивен, разубеждаващ характер и имат за цел да гарантират пълното прилагане на законовите разпоредби.
- Широк спектър от мероприятия, които правят достъпна практиката на Комисията за много по-широк кръг от лица и позволяват оценка на ситуацията в реална среда. Тук можем да посочим концепцията за реализиране на „изнесени заседания" в различни региони на страната.
- Целенасочена информационна политика. Тя включва провеждане на информационно-образователни кампании относно рисковете при обработване на данните, необходимостта от висока степен на осъзнатост на лицата за значимостта на техните лични данни и ролята на надзорния орган. Практиката на Комисията до провежда регулярни обучения за администратори и обработващи лични данни и студенти също е част от информационната политика на надзорния орган.
- Постоянен контакт с граждани по въпроси, свързани със защитата на техните лични данни. Това е не само начин за отговор на техни конкретни потребности, но и възможност за Комисията да следи за обезпокоителни тенденции и своевременно да им противодейства.

При осъществяването на превенцията, Комисията за защита на личните данни частично се доближава до предмета на дейност на гражданските правозащитни и академични организации и тясно си сътрудничи с тях за изпълнението на този общ приоритет.

Третият основен компонент от държавната политика е **засиленият контрол.** Той протича независимо и паралелно от превантивната дейност. Може да има планов характер, да се извършва според конкретния случай или да осъществява последващ мониторинг. Целта е стриктно съблюдаване на императивните норми на Закона, предотвратяване повтарянето на определени лоши практики и нарушения. Контролната дейност има *оздравителен* ефект върху администратора чрез посочване на конкретни препоръки за подобряване на процесите по обработка в технически, организационен и правен аспект.

За ефективно осъществяване на контролната си дейност Комисията се възползва от няколко механизма. Първият от тях е текущ анализ на дейността на администраторите за спазване на нормативните актове по защита на личните данни. Осъществяването на пряк контрол в публичния и частния сектор е сърцевината на

надзора. Третият, най-ефективният механизъм за въздействие, несъмнено е фактическото налагане на санкции.

Към надзорната дейност може да причислим и подходът за управление на риска , който е определящ критерий за нейната ефективност. Конкретно изражение на този подход е изборът на обектите-предмет на контрол. Приоритетни в това отношение са администратори от структури и сфери с висока обществена и социална значимост, структурите, които обработват голям обем данни или данни с чувствителен характер.

Не на последно място, обект на контрол са и субектите, чиято дейност по обработване застрашава правата и законните интереси на физическите лица. Това обстоятелство е отчетено и в българското законодателство. Именно рисковете при обработване на голям обем данни в сектора на телекомуникациите е причина в Закона за електронните съобщения да се разпише задължение за доставчиците на тези услуги да уведомяват Комисията за нарушения на сигурността на лични данни. Това е предпоставка за бързо задействане на контролния механизъм от страна на надзорния орган и гарантиране предприемането на адекватни действия за отстраняване на възможните неблагоприятни последици.

В съпоставка с превантивната дейност, контролната дейност на Комисията е изпълнително правомощие с подчертано правоприлагащ характер. Ефективното й осъществяване допринася за развиване на усещането за правдивост и държавност и носи пряка удовлетвореност на лицата чрез изразяване на конкретни решения по подадени жалби и сигнали.

В обобщение, можем да кажем, че целите, които си поставяме при изпълнението на държавната политика за защита на личните данни са именно съвместяване на най-добрите практики на гражданския сектор и на държавната власт. По този начин се отговаря на справедливите очаквания на обществото за гарантиране правото на защита. В този процес отчитаме и редица фактори, които придават определена динамика на държавната политика. Такива фактори са международните тенденции в областта на неприкосновеността, общовалидни норми (като свободното движение на данни), други области на защита (сигурност на информацията), както и редица области на обществения живот. Отговор остава да намери въпросът къде е мястото на фундаменталното право на защита на личните данни в съотношение с други фундаментални права, като правото на свободно изразяване, правото на достъп до обществена информация и свободата за обработване на данни за научноизследователски цели.

Динамика на държавната политика придават и многото неизвестни, свързани с бързо-променящите се информационни технологии. Затова, при изграждане на цялостната концепция трябва да се отчита, че защитата на личните данни има комплексен, отворен характер, факт, който се отчита и в настоящата европейска законодателна реформа. Въпреки че предлаганите с реформата нови правила спрямо онлайн средата, като „правото да бъдеш забравен" и „правото на преносимост на данните" будят сериозни опасения относно тяхната приложимост, предложеният законодателен подход е единственият начин за връщане на доверието на потребителите към онлайн услугите. Част от този сценарий включва връщането на реалния контрол върху обработваните лични данни в ръцете на предоставилото ги лице. Целта на реформата е гарантиране на защитата и сигурността на данните, без да се възпрепятства тяхното свободно движение. Европа е на прага на въвеждането

на първия висок, унифициран стандарт за защита на личните данни, който ще бъде приложим за всички световни компании, предлагащи стоки и услуги на вътрешния европейски пазар и който ще намери своята проекция както в националната политика и практика, така и с оглед на набиращите скорост глобални мрежи по неприкосновеността.

Литература:

1. Директива 95/46/ЕО на Европейския Парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

2. Закон за защита на личните данни.

3. Закон за електронните съобщения.

4. Съобщение от Комисията до Европейския парламент, до Съвета, до Европейския икономически и социален комитет и до Комитета на регионите. Защитата на правото на личен живот във взаимосвързания свят. Европейска рамка за защита на данните за 21-ви век.

5. Предложение за регламент на Европейския парламент и на Съвета 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).

МОДЕЛ ЗА ИЗГРАЖДАНЕ НА СИСТЕМА ЗА КИБЕРСИГУРНОСТ

Румен Ст. Гюров

Държавна комисия по сигурността на информацията
имейл: dksi@governmet.bg, gyurov.rumen@gmail.com

MODELING CYBERSECURITY SYSTEM

Rumen St. Gyurov

ABSTRACT. *Developing a model for cyber security system in not only a practical task, but it is also a very intriguing intellectual one. The initial approach to its solution is linked to the modern security paradigm. In this paradigm the comprehensiveness of the existing insecurity provokes the development of various concepts for overcoming it, in which the features of the information telecommunication technologies are always present. The focus is shifting to cyber space and its projections, to cyber security and the strategies for its achievement. The given preliminary concept framework postulates the complexity of the cyber security matters to be incorporated into the basis of the drafted model.*

KEY WORDS. *Application security, CERT, CSIRT, computer security, critical information infrastructure protection, critical information infrastructure, cyberactor, cyberattack, cyber counter-intelligence, cybercrime, cyberdefense, cyberespionage, cybergovernance, cyberintelligence, cybersecurity domain, cybersecurity strategy, cybersecurity system, cybersecurity, cyberspace, cyberwarfare, global security, human security, information security, information telecommunication technologies, internet security, model, network security, personal data protection, societal security.*

Подход за формиране на модела

Формирането на модел за изграждане на система за киберсигурност е не само практическа, но и силно интригуваща интелектуална задача. Предварителната представа за подхода към нейното решаване е свързана с новата парадигма на сигурността в днешния свят. В тази парадигма всеобхватността на съществуващата несигурност естествено поражда търсения за адекватното й осмисляне и преодоляване. Затова разработваните концепции неизбежно отчитат спецификата на информационното общество и високите технологии в телекомуникациите. Затова вниманието закономерно и последователно се насочва към киберпространството и неговите проекции, към киберсигурността и стратегиите за нейното постигане. Съгласно тази предварителна престава, отговорите на въпросите, свързани с киберсигурността, е необходимо да бъдат поставени в основата на разработвания модел. За да бъде обществено приложим, моделът трябва да акцентира повече върху нетехническите акспекти, отколкото върху технологичните [1].

[1] Sulek, David, et al. Asserting Global Leadership in the Cyber Domain. Ready for What's Next. 2011 Update. Booz Allen Hamilton Inc., 16.08.2011, PDF, p. 7, www.boozallen.com, 15.05.2013.

Новата парадигма и концепции за сигурност

Новата парадигма на сигурността се появи в началото на 90-те години на 20-и век. Форматът й бе програмиран от революцията във високите технологии и постоянно актуализиран от ускоряващата се динамика на окръжаващата ни среда [2]. Зашеметяващият скок на информатиката и телекомуникациите засяга пряко всекидневния живот на хората, като едновременно персонализира и засилва колективно изживявания опит, поражда неочаквани социални и културни (социетални) последици, които променят радикално икономиката и политиката. Опитът да бъдат осмислени промените наложи виждането, което мнозина обозначават с понятието „глобализация". Прието е, че тя представлява „бързо, нарастващо и неравномерно трансгранично проникване на стоки, услуги, хора, пари, технологии, информация, идеи, култура, престъпност и оръжия" [3]. Без съмнение глобализацията носи благосъстояние и свобода на общуване, но и поставя на изпитание нашата сигурност. Подхранва редица негативни тенденции: диспропорции и напрежения в икономиката и особено във финансовия сектор; политическа нестабилност поради липса на опит и в резултат от острите икономически проблеми; изостряне на демографските проблеми, ръст на масовата миграция и трансграничната организирана престъпност; предизвикан от информационния потоп културен шок, генериращ непрекъснато криза на идентичността [4].

Новите предизвикателства подтикнаха към нови подходи [5]. Един от тях е концепцията за устойчива сигурност, която признава взаимопроникващата връзка устойчивост-сигурност [6], държи сметка за жизнеността на обществото и преде-

[2] Moshchelkov, Evgeny. International and National Security in the World Community in the Twenty-First Century: Outlines of New Realities. Garmisch-Partenkirchen, 2003, PDF, p. 1-3, www.marshallcenter.org, 07.06.2006; Quille, Gerrard, et al. An Action Plan for European Defense: Implementing the Security Strategy. Brussels – Rome, 2005, PDF, p. 9-11, 12.06.2012; The National Intelligence Strategy of the United States of America. Washington, August 2009, PDF, p. 5-8, www.fas.org, 12.06.2012.

[3] Kugler, Richard, et al. Globalization and National Security. Vol. I–V. Washington, 2001, PDF, vol. I, p. 9-10 etc., http://permanent.access.gpo.gov, 25.04.2010.

[4] За последиците от глобализацията виж по-подробно: Choucri, Nazli. Migration and Security: Key Linkages. – In: Journal of International Affairs. New York, Fall 2002, vol. 56, № 1, p. 113; Drew, Dennis, and Donald Snow. Making Twenty-First-Century Strategy: An Introduction to Modern National Security Processes and Problems. Air University Press, Maxwell Air Force Base, Alabama, 2006, p. 44-233; Kicinger, Anna. International Migration as a Non-Traditional Security Threat and the EU Responses to This Phenomenon. Warsaw, 2004, p. 2-3; Kirshner, Jonathan (ed.). Globalization and National Security. New York, 2006, Google Books, p. 2-22, http://books.google.bg, 19.04.2010; Kugler, R., et al. Globalization..., vol. I, p. 8-40; Perl, Raphael. Terrorism and National Security: Issues and Trends. Washington: CRS, 2006, PDF, p. 7-9, www.http://fpc.state.gov, 20.04.2010; Quille, G., et al. An Action…, p. 5-7.

[5] Omand, David. The National Security Strategy: Implications for the UK Intelligence Community. A Discussion Paper for the ippr Commission on National Security for the 21st Century. Institute for Public Policy Research, February 2009, PDF, p. 3, http://dematerialisedid.com, 12.06.2012.

[6] Sustainable Security. Washington, Center for American Progress, 2009, PDF, p. 1-2, www.americanprogress.org, 14.06.2012.

финира националната сигурност около идеята за човешка сигурност [7]. „Човешката сигурност" е пряко свързана със защитата на правата и свободите на хората. Има множество допирни точки със стремежа към преодоляване на социалната несправедливост [8], към равен достъп до материални и духовни блага. Вменява на институциите отговорността за отстраняване на несигурността за отделните граждани и техните семейства, частните предприемачи и търговци, обществените активисти и организации, така че техните свободи, ценности, благополучие и всекидневен живот да бъдат защитени и да се развиват в по-устойчива, сигурна, справедлива и просперираща среда [9]. Модерният възглед за сигурността, с нейното неизбежно личностно измерение, все повече се налага в България: „Главен обект и субект на сигурността е човекът – най-ценното и уязвимото, но и най-опасното за себе си и за обитаваната среда създание на Земята", категорично заявяват българските експерти [10].

Подобно разбиране за сигурността откроява отделните й аспекти (равнища, измерения, пластове…): глобална, национална, социетална и лична сигурност [11]. В нашето разбиране е важно да избегнем буквалното тълкуване на понятията, като да приемем някои уговорки. Първата се отнася до т. нар. глобална сигурност, втората засяга националната, третата – т. нар. социетална сигурност. Четвъртата се отнася до уточняването на „информационния формат" на вече известните понятия.

Първо. Глобализацията „детронира" географията. Евклидовите очертания на държавните граници и традиционните общества радикално губят своето значение. Дори световен икономически и технологически лидер като Съединените американски щати не може да избегне тези влияния [12]. Ярка илюстрация на глобалната замяна на географията с информатиката е Дейтънският мир от 1995 г. Мирното споразумение става възможно, а мирът – неизбежен, благодарение на една нова реалност. Представителите на преговарящите страни (Остатъчна Югославия, Хърватия и Босна и Херцеговина) са въведени във виртуална зала на американската военна база „Райт-Патерсън" в Дейтън, Охайо. В нея те стават свидетели на симулации на териториите, за които спорят, и на обстановката, която обсъждат. Психологическият и културен шок от високата технология и демонстрираната американска военна мощ елиминират всяка съпротива, спомагат за договаряне между страните и допринасят за подписване на споразумението. Така географията успешно, за пръв път и буквално е изместена от информатиката [13]. Едва след това тази тенденция с цялата си сила става доминираща. За съжаление, сред най-шокиращите свидетелства за окончателно „детронираната" география са терористичните актове от 11 септември 2001 г. в Ню Йорк, 11 март 2004 г. в Мадрид, 7 юли 2005 г. в Лондон и още много други, както и не на последно място бомбеният атентат от 18 юли

[7] Omand, D. The National…, p. 3.

[8] Sachs, Stephen. The Changing Definition of Security. Oxford, 2003, HTML, www.stevesachs.com, 22.12.2009.

[9] Omand, D. The National…, p. 3.

[10] Желязков, Иван, и Тодор Трифонов. Енергийната сигурност на България. София, 2012, с. 15.

[11] Срв. Слатински, Николай. Измерения на сигурността, София, 2000, с. 19-21.

[12] Ó Tuathail, Gearóid, and Simon Dalby (eds.). Rethinking Geopolitics. London – New York, Routledge, 1998, PDF, p. 29, http://frenndw.files.wordpress.com, 13.04.2013.

[13] Ó Tuathail, G. and S. Dalby (eds.). Rethinking…, p. 28-29.

2012 г. в Бургас. Затова под „глобална сигурност" следва да се разбира сигурност, освободена от доминиращото влияние на географския фактор и силно повлияна от модерните информационни технологии и комуникации.

Второ. Националната сигурност е все още неотменима характеристика или проблем в заобикалящата ни действителност. Все още съществува основният й субект – националната държава. Но съществуването на националната държава вече не означава задължително прилагане на принципа на суверенитета, а по-скоро – своеобразното му несигурно възпроизвеждане: постоянната съзнателна промяна в субординацията между власт, територия, население и признание за самостоятелността на самата субординация [14]. В центъра на националната сигурност отново стои националният суверенитет, но форматиран вече не с картографски средства, а със средствата на новите технологии. Националната сигурност по подобие на глобалната придобива виртуални, но съвсем не недействителни, очертания. Недържавни и вътрешнодържавни актори придобиват все по-голямо влияние: екстремистки групи, склонни към насилие, международни терористи, метежници и транснационални криминални организации [15].

Трето. Социеталната сигурност е най-съществения аспект на сигурността. Тя означава свобода на избора на културна принадлежност, свобода при определяне на собствената идентичност, осъзната като вродено качество или придобито право и воля за съжителство в определена човешка общност. Социеталната сигурност е централно понятие, което изразява националната сигурност като такава и свежда преживяването й до отделната личност [16].

Четвърто. Отделните измерения на сигурността тук се разбират като степени на общност. Тези степени не са механично образуван сбор или численост на включените в нея индивиди – нито като глобална общност на цялото земно население, нито като населението на дадена национална държава, нито като численост на членовете на отделни социални групи и културни общности, нито като единичност на отделния индивид в обществото. Визираните степени на общност са формирани въз основа на спецификата на човешката дейност и потребности, форматирани от информационните и комуникационните технологии. В този смисъл глобална сигурност е не сигурност на земното кълбо, а представлява сигурност на цялостната човешка дейност, винаги и навсякъде в днешния свят, всеобхватна сигурност. Националната сигурност е сигурност на особен, споделен суверенитет, сигурност на цялостната човешка дейност върху онази територия, която днес е територия не в буквално географското й значение, а в значението на обособен в дадена област суверенен, самостоятелен, независим, но съобразен с останалите избор. Социеталната сигурност е защитена от суверенния избор свобода на самоопределянето като принадлежност към дадена общност. Личната сигурност се изразява в реализиране на правото на личността да се развива свободно, според собствените си потребности.

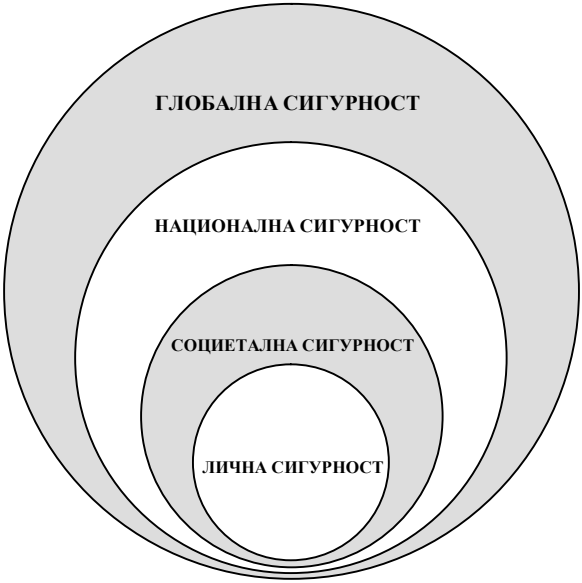
Разглежданите измерения на сигурността могат да бъдат представени в своеобразен модел, свързващ глобална, национална, социетална и лична сигурност. Моделът подсказва обхвата на отделните видове сигурност, може да бъде изобразен като вписани един в друг кръгове или като пирамида, чиято основа е глобалната

[14] Ó Tuathail, G. and S. Dalby (eds.). Rethinking…, p. 89-90.

[15] The National Intelligence…, p. 7-8.

[16] Мичев, Стефан. Илюзията за сигурност. София, 2012, с. 37-41; Уайт, Лесли. Науката за културата. Изследване на човека и цивилизацията. София, 1988, с. 160-161.

сигурност, а върхът – личната. Възможно е представяне и във форма, подобна на формата на небезизвестния НОРД-цикъл. Всъщност вложеното съдържание в модела е по-важно от графичния образ (фиг. 1).



Фиг. 1. Модел на равнищата на сигурността

Киберизмерения на сигурността и измерения на киберсигурността

Днешното общество разчита и зависи от новопоявилия се киберсвят. Показателна е следната киберстатистика. В развитите държави от Северна Америка, Европейския съюз и Г-20 интернет допринася за 8% от БВП. Всеки ден се изпращат над 294 милиарда имейл съобщения или над 3,4 млн. имейл съобщения всяка секунда от денонощието. Всяка минута SMS трафикът генерира 812 хил. USD или близо 630 хил. EUR. Глобалният пазар на мобилните услуги (телефони) обхваща над 85% от световното население, а 15% от него пазаруват чрез мобифоните си онлайн. Именно това (както и множество други факти, изразени със сходна статистика) доведе до безпрецедентен икономически ръст в света [17].

Една от най-ярките прояви на нарасналата стойност на социеталната и човешката сигурност е взривът на социалните мрежи, които обхващат вече 20% от населението в света [18]. Потребителите прекарват в тях средно между 5 и 6 часа месечно. Днес Фейсбук се радва на 750 милиона почитатели. Или всеки девети жител на Земята е във Фейсбук. Тиутър – на 100 милиона. Стойността на първата мрежа достига 80

[17] Klimburg, Alexander (ed.). National Cyber Security Framework Manual. NATO CCD COE Publication. Tallinn, 2012, PDF, p. 2-3, www.ccdcoe.org, 20.05.2013

[18] Klimburg, A. (ed.). National…, p. 2.

милиарда американски долара, на втората – 8 милиарда [19]. В YouTube всекидневно се качват над 864 хил. часа видео [20]. Всъщност освен взрив на споделената принадлежност и индивидуалност в киберпространството, взривът на социалните мрежи сполучливо може да бъде определен и като взрив на числата [21].

В социалните мрежи медиатор е самата аудитория. В тях хората се чувстват свободни за себеизява и затова са активни. Неограничените възможности на социалните медии свързват хората в активни общности, които постоянно общуват [22]. Затова днес те са най-мощният фактор, който спомага за споделяне на преживения човешки опит, формира глобална култура и персонализира и дава воля на колективния човешки дух. С тази своя уникалност те предизвикват потресаващи едновременно социални и културни промени, пораждат неочаквани икономически и политически последици. Разбира се, че това засяга пряко сигурността и обществената жизненост. Недвусмислените примери в тази посока са станалите азбучни аргументи за връзките между Фейсбук и Арабската пролет, Туитър и „Окупирай Уолстрийт"... Тези примери доказват също, че дори необхванатият от глобалните информационни и телекомуникационни технологии свят е киберформатиран.

Това са част от космическите и радикалните качествени измерения на пространството, създадено от информационните и телекомуникационните технологии – т. нар. киберпространство. То представлява съвкупност от: информационна инфраструктура и телекомуникационни системи; компютри и компютърни мрежи; дигитализирана информация и приложения; обработка на данни и комуникация и взаимодействията на информационната инфраструктура, телекомуникационните системи, компютрите, компютърните мрежи, дигитализираната информация, приложенията, обработката на данните и комуникацията с физическия свят [23]. Самото киберпространство се оказва уязвимо за злоупотреба [24]. Киберпространството е свръхпроводимо и неизследвано бойно поле, където вероятността от враждебна атака е почти неопределима. Евентуалните поражения от нея трябва да бъдат предвиждани по две основни линии: първата – в разрушаването и разстройването на хардуерните и софтуерните способности; втората – в прокарването на манипулативни идеи, включително идеи, насаждащи страх, криминални нагласи и екстремистки възгледи в обществения живот [25]. Изглежда, ние виждаме, но не разбираме напълно втората линия, заплашителната „червена нишка", която може да се окаже нашият „път към ада".

В резултат от киберизмами и киберпиратство икономиките на Г-20 губят годишно 2,5 млн. работни места, а правителствата и потребителите – 125 млн. USD (близо 97 млн. EUR), вкл. загуби от данъчни приходи. Приведената статистика е ярко доказателство за „киберсинтеза" между лична и глобална сигурност, разбира се, без да бъдат изключени от този процес останалите равнища на сигурността.

---

[19] The Social Media Data Stacks. Cambridge: HubSpot, 2011, PPT to PDF, p. 3, www.hubspot.com, 12.06.2012.

[20] Klimburg, A. (ed.). National…, p. 3.

[21] Serrano, Alfonso. The Social Media Explosion: By the Numbers. New York: The Fiscal Times, 12.09.2011, HTML, www.thefiscaltimes.com, 15.06.2012.

[22] Mayfield, Antony. What Is Social Media: What is Social Media? An E-Book Updated 01.08.2008. Brighton, 2008, PDF, p. 5, www.icrossing.co.uk, 12.06.2012.

[23] Вж. The National Cyber Security Strategy of the Netherlands. Copenhagen: Ministry of Security and Justice, 2011, PDF, p. 3, 12.06.2012.

[24] The National Cyber…, p. 3-4; Klimburg, A. (ed.). National…, p. 3.

[25] The National Cyber…, p. 14.

През 2011 г. Symantec отчита над 400 милиона уникални варианта на зловреден софтуер, който извлича лични, конфиденциални и частни данни. За периода 2011-2012 г. стотици компании, вкл. едни от най-големите, са пострадали от нерегламентираното извличане на техни данни – става дума за такива компании като Citigroup, e-Harmony, Epsilon, Linked-In, the Nasdaq, Sony и Yahoo; става дума за изтичане на над 175 млн. лични записа, при загуба от общо над 22 млрд. USD (над 17 млрд. EUR) за периода 2011-2012 г. [26].

Оставям на IT-специалистите уязвимостите и заплахите, свързани със софтуера и хардуера на киберпространството. Тясната софтуерна специализация и бързо развиващата се технология ще продължат да тласкат напред надпреварата в области като антивирусната защита, защитата от спам, контрола на достъпа, надеждността на личните данни и т. н. [27]. Физическото разрушаване или увреждане на хардуера носи по презумпция общи характеристики с разрушаването и увреждането на който и да било материален актив [28].

От друга страна обаче, съобщенията, посланията, образите и думите в киберсвета могат да имат светкавични вредоносни последици навсякъде и по всяко време. Това е път, по който глобалното се превръща в местно и обратно. Така киберпространството трансформира чужбина в у дома [29] и обратно. Съдържанието на част от информацията в киберпространството често представлява проблем за сигурността. Филтрирането на съдържанието – от терористичните послания до отвратителната педофилия, се сблъсква с основополагащия принцип за изграждане на киберпространството – принципа „открай-докрай". Според този принцип трафикът от информация преминава между крайните потребители и не засяга ядрото на киберсистемата. Мнозина виждат в този принцип гаранция за свободата на мисълта и нейното изразяване и това е неоспоримо. По тази причина, както и поради практическата невъзможност днес да се преформатира интернет, киберзащитата срещу неподходящо съдържание се свежда до блокиране на определени сайтове и до ограничено филтриране [30].

Понастоящем защитата срещу заплахите за киберсигурността е съсредоточена на индивидуално равнище. Там е нашата най-голяма уязвимост. Всеки от нас е самостоятелен киберпотребител, винаги индивидуално включен в Мрежата. В нея ние винаги индивидуално преследваме нечии интереси – нашите собствени интереси или интересите на другиго – на работодателите си, на държавата, на компанията или на организацията, на които принадлежим. **Винаги индивидуално**! Затова лично поемаме съответните рискове и лично трябва да познаваме техните източници: незнанието, безотговорността, съзнателното или несъзнателно себепреекспониране, достъпността до новите технологии, криминалните деяния [31]. Затова днес личната сигурност и защитата на личните данни трябва да бъде основният приори-

[26] Klimburg, A. (ed.). National…, p. 5-6.

[27] Вж. Sommer, Peter, and Ian Brown. Reducing Systemic Cybersecurity Risk. Paris: Organisation for Economic Cooperation and Development (OECD), 14 January 2011, PDF, p. 24-27, www.oecd.org, 12.06.201224-27.

[28] Вж. Sommer, P., and I. Brown. Reducing…, p. 27 etc.

[29] Omand, D. The National…, p. 3.

[30] Personal Internet Security. 5th Report of Session 2006 – 2007. Volume I. HL Paper 165–I. London: House of Lords, Science and Technology Committee, 24 July 2007 – 10 August 2007, PDF, p. 20-23, www.publications.parliament.uk, 12.06.2012: 20-23.

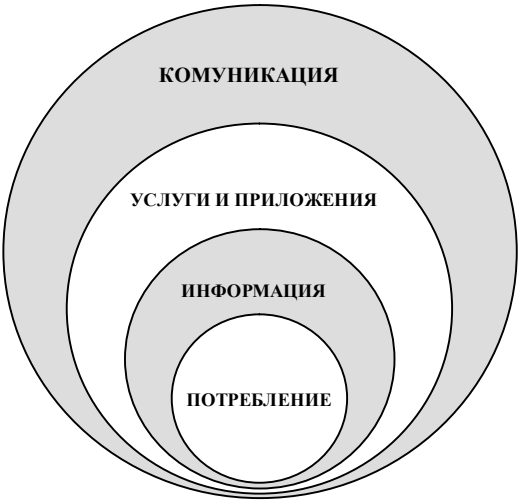
[31] Personal…, p. 61.

тет на системата за киберсигурност.

Разбира се, в съвременния свят традиционните заплахи – наличие на боеготова военна сила и шпионаж срещу нашите интереси, все още съществуват [32]. Различни транснационални фактори създават нови стратегически предизвикателства: глобална финансова и икономическа криза; съперничество за енергия и суровини, за достъп до вода и препитание; климатична промяна и пандемии [33]; кибершпионаж…

Киберсигурността може да бъде определена като свобода, неограничена от заплаха или вреда за инфраструктурата на киберпространството или за обмена и интегритета на информацията в него [34]. Киберсигурността е сигурност на киберпространството [35] и е нещо много повече от интернет сигурност. Киберсигурността засяга преди всичко хората във взаимодействията между хардуер, софтуер, информационни и комуникационни системи.

Характерна особеност, свързана с киберсигурността, е т. нар. дигитална конвергенция, която е резултат от сливането на дигитализираната комуникация, наличните услуги, приложения, информацията и потребителските устройства (фиг. 2). Обичайна грешка е третирането на комуникацията, мрежовите услуги и приложения, информацията и потребителската активност, като нещо отделно едно от друго, без тяхната дигитална, конвергентна взаимовръзка. Погрешното фрагментарно разбиране за киберсвета създава напрежения между правителствата, частните компании, обществото и гражданите при посрещане на общите киберпредизвикателства, филтрирането на съдържанието, защитата на личните данни, облагането на онлайн търговията, спазването на мрежовия неутралитет, прилагането на мрежовите протоколи и стандарти [36].



Фиг. 2. Дигитална конвергентна киберактивност

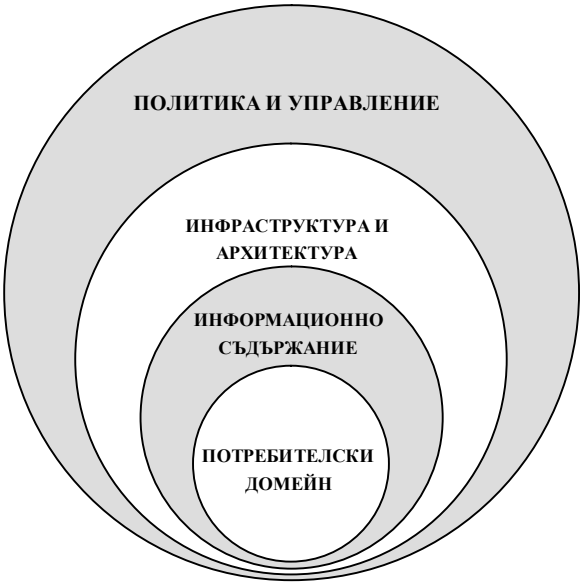
Фрагментарността може да бъде преодоляна с проекция на отделните равнища за сигурност върху кибервзаимодействията, с което да бъдат обединени частите на киберпространството. В такъв случай новополученият модел би изглеждал подобен на изходния и изпълнен с ново съдържание: комуникация, услуги и приложения, съхраняване и обработка на информация, потребление (фиг. 2).

Именно така структурира-

[32] Sustainable…, p. 1; The National Intelligence…, p. 7.
[33] The National Intelligence…, p. 8; Omand, D. The National…, p. 3.
[34] The National Cyber…, p. 4.
[35] Klimburg, A. (ed.). National…, p. 10.
[36] Sulek, D., et al. Asserting…, p. 3.

на, кибератвността позволява свързването ѝ с различните равнища на сигурност. Първо – на глобално, респ. национално и международно равнище, вкл. индустрия, търговия, интелектуална собственост, сигурност, технология, култура, политика и дипломация. Комуникацията на това равнище се осъществява наземно кабелно и безкабелно, с помощта на сателити и на системи за контрол на достъпа до данните. Второ – на оперативното равнище на услугите и приложенията, вкл. създаване, препращане, обработка и употреба на дигитална информация. Трето – на равнище съхраняване, обработка и обмен на информационно съдържание – обмен на гласови, видео и други данни, по същество обмен на електрони и фотони в кабелна и безкабелна среда. Четвърто – на равнището на потреблението с помощта на специфични устройства: от десктопи, лаптопи, смартфони и пр. до системи за наблюдение и контрол на достъпа до данни, оръжейни системи, комуникационни сателити [37]… Активността на крайния потребител прониква на всички равнища, формира съдържанието на „четвъртия домейн", с цялата условност на предложените тук идеализации.

Естествено продължение на този подход е структурирането на самото киберпространство. Според Дейвид Сулек и неговите партньори от Booz Allen Hamilton Inc., една от компаниите със силно влияние в информационния и комуникационния сектор, собственост на световноизвестната The Carlyle Group, киберпространството обхваща политиката и управлението, техниката и архитектурата, инфраструктурата и операциите, сигурността, проучването и развитието в киберпространството, което е много повече от технология, функционираща в някаква физическа инфраструктура [38]. Неговият модел, по аналогия от досега предложените, може да изглежда в 4-измерен вид: първо равнище, равнище на политиката и управлението на киберпространството, второ – инфраструктура и архитектура; трето – създаване, съхранение, обработка и обмен на информационно съдържание, четвърто – потребителски домейн (фиг. 3).



Фиг. 3. Равнища в киберпространството
(по идея от Booz Allen Hamilton,
по Sulek, D., et al. 2011: 6)

Ако се вгледаме внимателно в досега предложените модели, можем да установим, че ползваният единен подход в изграждането им спомага едновременно за обогатяване и уточняване на разнообразното им

[37] Sulek, D., et al. Asserting…, p. 1.
[38] Sulek, D., et al. Asserting…, p. 1-7.

съдържание. Обособените равнища подсказват съответствия, припокривания, разграничения и синтез на съдържанието между: първо, глобална сигурност, комуникация, политика и управление в киберпространството; второ, национална сигурност, кибертехнология на специализираните услуги и приложения, инфраструктура и архитектура на физическите компоненти на кибердомейна; трето, социетална сигурност, информационна обработка и информационно съдържание; четвърто, лична сигурност, потребителска активност и потребителски домейн. Допълнително към това разпределение, с цялата условност на предложената интерпретация, следва да отнесем съдържанието на понятия като киберсигурност (сигурност на киберпространството като цяло) и понятията за видовете киберсигурност: сигурност на информационните и комуникационните технологии, сигурност на приложенията, сигурност на комуникационните и информационните системи, сигурност на информационната инфраструктура, мрежова сигурност, интернет сигурност, компютърна сигурност, информационна сигурност, национална киберсигурност, сигурност на личните данни, киберконфликт, кибершпионаж, кибервойна, киберотбрана, кибероперации, киберпрестъпление и пр. [39] (табл. 1).

Таблица 1. Съотнасяне между равнищата на сигурност и на киберативност, структурата на киберпространството, киберсигурността и видовете киберсигурност

№	Равнища на сигурност	Конвергентна киберативност	Структура на киберпространството	Киберсигурност. Видове киберсигурност
1.	Глобална сигурност	Комуникация	Политика и управление	Сигурност на информационните и комуникационните технологии, сигурност на приложенията
2.	Национална сигурност	Услуги и приложения	Инфраструктура и архитектура	Сигурност на комуникационните и информационните системи, сигурност на информационната инфраструктура, мрежова сигурност, интернет сигурност, национална киберсигурност, киберконфликт, кибервойна, киберотбрана, кибероперации
3.	Социетална сигурност	Информационна обработка	Информационно съдържание	Информационна сигурност, кибершпионаж
4.	Лична сигурност	Потребление	Потребителски домейн	Компютърна сигурност, сигурност на личните данни, киберпрестъпление

[39] За определенията и разграниченията между понятията виж Klimburg, A. (ed.). National…, p. 8-16 etc.

Разбира се, както между отделните равнища, така и между отделните аспекти (сигурност, активност, слоеве/домейни) не съществуват резки и непреодолими граници. Дигиталната конвергенция допринася за тяхното неразделно сливане. Направените разграничения могат да бъдат полезни само за формулирането на модел за изграждане на система за киберсигурност. Онова, което остава, е поднесеното дотук съдържание да бъде съотнесено и включено в търсената система по такъв начин, че да обхваща всички сфери на обществения живот.

Киберосигуряване: критична инфраструктура, киберспособности, стратегии, организация

В развитите държави (например от Г-20) информационните и телекомуникационните системи и мрежи обхващат множество области на човешката дейност: земеделието и производството на храни; комуналното обслужване (водоснабдяване, електроснабдяване, газоснабдяване, сметосъбиране); масовия транспорт, административните, пощенските и телекомуникационните услуги за населението; здравеопазването и социалното осигуряване; критичната инфраструктура в областта на електропроизводството и електроразпределението, ядрената енергетика, добивната промишленост (добив на енергоресурси и полезни изкопаеми), преноса на петрол и природен газ (петроло- и газопроводите), химическата промишленост, преработката на индустриалните отпадъци и опазването на околната среда, банковото дело и финансите; системите за охрана и сигурност; държавното управление (електронно правителство, външна и вътрешна политика, отбрана, защитени комуникации…) и пр. [[40]].

Ползваният подход (фиг. 1-3) може бъде приложен за „форматиране" и на човешката дейност и нейната инфраструктура. Основен критерий за това е използването на автоматизирани информационни и комуникационни системи и мрежи за тяхното управление и контрол. Така могат да бъдат обособени следните нива на киберосигуряване: първо – добив на суровини и енергия (добивна промишленост и енергопроизводство), индустрия, земеделие и хранителна промишленост, опазване на околната среда, банково дело и финанси, стратегическо управление; второ – пренос на енергия и енергоносители, транспорт и съобщения, телекомуникации и прозрачно управление (електронно правителство, онлайн административни услуги и пр.); трето – комунално обслужване, здравно и социално осигуряване, образование и масова комуникация (медии); четвърто – крайно потребление (фиг. 4). Полученият модел без усилия дообогатява разбирането за отделните равнища и аспекти на киберпространството и позволява по-нататъшно структуриране на системата за киберсигурност.

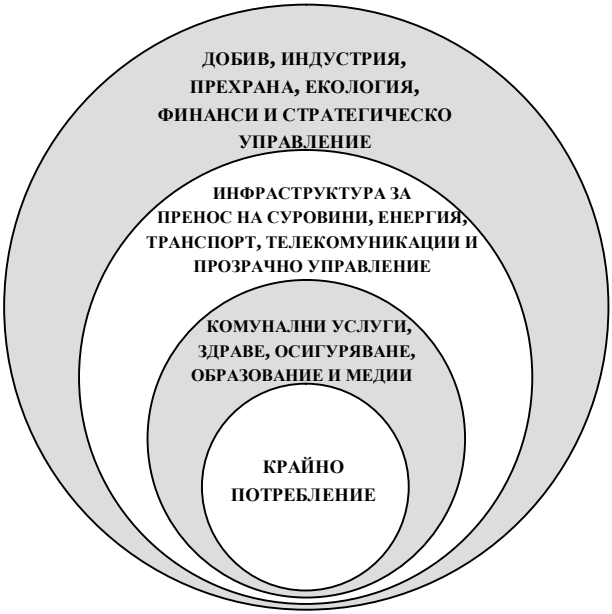
В контекста на извършения анализ прави впечатление почти безусловно налагащата се на преден план връзка лична сигурност – потребление[2] – потребителски домейн. Тя откроява приоритетното значение на защитата на личната сигурност и данни, която следва да бъде организирана при спазване на някои основни принципи:

1. Предоставянето, обработката, съхранението, ползването и заличаването на

[40] Critical Infrastructure Threats and Terrorism. DCSINT Handbook No. 1.02. Fort Eustis, Virginia: US Army Training and Doctrine Command (TRADOC), 10 August 2006, PDF, p. 17-27, www.fas.org, 15.05.2013; IT Security Architecture. Washington, US Department of Energy, February 2007, PDF, 53 p., http://energy.gov, 15.05.2013; etc.

данните трябва да бъде законно, в ограничени срокове, за конкретно определени цели, в защитена среда, само в точно определен необходим обем, при спазване на човешките права и свободи.

2. Данните трябва да бъдат сигурни, точни, достатъчни и относими към поставените изисквания за работа с тях [41].



Фиг. 4. Киберосигуряване на критичната инфраструктура и човешката дейност

Моделът за изграждане на система за киберсигурност трябва бъде изграден въз основа на тези принципи, с което да гарантира опазването на личната свобода и ефективната защита на личните данни. Освен това трябва да позволява решаването и създаването на механизми за решаване на някои постоянно възникващи дилеми. Една от тях е дилемата между национална сигурност и икономическо развитие. Тя изразява противоречието между необходимостта от икономически стимули, иновации, чуждестранни инвестиции и пр. и необходимостта от сигурност. Противоречията – между модернизиране и устойчивост на критичната инфраструктура, правителство и общество, частен и публичен сектор, военни и цивилни, служби за сигурност и служби за обществен ред, свобода на мнението и политическа стабилност, потребности и ресурси за защита на киберсигурността, защита на данните и споделяне на информацията – създават свои собствени дилеми, които много често притежават парадоксален характер: те са едновременно изкуствено формирани,

[41] Compliance Guide: Data Protection. A Practical Guide to Meeting Your Regulatory and Best Practice Obligations. Nottingham: Ex-perian, 2011, PDF, p. 4-27, www.experian.co.uk, 15.05.2013.

съзнавани като непреодолими, и реално съществуващи, но преодолими пречки в развитието [42].

Системата трябва да може да избягва или поправя обичайните грешки в политиката за киберсигурност. Международната компания KPMG предлага следната систематизация на тези грешки:

1. Виждането, че киберсигурността зависи от наблюдението. Истината е, че зависи в много по-голяма степен от способността да се извличат поуки от допуснатите слабости.

2. Виждането, че най-скъпите решения и средства гарантират сигурността в най-висока степен. На технологично равнище това може да се приеме с известна условност. Намесата на човека като най-уязвим за сигурността фактор радикално обезсмисля такова виждане.

3. Стремежът към постигане на 100% сигурност. Стопроцентната сигурност е невъзможна не само в сложния киберсвят, но и във всекидневния човешки живот.

4. Стремежът собствените кибероръжия да бъдат по-добри от кибероръжията на съперника. Реалността е, че сигурността трябва да се гарантира повече въз основа на собствените цели, отколкото според нечие застрашаващо ни поведение.

5. Стремежът да бъдат наети най-добрите специалисти. Реалността противопоставя на тази абсолютизация факта, че киберсигурността произтича от дисциплината в човешкото поведение, а не от подготвеността на даден експерт [43].

Ефективността на системата за киберсигурност зависи също от способностите ѝ за: адекватен анализ, своевременно разкриване и неутрализиране на киберрисковете и ефективно отразяване на киберзаплахите; елиминиране на сривовете в киберсистемите и опасните кибератори; умело съчетаване на реактивен и проактивен подход в прилаганите стратегии за киберсигурност.

Изпълнението на тези изисквания следва да бъде нормативно зададено в „носещата конструкция" на киберсистемата. Опорните ѝ точки могат да бъдат обединени в няколко групи: първо, разработване и приемане на необходимите правни норми (законодателни и подзаконови актове) и стратегически документи (концепция, стратегия, доктрина, план за действие); второ, разработване и прилагане на необходимите технически стандарти и процедури за гарантиране на киберсигурността; трето, формиране на организационната структура – система от органи за киберзащита и сигурност; четвърто, изграждане, натрупване и развитие на необходимия експертен опит в областта на киберсигурността; пето, интензивно сътрудничество като мултипликатор на способностите и ресурсите в различни сфери от обществения живот: на вътрешнонационално, национално и международно равнище, между правителството и гражданското общество, в публичния и частния сектор и помежду им, с привличане и обмен на идеи и знания между експерти и учени и пр.; шесто, определяне на приоритетите и актуалните стратегически цели в кибердомейна [44] (фиг. 5).

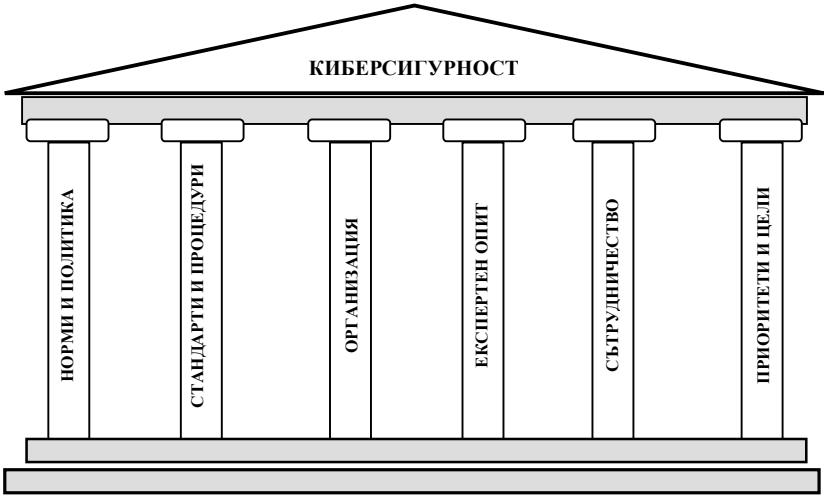
Системата за киберсигурност трябва да може да изпълнява едновременно няколко основни функции (вж. фиг. 7):

---

[42] Вж. Klimburg, A. (ed.). National…, p. 34-42, 86-94.

[43] Hermans, John, and Gerben Schreurs. The Five Most Common Cyber Security Mistakes. KPMG Advisory N.V. London, 2013, PDF, p. p. 8-10, www.kpmg.com, 15.05.2013.

[44] Wamala, Frederick. The ITU National Cybersecurity Strategy Guide. Geneva, September 2011, PDF, p. 20-21, 48-93, www.itu.int, 14.06.2012.



Фиг. 5. Изграждане на киберспособности

1. **Изпреварваща оценка и елиминиране** на вероятността от възникване и реализиране на несигурност. Става дума за проактивен подход в оценката и въздействието върху средата за киберсигурност, за насърчаване на благоприятното развитие на киберпространството.
2. **Превенция** на киберзаплахите.
3. **Подготовка** за отговор срещу потенциална или съществуваща несигурност.
4. **Разкриване** на предизвикателствата, опасностите, заплахите и рисковете в киберпространството.
5. **Защита** на киберсигурността при наличие на несигурност или на неблагоприятни киберактори.
6. **Възстановяване** при наличие на отрицателни последици от възникнала несигурност или от въздействия на неблагоприятни актори в киберпространството.
7. **Преоценка и актуализиране** на киберспособностите в съответствие с динамиката на киберпространството [45].

Системата за киберсигурност следва да прилага проактивен подход. Полето й на действие може да бъде структурирано в няколко приоритетни направления и обособени линии в тях. Разнообразието и сложността на киберпредизвикателствата по отделните направления и линии изискват тяхното обособяване като сфери на отговорност на различни институции (вж. фиг. 7). Те могат да изглеждат така:

1. **Защита на националния суверенитет** в киберпространството, по линиите киберразузнаване, киберконтраразузнаване и киберотбрана.
2. **Защита на критичната информационна инфраструктура**, с обособяване на специфична линия за управление при кризи. Усилията в това направление допринасят за изграждане на жизнеспособни общества и постигане на устойчиво развитие, икономически и културен напредък.

[45] Вж. Klimburg, A. (ed.). National…, p. 78-80, 113-114.

3. **Борба с киберпрестъпленията**.

4. **Киберуправление и кибердипломация**, с обособяване на специфична линия за интернет управление и интернет дипломация [46] (разбира се, не може да бъде отмината и нишата, в която се развиват т. нар. социални медии).

Важна способност на системата за киберсигурност е способността да разграничава отделните видове киберактори: самостоятелни киберактори (хакери, хактивисти и пр.), киберпрестъпници, кибертерористи и киберактори на национални разузнавателни, контраразузнавателни и военни структури [47].

Системата за киберсигурност следва да бъде ориентирана към бързо изработване и прилагане на адекватни стратегии в отговор на всяка несигурност. Според Франк Грегъри най-общо могат да бъдат разграничени четири типа стратегии или по-скоро четири аспекта на изработване и реализиране на дадена стратегия срещу несигурността – превенция, противодействие, готовност и възпиране [48]. Сходен подход в областта на киберсигурността предлагат Алекзандър Климбърг и Джейсън Хийли:

1. Стратегия на сдържане в две посоки: поразяване на източника на киберзаплаха или/и неутрализиране на самата кибератака. И в двата случая смисълът е недопускане на загуби в собствения кибердомейн.

2. Стратегия на изграждане и поддържане на жизнеспособността на собствената система за киберсигурност чрез противодействие също в две посоки: неприемливо за източника на киберзаплаха увеличаване на цената на предприетите от него вредоносни действия или/и недопускане на извличането на полза от източника на киберзаплаха [49].

Анализът показва, че посочените стратегии са формирани в координатната система от една страна между два противостоящи си актора, а от друга – между придобиването и отнемането на ресурс. Следователно гъвкавият стратегически подход изисква способност на системата за киберсигурност за разработване, поддържане и промяна на стратегията спрямо акторите и ресурсите: за целенасочено придобиване и отнемане на ресурс за самата система и за противостоящия й киберактор (фиг. 6).

На стратегическо равнище е необходимо създаването на централизиран орган за киберсигурност (подобна функция изпълнява националният орган по сигурността в Унгария, например). Централният орган по киберсигурност следва да координира усилията в национален и международен мащаб [50]. На тактическо равнище се препоръчва създаването на орган за управление при киберкризи/за компютърна сигурност, т. нар. CERT или CSIRT [51], какъвто формат вече съществува в България. На оперативно – междуинституционален център (или центрове) за киберана-

---

[46] Срв. Klimburg, A. (ed.). National…, p. 31-34.

[47] Bruce, Robert, et al. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. TNO Report 33680. Dartmouth, The Netherlands: Tuck School of Business, Center for Digital Strategies, 30 June 2005, PDF, p. 13-14, www.ists.dartmouth.edu, 14.06.2012; 31; Hermans, J., and G. Schreurs. The Five…, p. 5.

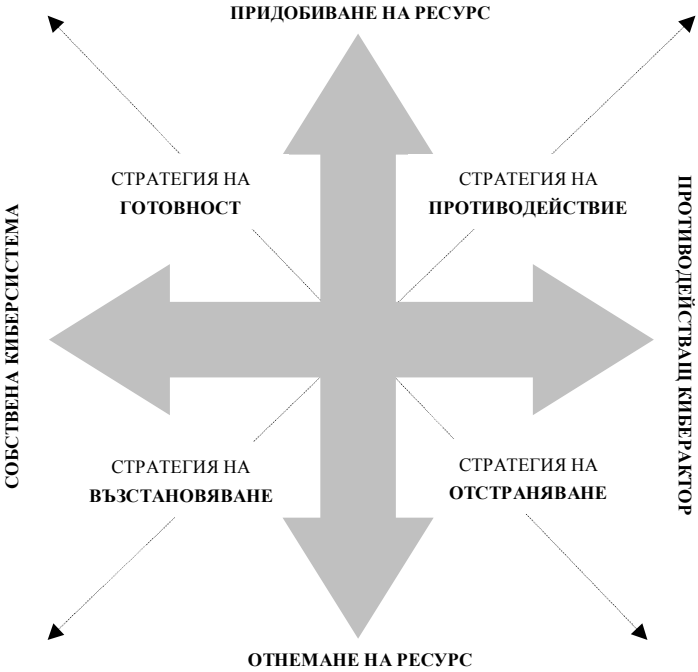
[48] Gregory, Frank. Intelligence-led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005. Madrid, 2005, p. 1-2. PDF, www.realinstitutoelcano.org, 07.06.2006.

[49] Klimburg, A. (ed.). National…, p. 84-86.

[50] Вж. напр. Wamala, Frederick. The ITU…, p. 83-84.

[51] Bruce, Robert, et al. International…, p. 55-56, 112-113.

лиз и обмен на информация [52]. С оглед развитието на информационното общество и образование, както и с оглед нарастващата сложност на информационните и комуникационните технологии, вероятно следва да се помисли за отделен киберцентър за изследвания и образование [53]. Разбира се, не бива да бъдат оставени настрана отделните направления и линии в областта на киберсигурността. Последното означава създаване или вменяване на правомощия на отделни органи по киберразузнаване, киберконтраразузнаване, киберотбрана, борба с киберпрестъпленията. Тези институции е необходимо да бъдат поставени в подходяща институционална рамка, което означава да работят по ясни правила за взаимодействие помежду си (с разпределени отговорности), за връзка и изграждане на доверие с гражданското общество, за гарантиране на свободата в интернет, за осигуряване на сътрудничество с частния сектор (предприятия и търговски дружества от критичната инфраструктура, провайдъри, високотехнологични фирми) и пр. (вж. фиг. 7).



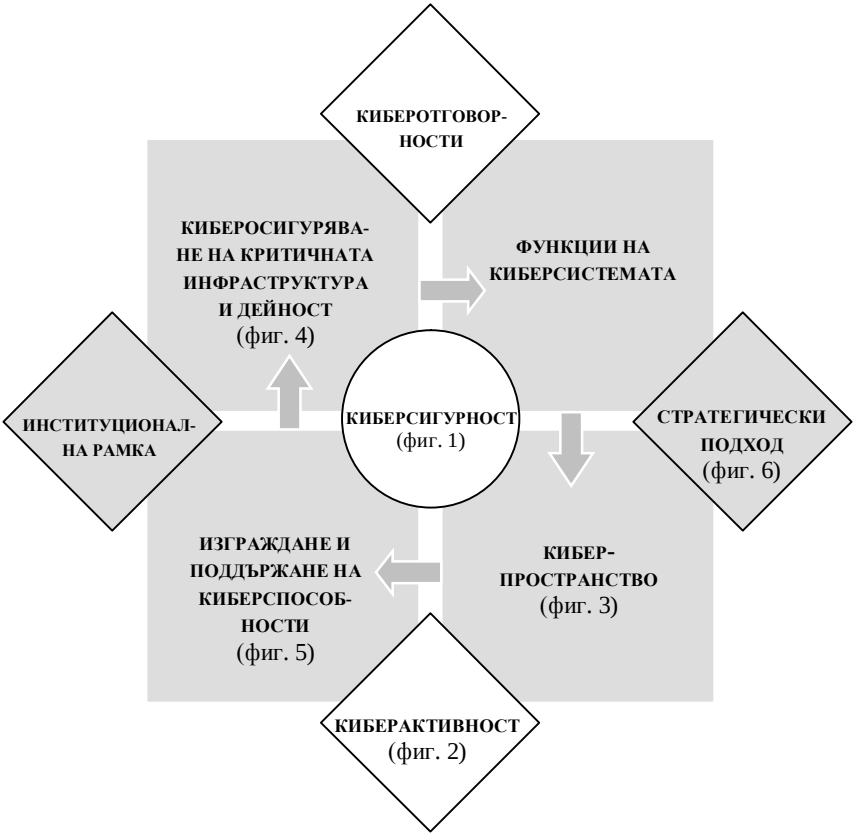
Фиг. 6. Стратегически подход

[52] Bruce, Robert, et al. International…, p. 18, 46, 56-57.
[53] Bruce, Robert, et al. International…, p. 150-151.

Заключение

Определянето на равнищата на киберсигурността, киберпространството и киберосигуряването, на изискванията спрямо киберспособностите, на функциите, направленията и линиите на отговорност, на необходимия стратегически подход и организационно изграждане, позволява формирането на всеобхватен модел за изграждане (и поддържане) на система за киберсигурност (фиг. 7).

Моделът, представен тук, е конструиран по подобие на т. нар. НОРД-цикъл. „Началното" му звено е изграждането (впоследствие и подържането) на киберспособностите (вж. и фиг. 5). На второ основно място идва киберосигуряването (вж. и фиг. 4). Киберспособностите за киберосигуряване са поставени в условията на точно установена институционална рамка по отделни направления и линии на отговорност. Третото основно звено е функционирането на системата, която упражнява съответното въздействие върху киберпространството, като следва актуал-



Фиг. 7. Модел за изграждане и поддържане на система за киберсигурност

но възприет стратегически подход (вж. и фиг. 6). Четвъртото основно звено в модела е самото киберпространство (вж. и фиг. 3), чиято динамика изначално и непрекъснато влияе върху собствените киберспособности. Отделните аспекти на това влияние се сливат в резултат от дигиталната конвергенция в киберсвета (вж. и фиг. 2). Разбира се, поредицата от взаимодействия не е еднопосочна, въздействията в предложения модел протичат и в обратен ред, на всички нива, във всички аспекти и измерения. Крайният резултат от така представеното комплексно взаимодействие е постигането или непостигането на сигурност (вж. и фиг. 1).

Моделът е формиран въз основа на разбирането, че системата за киберсигурност следва да постигне ефективността, необходима на всяка система за сигурност въобще. А това е възможно единствено ако в изграждането й бъдат заложени принципите, методите, техниките и организацията на разузнавателно-аналитичния процес. KPMG предлага подобен актуален модел, валиден за вече изградена система за киберсигурност, водена от разузнавателния анализ [54]. Предложеният модел (фиг. 7) е с по-богато съдържание от концепцията на KPMG. Моделът приема заложената в нея идея, която способства той да придобие всеобхватен и завършен вид, без да бъдат отричани възможностите за неговото модифициране, усъвършенстване и дори заместване с друг подобен модел.

Използвана литература на кирилица

1. Желязков, Иван, и Тодор Трифонов. Енергийната сигурност на България. София, 2012, 198 с.
2. Мичев, Стефан. Илюзията за сигурност. София, 2012, 136 с.
3. Слатински, Николай. Измерения на сигурността, София, 2000, 184 с.
4. Уайт, Лесли. Науката за културата. Изследване на човека и цивилизацията. София, 1988, 310 с.

Използвана литература на латиница

5. Bruce, Robert, et al. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. TNO Report 33680. Dartmouth, The Netherlands: Tuck School of Business, Center for Digital Strategies, 30 June 2005, PDF, 209 p., www.ists.dartmouth.edu, 14.06.2012.
6. Choucri, Nazli. Migration and Security: Key Linkages – In: Journal of International Affairs. New York, Fall 2002, vol. 56, № 1, p. 97-122.
7. Compliance Guide: Data Protection. A Practical Guide to Meeting Your Regulatory and Best Practice Obligations. Nottingham: Experian, 2011, PDF, 32 p., www.experian.co.uk, 15.05.2013.
8. Critical Infrastructure Threats and Terrorism. DCSINT Handbook No. 1.02. Fort Eustis, Virginia: US Army Training and Doctrine Command (TRADOC), 10 August 2006, PDF, 80 p., www.fas.org, 15.05.2013.
9. Demchak, Chris. Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered

[54] Marshall, Malcolm, et al. Cyber Threat Intelligence and the Lessons from Law Enforcement. London, KPMG International Cooperative, 2013, PDF, p. 3-4, www.kpmg.com, 15.05.2013.

World. Issue Brief. Washington, Atlantic Council, 12.08.2010, PDF, 8 p., www.acus.org, 15.05.2013.
10. Drew, Dennis, and Donald Snow. Making Twenty-First-Century Strategy: An Introduction to Modern National Security Processes and Problems. Air University Press, Maxwell Air Force Base, Alabama, 2006, 289 p.
11. Gregory, Frank. Intelligence-led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005. Madrid, 2005, 5 p., PDF, www.realinstitutoelcano.org, 07.06.2006.
12. Hermans, John, and Gerben Schreurs. The Five Most Common Cyber Security Mistakes. KPMG Advisory N.V. London, 2013, PDF, 16 p., www.kpmg.com, 15.05.2013.
13. IT Security Architecture. Washington, US Department of Energy, February 2007, PDF, 53 p., http://energy.gov, 15.05.2013.
14. Kicinger, Anna. International Migration as a Non-Traditional Security Threat and the EU Responses to This Phenomenon. Warsaw, 2004, 13 p.
15. Kirshner, Jonathan (ed.). Globalization and National Security. New York, Google Books, 2006, 613 p., http://books.google.bg, 19.04.2010.
16. Klimburg, Alexander (ed.). National Cyber Security Framework Manual. NATO CCD COE Publication. Tallinn, 2012, PDF, 253 p., www.ccdcoe.org, 20.05.2013.
17. Kugler, Richard, et al. Globalization and National Security. Vol. I-V. Washington, 2001, PDF, http://permanent.access.gpo.gov, 25.04.2010.
18. Marshall, Malcolm, et al. Cyber Threat Intelligence and the Lessons from Law Enforcement. London, KPMG International Cooperative, 2013, PDF, 12 p., www.kpmg.com, 15.05.2013.
19. Mayfield, Antony. What Is Social Media: What is Social Media? An E-Book Updated 01.08.2008. Brighton, 2008, PDF, 36 p., www.icrossing.co.uk, 12.06.2012.
20. Moshchelkov, Evgeny. International and National Security in the World Community in the Twenty-First Century: Outlines of New Realities. Garmisch-Partenkirchen, 2003, PDF, 3 p., www.marshallcenter.org, 07.06.2006.
21. Ó Tuathail, Gearóid, and Simon Dalby (eds.). Rethinking Geopolitics. London – New York, Routledge, 1998, PDF, 346 p., http://frenndw.files.wordpress.com, 13.04.2013.
22. Omand, David. The National Security Strategy: Implications for the UK Intelligence Community. A Discussion Paper for the ippr Commission on National Security for the 21st Century. Institute for Public Policy Research, February 2009, PDF, 17 p., http://dematerialisedid.com, 12.06.2012.
23. Perl, Raphael. Terrorism and National Security: Issues and Trends. Washington: CRS, 2006, PDF, 19 p., http://fpc.state.gov, 20.04.2010.
24. Personal Internet Security. 5th Report of Session 2006 – 2007. Volume I. HL Paper 165–I. London: House of Lords, Science and Technology Committee, 24 July 2007 – 10 August 2007, PDF, 121 p., www.publications.parliament.uk, 12.06.2012.
25. Quille, Gerrard, et al. An Action Plan for European Defense: Implementing the Security Strategy. Brussels – Rome, 2005, PDF, 73 p., 12.06.2012.

26. Sachs, Stephen. The Changing Definition of Security. Oxford, 2003, HTML, www.stevesachs.com, 22.12.2009.
27. Serrano, Alfonso. The Social Media Explosion: By the Numbers. New York: The Fiscal Times, 12.09.2011, HTML, www.thefiscaltimes.com, 15.06.2012.
28. Sommer, Peter, and Ian Brown. Reducing Systemic Cybersecurity Risk. Paris: Organisation for Economic Co-operation and Development (OECD), 14 January 2011, PDF, 119 p., www.oecd.org, 12.06.2012.
29. Sulek, David, et al. Asserting Global Leadership in the Cyber Domain. Ready for What's Next. 2011 Update. Booz Allen Hamilton Inc., 16.08.2011, PDF, 24 p., www.boozallen.com, 15.05.2013.
30. Sustainable Security. Washington, Center for American Progress, 2009, PDF, 4 p., www.americanprogress.org, 14.06.2012.
31. The National Cyber Security Strategy of the Netherlands. Copenhagen: Ministry of Security and Justice, 2011, PDF, 16 p., 12.06.2012.
32. The National Intelligence Strategy of the United States of America. Washington, August 2009, PDF, 24 p., www.fas.org, 12.06.2012.
33. The Social Media Data Stacks. Cambridge: HubSpot, 2011, PPT to PDF, 54 p., www.hubspot.com, 12.06.2012.
34. Wamala, Frederick. The ITU National Cybersecurity Strategy Guide. Geneva, September 2011, PDF, 119 p., www.itu.int, 14.06.2012.

ДЪРЖАВА И СИГУРНОСТ

СОЦИАЛНАТА ЕКОЛОГИЯ И ПРОБЛЕМИТЕ НА СИГУРНОСТТА

Маргарита Бонева

Шуменски университет „Еп. Константин Преславски”
Педагогически факултет

SOCIAL ECOLOGY AND PROBLEMS OF SECURITY

Margarita Boneva

ABSTRACT*: It the study present the problems of security in the context of social ecology*

KEY WORDS*: social ecology, security*

Предмет на социалната екология са принципите, отношенията, закономерностите, методите на оптимизация и хармонизация, законите за формиране и функциониране на ноосферата.

Социалната екология изучава отношението на човека и обществото към природата в съответствие с природните и социални закони във вид на социално-икономически, морални, естетически и правови норми. Взаимодействието на човека и околната среда включва отношението между природните и обществени фактори, промените в околната среда в границите на жизнената дейност на човека. Тя дава знания, които позволяват човек да защитава и подобрява както естествената, така и обществената среда, създавайки комфортна, изкуствено обитавана среда, отговаряща на биологични, социални, медицински, естетически и други изисквания, чрез преодоляване на ограниченията на зоологическия егоизъм, пазарния индивидуализъм, пораждащ хаос в системата «човек-околна среда».

Безусловно най-важният обект на социалната екология е човекът, обществото като цяло или отделни социални групи.

Днешното общество толерира създаването на нови технологии и целенасочено руши природата. Хората стремително изменят света около себе си и изчерпват ресурсите му, за да придобиват все повече и повече материални блага, в резултат на което се създават условия за глобална екологична криза.

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

Глобализацията създаде допълнителен натиск върху природните ресурси и околната среда. Крупномащабното обезлесяване и емисиите газове, предизвикващи

парниковия ефект, са важни фактори, които влияят върху измененията на глобалния климат.

Свързани тясно с глобализацията *цели,* по отношение на които е особено необходимо да се разширяват усилията на международно равнище са:

- образование, умения и технологични възможности;
- въпроси на сигурността и приспособяването;
- осигуряване на достоен труд.

Урбанизацията **през XX в. е** ***глобален процес,*** **в който все повече участва Третият свят, в които броят на градските жители ежегодно нараства с количество, равно на населението на Испания.**

Градът **е концентриран израз на противоречия, конфликти и проблеми,** ***свързани с бедност, етническо разделение, противопоставяне между бели и чернокожи, престъпност, несигурност.***

Световният демографски растеж, **особено в Третия свят заплашва да се превърне в** ***глобална катастрофа. В настоящия момент, глобалните ресурси в света не са достатъчни, за да осигурят в Третия свят жизнен стандарт, сравним с този в индустриалните страни.***

Днес над 95% от населението в света не разбира последствията от тоталната екокатастрофа за себе си и за поколенията и не се замисля за пътищата за излизане от кризата, която включва:

- ***световно изчерпване на всички ресурси на планетата;***
- ***прогресираща загуба на устойчивост на екосистемите на планетата вследствие на тяхното разрушение.***

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

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

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

Тези проблеми са обект на социалната екология и имат отношение към сигурността.

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. Редица от самостоятелно дефинираните социални или природни глобални проблеми имат индиректно отно-

шение към съвременните тенденции, явяващи се причина, ресурс или следствие от мащабността им, интензитета на проявление, степента на обратимост. Това са запазването на мира, отношенията между бедни и богати, недохранването на голяма част от населението, епидемиите, природните бедствия и катастрофи, повишаването на нивото на световния океан, ерозията на почвите, настъплението на пустините, обезлесяването и др.

Всъщност настъплението на пустините е резултат най-вече на климатичните промени на Земята, които от своя страна днес са предизвикани основно от нарастващите мащаби на земеделската, промишлената, транспортната и прочие *антропогенна дейност*. От своя страна *гладът* е демографски и икономически детерминирано явление и до голяма степен зависи от отношенията между богатите и бедните обществени слоеве и държави.

Ежегодно само при изгарянето на органични горива във въздуха се изхвърлят около 6 млд. тона въглерод, от които природата е в състояние да абсорбира само половината. Изключително агресивна форма на поразяване на глобалните и регионалните екосистеми е използването на токсични средства в земеделието. При химизацията на земеделието се наблюдава замърсяване на водите, почвите и водите, висока степен на токсикация на хранителните вериги при дивите и домашните животни, което директно рефлектира върху условията на живот и хранене при човека.

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

Бързи количествени и качествени промени се наблюдават при почвените и биологичните ресурси на планетата. Екстензивните от *екологична гледна точка* темпове и мащаби на механична и химична обработка на почвите, прекомерната паша, обезлесяването водят до *почвена ерозия*. Естествената растителност играе важна роля в поддържането на въглеродния баланс, регулиране на климата, водния кръговрат, биологичното равновесие. Най-важен индикатор за състоянието на естествената растителност са горите. Европа обаче е изгубила 2/3 от горите. Тропическите гори са намалели с около 20 % в сравнение с 1960 г. Годишно в резултат на пожари и изсичания се губят 16 млн. хектара гори.

Биологичните ресурси на планетата са най-уязвимият природен компонент и поради това са *най-важният индикатор за състоянието на екосистемите в глобален мащаб*. Годишно изчезват до 1000 вида. Най-голямо поражение върху видовото разнообразие се наблюдава при рибите – вече 33% от тяхното видово разнообразие е застрашено от изчезване. При бозайниците делът на застрашенити видове е 25%, а при птиците – 10%.

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

Основна цел на САЩ е контролът над стратегическите суровини – уран, нефт, газ и др., а техен глобален стратегически интерес – безпрепятственото снабдяване с тези суровини.

Мощният транснационален капитал "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.

Човекът, който е обект и субект на социалната екология, определя геохимичния облик на биосферата

На територията на Европейския съюз съществуват много субкултури и етнически малцинства, което прави проблемите на приобщаването много трудни. Политиката на Европейския съюз е изградена именно върху фундамента на зачитането на *културната идентичност* и *междуетническа толерантност*, гарантиращ сигурност в глобален мащаб.

Тероризмът, заплахата от ядрена война, глобалното затопляне, оскъдността на водните ресурси, нарушеното екологично равновесие са все глобални заплахи и рискове, с които националните правителства не могат да се справят сами.

Екологичните ценности в ерата на глобализацията са предизвикателство пред съвременното общество.

В продължение на хилядолетия човек постоянно увеличава своите технически възможности, засилва намесата в природата, забравяйки за необходимостта от поддържане на биологичното равновесие в нея.

Основната причина за *екологичната криза* е *глобалното изчерпване на природните ресурси*, съчетано със *замърсяването на жизнената среда*.

Много социални еколози разглеждат *екологичната криза* като неразрешим конфликт между природата и обществото, причина за който са научно–техническите постижения, ръста на населението, изтощаването на природните ресурси на планетата.

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

Новите заплахи за *националната сигурност* са гладът, бедността, демографския срив, незачитане на човешките права и правата на малцинствата, пораженията върху околната среда. С други думи социално-екологичните проблеми на глобализиращия се свят са непосредствено свързани с националната сигурност на всяка държава.

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

Рискове за *екологичната сигурност* произтичат от промишлени аварии с изпускане на вредни емисии, трансгранично замърсяване на въздуха, водите и крайбрежната ивица, както и от заплахата за терористична дейност с използване на вещества, които са особено опасни за природната среда. Защитата на корпоративни икономически интереси забавя предприемането на реални стъпки за разрешаване на тези проблеми в широк международен контекст.

Корупцията заплашва съществуването и спазването на социалните, правните и моралните норми, засилва потенциала на организираната престъпност, уронва авторитета на властите, отслабва тяхното функциониране и компрометира провеж-

даните реформи. Сред основните заплахи са *организираната престъпност* и *трансграничната престъпност*, особено *трафикът на наркотици*.

Възползвайки се от икономическата криза и разширяващите се възможности за пътуване, *организираната престъпност* се активизира в сферата на *нелегалната миграция* и *трафика на хора*, особено на жени и дори момичета, с цел сексуална експлоатация и включване в групи за улична престъпност.

Съществен конфликтен потенциал съдържат *социалната несигурност* и рязко изразената социална диференциация. Обществото чувство за социална справедливост ерозира поради случаите на неправомерно натрупване на богатство.

Развитието на ядрената енергетика има стратегическо значение за *националната ни сигурност*. Изграждането на нови мощности се подкрепя институционално предвид това, че е перспективен ресурс за производство на беземисионна електрическа енергия и поради натрупания успешен опит и професионален капацитет. При развитието й стриктно се спазват изискванията за управление на ядрените отпадъци и извеждане от експлоатация и мерките за сигурност.

Приоритет в политиката за *енергийна сигурност* е повишаване на енергийната ефективност и насърчаване на енергоспестяването. *Енергийната сигурност* на страната и *повишаването на качеството на околната среда* зависят от реализирането на политиката на Република България за увеличаване на дела в енергопроизводството на възобновяеми и алтернативни енергийни източници и заместването на електрическата енергия с природен газ.

Страната съдейства за технологичното развитие по отношение на ефективността на производството и внедряването на чисти въглищни технологии, както и за прилагането на технологични постижения, които са в съответствие с европейските изисквания и собствените икономически възможности.

Енергийната ни политика се основава на балансиран подход при комплексното използване на възобновяеми енергийни източници, ядрена енергия, природен газ, въглищни технологии и ВЕЦ за гарантиране на *енергийната сигурност* и икономическата ефективност.

Изграждането на значимите енергийни проекти изисква както *експертиза за влиянието върху националната сигурност*, така и екологична оценка и оценка за съвместимост с предмета и целите за опазване на защитените зони, за гарантиране сигурността на гражданите, обществото и държавата.

Политиката за сигурност в отношенията *човек – природа* се изразява в изпълнение на стандартите за екологична експертиза и защита и в присъединяване към глобални или регионални инициативи и екологични проекти, насочени към подобряване качеството на околната среда и защита на *екологичната сигурност*.

Сигурността на гражданина е основен критерий за ефективността на Системата за национална сигурност.

Гражданите и техните организации са потребители на *системата за национална сигурност* и същевременно участват активно според своите възможности в нейното функциониране. *Подготовката* и *запазването на човешкия ресурс* има особено голямо значение за функционирането на системата за *национална сигурност*.

Глобализацията означава изтощаване на ресурсите на Държавата за въздействие, отслабване на инструментите, с които правителството оказва контрол и влияние над събитията в собствената му страна. Светът все повече става свят на транс-

националните компании и на унификацията на мисленето, на ценностите и на целите, на критериите за успех и просперитет.

Известният руски учен академик С. Капица смята, че решението на проблемите ще бъде намерено в създаването на нови технологии, базиращи се на безотпадъчни циклични процеси, при които не се изисква голяма консумация на минерални суровини.

Още по-оптимистична е визията на члена на Римския клуб Умберто Коломбо, който е на мнение, че ще настъпи период на развитие на науката и технологиите, когато човечеството ще има способността да измисля и планира добива на суровинните източници, от които се нуждае.

Наред с тревогата за изчерпването на минералните ресурси съществува и опасението от изчерпването на енергийните източници и настъпването на т.нар. енергиен глад. Сега около 90% от добиваната енергия е за сметка на използването на нефт, газ и въглища. При запазването на сегашните темпове на изразходване прогнозите сочат, че запасите от природен газ и нефт са на изчерпване към края на XXI век, а залежите от въглища ще бъдат изконсумирани след около четири столетия. Засега единственият изход се вижда във все по-широкото използване на ядрената енергетика, защото се знае, че запасите на уран в земните недра са близо 200 пъти повече от другите изкопаеми източници на енергия. За съжаление обаче, получаването на ядрената енергия е свързано с отделяне на високорадиоактивни отпадъци, които в течен1ие на много години са източник на смъртоносно радиоактивно излъчване, а все още е трудно да се каже, че е открит надежден способ за тяхното съхранение.

От гледна точка на *сигурността* за бъдещето на планетата най-добрият начин може да бъде внедряването и усвояването на авангардни технологии и нови източници на енергия. Теоретично са възможни използването на слънчевите лъчи, водородната енергия и термоядрения синтез.

Учените в цял свят и главно работещите в Междуправителствената комисия по климатичните изменения към ООН са категорични – глобалното затопляне на Земята е вече факт.

Сериозни и главно негативни ще бъдат последиците от климатичните изменения върху здравето на хората – нарастване на нивото на смъртност и заболеваемост като пряк резултат от претоплянето на човешкия организъм, разпространението на разнообразни инфекции и епидемии. Изследванията показват, че вероятната зона на разпространението на маларията ще се увеличи и в нея ще живеят между 45 и 60% от населението на планетата, предимно в южните райони на света.

Стратегическите цели, свързани с *нооразвитието* и *опазването на околната среда* касаят водите, отпадъците, течните горива, замърсяването на почвите с нитрати, методите за обезвреждане на отпадъците, за пречистване на отпадните води, емисиите на вредни газове, екологичния мониторинг и пр.

В райони с активна селскостопанска дейност стои проблемът за отклонения по показателя *"нитрати"*. Най–разпространени са отклоненията до и около два пъти над нормата (50 мг/мл), но в някои водоизточници достига и до над 4 пъти над допустимото. Най–често замърсяването с нитрати се среща във водите на плитки подземни източници (извори, кладенци, сондажи), разположени в местности с обработваеми земеделски земи или в близост до населени места и черпещи вода от незащитени водоносни хоризонти. Проблемът има здравна значимост. Основната

причина е неправилното използване на азотни минерални торове в недалечното минало, както и неправилната земеделска и животновъдна практика като цяло. Възможностите за решаване на проблема са свързани преди всичко с изграждане на нови водоизточници или смесване на водите от проблемните водоизточници с води с добро качество, с цел разреждане на нитратите до допустимата стойност.

Проблем е *регулярното водоснабдяване* и качеството на питейните води, особено през лятото, както и недостатъчния брой пречиствателни станции, с цел снабдяване с вода, отговаряща на показателите по отношение на цвят, мирис, pH, съдържание на манган (Mn), желязо (Fe) или хром (Cr).

Канализационните мрежи са в незадоволително техническо състояние.

Проблем, който също чака решаването си е и този, свързан с *битовите отпадъци*, като се започне от нерегламентираните сметища в малките населени места и площи замърсени с битови отпадъци. Депата за строителни отпадъци позволяват в тях да се депонират 71% от тях. Това са изоставени кариери, заблатени терени, ерозирали брегови и други релефни форми.

Необходимо е предприемане на мерки за ограничаване на вноса на автомобили, които не могат да използват безоловен бензин, чрез подходяща система от мита, данъци и такси.

Намаляване на *емисиите от вредни газове*. България е една от страните с най–високи емисии на серни оксиди и прах на глава от населението.

Човекът днес е основната сила, променяща процесите в биосферата, като за целта трябва непрекъснато да се учи, защото икономическото развитие води до неспазване на законите на биосферата, нарушаване на биосферното равновесие, превишаване на възможността на природните системи да се самоочистват.

Пестицидите, изкуствените торове, промишлените отпадъци, особено радиоактивните утайки и канцерогенните въглеводороди, променят химическия състав на въздуха, водата и почвата. Постоянно нараства броят на населението на земното кълбо. Със своята стопанска дейност хората променят биосферата, създават нова среда за съществуване на всичко живо, в това число и за самите тях. Обаче ресурсите на биосферата не са безгранични.

Световен "*екологичен" пазар* или *пазар на природните ресурси* все още няма, а това в условията на глобалното въздействие на човечеството върху природата не може да се счита за нормално.

Днес положението е много сложно, и много учени твърдят, че човечеството, ако иска да запази цивилизацията, трябва да реши екологичните проблеми в най–близко време.

Човекът вече знае, какво огромно значение за живота има поддържането в биосферата на оптимален хидрологичен и газов състав на средата. Той прониква в тайните на такава функция на биосферата, каквато е биологичното очистване и най–важното, оценява своите грешки. Това позволява оптимистично да се отнася към бъдещето. С други думи " екологията става теоретична основа на поведението на човека от индустриалното общество в природата". Човекът е на прага на овладяване на методите за регулиране на числеността на популациите. Това дава възможност да се управляват редица процеси, без да се замърсява биосферата с вредни вещества. Всички тези постижения на науката имат огромно значение. Човечеството влиза в период, в който всяка негова дейност е необходимо да се измерва с възможностите на биосферата, за да се развива прогресивно и най–важното да се

научи да управлява много процеси, протичащи в нея, нейната еволюция, нейните преходи в *ноосферата.*

Обект на социалната екологоия за социално-екологичните проблеми на обществото.

Развитието на екологичната сигурност е свързано с глобализацията на екологичните проблеми, които са резултат от новите взаимоотношения в системата "природа – човек - общество".

Екологичната сигурност е определящ фактор за устойчивото развитие. От гледна точка на *екологичната сигурност* основните проблеми са свързани с:

- наличието на силно замърсяващи производства у нас;
- липсата на инвестиции за изграждане на пречиствателни съоръжения и инсталации за преработване на отделяните във въздуха и водите вредни емисии;
- несъвършенства и пропуски в нормативната база;
- неефективен контрол и взаимодействие между правоприлагащите институции.

Социално-екологичната сигурност е съвкупност от състояния на природните, антропогенните и социално-икономическите системи и на процесите на взаимодействие между тях, при които не възникват критични ситуации, дължащи се на появяване и развитие на екологично - опасни явления, действия и ефекти. *Социално-екологичната сигурност* е свързана с възможност за възникване на опасност и вреди, свързани с живота, здравето, смъртността, с увеличаване на диференциацията в доходите на населението, с престъпността и екстремизма.

Социално-екологичната сигурност е защита на природата, жизнените интереси на човека, обществото и държавата от вътрешни и външни въздействия, които пречат на процесите и тенденциите за съхраняване и подобряване на човешкото здраве, биологичното разнообразие, устойчивостта на екосистемите и опазване на човечеството. Тя обхваща всички политически, икономически, социални и екологични елементи, които са свързани с климатични промени, биологично разнообразие, устойчивост на екосистемите, опазване на човека.

Климатът на земната повърхност се затопля в резултат на т. нар. усилен *парников ефект*, породен от нарастващата концентрация на емисиите от парникови газове – въглероден диоксид, метан, азотни оксиди, аерозолни частици и др.

Дейността по опазване на околната среда и рационалното използване на природните ресурси. Тя трябва да се развива чрез изграждането на Национална система за екологичен мониторинг (НАСЕМ).

Реализирането на екологичната политика интердисциплинарни специалисти, в т. ч. и такива в областта на социалната екология.

Литература

1. Бекярова, Н., Демография и сигурност, С., 2004.
2. Бобылев, С. Н., Экологизация экономического развития. М., 1993
3. Бонева, М., Социална екология, Ш., 2008.
4. Василенко, В. Н., Экологические конфликты общества как предмет социологии и социальной Экологии, Ноосфера,1998, с. 73- 79.
5. Винокурова, Н. Ф., Трушин В. В., Глобальная экология, 1998
6. Гудие, Д., Енциклопедия на глобалните промени. Промяна на околната среда и човешкото общество, т.1 и т. 2, Оксфорд, 2001.

7. Доклад на Програмата за развитие на ООН „Новите измерения на човешката сигурност”, 1994.
8. Марков, К., Екстремална психология, Ш., 2007
9. Ситаров, В. А., Социальная экология. М., 2000.
10. Слатински, Н., Измерения на сигурността, С., 2000.
11. Слатински, Н., Петте нива на сигурността, С., 2010
12. Стратегия за национална сигурност на Република България, С., 2011.

СОЦИАЛНА ИНТЕЛИГЕНТНОСТ И СИГУРНОСТ

Маргарита Бонева, Георги Колев

Шуменски университет „Еп. Константин Преславски”
Педагогически факултет

SOCIAL INTELLIGENCE AND SECURITY

Margarita Boneva, Georgy Kolev

ABSTRACT: *It the presents the parameters of social intelligence.*

KEY WORDS: *social intelligence, social brain, social neurology, social sense, social abilites, security.*

Политиката на Република България в сферата на сигурността се изгражда върху ценностите на демокрацията, на националната ни култура, правата на човека и гражданина, на равните възможности за развитие на личността, както и на Конституцията на страната и основополагащите актове за гарантиране на международната сигурност. Стратегията за национална сигурност въплъщава миролюбивия характер и традициите на добросъседство и взаимноизгодно сътрудничество, характеризиращи политиката на нашата страна. Тя е част от усилията на Европейския съюз и НАТО към разширяване зоната на стабилност, сътрудничество и благоденствие посредством неутрализиране на заплахите от тероризма и екстремизма, преодоляване на регионалните конфликти и активно участие в решаването на глобалните проблеми. От особено значение е приносът на страната ни за стабилизиране на междудържавните отношения и прилагането на принципа за ненамеса във вътрешните работи на страните от Балканския полуостров и в Черноморския район.

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.

Подготовката и запазването на човешкия ресурс има особено голямо значение за функционирането на системата за национална сигурност.

Според едни автори интелигентността е способност да се вземат бързо правилни решения в непознати ситуации. Според други, интелигентността е вродена способност на даден съзнателен индивид да прави изводи върху дадена информация. Най-широко разпространено определение е това, което разглежда интелигентността като способност на човек да мисли, да разсъждава, да решава проблеми, да разбира материалното и абстрактното. Интелигентността се счита и за отражение на личността, на характера и поведението, творческите умения и знанията. Морфологичният анализ представя интелигентността като функция на социалния живот, образованието, възпитанието. Независимо от това, все още има автори, които смятат, че интелигентността има наследствен характер и е генетично обусловена.

Следователно начинът, по който се свързваме с другите, е неимоверно важен. Това ни навежда на мисълта, че трябва да проявяваме интелигентност и в нашия социален свят. Основните функции на социалния мозък – синхронизацията на взаимодействията, различните видове емпатия, социалното познание, комуникативните умения и грижата за другите – очертават и параметрите на социалната интелигентност.

Социална интелигентност означава да проявяваш интелигентност не само за своите социални контакти, но и в самите тях. Тя позволява да знаем как да се свързваме с другите, да калкулираме отношенията си с околните, като отчитаме тяхното въздействие върху нас и нашето върху тях. Следователно, социалната интелигентност се пренася в сферата на междуличностното общуване и включва онези способности, които обогатяват личните ни взаимоотношения, например емпатията и отзивчивостта.

Всеки индивид, който се опитва да действа във властова роля, поставя на изпитание своята емоционална и социална интелигентност. Хора с относително ниска емоционална интелигентност, за които са характерни липсата на самоувереност и ниско самоуважение са склонни „да се крият зад званието си". В много случаи те използват властта си, за да сплашват другите.

Социалната интелигентност в най-общ смисъл е способността да се разбираш с другите и да ги привличаш за сътрудничество. В интерес на сигурността е възходящото развитие на отношенията между страните в даден комфликт или страните имащи отношение към решаването на даден проблем. При наличието на достатъчна емпатия отношенията могат да се издигнат до нивото на двустранност, при което всяка от двете страни дава своя положителен принос за интересите на другата.

Социалната отговорност на мозъка изисква да бъдем мъдри, т.е. да си даваме сметка, че не само нашите настроения, но и самата ни биология се влияе и премоделира под въздействието на другите хора, които срещаме в своя живот, както и обратното, което пък означава, че трябва да отчитаме начините, по които нашите емоции и биология въздействат на околните.

Социалната интелигентност включва категориите социален усет и социални умения.

Компонентите на социалния усет са:

- Първичната емпатия (споделяне на чувства в т. ч. и на невербални емоционални сигнали).
- Настройката (внимателно изслушване и съобразяване с другия).
- Емпатичната акуратност (вникване в неговите мисли, чувства и намерения).

- Социалните познания (изградена представа за начините, по които функционира социалният свят).

Известно е, че само уменията, изградени на социалния усет, позволяват гладки и ефективни отношения. В спектъра им попадат:

- Синхронизацията (плавно и отмерено взаимодействие на невербално ниво).
- Самопредставянето (ефективна "презентация" на своя личен свят).
- Влиянието (формиране на резултата от самото социално взаимодействие).
- Активната съпричастност (съобразяване с потребностите на другия и предприемане на съответните действия).

Сигурността е много широко понятие, което може да се представи като същност, състояние, свойство, потребност. Същевременно то е и едно от най- употребяваните. Сигурността е всеобща същност на съществуване на материалния и духовния свят. Тя обхваща всички форми на тяхното проявление. Липсват явление, отношение, процес, дейност, които да не съдържат в себе си като свой съществен и градивен елемент сигурността. Сигурността, като същност може да се отнесе към системата от категории като движение, пространство, време, енергия, информация и др. Тя е всеобщо и системно състояние на всичко съществуващо и в днешния свят. "Сигурността" е едно от най-често употребяваните многозначни съвременни понятия. Представлява и увлекателна тема, защото засяга фундаментални проблеми на оцеляването на нациите и държавите. Може да бъде свързана едновременно с високите етажи на международните отношения и с практически всеки от аспектите на вътрешната политика. Представлява, както широко дискутирана публична страна, така може да бъде обвита в мистицизъм и загърната в конспиративност. Поради това наличието на ясни представи за сигурността се явява важно условие за правилното осмисляне на проблематиката, концепцията, стратегията и политиката за сигурност на страната ни. Понятието като форма на мисленето отразява същността и явленията в зависимост от усещанията, намиращи все повече място в сигурността. Усещането – считаме, че е отражение в мозъчната кора на отделни свойства на предметите и явленията от външния свят. Представлява и вътрешното състояние на организма. Между понятието и усещането има не само количествена, но и качествена разлика. Понятието за сигурността се изгражда в резултат на критичен анализ и обобщение и се съобразява с възгледите за водене на борба с негласните форми на престъпна дейност. Общото за сигурността, отразено в анализираните понятия за сигурността, е че те не се извеждат от разума или от емоцията, а съществуват обективно в реалната действителност.

Сигурността е нещо, което става проблем, според проф. Д. Йончев когато е поставена под въпрос. В този случай най - често се говори за несигурност. Авторът анализира несигурността и сигурността като двете части на една отсечка, която изобразява нечие присъствие, нечие ежедневие. Когато едната от двете части е по-голяма, то е за сметка на другата. Сигурността и несигурността са състояния, които са свойствени на хората в тяхното ежедневие. При обобщаване на мотивациите на обществото от държавните институции обществените организации и гражданите, приемаме че в терминът "сигурност" може да бъде определено присъствието – отсъствие на заплаха. Тази заплаха може да е както обща, така и конкретна, единична. Сигурността може да бъде свързана едновременно с високите етажи на международните отношения и с практически всеки от аспектите на вътрешната политика.

Н. Слатински разглежда сигурността, като: "комплекс от четири условия – система, процес, логика и абстракция", като те се изясняват чрез понятията "потребност", "равновесие" и "динамична устойчивост". Сигурността в този аспект е състояние на обществото, на фирмата, на службата, на държавата. Също така е състояние и на отделни лица, индивиди, граждани, което гарантира нормалното функциониране и осъществяване на поставените условия от тях за понятието сигурност.

Сигурността е стабилната основа на средствата и мерките за преодоляване на заплахите и изграждане на мир, просперитет и икономическо благополучие. Тя е ключ към доверието в идентичност, устойчивостта на демократичните системи, надеждността в държавните институции и доверието между съседите.

По-обширна дефиниция за сигурността, предложена от Арнолд Уолферс, която става стандарт в международните отношения, гласи: „Сигурността, в обективен план, измерва отсъствието на заплахи за постигнатите обществени ценности, а в субективен план – отсъствието на страх, че тези ценности могат да бъдат накърнени, атакувани, застрашени."

Съвременният теоретичен дебат в тази област поставя известни трудности при конкретно концептуализиране на сигурността и избор на подходяща дефиниция, която точно да характеризира понятието в съвременните му измерения и по-скоро да изключва, отколкото да включва твърде много аспекти. Въпреки това, новите академични изследвания в тази област създават предпоставки за развитие на нови политики и научни направления, като представят значимите хуманитарни аспекти на сигурността, които до тогава са пренебрегвани.

Сигурността е свързана с качествата на отделната личност в т.ч. и с нейната интелигентност.

Емпатичната акуратност е "венецът" на социалната интелигентност. В основата й стои вече познатата ни първична емпатия, но с появата на акуратността, тя се обогатява с още един важен нюанс – експлицитното разбиране на чувствата и мислите на другия. Умението за междуличностно общуване от десетилетия се признава за една от основните черти на социалната интелигентност. Социалното съзнание, емпатичната акуратност, която се гради върху умението да се вслушваш плюс първичната емпатия, за обогатяване съвместно на социалното познание, заедно с взаимното "усещане" са трите компонента на социалната интелигентност. Именно взаимното усещане, в който и да е от многобройните му варианти предлага една сигурна основа за развиването на социални умения, които са втория аспект на социалната интелигентност. Всеки опит обаче да се елиминират човешките ценности от социалната интелигентност се отразява пагубно на самото понятие. Според Даниъл Голман характеристиките на социалната интелигентност се вписват в модела на емоционалната интелигентност, защото на самопознанието като компонент на емоционалната интелигентност съответства социалното съзнание като компонент на социалната интелигентност с дефиниращите го –първична емпатия, емпатична акуратност, изслушване и социално познание. На параметъра самообладание (самоконтрол) от емоционалната интелигентност съответстват социалните умения (синхронизация, самопредставяне, влияние и загриженост). Предложените от автора черти на социалната интелигентност вероятно се вписват в стандартните определения за "интелигентността" в некогнитивните сфери, но това е така защото стигне ли се до интелигентност в социалния живот, самият

мозък комбинира най-различни похвати. По тази причина първичната емпатия, синхронизацията и загрижеността са адаптивни средства от човешкия социален арсенал за оцеляване. Понятието "социална интелигентност" се въвежда от Едуард Торндайк през 1920 г., за да опише умението на субекта да разбере и управлява други хора. Първите теоретици на социалната интелигентност явно са търсели някакъв аналог на IQ, който да е приложим в социалната сфера.

Днес много учени свеждат социалната интелигентност до приложението на интелигентността изобщо в социални ситуации, с други думи свързват това понятие с когнитивните способности. Според тях социалната интелигентност е просто набор от знания за околната социална реалност. Редица психолози разглеждат социалната интелигентност като "най-нормална интелигентност, само че приложена в социалната сфера".

Харвардския професор Хауард Гарднър, например в своята книга "Социалната интелигентност – новата наука за успеха" представя измеренията на социалната интелигентност – проницателността, усетът за ситуацията и умението за взаимодействие като ключ към успеха в работата и живота. Той определя социалната интелигентност като способност да се разбираш с другите, като ги привличаш за съдействие. Авторът представя социалната интелигентност като съчетание от чувствителност към потребностите и интересите на другите (т. нар. "социален радар"), великодушен и уважителен подход към тях и комплекс от практически умения за успешното взаимодействие с хората в каквато и да е среда. Според него социалната интелигентност има пет измерения:

- Осъзнаване на ситуацията: способността да разчитате ситуациите и да тълкувате поведението на хората, участващи в тях.
- Присъствие: наричано понякога "маниери", то включва цял набор вербални и невербални поведения, които създават представата за вас в съзнанието на другите.
- Автентичност: това са онези типове поведение, които карат другите да ви оценяват като честен, открит и "истински".
- Яснота: способността да обяснявате идеите си и да формулирате възгледите си.
- Емпатия: способността да "установявате връзка" с другите.

В нашия социален свят следователно трябва да проявяваме интелигентност или поне "съобразителност". Според Едуард Торидайк (1920 г.) "социалната интелигентност е способността да разбираме и ръководим хората", от която всички се нуждаем, за да живеем по-добре на този свят. С други думи под "социална интелигентност" следва да се разбира по–скоро друго – да проявяваш интелигентност не само за своите социални контакти, но и в самите тях. Следователно в спектъра на социалната интелигентност трябва да се включат и онези способности, които обогатяват личните ни взаимоотношения, например емпатията и отзивчивостта. Социалната отговорност на мозъка изисква от нас да бъдем мъдри, т. е да си даваме сметка, че не само нашите настроения, но и самата ни биология се влияе и премоделира под въздействието на другите хора, които срещаме в своя живот, както и обратното, което означава, че трябва да отчитаме начините, по които нашите емоции и биология въздействат на околните. С други думи трябва да калкулираме взаимоотношенията си с околните, като отчитаме тяхното въздействие върху нас и нашето върху тях.

Обобщавайки наличните в литературата факти може да се направи извода, че "социалната интелигентност" включва социалното познание, синхронизацията и настройката, социалната интуиция, симпатичната загриженост, социалните умения и разбира се импулса за състрадание.

Еволюционните теоретици разглеждат социалната интелигентност като изконно достойнство на социалния мозък.

Изхождайки от изследванията на понятието "интелигентност" може смело да се твърди, че интелигентността е производна на социалната интелигентност, а не обратното.

Социалната интелигентност не може да бъде разглеждана без понятието "социален мозък". Причината за възникване на нова верига в мозъка изисква тази верига да е с огромна стойност за този, който я притежава, а това пък увеличава шансовете притежателят й да я предаде и на следващите поколения. Социалният мозък е един от адаптивните механизми на Природата, с чиято помощ индивидът оцелява като част от групата.

Социалният мозък съдържа в себе си всички невромеханизми, оркестриращи нашите взаимоотношения, мисли и чувства, свързани с околните. Той е и единствената биосистема в нашите тела, която ни "настройва" на същата вълна, на която се намират онези, с които контактуваме, и съответно ни позволява да се влияем от тяхното вътрешно състояние. Всички други биосистеми – от лимфните жлези до гръбначния стълб най-често регулират своята дейност в отговор на сигналите, постъпващи не отвън, а от вътрешността на тялото. Каналите на социалния мозък са уникални със своята чувствителност към света като цяло. Всеки път, когато осъществяваме пряк контакт с някой друг, се задействат и нашите социални мозъци. С други думи, когато гневът и обидата станат хронично явление в живота ни или пък се чувстваме емоционално стимулирани от тези, с които най-често общуваме, това може да промени до неузнаваемост и нашия мозък. Взаимоотношенията с околните непрестанно ни оказват фино, но осезателно въздействие. Мрежата на социалния мозък ни свързва всички в нашата обща човешка същност.

В ситуации на избухнал гняв, отвращение, недоволство, т. е. някой ни "залива с порция токсични емоции", в нас се активират веригите, по които протичат абсолютно същите натоварващи усещания и в самите нас. Всеки наш контакт крие емоционален подтекст.

Социалните контакти са тези, които движат емоциите ни.

Социалната интелигентност се проявява в абсолютно всяка житейска сфера, от детската градина и игралната площадка до фабриката и магазина, но уви, не се поддава на стандартни лабораторни тестове. Тя е свързана с когнитивните способности и е своеобразен набор от знания за околната социална реалност.

Според редица психолози социалната интелигентност е "най-нормална интелигентност, само че приложена в социалната сфера".

Всички емоции са социални. Няма как да се отдели причината за една емоция от света на човешките контакти – нашите социални взаимодействия са тези, които движат емоциите ни, ето защо въпросът за социалната интелигентност става все по-актуален в контекста на новите заплахи за *националната сигурност*, каквито са гладът, бедността, демографския срив, незачитане на човешките права и правата на малцинствата, пораженията върху околната среда. С други думи социално-

екологичните проблеми на глобализиращия се свят са непосредствено свързани с националната сигурност на всяка държава.

Новото хуманистично разбиране за *националната сигурност* като сигурност на отделния индивид е възможно да се реализира единствено в условията на гражданско общество. Сигурността на гражданина е основен критерий за ефективността на *Системата за национална сигурност*

Гражданите с тяхната социална интелигентност са потребители на *системата за национална сигурност* и същевременно участват активно според своите възможности в нейното функциониране. Държавата осигурява възможната прозрачност на Системата за национална сигурност и съдейства за развитието на капацитета на гражданското общество за осъществяване на дейности в интерес на *сигурността*.

Литература

1. Албрехт, К., Социалната интелигентност Новата наука за успеха, С., 2006.
2. Бюканан, М., Социалният атом, С., 2011.
3. Голман, Д., Емоционалната интелигентност, С., 2002.
4. Голман, Д., Новата социална интелигентност, С., 2010.
5. Miller, G., New Neurons Strive to Fit In, Science 311 (2005), pp 938-940.
6. Узунов, Н., Основи на психологията, С., 2008.
7. Георгиев , П., Социология, С., 2006.

ОБРАЗОВАНИЕ И СИГУРНОСТ

Маргарита Бонева, Георги Колев

Шуменски университет „Еп. Константин Преславски”
Педагогически факултет

EDUCATION AND SECURITY

Margarita Boneva, Georgy Kolev

ABSTRACT: *In the article examined the problems of education in the context of national security*

KEY WORDS: *education, security, problem*

Стратегията за национална сигурност в чл.20 обръща особено внимание на развитието на образованието, възпитанието, науката и научно-приложните дейности в духа на националните и общоевропейски ценности като част от националните интереси на нацията.

Като основна предпоставка за постигане на високо качество на социалната сигурност в чл. 85 се посочва модернизирането на основното и средното образование както в обществените, така и в частните училища чрез стриктно прилагане на на-

ционалните стандарти. Развитието на висшето образование, изследователската и научната дейност, както и опазването на културно-историческото наследство са основа за предприемане на действия от стратегически характер при планирането и осъществяването на секторни и общи национални политики за развитие на личността и обществото.

Националната образователна система трябва да бъде част от общата система за сигурност, а това значи образованието да дава подходящи компетенции по всеки един въпрос на националната сигурност. Предоставянето на компетенции по аспектите на системите за сигурност и включване на политически, икономически, социални, етнически, духовни, военни и екологични компоненти в образователния процес е основна задача на съвременното образование. Не трябва да се забравя, че образованието е най-добрия начин за социализация на етносите.

Свързани тясно с глобализацията цели, по отношение на които е особено необходимо да се разширяват усилията на международно равнище са:

- образование, умения и технологични възможности;
- въпроси на сигурността и приспособяването;
- осигуряване на достоен труд.

Образованието е централен елемент на обществото и основа на демократичния избор.

За осъществяване възможностите на глобализацията всички страни трябва да инвестират в образованието, професионалното обучение и натрупването на технологични възможности, да се реформират системите на образование и да се води борба с неграмотността.

Пазарите на труда на висококвалифицирани професионалисти фактически са глобални, като тази тенденция се засилва и от глобализацията на системите за висше образование.

Глобализацията насърчава научния и технологичен процес, правейки европейското измерение още по-важно за развитието на знанието, мобилността, конкурентноспособността и иновациите.

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

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

Бурният растеж на Интернет рязко ускори глобализацията на свободния пазар. С появата на глобалните производствени системи, които съдействат за увеличаване на потока от преки чуждестранни инвестиции, възникват нови възможности за растеж и индустриализация в развиващите се страни. Около 65000 многонационал-

ни предприятия с приблизително 850000 техни чуждестранни дъщерни компании играят ключова роля във функционирането на тези глобални производствени системи. Те координират глобалните мрежи на доставки, свързващи фирмите в различните страни, включително дори местните поддоставчици, които работят извън формалната фабрична система и разпределят поръчките сред местните работници на основата на наряди.

Образованието е ключов елемент на глобалната икономика, защото в нея образованието, професионалните навици и знания имат все по-нарастващо значение за икономическото оцеляване, без да говорим за успеха.

Статистическите данни показват, че от 680 милиона деца на ранна училищна възраст в развиващите се страни 115 милиона не ходят на училище, от които 65 милиона са момичета. От всеки две деца, които посещават училище, само едно завършва.

Осигуряването на равен достъп до образование на всички деца е важна функция на държавния сектор в страните с ниски равнища на доходите на населението. Образованието е от полза не само за отделния човек, но и за обществото като цяло. При условие, че децата прекарват достатъчно много време в училище, и в частност, когато момичетата получават подходящо училищно образование, темповете на икономически растеж се увеличават, раждаемостта и детската смъртност намаляват и се подобряват успехите на следващото поколение в образованието. Подходящото начално и средно образование означава не само обогатяване на отделния човек, то обогатява обществото.

Постоянен проблем в много промишлено развити страни са неграмотността и ниската квалификация. Неравният достъп до образование задълбочава засилващото се неравенство в равнището на работната заплата на пазара на труда, а необразованите и неквалифицираните хора в промишлено развитите страни жестоко страдат в условията на засилващата се конкуренция на глобалния пазар.

Всички страни, които се възползваха от благата на глобализацията, направиха значителни инвестиции в системите си на образование и професионално обучение. Солидната образователна политика също предвижда важен инструмент за неутрализиране на такива отрицателни последици на глобализацията като увеличаване на неравенството в доходите, с помощта на средства за въздействие, които в крайна сметка могат да се окажат по-силни, отколкото политиката на пазара на труда. Потребността от образование и неблагоприятното положение, в което се намират етническите и религиозните малцинства, изискват особено внимание. Тези въпроси са актуални за всички страни, независимо от доходите на населението в тях.

В областта на професионалното обучение, могат да се прилагат разнообразни механизми и стимули, включващи мита, държавни стипендии, фондове за професионално обучение, данъчни привилегии и предоставяне на академични отпуски. Ефективната практика на обучение на работното място води до по-високо равнище на производителността, поради което бизнесът е заинтересован да финансира такова обучение.

Развитието на професионалната квалификация във всяка държава представлява също важен фундамент за участието в глобалната икономика, тъй като съдейства за обучение през целия живот, помага за уравновесяване на търсенето и предлагането на професионални умения и ръководи действията на отделните лица при избора им на кариера. Достъпът на жените до обучение и придобиването на умения често пъти

е ограничен от семейни задължения, което разкрива необходимостта от създаването на детски заведения и ползване на възможностите на дистанционното обучение. Други приоритети включват признаването и повишаването на професионалните умения на трудещите се в неформалната икономика и съобразяване на програмите за обучение с оглед обхващането на трудещите се без формално образование.

Една от основните причини за неравенството в света представляват крупните различия между страните от гледна точка на възможностите за образование. Нещо повече, международната миграция позволява на богатите страни да извличат изгоди от инвестициите за развитието на човешкия капитал, които са осъществени в бедните страни, а това възлага върху тях отговорността за оказването на подкрепа на образователните системи, към които се насочват тези инвестиции. Впрочем, по данни на Световната банка само 3% от бюджетните разходи на развиващите се страни за образование се финансират от международни източници.

Инициативата за спешно осигуряване на "Образование за всички" трябва да заеме по - високо място в списъка на приоритетите. Целта е да се изпълни международното задължение, поето на Световния форум по образованието, проведен в Дакар през април 2000 г., което предвижда предоставяне на всички деца до 2015 г. достъп до безплатно задължително и качествено образование и възможности да го получат в пълен обем, както и изкореняване на дискриминацията на половете. За постигането на тази цел е необходимо значително да се увеличи международната финансова подкрепа за образованието.

Дистанционното обучение в режим на реално време би могло да се превърне в мощно средство в ръцете на развиващите се страни, като едновременно с прилагането му намалява необходимостта от поддържането на скъпоструващи материални обекти на инфраструктурата на висшето и техническото образование и дава възможност да се пренасочват инвестиции в комуникационното оборудване. Глобалната мрежа за дистанционно обучение (ГСДО) е инициатива, която заслужава подкрепа. Тя представлява световна мрежа от институти, които разработват и прилагат технологии и методи за дистанционно обучение, като отделя особено внимание на решаването на задачите в областта на развитието.

Проблемите на сигурността са почти винаги екзистенциални, а решенията им са най-често политически. Говорейки за тези проблеми, трябва да се отчита, че те могат да се управляват сравнително успешно и до определен момент, само докато водят до количествени, и много по-трудно, когато водят до качествени промени.

В националната и световната литература понятието сигурност се дефинира по различен начин. Най- широко употребяваното определение за сигурност е: "Сигурността е състояние на обществото и личността, при което не съществува опасност от политическа и икономическа принуда, гарантирани са интересите и свободите на гражданите, отсъстват неравновесни и кризисни състояния на обществената система." Днес понятието "сигурност" е свързано със стабилно и ефективно функциониране на всички социални системи в обществото и с отделяне на по-голямо внимание на заплахите за околната среда, за правата и свободите на гражданите, на здравните и социални проблеми на бюджетния и търговския дефицит и макроикономическата стабилност.

Така на Международната конференция "Разоръжаване и развитие", проведена в рамките на Генералната асамблея на ООН през 1987 г. се стига до дефиниция, според която: "Сигурността е приоритет на всички нации. Тя представлява фунда-

мент както на разоръжаването, така и на общественото развитие. Сигурността се състои не само от военни, но и от политически, икономически, социални, хуманитарни и екологични аспекти. Тя е свързана и със спазването на човешките права, съгласно международните договори".

Понятието "сигурност" е сложно и комплексно понятие, което позволява множество интерпретации. От гледна точка на рисковете и заплахите сигурността се разделя на военна, икономическа, социална, екологична, демографска и информационна.

Сигурността е главната стока, която се търгува на пазара на международните отношения. С каквито принципи да се обосновава една външна политика, в края на краищата тя се оценява по това, дали в резултат от нея сигурността на държавата, обществото и хората нараства или поне не намалява.

Националната сигурност е свързана с образованието, културата, политиката, със средствата за масова комуникация.

На първо място, трябва да се съхранява родния език. В днешния свят без граници повече от всякога трябва да познаваме и уважаваме националната култура и традиции. «Днес повече от всякога трябва да изискваме уважение към историята и със самочувствие да отстояваме нейния автентичен прочит. Историята понякога е величествена, понякога е болезнена, понякога – дори жестока, но винаги е истинска».

Днес, особено внимание изисква все по-влошаващият се в здравен, в образователен и квалификационен разрез качествен състав на населението. Известно е, че индикатори за "качеството на населението" са главно:

- образованието;
- нивото на грамотност на възрастните хора;
- делът на учащите;
- здравното състояние на населението (средна продължителност на живота, заболеваемост, трудоспособност).

При грамотността пирамидата у нас е обърната: възрастното поколение е по-грамотно. Това са остри симптоми на боледуващо общество, белези на демодернизация, на оттегляне на държавата от присъщи, дори задължителни за нея социални функции. Ето защо в Стратегията за Национална сигурност се отделя специално място на развитието на образованието, възпитанието, науката и научно-приложните дейности в духа на националните и общоевропейските ценности.

В продължение на години се наблюдава влошаване на здравния статус на населението, както и изразени негативни тенденции в образователното и квалификационното равнище на значителни групи от българското общество, което е предпоставка и за недостатъчната интегрираност на някои общности, принадлежащи към етнически малцинства.

Предпоставка за постигане на високо качество на социалната сигурност е модернизирането на основното и средното образование както в обществените, така и в частните училища чрез стриктно прилагане на националните стандарти. Развитието на висшето образование, изследователската и научната дейност, както и опазването на културно-историческото наследство са основа за предприемане на действия от стратегически характер при планирането и осъществяването на секторни и общи национални политики за развитие на личността и обществото.

Правилно обръща внимание Михаил Мирчев върху проблема за опазването на нашите деца - към тях цялото общество, всеки един от нас – всички сме длъжници.

Да, у нас се раждат малко деца, но ние "похабяваме огромен контингент от ражданите деца". Това е така, защото не пазим децата от алкохолизъм, от наркотици, от уличното насилие. Първата задача на държавата е да създаде комплекс от мерки, които да пазят децата. И така те, като станат на 18 год., да са живи и здрави, да не са интелектуално и психически малоумни, да не са антисоциални. Едната мярка трябва да е в данъчната политика – семейното подоходно облагане. Друга мярка е образователната система, която трябва да се самообучи, да дава обучение и съвременни нагласи на децата в подготовката за семеен живот, сексуално партньорство. Учителите трябва да са отворени към тази тема и да общуват с децата още от 4-ти клас".

Образователното равнище и професионалната подготовка на българските граждани са един от най-важните критерии за тяхното използване в системата на отбраната и сигурността. Нивото на образованост на една нация има решаващо значение и за нейното цялостно развитие и мястото й в съвременните международни процеси.

През последните години в образователната сфера се очертават две трайни и противоположни тенденции. Едната е либерализацията в сферата на висшето образование, наличието на голям брой висши училища, рязко увеличаване на броя на хората с висше образование.

Другата определяща тенденция е свързана с все по-нарастващия брой на децата и младежите, които никога не са посещавали или са отпаднали от училище още в първите ученически години. Непрекъснато нараства броят на децата и младежите от малцинствен произход, които остават неграмотни или полуграмотни. Особено тревожно е положението след младото поколение от ромската и турската етническа група. Прави впечатление, че нараства броят и на българчетата, чиито семейства нямат материална възможност да изпратят децата си на училище.

Съвременната демографска характеристика на населението в България ще има трайни негативни последици върху всички аспекти на националната сигурност.

На първо място това ще даде отражение върху военната сигурност, защото демографското състояние на всяка държава е пряко обвързано с възможностите за реализация на нейната военна политика, на нейната отбрана и сигурност. Количеството и качеството до голяма степен определят едни от най-важните показатели за състоянието на националната сигурност, каквито са националната мощ, военните и бойните възможности на страната.

Обедняването, ниското качество на образованието, растящата безработица, енергийно неефективното икономика са най- сериозните рискове за националната сигурност на страната.

30% от българите днес живеят в условия на големи материални лишения като този социален срив е един от серизните рискове на националната сигурност.

Изложени на голям риск от маргинализиране са децата на застрашените от социално изключване групи.

Отричането от традициите на българското образование независимо дали причините са свързани с престъпна некомпетентност или да се харесаме на други може да се сравни с национално предателство.

Нивото на образование е ключов фактор за всяка една област на човешкото битие. То е пряко свързано с демографските проблеми на нацията, защото колкото по-малко образован е човек, толкова по-малко отговорен е за репродуктивното си поведение. Ниската образованост се дължи на затруднения достъп до образование, което изисква преодоляване на проблемите с бедността, сивата икономика в обра-

зованието и ограничаване на детския труд. Качественото образование освен това изисква модернизиране на материалната база на учебните заведения, повишаване на квалификацията на преподавателите, както преодоляване на застаряването им.

Учебните планове и програми трябва да съответстват на изискванията на икономиката към подготовката и квалификацията на съответните специалисти и към държавната политика в областта на образованието.

Осигуряването на мобилност на студенти и преподаватели с учебни заведения от други страни и всички проблеми, свързани с кредитирането на учащите се са проблеми, поставени на дневен ред

Все по-актуален днес става проблемът с чистотата на българския език. Опростяването, маргинализацията и безогледното вкарване в езика на чуждици най-често от английски, доведе до това, че българският език отдавна не е този, който нарича-ме "свещен".

Прекомерното изтъкване на компютърните умения и ролята на Интернет подриват авторитета на образованието.

Липсва превенция на асоциалното поведение и в резултат на това сред младите хора се ширят насилие, наркотици, алкохол.

Все още българското училище е катализатор на социално неравенство и създава потиснати, агресивни и комплексирани деца с разбити илюзии.

Българският народ днес се дезинтегрира, изчезва. Статистиката показва, че ние по-бързо ще изчезнем като култура, народ, език, който може да има място в Европа, отколкото демографски.

Високият процент на отпадащите ученици е заплаха за възпроизводството на знанието и за компетентността на нашата нация.

Светът ще продължи да се развива и да бъде многообразен. В бъдеще ще продължим да наблюдаваме пъстрота от общества, раси, етноси, нации, култури, икономически и политически модели. Всички те обаче, при цялото си многообразие ще се движат в една историческа посока – посоката на нооразвитието. Всяка от сферите на обществото ще претърпи ноотрансформация (нооикономика, ноотехносфера, ноополитика, ноогеокултура, ноопроизводство), изобщо нооразвитие на всички човешки дейности. Особено важна при това става човешката сигурност.

Нивото на човешката сигурност се измерва с индикаторите:

- бедност;
- здраве;
- образование;
- политическа свобода;
- демокрация.

Доброто образование е задължителна предпоставка за успех във всяка сфера на обществения живот. Липсата на качествено образование е спирачка за икономическия растеж, тя води до по-лошо управление, и в края на краищата – до по-малко сигурност.

В историята общества без стабилна духовна и културна основа не могат да съществуват дълго, ето защо е важно държавата да съхрани своята културна идентичност. В тази връзка принципът е ясен-съхраняване на традиционната ни идентичност чрез адекватно образование.

Образованието трябва да е приоритет на националната сигурност. Днес образованието не е разход, а инвестиция, - в по-доброто бъдеще на нашата държава.

В началото на XXI - век образованието се превръща в критерий от първостепенна важност в световната икономическа битка (нови технологични производства, световен пазар и др.). Ето защо бъдещето на всяка страна, независимо от нейната степен на социално-икономическо развитие, се определя от способността й бързо да се ориентира и пълноценно да се включи в световните процеси. В голяма степен това ще зависи не само от икономическата мощ, но и от равнището на образованост, професионална мобилност и комуникативност на нейните граждани. От тези позиции може да се твърди, че образованието през XXI век става един от главните приоритети на държавата, свързани със сигурността.

Литература

1. Будыко, М., Глобальная экология, М., 1977.
2. Буут, К., Сигурност и еманципация, В., 1991.
3. Бюканан, М., Социалният атом, С., 2011.
4. Бяла книга за отбраната, С., 2002.
5. Василев, Г., Химия и опазване на околната среда, С., УИ "Св. Кл. Охридски", 2001.
6. Костова, З., Концептуализация на екологичното образование, С, 2003
7. Моисеев, Н., Устойчивое развитие и экологическое образование// Философские аспекты социальной экологии. М., 1996.
8. Стиглиц, Дж., Глобализацията и недоволството от нея., С., 2003.
9. Стратегия за национална сигурност на Република България, С., 2011.

ПОСЕГАТЕЛСТВАТА СРЕЩУ ЛИЧНИ ДАННИ В ОРГАНИЗАЦИЯТА – СПЕЦИФИЧНИ АСПЕКТИ

Христо А. Христов

Шуменски университет „Епископ Константин Преславски”

THE PROTECTION OF PERSONAL DATA – OBJECTIVE NECESSITY IN THE ORGANIZATION

Christo A. Christov

Shumen University “Bishop Konstantin Preslavski”

Abstract: *Unprotection and encroachments upon personal data in organization both correspond directly with safety of each individual. Encroachments upon personal data are objectively existing in reality as negative social side effects. In relation with this an effective system for defence of personal data is impossible to be worked out for one organization without revealing and analyzing particular encroachment’s forms and methods. The reverse method might be conceptually very wrong and can provoke the occurrence of absolutely inadequate system of defence in comparison with reality.*

Key words: *Personal data, encroachments upon personal data, encroachments’ forms and methods against personal data, engagement, special reconnaissance methods, defence of personal data, confidential information*

През 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” като един от дълбинните фактори на днешната глобална революция [2]. По тази причина нараства броя на мениджърите, приемащи частната разузнавателна дейност като задължителен елемент от управлението на организациите, характеризираща се с изключителна динамика.

В тази връзка посегателствата срещу фирмената сигурност стават част от оперативната среда на бизнес организациите. Това е нещо, от което нито един собственик не може да избяга. Редовни заглавия за промишлен шпионаж, бизнес разузнаване и кражба на информация показват, че адекватната защита на чувствителна за фирмата информация, се превръща в световен проблем. Бизнесът все по-ясно разбира значението на запазването на своите вътрешни секрети и последиците от несанкциониран достъп на терористични организации и чужди разузнавателни сили до тях. Несигурността за бъдещето на организацията пряко кореспондира с изпреварващото определяне и предвиждане на възможни заплахи и посегателства.

В процеса на утвърждаване като компонент на националната система за сигурност, оргаизацията е обект на въздействие на многообразни и сложни съвременни

посегателства, дейности са свързани с неетични и незаконни действия, които не следва да бъдат подценявани и пренебрегвани.

Посегателствата и заплахите за сигурността на организациите са с висока степен на неопределеност, проявяват се в сложна взаимозависимост и са трудно предвидими. Необходимо е извършване на трансформация в политиката за сигурност на организациите, с цел създаване на благоприятни условия за изпълнение на мисията им и гарантиране устойчивото развитие на индивидите и обществото.

Голяма част от българските организации, решили да вземат мерки за сигурността на личните данни, защитата приключва с назначаване на администратор на лични дани и въвеждане на технически и организационни мерки за тяхната защита [2] и [3]. Организирайки тези мероприятия, много от мениджърите не си дават сметка, че това са само елементи на сигурността на организацията. Обикновено организациите решават проблемите със защитата на личните данни „на парче". Масово се подценява и не се познава същността на посегателства срещу личните данни в организацията. В тази връзка, поставените цели на доклада ще бъдат насочени към изследване на посегателства на лични данни и техните възможни форми и способи за реализиране.

Защитата на правата на физическите лица при обработването на личните данни е ангажимент на всяка социална организация в Р.България. Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци [2].

В организацията администраторът на лични данни предприема необходимите технически и организационни мерки, за защита на данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Администраторът е длъжен и да вземе специални мерки за защита, когато обработването включва предаване на данните по електронен път [2].

Комисията за защита на личните данни" определя минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. Целта е осигуряване на адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от случайно или незаконно унищожение, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване [3].

Нивото за защита представлява съвкупност от технически и организационни мерки за физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи, както и криптографска защита на личните данни [3].

Обобщавайки изложеното по-горе, основателно може да се постави въпроса: „Подготвени и готови ли са нашите организации, за организиране на ефективно противодействие срещу професионални атаки от външни сили, използващи конспиративни методи за неправомерно извличане на лични данни ?".

Преди да се пристъпи към организиране на защитата на личните данни, е необходимо добре да се разберат и различат формите на посегателства и способите, чрез които те се реализират.

Съществуват различни определения за личната и обществената сигурност. Понятието сигурност може да се формира като: -безопасност и защитеност на обществената формация или индивид, осигуряващи съхранението и развитието им. Чо-

вешката сигурност включва „същностните" елементи които са „достатъчно важни за хората, така че да са готови да се борят за тях или да поставят на значителен риск своя живот или собствеността си" [4].

Следователно незащитеността и посегателствата на личните данни кореспондира пряко със сигурността на индивида и организацията. Не може да бъде разработена система за защита на личните данни за конкретна организация, без да са разкрити и анализирани конкретните форми и способи на посегателствата. Обратният подход би бил дълбоко концептуално погрешен и води до абсолютно неадекватна на действителността система за защита.

Посегателствата срещу личните данни са обективно съществуващи в действителността негативни обществени явления. Посегателствата срещу личните данни не съществуват по принцип. Проявлението на конкретни форми и способи в действителността зависи от волята на инициатора. Формите и способите на видовете посегатества не са абстрактни понятия, а конкретни понятия имат своите индивидуализирани субекти (инициатори), ясен предмет на посегателство (лични данни), реализира се определен и съзнателно търсен от инициатора резултат.

Видовете посегателства са изключително разнообразни и затова нерядко подценявани от мениджърите. Във всяко посегателство обаче участват хора и почти няма такова, в което да не е използвана информация или съучастие на вътрешен човек. Помощта от вътрешния човек бива доброволна или принудителна, умишлена или неумишлена, но във всички случаи демонстрира едно от най-важните и най уязвими звена на системата за сигурност – хората.

Всяко посегателство има предистория и причина. Обикновено всяко посегателство се реализира на няколко етапа: формиране на намерение, събиране на информация, анализ на информацията, изготвяне на план, осигуряване на необходимите ресурси, предприемане на действия.

Заплахите на личните данни на една организация могат да се разделят условно, в зависимост от факторите на въздействие, на външни и вътрешни. Към външните заплахи спадат всички онези действия, които са в резултат от дейността на злоумишлени действия на трети лица –чужди разузнавания, терористични организации, криминален контингент, контрагенти, конкуренти, и др. Вътрешните заплахи съотнасяме към действията от страна на съдружници, служители и др.

Вътрешните заплахи са особено трудно разрешим проблем, защото има толкова много начини вътрешните зложелатели във фирмата (т.н. „инсайдери", от англ. insiders) да откраднат информация от корпоративната мрежа. Проблемът на тези заплахи е толкова актуален, че той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List) на Американският съвет за изследване на сигурността на информационните системи – INFOSEC. Това е списък на най-трудните и най-критичните предизвикателства в INFOSEC изследванията, които трябва да бъдат решени за разработването и внедряването на надеждни системи за правителството на САЩ [5].

Посегателствата срещу личните данни се извършват тайно, с използване на конспиративни средства и методи. Така например, за да получат информация за лични данни, чужди служби и конкурентни фирми е възможно да използват способи, като: вербовки на служители на фирмата; подслушвания на разговори и телефони; тайни огледи; кражби на документи; включване в комуникационните канали и линии за връзка; скрито наблюдение; копиране на документи; унищожаване на

информация. В действителност защитата на личните данни осъществявана от службите за сигурност на организациите /администраторът на лични данни в частност/ се изразява в противопоставяне на конкретни посегателства срещу личните данни.

Посегателствата на лични данни са съзнателни, тайно извършвани противоправни обществени деяния, с които се нанасят вреди на интересите на индивида, но не представляват престъпления. В тази връзка за нарушаване на закона за защита на личните данни се налагат глоби и имуществени санкции по реда на административно процесуалния кодекс [2].

Посегателствата на лични данни имат свои **субект и обект.** Под субекти се разбират лицата, организациите, поставили си за цел придобиване на лични данни чрез незаконни средства – наричат се инициатори. Обекти са индивидите и организациите, които в резултат от действията на инициаторите търпят преки вреди – те са потърпевши.

Цел на инициаторите на неправомерен достъп до лични данни е нанасяне на вреди на потърпевшите.

Предмет на посегателство са личните данни обработвани в организацията.

Посегателството на лични данни е умишлено деяние, и се индивидуализира с конкретен извършител – физическо лице. То се материализира, посредством определени свои способи и се реализира със специфични средства.

Посегателствата на личини данни най-често се реализират с множество взаимосвързани действия (актове) за продължителен период от време, обединени от общ замисъл.

Тази съвкупност от множество деяния, осъществяващи се чрез специфични способи, под единен замисъл, за продължителен период от време, характеризираща се с неправомерен достъп до лични данни, определя същността на понятието **форма на посегателствата.**

Различните способи на посегателства се реализират по предварително съставен план, чрез застрашаващи потърпевшия средства, прилагани от недобросъвестни субекти .

Посегателствата на лични данни се характеризират със съответни практически (изпълнителски) способи за реализирането си.

Под способ на посегателство на лични данни можем да определим практическия (изпълнителския) начин или конкретното действие (акт), посредством който дадено посегателство, се материализира в действителността [6].

Изчерпателното посочване на способите за осъществяване и изясняване на посегателствата е практически невъзможно, ето защо в изследването ще посочим само някои от тях.

В действителност способите за практическо изпълнение са идентични с тези, които държавните спецслужби използват в дейността си.

Изграждането на доверителни отношения със служител на конкурент е едно специфично вербуване на служител от атакувана организация с намерение чрез него да се реализира неправомерно извличане на лични данни [7].

Резултатът от това, обикновено, е изнасяне на конфенденциална информация за лични данни от организацията посредством такъв вербуван служител. За вербуване се пристъпва към такъв служител от персонала на организацията, за когото се знае или предполага, че е в пряк досег с личните данни обработвани в организаци-

ята. Обектът на вербуването трябва да разполага със съответна позиция в йерархията на атакуваната организация и това е една от двете най-важни предпоставки за начало на доверителните отношения. Другата предпоставка са личните качества на кандидата за доверителни отношения.

При изграждане на доверителни отношения със служител от атакувана организация компрометирането, принудата, поставянето в зависимост и поставянето в заинтересованост са способи използвани във вербовъчния процес [7].

Способът „поставяне в заинтересованост" има две главни разновидности – поставяне в материална заинтересованост и поставяне в служебна (кариеристична) заинтересованост.

Способът „поставяне в зависимост" е в различни разновидности, от които най-важните са сексуалната, наркотичната и алкохолната, т.е. базира се на най-разпространените и устойчиви човешки пороци.

Трябва да се има предвид, че способите за поставяне в зависимост или заинтересованост при изграждане на доверителни отношения са предпочитани от професионалистите в тази област. Те са основа за по- трайни и стабилни доверителни отношения със служителя на атакуваната организация. Компрометирането и принудата са предпоставка за краткотрайни и лабилни доверителни отношения. Те биват веднага отхвърляни след отпадане на принудата или преодоляване на стреса от възможно компрометиране. Използват се само когато се налага еднократно (инцидентно) придобиване на информация за лични данни от дадена организация или когато придобиването на тази информация е особено належащо и вербуващият не разполага с време, за да използва другите способи.

Внедряване на доверено лице сред персонала на атакувана организация. Реализира се посредством два основни способа – със и без участие на лице от персонала на потърпевшия, с което предварително са изградени доверителни отношения.

Следващ способ е използване на специални разузнавателни средства срещу организация обработваща лични данни.

Съвременното развитие на специалната техника е такова, че предоставя на инициаторите изключително богати и разнообразни възможности за нерегламентирано придобиване на чужда информация за лични данни. За нуждите на изследването практически е невъзможно и ненужно да се спираме на всички познати от практиката способи за противозаконно извличане на лични данни със специални разузнавателни средства. Ето защо ще се спрем само на тези от тях, които са разпространени най-много и чието използване е особено опасно за индивида и организацията.

Способите за посегателства на лични данни чрез специални разузнавателни средства се поделят в зависимост от източника на информация и ползвания канал за изпращане или получаване на информация, за чието контролиране те са предназначени. Затова сме длъжни да изясним първо видовете и същността на източниците на информация и комуникационните канали, срещу които са насочени практическите способи на неправомерен достъп [7].

Хората. Те са главен източник на информация при неправомерен дотъп. Информацията от човешки говор се разпространява във въздушното пространство чрез звукови вълни. Човешкият говор се разпространява по кабел – при разговор по жичен телефон, и чрез ефира – при разговор по радиостанция или по мобилен телефон. Информацията от човешки говор може да се съхранява и върху магнитен

носител – аудиокасета или диск, а също в човешката памет на присъствалия при даден разговор. Информацията за човешкото поведение или конкретно действие също е изключително ценна. Тя подлежи на съхраняване, посредством фотоснимки, видеозаписи и други, а също и на възпроизвеждане по описание на очевидци.

Компютрите. Компютърната информация може да се предава по жичен път посредством модем, например в световната мрежа Интернет или в локална мрежа; чрез диск или дискета, когато на тях е записана компютърна информация; чрез електромагнитното лъчение на монитора на компютъра; чрез промяната на някои физически характеристики на електрическия ток по захранващата компютъра мрежа. Компютърната информация подлежи на извличане от твърдия диск на компютъра, както и по други начини.

Документите. Под документ разбираме стандартния хартиен информационен носител, както и магнитни или други информационни носители. Документът може да съдържа човешка мисъл или да възпроизвежда разговор посредством условни обозначения – букви. Документът може също да съдържа изчисления, формули, технически схеми и други, възпроизведени посредством цифри и специфични за различните науки условни знаци. Той подлежи на създаване, прочитане, движение, преписване, съхранение, ксерокопиране, фотофилмиране, запомняне, възпроизвеждане по памет или от негатив, изпращане по поща, унищожаване и прочие действия, всяко от които може да бъде контролирано от нелоялен конкурент.

Всеки източник на информация поражда и обменя информация, а всяка информация се движи по свой характерен комуникационен канал. На контрол от страна на инициатор на посегателства на лични данни подлежи информацията, съдържаща се в съответния източник – чрез вербуването му за доверителни отношения (при хората) или чрез кражба (за останалите). На контрол подлежи и информацията по време на нейния обмен с даден потребител по някакъв комуникационен канал или пък чрез директно извличане (например от паметта на компютър). Информация може да бъде придобита от инициатора на посегателство и когато той привидно заеме ролята на истински потребител на информацията, т.е. когато въведе в заблуждение организацията обработваща търсените лични данни.

Най-често прилаганите на практика способи за посегателства с технически средства на чужда информация за лични данни са:

Радиомикрофонно подслушване. Чрез него се контролират звуковите вълни на човешки говор във въздушно пространство.

Подслушване с лазерен (насочен) микрофон. Така се подслушва човешки говор, посредством контролиране на предизвиканите от звуковите вълни трептения на прозорците на помещението, в което се провежда разговорът.

Подслушване със стетоскопичен микрофон. Извършва се през стената на съседно помещение. Стетоскопът улавя и усилва трептенията в стената на помещението, които се предизвикват от звуковите вълни на провеждания там разговор.

Подслушване на затворено пространство с жичен микрофон. Контролира се човешки говор в затворено пространство (помещение). Уловеният от микрофона сигнал се предава на нелоялния конкурент по телефонната линия, по специално изведен до съседно помещение кабел или по електрическата захранваща мрежа.

Подслушване на жична телефония.

Подслушване на разговор по радиостанция. Инициаторът на посегателството на лични данни разполага с приемник, настроен на честотата на контролирания разговор.

Подслушване на разговор по мобилен телефон. Всеки разговор, по която и да било система за мобилни телефонни комуникации, подлежи на подслушване с несложни технически и организационни средства.

Скрито записване на разговор с миниатюрен диктофон. Скритият магнитофон се намира винаги у единия от събеседниците. Този способ е особено ефективен, тъй като разкриването на работещ диктофон с технически средства е изключително трудно.

Извличане на компютърна информация чрез улавяне на електромагнитното излъчване на монитора.

Извличане на компютърна информация, предавана по телефонна линия.

Извличане на компютърна информация по кабела на електрическото захранване.

Отваряне на чужда кореспонденция. Има се предвид контрол от страна на нелоялния конкурент върху пощенския канал за размяна на информация от потърпевшия.

Кражба на информация

За разлика от специалните разузнавателни средства, при кражбата на информация имаме физическо посегателство (отнемане) срещу информационен носител – предмет, хартиен документ, магнитен носител и други, а не технически контрол върху комуникационна линия или информационна среда. Способите за реализиране на този метод са:

Кражба на предмет.

Кражба на документ. Има се предвид скритото изнасяне на информация, качена на хартиен носител от архива на конкурента.

Кражба на фотоснимки, звукозаписи, видеофилми, компютърни дискове, компютърни дискети и други информационни носители.

Хакерство. Този способ на неправомерен достъп придоби небивали мащаби напоследък. По същество той е скрито проникване с технически средства и специални познания в компютърни бази данни по електронен път, извличане на информация от тях и промяна на тези бази данни.

Тайно ксерокопиране, фотозаснемане, видеофилмиране и други способи за възпроизвеждане на документ.

Извличане на информация от неунищожен документ.

Интегрирайки характеристиките на формулираните подходи за анализ на понятията посегателства срещу лични данни обработвани в социална организация, могат да се направят следните изводи:

Посегателствата срещу лични данни са обективно съществуващи в действителността негативни обществени явления, представляващи съзнателни, тайно извършвани действия, с които се нанасят вреди на интересите на индивида и организацията.

Посегателствата срещу лични данни се реализират с конспиративни методи, средства и способи единтични с тези на държавните разузнавателни служби.

Познаването на съдържанието на посегателствата на лични данни е задължително условие за организиране на ефективно и надеждно противодействие и защита на интересите на индивида и организацията.

Литература:

1. Тофлър, А., и Тофлър, Х. „Революционното Богатство”. Обсидиан, София, 2010, с.149.

2.Закон за защита на личните данни. http://lex.bg/laws/ldoc/2135426048 [онлайн]. [прегледано 10.04.2013].

3 .Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. [онлайн]. [прегледан 2.04.2013]. http://ciela.net/FreeStateGazette/ OpenDocument.aspx?id = 2135836487.

4. Сандев, Г. Сигурност на организациите. Университетско издателство „Еп.Константин Преславски” Шумен.2012. ISBN 978-954-577-621-2.

5. Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. [прегледано 20.04.2013]. http://www.sarc- wv.com/news/press_releases/2013/steganography_insider_threat.aspx.

6. Сандев,Г. „Стратегии за сигурност на фирмата”,Университетско издателство „Еп. Константин Преславски”, Шумен, 2005, с. 12. и Василев, Ем. „Фирмена сигурност”. Труд, 2000.

7. Асенов, Кипров. Теория на контраразузнаването. София : Труд, 2002.

8. Станев, С, С. Железов. Компютърна и мрежова сигурност. Шумен: Университетско издателство, 2002.

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ – ОБЕКТИВНА НЕОБХОДИМОСТ В ОРГАНИЗАЦИЯТА

Христо А. Христов

Шуменски университет „Епископ Константин Преславски”

THE PROTECTION OF PERSONAL DATA – OBJECTIVE NECESSITY IN THE ORGANIZATION

Christo A. Christov

Shumen University “Bishop Konstantin Preslavski”

Abstract: *The matter about protection of personal data is straight connected with organizations’ responsibilities in the process of building effective defence for existing possibilities which can be used for the aim of applying reconnaissance methods to secretly elicit information about personal data, that are updated in organization. This official report presents personal information administrator’s framework knowledge and methodology of his behavior that are necessary for him to acquire and do his obligations in order to reveal and neutralize eventual actions against organizations by means of usage of reconnaissance methods to elicit personal data which can favour minimization of indefence and unwanted consequences for workers in organization. Work hypothesis of this report is that reaction against usage of reconnaissance methods used to elicit personal data information is objective necessity in the process of protecting personal data in organization.*

Key words: *Personal data, counteraction of encroachments, reconnaissance methods, protection of personal data, revealing and neutralizing, confidential information.*

Факт, който не подлежи на съмнение и с който и практици и учени са съгласни е, че в началото на XXI век в средата за сигурност са настъпили и продължават да се случват промени. Формиралата се, съвременната глобална среда за сигурност се характеризира с висока сложност и хаотична динамика на промените, нарушаваща стабилността и устойчивостта на развитието на обществото.

Динамично променящите се заплахи и произтичащите посегателства, пораждат редица проблеми, касаещи: оценяването, гарантирането на сигурността и развитието на организациите и индивидите.

Адекватната защита на сигурността на организацията се превръща в световен проблем. Мениджърите все по ясно разбират значението на запазването на своите вътрешни секрети и последиците от несанкциониран достъп на конкуренти, терористични организации и чужди разузнавателни сили до тях. В тази връзка за защита на информацията си и за контраразузнаване западните фирми отделят до 20 % от чистата си печалба. За съжаление, живота показва, че методите и средствата на разузнаването винаги изпреварват средствата за защита [1].

Обобщавайки изложеното по-горе, основателно може да се постави въпроса: „Подготвени и готови ли са нашите организации, за организиране на ефективно противодействие срещу професионални и сложни атаки от местни и чуждестранни сили?". Ето защо, всеки опит те да бъдат осмислени, да бъдат изследвани и да се посочат начините за тяхното управлявано противодействие си заслужава усилието. Още повече, че сигурността на организацията, като важен фактор за повишаване на сигурността на гражданите и, в крайна сметка, за повишаване на националната сигурност, не е стояла на вниманието с такава острота. В тази връзка, намирането на отговори на тези въпроси е особено важно и това предпоставя избора на темата на настоящия доклад.

Целта на настоящата разработка е да се разкрият възможностите за използване на класическите контраразузнавателни методи и способи за противодействие на каналите за изтичане на конфеденциална информация /каквито са личните данни/ от вътрешни за дадена организация нарушители, и да се предложи активна система за наблюдение от страна на службите за сигурност на организацията.

Под канал за изтичане на информация се разбира метод, позволяващ на нарушител да получи достъп до информацията, обработвана или съхранявана в системата [2].

Надеждната защита на информацията в организациите от несанкциониран достъп е актуален, но много труден и нерешен проблем. Като резултат, вътрешните кражби на чувствителна информация, се увеличават с обезпокоителни темпове, без да се откриват следи от действия на вътрешни служители. Службите за сигурност извършват огромна работа по защита на своите инфраструктури и компютърни мрежи от външни атаки и разузнаване. Дали вътрешната или външната заплаха е по-сериозна е било обект на многогодишни дискусии. Вътрешните заплахи са особено трудно разрешим проблем, защото има толкова много начини вътрешните зложелатели във фирмата (т.н. „инсайдери", от англ. insiders) да откраднат информация от корпоративната мрежа. Проблемът на тези заплахи е толкова актуален, че той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List) на Американският съвет за изследване на сигурността на информационните системи – INFOSEC. Това е списък на най-трудните и най-критичните предизвикателства в INFOSEC изследванията, които трябва да бъдат решени за разработването и внедряването на надеждни системи за правителството на САЩ [3].

Разкриването на канала за изтичане на конфиденциална информация е основна задача на службата за сигурност на организацията, с цел пресичане на престъпната дейност. Нейна отговорност е и организиране на ефективо противодействие на съществуващите възможности за скрито извличане на конфиденциална информация.

Противодействието на посегателствата върху конфеденциалната информация кореспондира пряко с политиката за сигурност на атакуваната организация. Политика на сигурност включва множество правила, които определят как организацията управлява, защитава и разпределя класифицирана и друга важна информация. Това е рамката, в която една система осигурява защитата. Политиката за IT-сигурност за компютрите и мрежите на една организация обхваща мерки в няколко области: организационни, административни, технически и програмни **[2].**

Въпросът за защита на личните данни в организацията, е свързан пряко с противодействието на посегателства срещу конфеденциална информация в организацията.

В тази връзка значимостта на доклада е свързана с отговорностите на организацията при изграждането на ефективна защита от съществуващите възможности за използване на оперативни разузнавателни методи за скрито извличане на информация за лични данни обработвани в организацията.

Доклада предоставя структурирано знание и методология за поведение на администратора на лични данни, необходими за усвояване и изпълнение на задълженията си за разкриване и неутрализиране на дейност срещу организацията с използване на разузнавателни методи за извличане на лични данни, с което да се осигури понижаване на незащитеността и вредоносните последици за физическите лица в организацията.

Работната хипотеза на доклада е, че противодействието на използването на разузнавателни методи за извличане на информация за лични данни, е обективна необходимост в дейността по защитата на личните данни в организацията.

Съществуват различни определения за личната и обществената сигурност. Понятието сигурност може да се формира като безопасност и защитеност на обществената формация или индивид, осигуряващи съхранението и развитието им. Човешката сигурност включва „същностните" елементи които са „достатъчно важни за хората, така че да са готови да се борят за тях или да поставят на значителен риск своя живот или собствеността си"[4].

Следователно незащитеността и посегателствата на личните данни кореспондира пряко със сигурността на индивида и организацията. Не може да бъде разработена система за сигурност на организацията изключваща защитата на личните данни за конкретна организация. Обратният подход би бил дълбоко концептуално погрешен и води до абсолютно неадекватна на действителността система за защита на лични данни.

В Р.България законодателят е определил, че защитата на личните данни е функция на организацията като цяло и тя се осъществява от нейните структури за сигурност /администратор на лични данни [5], [6]./, в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейност, под ръководството на управленските й органи. В същото време службите за сигурност в организацията имат за своя основна цел да **се** противопоставят на видовете посегателства в това число и посегателства срещу лични данни, нанасящи вреди на интересите на индивида и организацията.

Службите за сигурност са част от механизмите в организацията, които са специално създадени и предназначени за опазване на сигурността на организацията. Подчинени на тази обща цел, те имат своите особености в конкретни задачи и дейност, които ги отличават и обособяват във функционално, структурно, организационно и тактическо отношение. Това е причината, поради която тяхната дейност е обект на внимание на теорията на контраразузнаването [7].

Контраразузнаването е основа на системата за сигурност в организацията, защото контраразузнаването, освен като специфична държавна дейност, може да се разглежда и като дейност на недържавни органи за защита на техни и други частни интереси и за гарантиране на тяхната сигурност.

Една от основните задачи на контраразузнавателна дейност е разкриване и неутрализиране на опити на чужди сили да се доберат до фактите, сведенията и предметите, представляващи фирмена тайна [7].

Специфичността в дейността на контраразузнавателните служби се определя от три фактора [7]:

Първо, те се противопоставят на конкретни посегателства срещу сигурността на организацията – съзнателни, тайно извършвани действия или бездействия, с които се нанасят вреди на интересите на индивида и организацията.

Вторият фактор, определящ специфичността в дейността на контраразузнавателните служби **е, че те се противопоставят на конкретни *сили,* които извършват посегателства** срещу сигурността на организацията. Това са външни и вътрешни сили, които, използвайки законспирирани средства и методи, извършват дейност, с която нанасят вреди на сигурността на организацията и индивида.

Третият фактор, който определя специфичността в дейността на контраразузнавателните служби**, е начинът, по който те се противопоставят на посегателствата, извършвани от външни и вътрешни сили.** Тези сили се стремят да прикриват своята дейност, като използват конспиративни методи и форми. Това изисква в борбата срещу тях да се използват органи, които умеят да прилагат адекватни сили, средства и методи, способстващи да се разкриват замислите, намеренията и приготовленията им и да неутрализират техните опити за извършване на посегателства против организацията.

Специфичността в дейността на тези служби е заложена и в основната **им цел – да защитават сигурността на организацията, като използват своите специфични средства, методи и форми за превенция, разкриване, неутрализиране и подпомагане откритото пресичане на дейността на онези външни и вътрешни сили, които извършват посегателства срещу организацията. З**ащитата на външната и вътрешната сигурност са взаимносвързани и не могат да се отделят механично една от друга. Те са части от по-общото явление – дейността по защита на сигурността на организацията. Общата функция определя еднаквия характер на целите и задачите, които те осъществяват. Обвързването на тези два вида дейности се дължи и на факта, че се използва еднакви по своята същност средства, методи и форми на дейност. Тези мерки се наричат оперативно-издирвателни, а дейността по тяхното прилагане, съответно – оперативно-издирвателна.

Оперативно-издирвателната дейност, изразяваща същността на дейността на службите за сигурност на организацията, целяща защита от посегателства насочени срещу организацията, живота и здравето на нейните служители /каквито са и посегателтвата срещу личните данни/[8] .

В тази връзка са анализирани основните понятия в оперативно-издирвателната дейност: субект; обект; сили; средства; методи и форми.

Субект на оперативно-издирвателната дейност е организацията, която създава специални органи за разкриване, предотвратяване и пресичане на посегателства срещу организацията.

Обект на оперативно-издирвателната дейност са онези лица, групи, организации, сили, които извършват конкретни посегателства срещу сигурността на организацията.

Силите на оперативно-издирвателната дейност са щатните служители на службите за сигурност в организацията.

Средствата на оперативно-издирвателната дейност са доверени лица и специални разузнавателни средства.

Методите на оперативно-издирвателната дейност представляват прийомите (способи, начини), които се използват за осъществяване на основните нейни дейности.

Формите на оперативно-издирвателната дейност определят организационните рамки, в които се провежда дейността по разкриването, предотвратяването и пресичането на посегателства срещу организацията.

Интерес за всички, занимаващи се с работата по осигуряване защита на личните данни, разглеждана като елемент от сигурността на организацията, представляват видовете дейност, осъществявана от звената за сигурност в организацията, която по своята същност е контраразузнавателна дейност. Пояснено е, че тя се изразява в „наблюдение, разкриване, предотвратяване и пресичане на замислени, подготвени или осъществявани посегателства срещу фирмената сигурност, подпомагане на административно производство и превантивна дейност".

Оперативното разкриване представлява дейността на службите за сигурност по събирането, анализа и оценката на информация, която се отнася до извършващи се посегателства срещу сигурността на организацията [8]. Тази дейност изяснява кои организации, групи и лица извършват посегателства срещу фирмента сигурност и в какво конкретно се изразяват те. Така събраната и оценена информация може да се използва в няколко насоки:

- информиране ръководството на организацията за нея, като се посочат причините и условията, благоприятстващи извършването на посегателства.
- прдприемане мерки за предотвратяване и пресичане на посегателства и нарушения, нанасящи вреди на сигурността на организацията.
- предприемане мерки за подпомагане на бъдещото административно производство /в случаите на посегателства на лични данни/.
- предприемане допълнителни мерки за засилване на ефекта от превантивната дейност.

В теорията на контраразузнаването предотвратяването и пресичането се обобщят и с понятието неутрализиране. „Предотвратяването и пресичането е вид оперативно издирвателна дейност, при която с помощта на оперативни сили, средства и методи не се допуска извършването на отделни действия или продължаването на дейността от страна на дадено лице, група или организация, вършещи посегателства срещу сигурността на организацията" [7].

Когато тези оперативни мерки не дават възможност лицето да извършва отделни действия, става въпрос за предотвратяване. Когато обаче довеждат лицето до невъзможност да продължи престъпната си дейност, говорим за пресичане.

Същност на подпомагане на наказателното и административно производство.

Основна цел на всяка служба за сигурност е да разкрива, предотвратява и пресича посегателства срещу сигурността на организацията. Когато се установи по оперативен път, че дадено лице (лица) действително се е ангажирало с престъпна дейност и е консумирало състава на дадено престъпление, се поставя въпросът за откритото пресичане на тази му дейност чрез предприемане на наказателни мерки по отношение на него. Ако се установи, че то е извършило дейност, която не представлява престъпление, но е в нарушение на административни разпоредби /какъвто е случая с посегателства на лични данни/, могат да се предприемат административни или дисциплинарни мерки спрямо него. В такива случаи пред службите за сигурност възникват две задачи. Първата е да уведоми писмено органите

на досъдебното производство (прокурора) за подготовката, извършващото се или извършено престъпление и това да послужи като законен повод за започването на наказателното производство. Ако се касае за административни нарушения, трябва да се уведоми писмено фирменото ръководство с цел да вземат административноправни и дисциплинарни мерки по отношение на лицето.

Превантивната дейност представлява система от организационни, възпитателни, правни и оперативни мерки, осъществявани от органите на сигурност на организацията за недопускане извършването на посегателства срещу нейната сигурност.

Органите за сигурност в организацията имат за основна задача да разкриват, предотвратяват и пресичат престъпления и да подпомагат наказателното и административно производство. Наред с това обаче те отделят важно място на премахването на причините и условията, които ги пораждат или играят благоприятна роля за тяхното извършване, на своевременното възпиране на лица от извършване на посегателства. Важността на тази задача оформя дейността по нейното осъществяване като отделен вид, наричан превенция.

Превенция е с латински произход и означава предотвратяване. Профилактика е дума от гръцки произход и означава предпазвам. И при двата случая става въпрос за предприемане на система от конкретни мерки, насочени към отделни лица, които са склонни да се ангажират с дейност, нарушаваща сигурността на организацията. Те са възможни във фазата на формиране на решението и преди осъществяване на някой от стадиите на приготовление, опит, довършено посегателство.

Съществуват различни варианти за класифициране на превантивната дейност. Може да бъде обща, групова и индивидуална превенция. Когато се говори за превантивна дейност на службите за сигурност в организацията, обикновено тя се представя като обща и частна. Основният критерий за това деление е насочеността на превантивните мерки, т.е. дали те се отнасят за целия състав или групи на организацията или за отделни служители.

В заключение може да бъде обобщено, че посегателствата срещу лични данни се извършват от хората, и може да се приеме тезата, че „Проблема на защита на личните данни е най-напред проблем на човешките ресурси", и при наличие на правилна кадрова политика, проблема остава нерешен. Не е възможно да се подбере абсолютно верен на ръководството персонал, а освен това, могат да се допускат и случайни, неумишлени нарушения.

Общоизвестно е, че техническите средства не могат да се контролират на 100%, затова е необходимо и съчетано прилагане на оперативни мерки за противодействие, свързани с осигуряване на оперативен контрол на поведението и действията на служителите с цел проверка на тяхната лоялност **[10].**

В тази връзка за постигане на желаната надеждност при защитата на лични данни в организацията, задължително условие е съчетанието на мерки посочени в закона за защита на личните данни и наредбата **[3]** с класически оперативни мерки за противодействие **[7].**

Ефективно противодействие на посегателства срещу лични данни в организацията може да бъде постигнато, чрез задължително осъществяване на видовете контраразузнавателна дейност, изразяваща се в разкриване, предотвратяване и пресичане на замислени посегателства срещу сигурността на организацията, подмагане на административното производство и превантивна дейност.

Литература:

1. Дворянкин, С. Компьютерные технологии обеспечения безопасности оперативных аудиоданных в условиях информационно-технического противодействия. Дисертация. [онлайн]. Москва: 2000. http://www.referun.com/n/kompyuternye-tehnologii-obespecheniya-bezopasnosti-operativnyh-au-diodannyh-v-usloviyah-informatsionno-tehnicheskogo-protivodejstviya. [прегледан 20.04.2013].

2. Станев, С, С. Железов. Компютърна и мрежова сигурност. Шумен: Университетско издателство, 2002.

3. Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. [прегледано 20.04.2013]. http://www.sarc- wv.com/news/press_releases/2013/steganography_insider_threat.aspx.

4. Сандев, Г. Сигурност на организациите. Университетско издателство „Еп. Константин Преславски" Шумен. 2012. ISBN 978-954-577-621-2.

5. Закон за защита на личните данни. http://lex.bg/laws/ldoc/2135426048. [онлайн]. [прегледано 10.04.2013].

6. Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. [онлайн]. [прегледан 2.04.2013]. http://ciela.net/FreeStateGazette/ OpenDocument.aspx?id = 2135836487.

7. Асенов, Кипров. Теория на контраразузнаването. София : Труд, 2002.

8. Асенов. Основи на оперативно – издирвателната дейност. ВСУ „Черноризец Храбър" . ISBN 978-954-715-432-2, 2009.

ПРОБЛЕМИ НА СТРАТЕГИЧЕСКИЯ АНАЛИЗ

Красимир М. Марков

Шуменски университет „Еп. Константин Преславски"
Катедра „Психология"

PROBLEMS OF STRATEGIC ANALYSIS

Krasimir M. Markov

ABSTRACT: *The problems of strategic analysis in terms of the organization in the market environment and offer models of analysis.*

KEY WORDS: *organization, strategic analysis models.*

Стратегическият анализ на всяка една организация е един от основните елементи на процедурата за формиране на стратегическия план за развитието на организацията. Обикновено в литературата под стратегически анализ разбираме етап на предпланови изследвания, в който системно се анализират факторите на околната среда (външните възможности) и ресурсния потенциал на организацията (вътреш-

ните възможности), за определяне на ситуационното състояние на организацията и определяне на условията за нейното по-нататъшно успешно развитие. Това означава, че в етапа на анализа се създава необходимата информационна база позволяваща най-ефективно да се проведе процеса на определяне на целите и избора на алтернативите. Съвременните учени от Западна Европа и САЩ отделят голямо внимание на управлението на стратегическия анализ, който се разглежда като един от основните фундаментални етапи на планирането. Като правило стратегическия анализ на една организация се провежда в четири раздела и включва: анализ на производствената дейност; анализ на инвестиционната дейност; анализ на социалното развитие на организацията; финансови показатели за дейността. На тяхна основа се изготвят изводи и предложения. Видимо, че при такъв подход основния акцент се поставя върху изследването на ресурсния потенциал на организацията. Влиянието на външната среда се отчита косвено. Такава идея за разбирането на процедурата на стратегическия анализ има своите причини: **на първо място,** наследството за България от идеите за планиране на дейността на основните организации в условията на директно управление. В условията на пазарната икономика такова разбиране и остарели нагласи влияят доста отрицателно върху развитието на организацията, но видимо причината е чисто психологическия момент, в много от организациите голяма част от кадрите са запазили старото си мислене и подхождат по инерция със стари, проверени с годините подходи, които макар и, така или иначе донякъде „осъвременени" в опита да бъдат адаптирани към новите условия, видимо не са адекватни на съвременната ситуация на управление на организациите; **на второ място**, независимо, че в България вече повече от 20 години се опитваме да установим механизмите на пазарната икономика, то пазарната инфраструктура все още се намира в стадий на формиране (в много отрасли, включително и в енергетиката съществува липса на конкуренция, основните играчи на пазара сключват картелни споразумения, което така или иначе, не формира истинска пазарна среда и най-малкото водят до формиране на цена, която не се контролира от пазара). Освен това икономическата нестабилност на националната икономика в последните няколко години, в никакъв случай не способства за определяне на ясни параметри и точно изработване на прогнозни планове, разчети, анализи и др., което видимо затруднява организациите при провеждането на стратегическия анализ.

Стратегическия анализ на дейността на организацията изисква да се приложи подход, както в методологически, така и в практически план. Обикновено при методологическия подход се прилагат следните принципи:

- анализът на организацията се състои от два самостоятелни етапа – анализ на външната среда и анализ на ресурсите или вътрешната среда. Тези два етапа са взаимосвързани, доколкото резултатите от анализа представляват синтез от изводите, от тези два етапа;
- специалистите в областта на стратегическото управление предлагат подход, при който се поставя задачата за построяване на „идеален модел", което позволява от една страна ръководството на организацията да представи стратегическия анализ като системен, и от друга страна да предявят изисквания към пазарната инфраструктура за предоставяне на необходимите показатели нужни за провеждането на аналитични изследвания по проблемите на функциониране на организацията;

- процедурата на стратегическия анализ на всеки етап изисква по-нататъшно дообработване, от гледна точка на внедряване в практиката на методическите препоръки установени на етапа на анализа.

Първи основен елемент на анализа, както подчертахме се явява **анализа на външната делова околна среда**. Под външна делова околна среда разбираме съвкупността от социално, еколого, икономически фактори, въздействащи на организацията и оказващи влияние върху ефективността на неговото функциониране [2]. Когато описваме природата на деловата околна среда, трябва да обърнем внимание на два момента, които в литературата [2, 4, 5] се наричат динамизъм и сложност. Динамизмът на околната среда се определя като функция на честотата, с която протичат измененията във вътрешните процеси на съответстващите елементи (степен на различие вътре във всяко изменение и степен на различие в общата схема). Сложността произхожда от факта, че за околната среда е характерно наличието на голямо количество променливи, създаващи неопределеност във стратегически план. За организация действаща в условията на пазарната икономика, можем да изброим: наличието на диверсификация на влиянието на околната среда (влияние на промените в законодателството, потребителските вкусове и др.); недостатъчно знание за външната делова среда. Най-общо анализите показват, че съществуват минимум 12 променливи влияещи върху динамизма на средата и минимум 9 елемента определящи сложността на околната среда.

Променливи определящи динамизма [2]:

- Степен на промяна на цените на доставчиците;
- Степен на промяна на цените на конкурентите;
- Степен на промяна в пазара на труда;
- Степен на промяна в търсенето на дадения продукт;
- Степен на изменение възможностите за финансиране;
- Степен на промяна в методите на конкуренция;
- Степен на промяна в стойността на капитала;
- Степен на промени в политиката по регулиране на пазара;
- Ниво на продажбата, при излизане на пазара с нов продукт;
- Ниво на активност, като резултат на много конкуренти;
- Степен на промени в резултат на отклонение от нормите на жизнения цикъл на стоката;
- Степен на промени в резултат на влияние на нова технология.

Елементи определящи сложността на околната среда[2, 4]:

- Количество различни доставчици на една категория материали в определена пазарна ниша;
- Ниво на географска концентрация и дисперсия на доставчиците в определен пазарен сектор;
- Ниво на географска концентрация и дисперсия на пазара на труда в определен сектор;
- Ниво на географска концентрация и дисперсия на отрасловите продажби в определен пазарен сектор;
- Ниво на продуктова диференциация по сегментите на отраслите вътре в определен пазарен сектор;

- Ниво на географска концентрация и дисперсия на компаниите конкуренти в определен пазарен сектор;
- Ниво на социокултурна диверсификация в пазарната ниша;
- Ниво на диверсификация на всички форми на бизнеса в пазарната ниша;
- Ниво на технологична диверсификация, вътре в отрасъла.

Анализът на динамизма и сложността на външната делова околна среда е много важен за избора на методи на изследване. Очевидно е, че с увеличаването на динамизма и сложността се изменя ролята на формализираните методи за прогнозиране и се повишава ролята на неформалните експертни оценки.

Анализ на общата околна среда

Анализът на общата околна среда включва в себе си икономическите, социополитическите и технологичните прогнози (система PEST) за определяне дългосрочните възможности на организациите в условията на прогнозируеми проблеми в средата.

Анализът на икономическата сфера е първия най-важен компонент при анализа на общата околна среда. В себе си той включва прогнози за изменението на икономиката, които се изразяват в показателят за инфлацията, нивото на заетост, циклите на делова активност, паричното обръщение и т.н.. Най-общия показател използван в такава прогноза, е брутния национален продукт. За една организация, особеното при иконическия анализ е да се даде отговор на въпроса, на кой етап от цикъла на делова активност се намира националната икономика в дадения момент и кога ще настъпи следващия етап от цикъла? Данните от характеристиката на цикъла и данните от развитието на предприятието помагат да се избере най-ефективната стратегия за развитие. В този смисъл под цикъл на деловата активност разбираме дъното на икономическия цикъл, разширението, пика и спада на деловата активност. Този показател е предмет на много сериозно изучаване и обсъждане от западните икономисти, като важно при прогнозата на този цикъл е не толкова определянето на дължината на етапа във времето и степента на неговото изменение, колкото отчитането на върха и спада на икономическия цикъл. Това се обяснява с факта, че всеки етап на деловата активност се характеризира с особености на поведението на икономиката, които са характерни само за него.

Социополитическа среда – естествено е, че политическата стабилност на държавата е един от факторите, позволяващ да се намали риска в развитието на организацията в рамките на приемането на стратегическите решения. Освен прогнозата за развитието на политическата обстановка, организацията е необходимо да получи информация за следните области на държавна дейност: социална защита на населението; външна търговия; политика на ценообразуването; политика в сферата на екологията; здравословни и безопасни условия на труд и ограничаването на производството на един или друг продукт за сметка на контрола на неговото качество. Освен тези показатели в последно време, в процеса на стратегическия анализ започват да се отчитат и фактори от социокултурен характер: демографски признаци на населението; разпределение на населението по ниво на доходи; социална мобилност в обществото; изменение в начина на живот, включително националните традиции и обичаи; отношение към работата и почивката; ниво на образование на населението, и ниво на потребление на стоки и услуги.

Технологична среда – т я се анализира с помощта на научнотехнически прогнози, които на всеки един етап решават три основни цели [2]:

1. прогнозират се научнотехническите тенденции в науките, които се отнасят към дадената сфера на дейност на организацията.

2. определя се стратегията на организацията в областта на научноизследователската дейност.

3. съпоставят се собствените възможности с възможностите на конкурентите от гледна точка на техническото ниво на производството или научнотехническото ниво на извършваната дейност.

Анализ на специфичната околна среда – обикновено се асоциира с анализа на пазара. Такъв анализ включва: производствени прогнози – те съдържат информация за перспективите в повишаването и понижаването на производството, както и основни параметри на развитието, като доходност, капиталовложение, динамика на основните производствени фондове и др.; структурни промени – прогнозират се с оглед намаляне на неопределеността при вземане на стратегическите решения; анализ на конкуренцията – включва структурен анализ на конкурентното обкръжение, определяне на конкурентните позиции и анализ на структурата.

В структурния анализ на конкурентното обкръжение се определя по методика на американския икономист М. Портър [3]. Той определя пет сили на конкуренцията, които определят нивото на печалба в отрасъла:

– Заплаха от поява в отрасъла на нови конкуренти;

– Способност на вашите потребители да постигат занижаване на цената;

– Способност на вашите доставчици да постигат повишаване на цената на тяхната продукция;

– Заплаха от появата на пазара на продукти и услуги, които могат да заменят вашите;

– Степен на ожесточеност на борбата между съществуващите в отрасъла конкуренти.

Определяне на конкурентната позиция – обикновено под това определение се разбира анализа на стратегическите групи. Изхожда се от положението, че понятието за конкуренция на предприятията от един отрасъл представлява доста опростено разбиране, тъй като самите граници на отрасъла са много размити. М. Портър [3] предлага промеждутъчно ниво между фирмата и отрасъла, което позволява да се проведе първичен анализ от гледна точка на разбирането на съдържанието на конкуренцията и структурата на конкурентите. Същността на анализа на стратегическите групи се заключава в обединяване на организациите в групи с еднакви стратегически характеристики и конкуриращи се на една и съща основа. Този процес се разбира в динамика, защото и ресурсната база и стратегическите цели могат съществено да се променят, което от своя страна означава, че организацията може да преминава от една стратегическа група в друга и по този начин да променя своето конкурентно обкръжение. Джонсън и Шолес [цит. по 2] определят следните групи показатели, които се използват при анализа на стратегическите групи:

– Ниво на продуктовото разнообразие;
– Ниво на географския обхват;
– Брой на определените пазарни сегменти;
– Използвани канали за разпределение;
– Брой търговски марки;
– Условия в областта на маркетинга;
– Ниво на интеграция;

- Качество на стоките и услугите;
- Лидерство в областта на технологията;
- Възможности в областта на научноизследователската дейност;
- Позиции в областта на издръжките;
- Използване на производствените мощности;
- Политика в областта на ценообразуването;
- Структура на собствеността;
- Размер на организацията.

Гринли [цит. по 2] привежда абстрактен пример, при който разделя организациите на три стратегически групи, изхождайки от два признака: корпоративен имидж и брой произвеждани продукти. Организации от група А – произвеждат множество продукти, способни са да удовлетворят голям спектър от потребностите на населението, при което полагат своите взаимоотношения с потребителите на дългосрочна основа и затова отделят голямо внимание на поддържането на висок корпоративен имидж и завоюване на доверието на потребителите. Организации от група Б се конкурират на тесен сегмент от пазара, където се продава един продукт. Ограниченото количество потребители и техния постоянен състав не изискват от фирмите големи средства за поддръжка и обезпечаване на висок корпоративен имидж. Затова при формирането на стратегия, на този аспект не се отделя внимание. Организациите от група В, както и при група А са основани на широк асортимент на продукция за различни сегменти на пазара, но тук в качеството на основен елемент за достигане на своите цели, прилагат стандартни тактически прийоми на маркетинга, а не създаване на висок корпоративен имидж.

М. Портър [3] е направил няколко стратегически извода, изхождайки от анализа на стратегическите групи: първият извод се отнася до възможностите фирмата да премине от една стратегическа група в друга, при това преодолявайки т.нар. бариери на мобилността включващи в себе си такива понятия като икономия на мащаба на производството, продуктовата диференциация, технологията и капитала. Вторият извод се отнася до случаите, когато не всички фирми могат да бъдат отнесени достатъно точно към стратегическите групи. В такъв случай по-скоро е необходимо да се променят признаците на класификация. Третият извод – определянето на стратегическите групи може да се разглежда като основа за прогнози на потенциалните изменения в конкурентната среда и следователно за корекции на конкурентните стратегии.

Анализ на ресурсния потенциал на организацията

Анализът на вътрешните възможности на организацията е втория основен етап на стратегическия анализ. Изследвайки производствените фактори, както в съвкупност, така и поотделно определяме възможността на организацията да функционира ефективно. В повечето случаи западните методики за оценка на вътрешните възможности се базират на системата на ценностите, разработена от М. Портър [3] Той обосновава принципите на създаването на конкурентни преимущества на предприятието, които се формират по пътя на създаването на свои ценности на всеки етап. Ако се разработва продукт, това означава да се направи сравнителен анализ на неговите потребителски свойства, които се създават на различните етапи от неговата разработка, производство, маркетинг и продажба, в съпоставка с разходите направени за достигане на тези ценности.

Обикновено се определят пет основни етапа на дейност в организацията, при които се създават главните ценности:

– Материалнотехническо осигуряване;
– Изготвяне на продукцията;
– Складиране, доставка и разпределение на продукцията;
– Маркетинг и продажба;
– Гаранционно обслужване.

Към тях можем да прибавим като предмет на анализа общите спомагателни видове дейност, в които се включва:

– Управленската структура;
– Управлението на персонала;
– Технологичното осигуряване на производството;
– Осигуряване на материали вътре в организацията.

На тази методологическа основа се провежда анализа на потенциала на предприятието в следната схема:

1. Оценка на ресурсите и ефективността на предприятието, в която влизат:
– физически ресурси;
– човешки ресурси;
– финансови ресурси;
– нематериални активи.
2. Финансов анализ на дейността на организацията, определя финансовите възможности при създаването на основните фондове, повишаването на производителността и др.
3. Сравнителен анализ на ресурсния потенциал на предприятието, включва:
– исторически анализ на предприятието;
– сравнение с отрасловите нормативи.
4. Организация на процедурите за оценка на ресурсния потенциал на организацията, разглежда се като система. От една страна трябва да бъде комплексна, т.е. да осигурява пълното събиране и обработване на информацията, от друга страна, най-добрия вариант е да се съчетае тази функция с функцията на системата за контрол.

В заключение можем да кажем, че към момента да се определят два подхода при анализа на ресурсния потенциал на организацията. Първият, който се основава на системата за ценностите на М. Портър, която описахме и втория, който представлява традиционен анализ на стопанската дейност, който се свежда обикновено до финансов анализ. Авторите [2] изследващи проблема посочват, че нито единия, нито другия подход могат да бъдат признати за ефективни в съвременни условия, доколкото от една страна са ориентирани към други методологически принципи и информационна база, а от друга повече отговарят на целите на тактическото, а не на стратегическото управление.

Литература:

1. Виханский О. С. Стратегическое управление. М., 1995.
2. Петров, А. Н. и др., Стратегический менеджмент. Питер СПб. 2005
3. Портер, М. Международная конкуренция. МО, М. 1993

4. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
5. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
6. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
7. Mintzberg H. Power in and around organizations. N.Y., 1983.
8. Robey P., Sales A. Designing organizations. Burr, 1996.
9. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
10. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical pproach. N.Y., 1989.

МЕТОДИ НА СТРАТЕГИЧЕСКОТО ПЛАНИРАНЕ

Красимир М. Марков

Шуменски университет „Еп. Константин Преславски”
Катедра „Психология”

METHODS OF STRATEGIC PLANNING

Krasimir M. Markov

ABSTRACT: *Discuss the methods of strategic management and analyzed their feasibility.*

KEY WORDS: *organization, management, methods.*

В условията на кризата, обхванала света, се наблюдава нарастваща нестабилност на околната външна делова среда, което изисква организациите да разработват все по-сложни и детайлни системи за управление. Това от своя страна налага и детайлизация при разработване на целите и задачите на организацията. В стратегическия мениджмънт е ясно, че при разработването на идеите на стратегическото планиране и управлението, възможността за преход към решаване на нови задачи се определя от това, доколко организацията е способна да функционира в новите променени условия. В такива моменти би трябвало да се използват подходи, като: управление на основата на йерархирането на задачите; управление по силни и слаби сигнали; управление в условията на стратегическа неочакваност; управление на основата на стратегическия избор и др. Всички тези подходи заслужават своето внимание и необходимостта от разглеждането им.

Управление въз основата на йерархирането на задачите, нарича се още планиране на своевременни решения и представлява процес засягащ всички нива на организацията, който продължава месеци, същевременно това е един доста сложен за организацията процес, тъй като в локалните организации не съществуват сили и възможности за самостоятелно справяне с предизвикателствата на външната среда. Независимо от това, можем да каже, че в рамките на такова управление една организация би трябвало да изпълни следните мероприятия [2]:

– Провежда се постоянно отчитане на тенденциите на измененията на външната среда;

– Осъществява се анализ на изследваните тенденции за изменение и се прави оценка за срочните решения;

– Висшето ръководство разглежда получените резултати на анализа на външните и вътрешните тенденции и от своя страна ги ранжира в следните категории: най-спешни и важни задачи, изискващи незабавно разглеждане и реакция; важни задачи със среден срок на изпълнение, които могат да бъдат решени в по-късен период; важни, но не спешни задачи, изискващи постоянен контрол; задачи, които не са съществени и не заслужават по-нататъшно разглеждане;

– Висшето ръководство на организацията контролира решенията, които се вземат в нейните подразделения и ги оценява от гледна точка на възможните стратегически и тактически последствия;

– Ръководството е необходимо постоянно да разглежда и да обновява списъка на възникващите проблеми, като ги ранжира по приоритети.

Управлението по силни и слаби сигнали [2] се налага от факта, че в хода на наблюдението на външната среда може да възникнат проблеми в информационното осигуряване. Едни от тези проблеми са очевидни, конкретни, което означава, че дадената организация може да ги оцени и да вземе мерки за тяхното решаване в условията на понижена сложност. Такива проблеми наричаме определяни по силни сигнали.

Други проблеми, които наричаме определяни по слаби сигнали се базират на ранни или неточни признаци за настъпване на някакви събития във външната или вътрешната среда на организацията. При тях не може с увереност да се предскаже кога ще възникнат и каква форма ще приемат. Но с наближаването на периода на тяхното настъпване, те показват тенденция за определено време да станат по-ясни и силни, което да ги превърне в определяни по силни сигнали. Ако нивото на нестабилност е незначително организацията може да си позволи изчакване на посилен сигнал, тъй като има време за вземане на определено управленско решение, когато момента за това назрее. Но в случай, че значението на нестабилността очевидно нараства и положението започва бързо да се променя, ако организацията все очаква силен сигнал, може да се окаже, че или ще закъснее с решението, или ще се откаже при възможност да го приеме в този момент, когато интересите й са поставени под удар. В този случай възниква необходимостта да се подготвят решенията още тогава, когато за настъпващите събития има много слаби сигнали.

Управление в условията на стратегическа неочакваност. Независимо, че сяка една организация се стреми да следи за проблемите, които възникват във външната и вътрешната среда, някои от проблемите се изплъзват от наблюдението и се превръщат в стратегическа неочакваност или стратегическа изненада. Това се случва когато проблемите [2]:

– Възникват неочаквано, внезапно;

– Поставят нови задачи, които не съответстват на миналия опит на организацията;

– Невъзможността организацията да приеме съответните контрамерки води или до сериозни финансови загуби, или до влошаване на възможността за осигуряване на печалба;

– Трябва да бъдат приети срочни контрамерки, но съществуващите в организацията ред и условия не позволяват това да се случи.

При условие, че една организация предполага или оценя нивото на външна нестабилност като съществена, то тя трябва да подготви система от извънредни мерки за реакция в условия на стратегическа неочакваност. Такава система има няколко характерни черти [2]:

– В условията на стратегическа неочакваност трябва да се задейства мрежата от връзки и контакти, която организацията би трябвало да има за условията на извънредни ситуации, което означава, че връзките между отделните подразделения на организацията започват да се пресичат, информацията по-бързо се филтрира и по-бързо се предава до всички звена;

– При стратегическата неочакваност ръководството трябва да преразпредели задълженията си, като общо взето се очертават три групи в ръководството: първата група се занимава с контрола и съхраняването на здрав социалнопсихологически климат в организацията; втората извършва обичайната си дейност, като се стреми да работи с минимално ниво на пропуски; третата се занимава с разработването и приемането на извънредни мерки;

– При разработването и прилагането на извънредните мерки се налага организацията да въведе в действие, т.нар. оперативни групи;

– Оперативните групи и връзките между тях трябва да са създадени в организацията и да са проиграли определени неочаквани събития.

В литературата посветена на стратегическото управление [4, 7, 8, 9] болшинството автори правят извод, затова че отделни хора включително и цели организации не могат да се справят с проблеми в сложността на които превишава някакво определено ниво (концепция за ограничената рационалност), не са в състояние да разберат какво се случва във външната среда и следователно не могат да осъществяват адекватна стратегия на организацията. Стига се даже до извода, че сега сложността на външната среда е превишила значително възможността за разбиране от тези, които отговарят за ръководството й, а мащабите и сложността на дейността на някои организации вече са превишили всички възможности на управляващите. За да бъде решен този парадокс е необходимо да се понижи сложността на проблемите, както на ниво общество, така и на ниво организация.

Управление чрез стратегически избор. В осъществяване на процеса на стратегическото планиране ръководството на организацията се сблъсква с редица проблеми определяни от нейното положение в обществото и на пазара. Тези проблеми опират до следните въпроси:

– Какви направления от дейността на организацията трябва да се свият?;

– Какви направления от дейността на организацията трябва да се разширят?;

– Можем ли да преминем в друг бизнес?.

За решаването на тези въпроси се използва, т.нар. матричен анализ, като за най-удобен инструмент авторите занимаващите се с проблема [4, 7, 8, 9] сочат матрицата за баланс на жизнените цикли.

Вътрешната гъвкавост на организацията се разрешава по пътя на вътрешно организационна координация, при която материалните, професионалните и управленските ресурси на организацията могат леко и своевременно да се преразпределят от една форма в друга. Втори момент при управлението чрез стратегическия избор е определяне на стратегическата уязвимост на организацията, за определянето на която трябва да се проведе анализ на въздействието на външната за организацията среда, при което трябва да се определят най-вероятните и съществените за

организацията неочаквaности. Третият момент се определя като синергизъм и вътрешни взаимовръзки, в случая за организацията основна задача се явява определянето на стратегическата сегментация, както и решаването на въпроса за взаимодействието на различните звена и центрове в организацията.

Управление чрез стратегически задачи. Стратегическите задачи представляват бъдещи събития, както вътре, така и вън от организацията, които могат силно да повлияят на нейната способност за постигане на поставените цели. То е свързано с появата във външната среда на определени възможности, използването на които може да донесе изгода, така и на определени заплахи, които могат до донесат определени вреди.

В тази връзка е необходимо да се формира система за управление по стратегически задачи, разбирана като последователни мероприятия за ранно откриване на неочаквани изменения вътре и вън в организацията, и като мероприятия за бързо реагиране.

Мерки за своевременно определяне на измененията:

– Решаването на стратегическите задачи трябва да протича непрекъснато, което включва и периодичното преразглеждане и коригирането им;

– Непрекъснато отчитане на външните и вътрешните проблеми в промеждутъка между корекциите.

Мерки за бързо реагиране:

– Пълномощията за управлението на системите се възлага така, че да може оперативно да се вземат мерки за бързо реагиране;

– Системата за реагиране може понякога да влезе в разрез със съществуващата в организацията йерархия и със съществуващите принципи на управление. Това налага да се създават експертни групи, които да се разпореждат с определени ресурси и имат определени права;

– Системата за управление чрез стратегически задачи подразбира в себе си решението, коригирането и преразглеждането на стратегическите задачи, но не включва планиране на реакцията, затова и планирането се осъществява едновременно с реакцията за система от мерки.

Управление в условията на спонтанни изменения. Към настоящия момент спонтанните изменения стават все по-чести и водят след себе си нежелателни последствия за организацията, поради което и управлението на преходните процеси става неотделна част от стратегическото управление. В съвременната литература [2, 4, 7, 8, 9] се определят четири методически подхода за реагиране при спонтанни изменения:

– Принудителен метод за провеждане на измененията – самото име означава, че се прилага сила, за да се преодолее съпротивлението. Самото принудително изменение е достатъчно дълъг процес, но дава определено преимущество във времето за стратегическо реагиране, т.е., този метод е оправдан, когато се изисква незабавна реакция на протичащите изменения. Същевременно при използването му могат да се очертаят определени трудности, заключаващи се: неспособност да се предвидят източниците и силата на съпротива; невъзможност да се открие първопричината за съпротива; неразбиране от необходимостта за създаване на нов управленски потенциал; снижаване на качеството на стратегическите решения;

– Метод на адаптивните изменения – представлява осъществяване на постепенни, незначителни промени, които продължително време оказват влияние

върху основните критерии на организацията. Авторите определят този метод като организационна адаптация. Обикновено той протича по метода на пробата и грешката, и се явява реакция на протичащите организационни изменения. Дотолкова, доколкото измененията протичат дълго време, то възникващите конфликти се решават по компромисен път;

– Управление в кризисни ситуации – осъществява се при недостиг на време за реагиране на заплахи съществено влошаващи положението в организацията. Когато нараства недостига на време, основата задача на ръководството става борбата със съпротивите. За тези случаи когато възникването на кризи е неизбежно управленския персонал е необходимо да приеме следните мерки: да убеди висшето ръководство да приеме предохранителни мерки; да изработи мерки за бързо реагиране при настъпването на кризата; да прогнозира бъдещата ситуация и да разработи няколко алтернативни варианта за реакция в различни случаи;

– Управление на съпротивите - това е промеждутъчен метод реализиран в срокове диктувани от развитието на събитията във външната среда. Прилага се в случай, когато има време за реакция. В нормални условия той се счита за достатъчно ефективен и включва в себе си следната последователност на действието: създаване на база от предпоставки осигуряваща баланс между действащите сили и силите на съпротивата, което осигурява възможността да започне осъществяването на измененията; разработка на модулен план за измененията. Модулнат структура на планирането включва в себе си използването на стратегически анализ, избор на последователност от модули, обучение в началото на всеки модул и вземане решения в края на всеки; осигуряване на внедряването на плана.

Методът на управление на съпротивите има редица положителни моменти заключаващи се в: разпределение на решенията по време позволява равномерно да се разпредели натовареността на персонала; затова помага и ранното внедряване на програмите; внедряването върви паралелно с планирането, което осигурява обратна връзка; ранното внедряване на стратегическите решения дава възможност за контрол на процеса на стратегическото планиране.

Същевременно този метод има и недостатъци определяни като: допълнително натоварване на управленския и работния персонал; повишена сложност на този процес.

В заключение можем да кажем, че организациите могат да осъществяват спонтанните изменения в следната последователност [2] :

– Изясняване различията между управленската компетентност и нивото, което е необходимо за реализация и поддръжка на измененията;

– Определяне на времето за въздействие на измененията върху организацията, за да могат да се предприемат мерки по тяхното отстраняване, изхождайки от скоростта на разпространение на измененията и вероятната динамика на конкуренцията;

– На базата на проведения анализ и сравняване на силите на организацията, и силите на съпротива се определя минималното и максималното съпротивление;

– Определяне на времето за предприемане на ответните мерки и времето за адаптивната реакция;

– Сравнение между максималното и минималното съпротивление, с оглед определяне силите и средствата за прилагане на адаптивния метод;

– При недостатъчни сили в организацията и отчитане на възможността от настъпване на криза, да се провеждат мероприятия предвидени за кризисна ситуация;

– Ако силите са недостатъчни, но ситуация все още не се определя като критична, да се приложат мерки за достигане на необходимото минимално ниво осигуряващо внедряването на измененията.

Литература:

1. Виханский О. С. Стратегическое управление. М., 1995.
2. Петров, А. Н. и др., Стратегический менеджмент. Питер СПб. 2005
3. Портер, М. Международная конкуренция. МО, М. 1993
4. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
5. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
6. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
7. Chang Y. N., Campo-Flores F. Business Policy and Strategy, Text and Cases. Good year Publishing Company. — Santa Monica, 1980.
8. Greenly G. E. Strategic Management. — Prentice Hall, London, 1989.
9. Jonson G., Scholes K. Exploring Corporate Strategy. An Aproach to Strategic Management. — Pitman, London, 1992.
10. Mintzberg H. Power in and around organizations. N.Y., 1983.
11. Robey P., Sales A. Designing organizations. Burr, 1996.
12. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
13. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical pproach. N.Y., 1989.

ОПРЕДЕЛЯНЕ НА ЦЕЛИТЕ КАТО ЕТАП НА СТРАТЕГИЧЕСКОТО ПЛАНИРАНЕ

Красимир М. Марков

Шуменски университет „Еп. Константин Преславски”
Катедра „Психология”

DETERMINATION OF PURPOSES AS A STAGE OF STRATEGIC PLANNING

Krasimir M. Markov

ABSTRACT: *Discussed are the possible ways to define the objectives and stage of strategic planning.*

KEY WORDS: *organization, goals, planning*

След стратегическия анализ определянето на целите, на дадена организация е втората важна стъпка от етапа на стратегическото планиране, но понятието цели на

организацията съвсем не е еднозначно, както би могло да се предполага. Литературата занимаваща се с целеполагането предлага голямо количество интерпретации на проблема, при които понятието цел се съотнася с различни други променливи. Някои сравняват целта и политиката на организацията (Янг и Кампо-Флорес), други сравняват целта с плановите задачи (Акофф) [2]. Независимо кой от предложените варианти ще изберем ясно е, че при всички тях общо се явява определянето на целите. При това определяне би следвало да отчетем два основни момента: първо – целта характеризира насоката на развитието на организацията за определен период от време, и второ – в целта се залага желаното бъдещо състояние на дадената организаци, което би могло да бъде достигнато след определен период от време. Това по същество са две ключови характеристики – качествена и количествена.

Самият процес на определянето на целите включва в себе си два етапа, първия от които е определяне на мисията на предприятието. Независимо, че в България във военните организации проблемът за определяне на мисиите им беше детерминират след влизането в НАТО, то за цивилните организации този въпрос още не е ясен.

Под мисия на организацията разбираме отделни твърдения, представени във вид на устав на организацията, които определят нейната икономическа, социална и управленска философия. Формулирането точно на мисията на организацията съдейства за подобряване на качествата на стратегическите решения. Затова има няколко причини [2]:

– Мисията на организацията под формата на делова философия в повечето случаи се формулира на базата на опита на основателя на организацията и на последващите го ръководители, което означава, че в този смисъл тя е своеобразно излагане на предишния опит;

– Мисията на организацията в повечето от развитите страни включва в себе си, т.нар. социална отговорност, което прави организацията по-социално ориентирана;

– Мисията на организацията точно трябва да показва къде да бъдат насочени усилията на хората от организацията, смисъла на тези усилия, което само по себе си повишава и чувството за съпричастност на персонала с организацията;

– В условията на стратегически избор, мисията на организацията се явява един от елементите, позволяващ да се вземе компромисно решение;

– Мисията на предприятието позволява, то по-добре да се ориентира в условията на пазара.

Като правило мисията на една организация включва в себе си различни елементи:

– Първи елемент – основни насоки, който включва в себе си основните насоки в системата продукт-услуга, основните насоки в системата потребител-пазар, и основните насоки на технологичните усилия;

– Втори елемент – ръст и печалба, явява се най-важния за организацията. Икономическият ръст на всяка една организация й осигурява съхраняване на определени позиции на пазара, а осигуряването на печалба всъщност осигурява устойчивото развитие на организацията;

– Трети елемент – ниво и структура на предприемачеството, това е елемент, който се определя в повечето случаи от собствениците на организацията или нейното висше ръководство. Под ниво на предприемачество разбираме състоянието на дейност – икономическа, производствена и т.н. в организацията, което се счита за приоритетно за нея, за определен период от време;

– Четвърти елемент – социална отговорност, някои автори като Денис и Бломстром [2], определят социалната отговорност като „задължение на висшето ръководство да действа по такъв начин, че да защитава и да повишава благосъстоянието на обществото като цяло, съобразявайки се при това със своите собствени интереси.

Янг и Кампо-Флорес предлагат собствена класификация на сферата на социалната отговорност [7]:

– Повишаване на жизненото равнище на населението, осъществява се от организации и фирми имащи много свободни средства, може да се осъществява по много начини, примерно със създаване на много работни места, финансиране на научни проекти, меценатство в областта на културата и спорта, или подпомагане на социално слаби граждани;

– Социална защита на хората от организацията, това направление е особено важно, тъй като освен социален имидж на организацията, е предпоставка за повишаване на производителността на труда, а следователно и за повишаване на ефективността на организацията;

– Самоконтрол за своите действия на пазара, което включва няколко елемента, като контрол за качеството на произвеждана продукция, за достъпността й от ценова гледна точка, водене на цивилизована конкурентна борба и т.н.

Както счита Гринли (цит. по 8) организацията не декларира своята социална отговорност, за нея говори, това, което тя прави в тази област.

Освен мисията в организацията, при изработването на целите своя отпечатък налагат и ценностите на висшето ръководство, тези ценности могат да бъдат материални или нематериални, и могат да бъдат определени като знания, мнения и убеждения, определящи предпочитания избор на поведение на определените ръководители. Определящо в случая се явява опита, който те имат. Джонсън и Шолес [9] определят три фактора, които детерминират ценностите на висшето ръководство в процеса на стратегическото управление:

– Външно влияние на ценностите на обществото;

– Видът на бизнеса от гледна точка на пазарната ситуация и важността на произвеждания продукт, от гледна точка на удовлетворяване на потребностите на обществото;

– Култура на фирмата, включваща историята на компанията, упражнявания стил на управление и наличната в организацията форма на планиране и контрол.

Процесът на определяне на целите на предприятието се намира в тясна връзка и с процеса на формиране и развитие на организационните подходи. Дотолкова, доколкото тези два процеса оказват съществено влияние един върху друг, те би трябвало да се разглеждат в единство. Най-общо под организационна култура разбираме, системата от ценности, обичаи, традиции, норми и правила на поведение, установени или формиращи се в организацията, с цел на нейната вътрешна интеграция и адаптация към условията на постоянно променящата се външна среда. Организационната култура изпълнява няколко основни функции:

– Координация на дейността, установява се с помощта на уточнени процедури и правила на поведение;

– Мотивация, осъществявана по пътя на разясняване на членовете на организацията на смисъла на дейността, която те вършат;

– Профилиране, позволяващо да се определят принципните разлики от другите организации;

– Привличане на кадри, по пътя на агитация за преимуществото на собствената организация пред другите.

Формирането на организационна култура е свързано с комуникационната политика и комуникационното поведение на организацията, които би трябвало да се разглеждат като важни стратегически инструменти в областта на рекламата, връзките с обществеността, маркетинга и др.

Целите на развитието на предприятието представляват сами по себе си насоки, по които би следвало да се осъществява дейността на първичното звено. От една страна това се явява качествена характеристика на целта, а от друга, целта би трябвало да определи желаното състояние на системата, което ще се постигне селд определено време, което се явява количествена страна на проблема. Формулирането на целите е логически процес, при който може преди всичко да се систематизира процеса на целеполагането, а не да се формализира. Това формулиране зависи от опита, а донякъде и от интуицията на висшето ръководство на организацията. Това означава, че не може да се напише рецепта за всички случаи, при които трябва да се формулират цели. Затова и повечето автори предлагат преди всичко принципни подходи към процеса на целеполагането. Целите на една организация са различни по обхват, те биха могли да се разгледат като йерархична система, аналогична на системата на планирането, общо взето, авторите са единодушни, че целите могат да бъдат разделени на две групи: група цели на системата и група цели на участниците. В реалната практика тези две групи цели, в своето съчетание, образуват пълната йерархия на целите в организацията. Предлагат се ред общи характеристики, които би следвало да се отчитат при построяване на пълната йерархия на целите на развитието на организацията [2]:

– Целта на по-ниско ниво в йерархията, трябва да бъде положена под целта от по-високо ниво;

– Целта на по-високо ниво, следва да бъде разчитана за по-продължителен период от време;

– Целите на отделните подразделения на организацията, следва да бъдат съпоставими с делегираните властови пълномощия на техните ръководители;

– Целите могат да бъдат качествени и да нямат количествена оценка, което в никакъв случай не снижава тяхната значимост;

– С течение на времето мотивацията на хората в организацията се променя, поради това и йерархията на целите не е постоянна величина, а се нуждае от коригиране при промяна на целевите нагласи на висшия персонал.

В най-общи линии можем да представим следната характеристика на целите на развитие на организацията, дефинирайки ги на групи (цит. по 2):

Първа група – цели на посоката на развитието, като такива биха могли да се посочат – осигуряване на лидерство на пазара, разпространение на продуктите на пазара, обслужване на потребителите, и могат да се заключават в осигуряване на конкретни позиции, повишаване нивото на иновациите, внедряване на нови технологии, увеличаване количеството на завоюваните пазари или сегменти от пазара, увеличаване броя на потребителите на организацията, повишаване на качеството на продуктите на организацията и др.;

– Втора група – цели характеризиращи ефективността на функционирането на системата, обикновено те се заключават в повишаване ръста на производството и ръста на печалбата, и могат да бъдат формулирани като – повишаване обема на продажбите, повишаване обема на производството, повишаване обема на печалбата;

– Трета група – вътрешни цели, отнасят се до рентабилността на производството и до мотивацията и управлението на персонала, те могат да се заключават в повишаване на обема на запасите, намаляване на сроковоте за издължаване на кредитите, намаляване на ликвидността, намаляване на текущите разходи за единица продукт, отношение между работници и мениджмънт, развитие на персонала, средна заплата в организацията;

– Четвърта група – външни цели, отнасят се до социалната отговорност и могат да се формулират в областта на имиджа на организацията, използването на ресурсите, обществената активност, повишаване на благосъстоянието на хората в населеното място, в което е разположена организацията.

Практиката на стратегическо планиране във фирмите на запад показва, че количеството показатели, които се използват при формирането на целите и целеполагането, зависи от няколко фактора заключаващи се в:

– Степен на отработеност на плана на организацията;

– Формата на собственост;

– Типа организация (специализирана или диверсифицирана);

– Мащаба на организацията (малка, средна или голяма).

При формулирането на целите на организацията, управлението й трябва да се ръководи от някои изисквания, които по същество се явяват в някаква степен и ограничители на целеполагането, към тези общи изисквания можем да причислим следните (цит. по):

– Достижимост – желаното състояние, което организацията трябва да достигне след определен период от време. Това не може да бъде установено напълно реалистично, доколкото зависи и от ключовите ресурси, с които разполага предприятието, и които е възможно да достави;

– Гъвкавост – при пазарната икономика всеки стопански субект действа в условията на неопределеност, което предполага гъвкавост при отношенията с външната среда и гъвкавост при измененията на вътрешните условия в организацията;

– Измеримост – доколкото е осъществимо всяко качествена характеристика на целите да има и количествено измерение;

– Стимулиране за постигане на желаното състояние – формулирането на целите на дадената организация трябва да има стимулиращ ефект, както за организацията като цяло, така и за всеки неин член;

– Йерархичност при построяване на целите на развитието, този проблем беше вече разгледан;

– Точност на формулировките – формулирането на целите не е самоцел, залагането им в плана за стратегическо развитие на организацията, означава, че те би трябвало да бъдат разбрани и приети от всички членове на организацията, и на всички нива на организацията, а за да бъдат те приети и разбрани е необходимо да бъдат точно формулирани.

При целеполагането от гледна точка на стратегическото планиране се предявяват и някои специфични изисквания, които трябва да се отчетат:

– Ориентиране към тенденциите на външната делова среда;

– Координиране на вътрешните цели;

– Осигуряване на възможност за конкретни планови действия и контрол за тяхната реализация.

При това трябва да се отчитат следните обстоятелства:

– Целите трябва да бъдат системни, т.е., да описват организацията като цялостна система;

– Целеполагането да се осъществява в рамките на цялостната организационна структура, което означава целеполагане на всяко нейно ниво, което от своя страна означава съгласуване на целеполагането по нивата.

В заключение можем да обобщим: процесът на формиране на целите на организацията не завършва с целеполагането, на всички останали етапи на стратегическото планиране ние се връщаме към целите, тъй като всичко, което правим е ориентирано към тяхното постигане. Следователно на всеки следващ етап бихме могли да коригираме целите, или да ги преформулираме. В литературата се оказват следните възможни причини, които да водят до преформулиране на целите:

– Промяна в желанията, оценките и очакванията на ръководството;

– Обективни промени в жизнения цикъл на продуктите на организацията;

– Изменения протичащи в групата на стейкхолдерите (тези, които се влияят от целите и влияят върху целите.

Всичко това означава, че процесът на целеполагането на дадена система или организация е процес интегративен, многопланов и непременно изискващ обратна връзка. Задачата, която се решава в процеса на целеполагането включва преди всичко, определяне на баланс между целите и конкретните програми за действия на организацията, които да обезпечават постигането на определените в процеса на стратегическото планиране цели.

Литература:

1. Виханский О. С. Стратегическое управление. М., 1995.
2. Петров, А. Н. и др., Стратегический менеджмент. Питер СПб. 2005
3. Портер, М. Международная конкуренция. МО, М. 1993
4. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
5. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
6. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
7. Chang Y. N., Campo-Flores F. Business Policy and Strategy, Text and Cases. Good year Publishing Company. — Santa Monica, 1980.
8. Greenly G. E. Strategic Management. — Prentice Hall, London, 1989.
9. Jonson G., Scholes K. Exploring Corporate Strategy. An Aproach to Strategic Management. — Pitman, London, 1992.
10. Mintzberg H. Power in and around organizations. N.Y., 1983.
11. Robey P., Sales A. Designing organizations. Burr, 1996.
12. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
13. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical pproach. N.Y., 1989.

ПРАВНИ АСПЕКТИ НА ЕЛЕКТРОННАТА ТЪРГОВИЯ

Велико П. Петров

Национален военен университет "В. Левски", Факултет "Артилерия, ПВО и КИС", катедра "Организация и управление на тактическите подразделения от Полевата артилерия" гр. Шумен

LEGAL ASPECTS OF ELECTRONIC COMMERCE

Veliko P. Petrov

Abstract: *E-commerce means doing business transactions electronically via the Internet and can be defined as the business of the future, the rapid development of high technology and the proliferation of the Internet worldwide. It is revolutionizing the whole system of international economic relations and gradually replacing traditional forms of marketing.*

Keywords: *E-commerce, Internet economy.*

Развитието на информационните и комуникационните технологии (ИКТ) е неограничен източник на възможности, но същевременно и предизвикателство пред различните сфери на обществения живот. С развитието на световната компютърна мрежа и неизбежната й комерсиализация в ежедневието на хората се появиха множество нови понятия, които придобиват все по-голяма популярност в съвременното общество, като електронна търговия, електронен бизнес, електронна услуга и електронно обучение.

Интернет вече промени радикално ежедневието на европейците подобно на индустриалните революции от последните векове. Електронната търговия и изобщо интернет услугите[1] са вече неразделна част от живота на потребителите, на предприятията (от най-големите до най-малките) и като цяло на гражданите. Днес те сравняват, купуват или продават стоки и услуги, търсят или предлагат информация, извършват своите плащания или боравят с данни, учат или се образоват, контактуват, общуват и споделят вече по различен начин в сравнение с отпреди двадесет, десет или дори пет години.

Електронната търговия променя революционно цялата система на международни икономически отношения и постепенно измества традиционните форми на търговия. Печалбата от нея ще достигне няколко трилиона долара. В тази връзка се създава специална и специфична международно законова база за регулиране на електронната търговия:

[1] Съобщение на ЕК,Съгласувана уредба за повишаване на доверието в цифровия единен пазар за електронната търговия и интернет услугите, Брюксел, 11.1.2012 г.COM(2011) 942 final - Под „**интернет услуги**" (или „онлайн услуги") тук разбираме услугите, предоставяни от разстояние по електронен път по искане на получателя на услугата и срещу заплащане. **Електронната търговия** на стоки (в това число културни блага, лекарства) и услуги (в това число интернет игри) също се включва в това понятие, както и социалните мрежи, професионалното обучение от разстояние и т.н.

– въвеждане на общи електронни стандарти;
– въвеждане на електронен подпис;
– електронни форми на типови контракти;
– специфичен електронен език.

Въвеждат се специфични форми, като:

– интернет магазини;
– електронен маркетинг, електронни каталози;
– електронни борси и аукциони и др.

Понятието за електронна търговия еволюира непрекъснато, като на практика то означава извършването на бизнес сделки по електронен път чрез Интернет, вместо чрез физическото участие или присъствие на страните.

Електронната търговия е непрекъснат цикъл от обработка и обмен на данни, чрез които се осъществява унифицирано и интегрирано информационно осигуряване на участниците в цялостната търговска транзакция, независимо от сферата на дейност, отрасъла, държавата и пр.[2]

Електронната търговия не е друг вид търговия, а е друг начин на осъществяване на търговска дейност и представлява размяна на блага чрез използване на електронни средства за комуникация и най-вече на Интернет като бизнес среда и средство. Интернет се превърна в пространство за търговски и бизнес отношения по повод продажба и предоставяне на стоки и услуги, включително техния маркетинг, поддръжка, разпространение и т.н.[3]

Електронна търговия по смисъла на Закона за електронната търговия[4] е предоставянето на услуги на информационното общество. Услуги на информационното общество са такива услуги, включително предоставяне на търговски съобщения, които обикновено са възмездни и се предоставят от разстояние чрез използването на електронни средства след изрично изявление от страна на получателя на услугата.

С термина електронна търговия се означава:

1) *Един нов дял на модерната икономика*, а именно сключване на сделки и предоставяне на стоки и услуги по електронен път;

2) *Начина на извършване на търговска дейност* посредством приложение на информационни и комуникационни технологии в производството или разпространението на продуктите на компаниите;

3) *Съвкупността от правоотношения*, които възникват между субектите на търговското право при или по повод осъществяване на търговска дейност.

Основните предимства на електронната търговия са:

– глобалното присъствие;
– добрата информираност по цялата верига;
– бързото разпространение на продуктите;
– новия канал за продажби;
– съкращаването на разходите;
– намаляването на времето за достигане до пазара;
– подобряването на услугите за клиентите;
– налагането на търговска марка и корпоративен имидж;

---

[2] Националната стратегия за Електронна търговия, одобрена от МС на Р.България през 2000 г.
[3] Георги Г. Димитров, Електронната търговия. Електронни подписи. Правни аспекти, стр. 3, http://education.netlaw.bg/issues/Pravni_aspekti_na_elektronnata_turgovia_i_elektronnite_podpisi.pdf
[4] Закон за електронната търговия (в сила от 24.12.2006 г., посл. изм. от 29.12.2011 г.), чл. 1.

– реорганизирането на фирмената структура;
– по-добрите взаимоотношения с потребителите;
– разширяването на продуктовите листи;
– новите бизнес модели.

Могат да се посочат следните недостатъци на електронната търговия:

– липсата на доверие в сигурността на системата от страна на потребителите;
– несигурност относно разпространението на личната им информация;
– лесната възможност за извършването на измама в интернет пространството, което прави потребители скептично настроени към предлагания онлайн продукт;
– различните законодателни рамки в страната на купувача и в страната на продавача;
– съмнението в истинността на рекламата и качеството на предлагания продукт;
– възможността за получаване на грешна или дефектна стока или такава, неотговаряща на представите на купувача;
– желанието на потребителя за незабавно получаване на стоката.

Необходимо е да се решат няколко основни проблема свързани с електронната търговия, за да може тя да разгърне всички свои възможности:

1) Глобализация – търговията в глобалната мрежа е възможно да се прави с компания от най-отдалечение край на Земята, така, както с фирма от съседната улица. Но, как могат компании от различни континенти да се убедят в реалното си правно-законово съществуване. Как една компания може да разбере и приеме традициите и правилата за провеждане на бизнес сделки в страна, разположена на другата страна на земното кълбо? Как може добре да се поддържа лингвистичното и културно многообразия на милиардното общество от потребители?

2) Договорни и финансови проблеми – да предположим, че чужда компания разглежда електронен каталог на българска фирма и поръчва продукт, който да бъде доставен по електронен начин и да бъде платен по електронен път. Този пример предизвиква няколко фундаментални въпроса: На какъв етап може да се счете договора между компаниите за приключен? Какъв е юридическият статус на този контракт? Под юрисдикцията на коя страна попада? Какви трябва да бъдат данъците и митническите такси? Как да се вземат?

3) Право на собственост – Стоките, които се разпространяват по електронен път могат лесно да бъдат копирани. Проблемът за защитата на интелектуалната собственост стои особено остро.

4) Секретност и безопасност – Механизмите на електронната търговия трябва да осигуряват конфиденциалност, аутентификация (всяка страна да се легитимира) и гаранция, че в последствие всяка стана няма да се отрече от своето участие в сделката. Дотолкова, доколкото признатите механизми поддържат безопасност, която се основава на сертифициране от трета страна и международната електронна търговия изисква наличието на международни сертифициращи системи.

5) Съвместимост на информационните системи – Пълното разгръщане на потенциала на електронната търговия изисква универсален достъп – всяка компания и всеки потребител трябва да имат възможност за достъп до всички организации, предлагащи продукти и услуги, независимо от тяхното географско местоположение или особеностите на техните информационни системи. Това изисква универсални стандарти за взаимодействие и съвместимост на използваните за целта средства.

Фиг. 1. Видове отношения в електронната търговия

На фиг. 1 са показани видовете отношения в електронната търговия и те са:[5]

1) Отношения B2B (бизнес към бизнес). Тези отношения протичат между отделните компании в процеса на производството, разпространението и поддръжката на техните продукти и са насочени към обслужване на процесите, които осигуряват функционирането на електронната търговия. В последните години някои компании насочиха изцяло своята дейност към предоставяне на продукти и услуги, които не са ориентирани към крайния потребител, а осигуряват функционирането на отделен процес от бизнес модела на компаниите, осъществяващи електронна търговия.

2) Отношения B2C (бизнес към клиент). Тези отношения осъществяват връзката между субектите на електронната търговия и крайните потребители на стоки и услуги, като чрез тях се реализира целта на бизнес модела на компаниите, чиито продукти и услуги са насочени към крайния потребител. Особеностите на моделите на компаниите, който използват B2C отношенията е, че те са насочени към производство и разпространение на продукти, които имат самостоятелно значение извън бизнес модела на определена компания (за разлика от B2B отношенията). Отношенията B2C са насочени към крайните потребители, но бизнес моделът на електронната търговия включва в себе си отношения с други компании по осигуряването на бизнес процесите.

3) Отношения C2C (потребители към потребители). Тези отношения са проявление на възможностите на новата среда за комуникация между потребителите в електронната търговия. Интернет улеснява договарянето между страните по сделките, с което стимулира стокообмена между отделните потребители. Тези отношения се проявяват най-явно в организираните аукциони за продажба на използвани вещи между физически лица.

4) Отношения B2A (бизнес към администрация). Отношенията бизнес към публична власт са отношения по повод на предоставяне на административни услуги от държавата към субектите на електронната търговия. Тези отношения са административни по своя характер и са проявление на стремежа на повечето държави да предоставят административни услуги, чрез използване на модерни информационни и комуникационни технологии. Друга съществена разлика е и метода на правно регулиране, който се използва в административните нарушения – метода на власт и подчинение, за разлика от равнопоставеността на субектите в гражданското право. Отношенията бизнес към публична власт могат да се разгледат като проявление на потреблението на държавната администрация на стоки и услуги.

[5] Кристиян Масарлов, Чудото покорило света: електронната търговия, www.e-training.bg /elgg/ mod /file/download.php?file_guid=1645

5) Отношения С2А (потребител към администрация). Това направление е най-слабо развито, но то има достатъчно висок потенциал, който може да бъде използван, за да се организира взаимодействието между държавни структури и потребители, особено в специалната данъчна сфера.

Международните нормативни актове в сферата на електронната търговия биват:

1) Типов закон ЮНСИТРАЛ „За електронна търговия"[6]. Това е първата крачка на развитие на международното право в областта на електронната търговия. Този документ има рамков характер и е предназначен на първо място за използване от държавите при разработка на национално законодателство. Той залага основите на дейността в сферата на електронната търговия, дава определенията на основните понятия като (електронен документ, електронен документооборот, електронен подпис, автор на електронен документ, информационна система, признава юридическата и доказателствената сила на документите в електронна форма, определя условията, на които трябва да отговаря електронният подпис, както и средствата за потвърждаване истинността и целостта на електронния документ).

2) Директива 1999/93/ ЕИО на Европейския парламент и на Съвета от 13.12.1999 г. относно правната рамка на Общността за електронните подписи. Този документ пълно урегулира отношенията в сферата на използване на електронните подписи и установява изискванията, на които трябва да съответства електронния цифров подпис, определят се принципите на неговото използване, дейността на сертификационните центрове, както и определянето на реда на предоставяне на сертификационни услуги.

3) Директива 2000/31 на Европейския парламент и на Съвета от 08.06.2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар. С нея се цели насърчаване на развитието на тази услуги, по-специално чрез разпоредбата за страната на произход, чрез задълженията за информиране на потребителя, чрез регламентиране на търговските съобщения по интернет и чрез разпоредбите, свързани с електронните договори и отговорността на междинните интернет доставчици.

Директивата за електронната търговия, която днес продължава да бъде актуална, има за цел да премахне пречките пред установяването на доставчици на услуги на информационното общество и пред трансграничното предоставяне на онлайн услуги на вътрешния пазар, като по този начин дава правна сигурност на предприятията и на гражданите. Технологично неутрална, тя има широко приложно поле: не само електронна търговия (между предприятия и между предприятия и потребители) в тесния смисъл на понятието (включително онлайн аптеки), но и онлайн вестници, онлайн финансови услуги, услуги на регламентираните професии и т.н. Хазартните дейности онлайн обаче са изключени.[7]

4) Директива 2002/65/ЕС на Европейския парламент и на Съвета относно дистанционния маркетинг на потребителски финансови услуги;

[6] На 30 януари 1997 г. с Резолюция на Генералната Асамблея на ООН беше приет разработения от Комисията на ООН по право на международната търговия Типов закон „За електронната търговия" (Типов закон ЮНСИТРАЛ „За електронна търговия").

[7] Съобщение за членовете на ЕП, (IMCO/CM/03/2011) от 30.6.2011, относно: Електронна търговия, стр. 2.

5) Директива 2002/58/ЕС на Европейския парламент и на Съвета относно оперирането с лични данни и защитата им в сектора на информационните и комуникационни технологии;

6) Директива 97/7/ЕС на Европейския парламент и на Съвета за защита на потребителите при дистанционни договори.

Наред с международното право активно се развива и националното законодателство. В различни държави са приети закони, регулиращи дейността в сферата на Интернет (САЩ, Германия, Великобритания и др.) Особено напреднали в тази насока са САЩ, където са приети повече от 15 федерални закона регулиращи отношенията в Интернет.

Нормативна уредба за електронната търговия в Република България.

Правният режим на електронната търговия се съдържа в множество и различни по ранг нормативни актове. Тя се съдържа в Закона за електронна търговия (ЗЕТ), както и в редица по-общи актове като Закона за електронните съобщения (ЗЕС), Закона за електронния документ и електронния подпис (ЗЕДЕП), Закона за авторското право и сродните му права (ЗАПСП), Закон за защита на личните данни (ЗЗЛД), Закон за задълженията и договорите (ЗЗД), Търговски закон (ТЗ), Закон за защита на потребителите (ЗЗП) и други. Технологичното развитие и съпътстващите го социално-икономически отношения, в това число бизнесът в Интернет, често изпреварват нормативното уреждане на новите области, така че, когато даден нов закон или изменение е вече в сила, пазарът и технологиите вече са поставили множество нови въпроси за решаване.

ЗЗД дава общата нормативна уредба на регулиране на облигационните правоотношения между гражданско-правните субекти и доколкото липсва изрична уредба в търговския закон, регулира субсидиарно и търговските правоотношения при всяка форма на търговия, включително електронната - действие на договора, права и задължения на страните, изпълнение, неизпълнение и недействителност на договорите и пр.

До влизането в сила на ЗЕДЕП в България електронна търговия се осъществяваше на законна основа, като отношенията се регулираха от общите правни норми за извършване на търговска дейност. Основните действащи нормативни актове, за които може да се твърди, че уреждат правоотношенията при търговията в широк смисъл и следователно на електронната търговия са - Търговски закон (ТЗ), Закон за защита на потребителите (ЗЗП), а освен това с оглед общите правила за търговия, се прилагат и всички закони, свързани със защита на потребителите (ЗЗППТ), защита на конкуренцията (ЗЗК), специалните закони регулиращи банкова дейност, застрахователна дейност, и т. н. Специална уредба на финансовите услуги, предоставяни от разстояние, се съдържа в Закона за предоставяне на финансови услуги от разстояние.

ТЗ урежда сделката при електронната търговия като търговска сделка, независимо от това дали само едната страна има качеството търговец, а другата е потребител – нетърговец или и двете страни са търговци.

Основата на развитието на българското законодателство в областта на Интернет е ЗЕДЕП в сила от 07.10.2001г., който се явява основния правен акт на Р. България непосредствено регулиращ отношенията в Интернет. Законът определя правните основи за използването на електронните документи, заверени с електронен подпис, определя основните изисквания, на които трябва да отговарят тези доку-

менти, а така също правата, задълженията и отговорността на участниците в електронния документооборот. Той установява, че посредством обмена на електронни документи могат да се сключват сделки, да се осъществяват електронни плащания, да се извършва преписка и да се предават документи и друга информация.

Законът също установява, че в случай, че законодателството на Р. България изисква даден документ да бъде оформен писмено или да бъде представен във писмена форма, то електронния документ се счита за съответстващ на тези изисквания. Електронният документ на машинен носител се приравнява към електронния документ на хартиен носител и има еднаква с него юридическа сила.

В закона е посочен редът за прилагане на електронния цифров подпис за удостоверяване на информация и потвърждаване на достоверността и целостта на електронния документ.

Законът за електронната търговия (ЗЕТ) въвежда като част от действащото законодателство разпоредбите на Директива 2003/69/ЕО на Европейския парламент и Съвета и е насочен към хармонизиране на българското законодателство с действащите в ЕС правила за защита на потребителите. ЗЕТ допълва съдържащия се общ режим в Закона за защита на потребителите (обн., ДВ, бр. 99/2005 г.), като съдържа специална защита на правата и законните интереси на потребителите на услуги на информационното общество. Затова в по-голямата си част разпоредбите на ЗЕТ са императивни и не позволяват дерогирането им по договорен път. От обхвата на ЗЕТ изрично са изключени услугите, свързани с установяването и събирането на публичните вземания, защитата на личните данни, включително в областта на електронните съобщения, споразуменията, решенията и съгласуваните практики по смисъла на чл. 9 от Закона за защита на конкуренцията, нотариалната дейност и други професионални дейности, свързани с осъществяване на публични функции, процесуалното представителство, както и хазартните игри (чл. 1, ал. 4 от ЗЕТ). Законът за предоставяне на финансови услуги от разстояние (ЗПФУР) допълва тази защита относно финансовите услуги, предоставяни от разстояние на територията на страната, съобразно техните характерни особености и присъщ риск.[8]

Принцип на свобода на електронната търговия. ЗЕТ[9] изрично прогласява принципа на свобода при извършване на електронна търговия, подобно на всяка друга търговия. Действието на посочения принцип обаче, не е безгранично. Съгласно чл. 2 от ЗЕТ услугите на информационното общество се предоставят свободно, освен, ако в закон е предвидено друго.

Съгласно ЗЕТ доставчик на услуги може да бъде всяко физическо или юридическо лице, което предоставя услуги на информационното общество, а получател – всяко физическо или юридическо лице, което ползва услуги на информационното общество с професионална или друга цел, включително за нуждите на търсене на информация или предоставяне на достъп до нея.

Информационни задължения на доставчика. Доставчикът на услуги на информационното общество е длъжен да предоставя безпрепятствен, пряк и постоянен достъп на получателите на услугите и на компетентните органи до информация за името или наименованието си, постоянния си адрес или седалището и адреса си на управление, адреса, на който упражнява дейността си, ако е различен от адреса на

[8] Велко Джилизов, Правен режим на електронната търговия, Български законник, бр. 09, Септември 2007 г., стр. 1.

[9] Закон за електронната търговия (в сила от 24.12.2006 г., посл. изм. от 29. 12.2011г.)

управление, данни за кореспонденция, включително телефон и адрес на електронна поща, за осъществяване на пряка и навременна връзка с него, както и данни за вписване в търговски или друг публичен регистър.

Доставчикът предоставя информация и за органа, осъществяващ контрол върху дейността му, когато дейността му подлежи на уведомителен, регистрационен или лицензионен режим, съответно указание, ако е регистриран по ЗДДС, както и всяка друга информация, предвидена в нормативен акт. Когато доставчикът осъществява регулирана професия, същият е длъжен да предостави информация за камарата, професионалния съюз или организацията, в която членува или е регистриран, професионалното звание и държавата, в която то е предоставено, както и препратка към приложимите разпоредби относно правото на упражняване на занаята или професията и указания за достъпа до тях.

Когато при предоставянето на услуги на информационното общество се посочват цени, те трябва да се обозначават по ясен и разбираем начин. Доставчикът на услуги е длъжен да указва дали цените включват данъци, такси и разноски, които формират крайната цена.

По отношение на финансовите услуги, доставчикът също така е длъжен да уведоми специално потребителя, ако съответната финансова услуга е свързана с инструменти, които предполагат особени рискове, произтичащи от тяхната специфика или от операциите, които предстои да бъдат извършени или чиято цена зависи от колебанията на финансовите пазари, върху които доставчикът не може да влияе и че постигнатите до момента резултати не позволяват извършването на надеждни прогнози.

ЗЕТ изрично разграничава информационните задължения на доставчиците от търговските им съобщения. Съгласно чл. 5 от ЗЕТ търговски съобщения са рекламни или други съобщения, представящи пряко или косвено стоките, услугите или репутацията на лицето, извършващо търговска или занаятчийска дейност или упражняващо регулирана професия. Не представляват търговски съобщения по смисъла на закона самостоятелното използване на информация, осигуряваща директен достъп до дейността на лицето, като наименованието на неговия домейн или адрес на електронна поща, нито съобщения за стоките, услугите или репутацията на лицето, информацията, за които е събрана по независим начин, без за това да е заплатено. Търговските съобщения, които са част от услуга или представляват услуга на информационното общество, трябва да отговарят на особени изисквания, установени в закона, а именно: да бъдат лесно разпознавани като търговски; да позволяват ясна идентификация на физическите или юридическите лица, от името, на които са направени; да определят ясно и недвусмислено условията за ползване на промоционни предложения, като отстъпки, премии и подаръци, ако включват такива; да осигуряват лесен достъп до ясни и недвусмислени условия за участие в състезания и игри с обявени награди, ако съдържат такава информация; както и да съдържат информацията, предвидена в нормативните актове.

Съгласно чл. 6 от ЗЕТ доставчик на услуги, който изпраща непоискани търговски съобщения по електронната поща без предварително съгласие на получателя, е длъжен да осигури ясното и недвусмислено разпознаване на търговското съобщение като непоискано още с постъпването му при получателя. Комисията за защита на потребителите води електронен регистър на електронните адреси на юридическите лица, които не желаят да получават непоискани търговски съобщения, по ред,

определен с наредба на Министерския съвет. По силата на чл. 6, ал. 3 от ЗЕТ изрично се забранява изпращането на непоискани търговски съобщения на електронни адреси, вписани в регистъра на Комисията. Законът забранява и изпращането на непоискани търговски съобщения на потребители без предварителното им съгласие (чл.6, ал.3 от ЗЕТ). Предоставянето на финансови услуги от разстояние на потребителя срещу заплащане без изрично и предварително искане от негова страна е забранено (чл. 14, ал. 1 от ЗПФУР).

Лицата, упражняващи регулирани професии, могат да използват търговски съобщения като част от услуга или представляващи услуга на информационното общество. Търговските съобщения на такива лица обаче, трябва да отговарят на професионалните правила и етичните кодекси за поведение на лицата с регулирани професии, по-специално на правилата за независимостта, достойнството и честта на професията, професионалната тайна и честното отношение към клиентите и другите членове на професията.

Договор за предоставяне на услуги на информационното общество. По своята правна същност продажбата на услуги на информационното общество представлява търговска сделка, тъй като предоставянето на услуги от разстояние обикновено има възмезден характер (чл.1, ал.3 от ЗЕТ). По смисъла на чл.6 ЗПФУР договор за предоставяне на финансови услуги от разстояние е всеки договор, сключен между доставчик и потребител като част от система за предоставяне на финансови услуги от разстояние, организирана от доставчика, при която от отправянето на предложението до сключването на договора страните използват изключително средства за комуникация от разстояние - едно или повече.

Съгласно чл. 8 от ЗЕТ при предложение за сключване на договор чрез електронни средства доставчикът на услуги е длъжен предварително да информира получателя на услугата по ясен, разбираем и недвусмислен начин относно техническите стъпки по сключването на договора и тяхното правно значение, дали договорът ще бъде съхраняван от доставчика на услугата и какъв е начинът за достъп до него, относно техническите средства за установяване и поправяне на грешки при въвеждането на информация, преди да бъде направено изявлението за сключване на договора, както и за езиците, на които договорът може да бъде сключен. Доставчикът на услуги е длъжен да указва начина за достъп по електронен път към етичен кодекс за поведение, към който се придържа.

Доставчикът на услуги е длъжен също така да предостави на получателя на услугата общите условия и съдържанието на договора по начин, който позволява тяхното съхраняване и възпроизвеждане.

Законът изисква от доставчика на услуги да осигури подходящи, ефективни и достъпни технически средства за установяване и поправяне на грешки при въвеждане на информация, преди получателят на услугата да направи изявление за сключване на договора (чл. 10, ал.1 от ЗЕТ). Доставчикът на услуги без неоправдано забавяне е длъжен да потвърди чрез електронни средства получаването на изявлението за сключване на договора. Съгласно чл. 11 от ЗЕТ изявлението за сключване на договора и потвърждението за неговото получаване се смятат за получени, когато техните адресати имат възможност за достъп до тях. Законът предвижда посочените изисквания да се прилагат задължително в случаите, когато получател на услугата е потребител по смисъла на Закона за защита на потребителите (чл. 12, ал.1 от ЗЕТ). Изключение се допуска само за договори, сключени изключително

чрез електронна поща или други равностойни средства за размяна на индивидуални изявления. По смисъла на §1, т.8 от ЗЕТ електронна поща е електронно средство за съхраняване и пренос на електронни съобщения през интернет мрежа чрез стандартизирани протоколи.

За договора за предоставяне на финансови услуги от разстояние се прилагат и разпоредбите на чл. 143 – 148 от Закона за защита на потребителите относно неравноправните клаузи. Потребителят на финансови услуги, предоставяни от разстояние, има гарантирано от закона право, без да дължи обезщетение или неустойка и без да посочва причина, да се откаже от сключения договор в срок 14 дни, считано от: датата на сключване на договора; или деня, в който потребителят получи условията на договора и информацията по чл. 10, ал. 1 и 2 от ЗПФУР, когато това става след сключване на договора (чл. 12, ал. 1 ЗПФУР).

Потребителят може, без да дължи обезщетение и/или неустойка и без да посочва причина, да упражни правото си на отказ от сключения от разстояние договор за допълнително доброволно пенсионно осигуряване с лични вноски или за застраховка „живот" в срок 30 дни, считано от датата на сключване на договора за допълнително доброволно пенсионно осигуряване с лични вноски или от момента, в който застрахованият е уведомен от застрахователя за сключването на договора за застраховка, или от деня, в който потребителят получи условията на договора и информацията по чл. 10, ал. 1 и 2 от ЗПФУР, когато това става след сключване на договора. Съгласно чл. 12, ал. 3 от ЗПФУР правото на отказ от договора не възниква в следните случаи:

1) за финансови услуги, чиято цена зависи от колебанията на финансовия пазар, които могат да възникнат през периода, през който потребителят има право да се откаже от договора, и върху които доставчикът не може да влияе, като услуги, свързани със: обмяна на валута; инструменти на паричния пазар; прехвърлими ценни книжа; дялове в предприятия за колективно инвестиране; договори за финансови фючърси, в т.ч. еквивалентни инструменти, задълженията по които могат да бъдат изпълнени чрез парично плащане в брой; форуърдни лихвени споразумения; лихвени суапове, валутни суапове и суапове с акции; опции за закупуване или продажба на инструменти, в т.ч. еквивалентни инструменти, задълженията по които могат да бъдат изпълнени чрез парично плащане в брой, включително опции върху валута и върху лихвени проценти;

2) при застрахователни договори във връзка с пътуване, багаж или други краткосрочни застрахователни договори със срок, по-малък от един месец;

3) при договори, които са изпълнени от двете страни по изричното искане на потребителя, преди той да е упражнил правото си на отказ от договора;

4) при договори за кредит, предназначени за придобиване или запазване правото на собственост върху земя или сграда, която е построена или която предстои да бъде построена, както и за извършване на ремонт или подобрения в недвижим имот.

При упражняване на правото си на отказ от сключения договор потребителят уведомява доставчика преди изтичането на установения в закона срок. Срокът се смята за спазен, ако уведомлението, направено на хартиен или друг траен носител, достъпен за получателя, е било изпратено преди изтичането на съответния срок.

Когато потребителят упражни правото си на отказ от сключения договор за предоставяне на финансови услуги от разстояние и доставчикът не може да дока-

же, че го е информирал за цената на финансовата услуга, потребителят не дължи заплащане на получената услуга.

Случаи на ограничаване отговорността на доставчика. Съгласно чл. 13 от ЗЕТ при предоставяне на достъп до или пренос през електронна съобщителна мрежа доставчикът на услуги не отговаря за съдържанието на предаваната информация и за дейността на получателя на услугата, ако не инициира предаването на информацията, не избира получателя на предаваната информация, и не избира или не променя предаваната информация. Предоставянето на достъп до или пренос през електронна съобщителна мрежа включва автоматично, междинно и временно съхраняване на предаваната информация, извършено единствено с цел осъществяване на преноса през електронна съобщителна мрежа, като информацията не се съхранява за срок, по-дълъг от обикновено необходимия за осъществяването на преноса.

Доставчик, който предоставя услуги, осигуряващи автоматизирано търсене на информация, не отговаря за съдържанието на извлечената информация, ако не инициира предаването на извлечената информация, не избира получателя на извлечената информация, и не избира или не променя извлечената информация. Посоченото ограничение на отговорността не се прилага, ако информационният ресурс, от който се извлича информацията, принадлежи на доставчика или на свързано с него лице.

Доставчик на услуги, който пренася информация, въведена от получателя на услугата в електронна съобщителна мрежа, не отговаря за автоматичното, междинното и временното съхраняване на информацията, необходимо за нейното ефективно предаване към други получатели на услугата по тяхно искане, ако не изменя информацията, спазва изискванията за достъп до информацията, спазва общоприетите правила за актуализация на информацията, правомерно използва общоприетите технологии за получаване на данни за използване на информацията и незабавно премахва информация, която е съхранил, или преустановява достъпа до нея с узнаването на факта, че информацията е била отстранена от мрежата на първоначалния източник или достъпът до нея е бил преустановен, или е налице акт на компетентен държавен орган за премахване на информацията или преустановяване на достъпа до нея, когато това е установено със закон.

Доставчик на услуга, представляваща съхраняване на предоставена от получател на услугата информация, не отговаря за нейното съдържание, както и за дейността на получателя на услугата, ако не е знаел за противоправния характер на дейността или информацията, или не са му били известни фактите или обстоятелствата, които правят дейността или информацията явно противоправна. Ограничението на отговорността не се прилага, ако получателят на услугата е свързано с доставчика на услугата лице, когато доставчикът е узнал или е бил уведомен за противоправния характер на информацията или е бил уведомен от компетентен държавен орган за противоправния характер на дейността на получателя и не е предприел незабавни действия за преустановяване на достъпа до нея или за премахването ѝ. Посоченото изискване обаче, не освобождава доставчика от произтичащо от закон задължение да запази информацията. По искане на компетентен държавен орган в случаите, установени със закон, доставчикът е длъжен да предостави всяка информация относно получателя на услугата и дейността му.

Съгласно чл. 17 от ЗЕТ доставчикът на услуги не е длъжен да извършва наблюдение на информацията, която съхранява, пренася или прави достъпна при предос-

тавяне на услуги на информационното общество, нито да търси факти и обстоятелства, указващи извършването на неправомерна дейност.

Посочените по-горе основания за освобождаване и ограничаване отговорността на доставчика се прилагат и за доставчици на услуги на информационното общество, предоставяни безплатно (чл. 18 от ЗЕТ).

Потребителски спорове и тежест на доказване. Съгласно чл. 22 от ЗЕТ Комисията за защита на потребителите и сдруженията за защита на потребителите могат да предявяват искове за преустановяване или забрана на действия и търговски практики по ЗЕТ, които са в нарушение на колективните интереси на потребителите, както и искове за обезщетение при условията и по реда на Закона за защита на потребителите.

Потребителите имат право да подават жалби до Комисията за защита на потребителите, свързани с договори за предоставяне на финансови услуги от разстояние (чл. 19 ЗПФУР). Исковете за преустановяване или забрана на действия или търговски практики по ЗПФУР, които са в нарушение на колективни интереси на потребителите, и исковете за обезщетение се предявяват при условията и по реда на чл.чл. 186 - 190 от Закона за защита на потребителите (чл. 20 ЗПФУР).

Потребителите имат и правото да сезират помирителните комисии, създадени по реда на чл.чл. 182 - 184 от Закона за защита на потребителите, когато са нарушени техните права и законни интереси във връзка с предоставянето на финансови услуги от разстояние.

По силата на чл. 18 от ЗПФУР доставчикът е длъжен да докаже, че е изпълнил задълженията си за предоставяне на информация на потребителя; спазил сроковете по чл. 12, ал. 1 или 2 ЗПФУР относно упражняване правото на отказ от договора; и е получил съгласието на потребителя за сключване на договора, а ако е необходимо, и за неговото изпълнение през периода, през който потребителят има право да се откаже от сключения договор.

За доказване предоставянето на преддоговорна информация, както и на изявления, отправени съгласно ЗПФУР, се прилага чл. 293 от ТЗ, а за електронните изявления - Законът за електронния документ и електронния подпис.

Изводи:

1) Електронната търговия е инструмент с огромен потенциал за преустройване и подобряване на конкурентоспособността на европейската икономика и европейския вътрешен пазар.

2) Необходимо е онлайн пазарът да бъде превърнат в реална възможност за борба срещу икономическата криза. Правилата за електронна търговия в Европа трябва да се актуализират, за да отговарят на обществото на цифровите технологии на XXI век.[10]

3) Електронната търговия може да бъде определена като бизнеса на бъдещето, поради бързото развитие на високите технологии и масовото разпространение на Интернет в световен мащаб. Интернет бизнеса постепенно заема голяма част от икономическия живот и е въпрос на време онлайн сделките да се превърнат в ежедневие. Фирмите, които искат да бъдат в крак с времето, трябва да преосмислят бизнес поведението си и да вземат предвид новата Интернет икономика, за да бъдат конкурентоспособни и печеливши на пазара.

[10] Съобщение за членовете на ЕП, (IMCO/CM/03/2011) от 30.6.2011, относно: Електронна търговия

Литература:

1. Съобщение на ЕК, Съгласувана уредба за повишаване на доверието в цифровия единен пазар за електронната търговия и интернет услугите, Брюксел, 11.1.2012 г. COM (2011) 942 final.

2. Националната стратегия за Електронна търговия, одобрена от МС на Р. България през 2000 г.

3. Георги Г. Димитров, Електронната търговия. Електронни подписи. Правни аспекти, стр. 3.

4. Закон за електронната търговия (в сила от 24.12.2006 г., посл. изм. от 29.12.2011 г.).

5. Кристиян Масарлов, Чудото покорило света: електронната търговия.

6. Типов закон ЮНСИТРАЛ „За електронна търговия".

7. Съобщение за членовете на ЕП, (IMCO/CM/03/2011) от 30.6.2011, относно: Електронна търговия.

8. Велко Джилизов, Правен режим на електронната търговия, Български законник, бр. 9, Септември 2007 г.

СЪСТОЯНИЕ И УПРАВЛЕНИЕ НА ЕЛЕКТРОЕНЕРГИЙНИТЕ СИСТЕМИ В РАМКИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Здравко Ю. Кузманов

Национален военен университет „Васил Левски",
Факултет „Артилерия, ПВО и Кис", Шумен
Катедра „Информационна сигурност"

STATE AND MANAGEMENT OF POWER SYSTEMS WITHIN THE EUROPEAN UNION

Zdravko Y. Kuzmanov

KEY WORDS *European union, power systems, management.*

Основен орган, отговарящ за разработката и съгласуването на електроенергийната политика в рамките на Европейския съюз (ЕС), е Генерална дирекция по енергетика (до 2012 г., Генерална дирекция по енергетика и транспорт). Следващите степени на регулиране се отнасят на ниво отделни страни-членки на съюза, във всяка от които се прилагат различни подходи и системи за управление на отрасъла. По тази причина и с цел подобряване на координацията между националните регулатори в сферата на енергетиката на страните-членки на евросъюза те са обединени в асоциация на регулаторите (Agency for the Cooperation of Energy Regulators – ACER).

Асоциацията е създадена по инициатива на Европейската комисия в качеството на консултативен орган, по въпросите касаещи създаването на вътрешен електрое-

нергиен пазар. Основната дейност на *ACER* е разработката на законопроекти и стратегически ръководни документи за развитието на отрасъла. [1]

Процеса на либерализация на електроенергийния сектор в ЕС не предполага задължителна приватизация, в много страни голяма част от акциите на водещи компании в сектора продължават да принадлежат на държавата (напр. Италия, Швеция). В цялост за ЕС е характерно, крупномащабни компании да притежават значителен дял на електроенергийния пазар в съответните страни, *EDF* във Франция, *EDP* в Португалия, *Electrabel* в Белгия и др. Най-големите производители на електроенергия в Европа са *EDF, RWE, Eo.N, ENEL, Endesa* и *CEZ,* чиито генериращи мощности общо надхвърлят 250 000 мВт. Същите, посредством дъщерните си компании, са и основни доставчици и търговци на електрическа енергия на територията на ЕС.

Функциите по преноса на електроенергия и **управление на режимите на работа** в електроенергийните системи, в повечето страни-членки са обединени и се изпълняват от системни оператори. На територията на ЕС, към момента оперират 42 системни оператора в 34 страни, [2] обединени в асоциацията *ENTSO-E* (The European Network of Transmission System Operators for Electricity), която в съответствие с Третия пакет електроенергийни законови актове, приет от съюза, осъществява функции по общоевропейско планиране и координация на паралелно работещите синхронизирани електроенергийни системи в Европа. [3]

С цел анализиране на международния опит в управлението на електроенергийните системи (ЕЕС), следва да се извърши анализ на състоянието и управлението на ЕЕС, на:

- избрани държави-членки на Европейския съюз, в които протичат процесите установени от общността по отношение на политиката за дерегулация и либерализация на електроенергийните пазари и формиране на общ такъв за територията на съюза – напр. Великобритания и Чешката република.

Електроенергийната система на Великобритания е обект на интерес за изследването поради факта, че електроенергетика на страната към момента е една от най-конкурентните и най-либерализираната в състава на ЕС. Процесите в това направление за страната започват още през 1990 г.

Чешката република е с относително сходна на Р. България по територия и брой на населението страна, също преминаваща през процесите на децентрализация и преход към пазарна икономика в последните повече от две десетилетия. ЕЕС на страната е конструктивно изпълнена по сравнително сходен начин с тази на Р. България. От особен интерес се явява факта, че две от големите инфраструктурни компании, участващи на електроенергийния пазар в Република България, са активни участници и на чешкия, а техния капитал също е чешки.

Електроенергетиката на Великобритания е една от най-конкурентните и либерализирани в Европа. Приватизацията на електроенергийната индустрия започва още в началото на 1990 г. след приемането на закона за Електроенергетиката от 1989 г., [4] който предвижда:

- рамката за процеса на приватизация;
- въвеждането на конкурентни пазари;
- система за независимо регулиране.

Основен момент е постигнат през май 1999 г., когато всички клиенти стават свободни да избират доставчика си на електроенергия.

До началото на приватизацията и установяването на сегашната система, съществуват три географски обособени пазара на електроенергия в Обединеното кралство: Англия и Уелс, Шотландия и Северна Ирландия.

През 2005 г. е въведена системата от мерки *BETTA* (British Electricity Trading and Transmission Arrangements) с цел създаване на единна интегрирана електроенергийна система на Англия, Шотландия и Уелс (наречена National Grid). [5] Северна Ирландия разполага със собствена мрежа и електроенергиен пазар, под надзора на местното правителство и собствен енергиен регулатор (Utility Regulator). Съществуват значителен брой области, в които има известна степен на сходство между двата установени регулаторни режима в електроенергетиката на Северна Ирландия и Великобритания (тоест, Англия Шотландия и Уелс). Например, и двете системи в момента използват т.нар. облигации за възобновяеми енергийни източници (Renewables Obligation), [6] като основен стимул за производство на електроенергия от възобновяеми източници. Въпреки това, двете системи са отделни и тази точка се фокусира върху състоянието и управлението на електроенергийната система във Великобритания.

Националното правителство ръководи стратегическата политиката в електроенергийния сектор на Великобритания, чрез *Министерството на енергетиката и климатичните промени* (Department of Energy and Climate Change – DECC), което е отговорно за определяне и провеждане на енергийните политики и ограничаване на изменението на климата, както и създаване на рамката, необходима за постигане на целите на политиката в тези области. [7]

Националният енергиен регулатор Ofgem (Office of Gas and Electricity Markets), отговаря за регулирането на пазара на електроенергия във Великобритания. Основната функция на *Ofgem* е да защитава интересите на съществуващи и бъдещи потребители, като част от тези интереси включват намаляване на парниковите газове и гарантиране сигурността на доставките. [8] Основните задачи на регулатора включват: [8]

- издаване, промяна, налагане и отменяне на лицензи;
- осъществяване на ценови контрол над лицензираните сектори;
- разследване и санкциониране при нарушения на лицензионните условия.

Ofgem не е официално определен като представителен регулаторен орган на Великобритания за целите на Третия енергиен пакет на ЕС.

Производството и доставката и търговията с електроенергия във Великобритания се доминира от т.нар. „голяма шесторка“ (The Big Six) на електроенергийните компании, която включва: *British Gas, EDF Energy, E.ON, nPower, Scottish Power* и *SSE*. [9]

British Gas е водещ доставчик в страната на природен газ и електроенергия. Обслужва повече от 20 милиона клиенти. Компанията е дъщерно дружество на Centrica, която оперира с филиала *Scottish Gas* в Шотландия и *Direct Energy* в Северна Америка. [9]

EDF Energy е най-големият производител на електроенергия във Великобритания. Изцяло собственост на френската държавна *EDF SA*. Обслужва 5,7 милиона домакинства в страната. [9]

E.ON обслужва над 5,3 милиона частни и търговски клиенти, с водеща позиция в комбинираното производство на топлинна и електрическа енергия във Великобритания. Собственост на германската корпорация *E.ON AG*, която е най-голямата електроенергийна компания в световен мащаб, с над 26 милиона клиенти по цял свят. [9]

nPower е собственост на германската *RWE*. Водещ доставчик на природен газ и електроенергия за над 6,5 милиона клиенти. [9]

Scottish Power, дъщерно дружество на испанската *Iberdrola*, е оператор на електроразпределителната мрежа в централната и южната част на Шотландия и област Мърсисайд в Северен Уелс. Към 2012 г. *Scottish Power* е „най-малката" от големите шест енергийни компании с 5,2 милиона клиенти във Великобритания. Въпреки, че е дъщерно дружество на *Iberdrola*, притежава активите на *PPM Energy*, оперираща на пазара в САЩ. [9]

SSE е втория най-голям енергиен доставчик във Великобритания с 9,6 милиона клиенти. Водещ производител на електроенергия от възобновяеми източници в страната. [9]

От икономикогеографска гледна точка **електроенергийната система** на Великобритания е разделена на три, привидно относителни звена. Първото обхваща географската територия на Англия и Уелс, като оперативното управление се осъществява от системният системен оператор *National Grid Electricity Transmission plc* (*National Grid/NGET*). В Шотландия системата се подразделя на две отделни звена, едната обхваща южната и централната част, другата – Северна Шотландия. Свързани в паралелна работа чрез междусистемни връзки помежду си. Първата е собственост и се поддържа от *SP Transmission Limited* (SPTL), дъщерно дружество на *Scottish Power*, втората от *Scottish Hydro-Electric Transmission Limited* (SHETL). И двете осъществяват и функции по оперативно управление. Въпреки този факт, *NGET* остава единен системен оператор на цялата ЕЕС на Великобритания, осъществяващ единното оперативно управление.

ЕЕС на Великобритания е свързана в паралелна работа, посредством междусистемни връзки, с електроенергийните системи на Франция (чрез *Cross-Channel* – подводен електропровод 270 кВ [10], Северна Ирландия (чрез *Moyle* – електропровод 250 кВ [11], остров Ман (чрез *Isle of Man Interconnector* – подводен електропровод 90 кВ, [12] най-дългият в света [13], Холандия (чрез *BritNed* – подводен електропровод 450 кВ [14] и Република Ирландия.

Сумарната инсталирана **генераторна мощност** на електрическите централи във Великобритания, по състояние към края на 2011 г., възлиза на 89 115 мВт, от които дялово: ТЕЦ – 78%; ВЕЦ и ПАВЕЦ – 5%; АЕЦ – 12%; ВЕИ (други) – 5%. [15]

Брутното производство на електрическа енергия във Великобритания, за същия период, възлиза на 364,897 гВтч. [15]

Основния дял от произведената електроенергия се пада на повече от 180 крупномащабни електрически централи.

Електропреносната мрежа, разгърната на територията на страната, се състои от електропреносни линии с номинално напрежение 400 кВ (11 500 км), 275 кВ (9800 км) и 132 кВ (5250 км). [16]

Електроразпределението се осъществява от четиринадесет лицензирани оператори на разпределителни мрежи, всеки от които оперира в определена област. Операторите са собственост на шест електроразпределителни компании: [17]

- *Scottish & Southern Energy* (Северна Шотландия и Южна Англия);
- *Scottish Power* (Южна Шотландия, Северен Уелс, Мърсисайд и Чешър);
- *Northern Powergrid* (Североизточна Англия и Йоркшир);
- *Electricity North West Ltd* (Северозападна Англия);
- *Western Power Distribution* (Централна източна, Централна западна и Югозападна Англия, Южен Уелс);
- *UK Power Networks* (Източна Англия, Югоизточна Англия и столицата Лондон).

В допълнение, има няколко независими оператори на разпределителните мрежи, които притежават и експлоатират нови инфраструктури за дистрибуция на електроенергия извън основните четиринадесет. Това са предимно мрежови разширения, разработени за осигуряване на нови жилища или промишлени райони.

Министерството на промишлеността и търговията (Ministerstvo průmyslu a obchodu České republiky – MPO) е носител на главната отговорност за провеждането и осъществяването на **националната политика** в **енергийния сектор на Чешката република** (ЧР). Регулиране на прякото изпълнението е отговорност на *Службата за енергийно регулиране* (Energetický regulační úřad – ERU), която е създадена на 1 януари 2001 г. в съответствие с разпоредбите на Закона за енергетиката № 458/2000. *ERU* е автономен орган, пряко отговарящ за регулирането на енергийния сектор. [18]

Законът изрично възлага на *ERU* задачата за регулиране на пазара с цел поддържане на пазарни механизми гарантиращи свободната конкуренция в областта на енергийната промишленост. Службата участва в изготвянето на необходимите нормативни актове, подпомага дейността на *MPO* чрез технически консултации и експертизи. Упълномощена е да издава наредби (главно публични съобщения и решения за ценообразуването), чрез които осъществява своите правомощия, които включват: [18]

- ценови контрол;
- издаване, изменение и отнемане на лицензи;
- поддръжка за използване на възобновяеми и вторични енергийни източници, както и комбинирано производство на топлинна и електрическа енергия;
- защита на интересите на потребителите (частни интереси);
- защита на притежателите на лицензии (корпоративни интереси);
- проверки по прилагането на условията за гарантиране на свободна конкуренция;
- сътрудничество със Службата за защита на конкуренцията (ÚOHS);
- подкрепа за свободната конкуренция в енергийната индустрия;
- надзор върху пазарите в енергийната промишленост.

Електроенергийния сектор на ЧР е доминиран от три вертикално интегрирани частни компании: *CEZ Group, E.ON Energie* и *Pražská energetika a.s.* Тези компании притежават лицензии за производство, разпределение, доставка и търговия с електрическа енергия, но чрез дружества, които са юридически разделени.

Като доставчици, трите компании имат пазарен дял над 95% от общото потребление, с ясно изразено лидерство на *CEZ*. Съотнесено към малките битови потребители, делът им е над 99%. В страната активно оперират и около десет независими малки доставчици, работещи на пазара на дребно.

Електроенергийната система на Чешката република е систематично разработвана повече от 110 години. Обединява една единна електропреносна мрежа, три регионални електроразпределителни мрежи (свързани към преносната), и повече от 300 местни електроразпределителни мрежи, свързани към регионалните разпределителни системи. Приблизително 5,8 милиона потребители са свързани към ЕЕС на ЧР от всички нива на напрежение. [19]

Инсталираната **генераторна мощност** на електроцентралите присъединение към ЕЕС на ЧР възлиза на 20 250 мВт, по данни към края на 2011 г. От тях: ТЕЦ – 11 887 мВт (59%); ВЕЦ и ПАВЕЦ – 2200 мВт (11%); АЕЦ 3970 – (20%); ВЕИ – 2189 мВт (11%). [20] Повечето от големите генератори са присъединени към електропреносната и електроразпределителните мрежи на ниво 110 кВ. [19]

73% от капацитета на националното производство е собственост на доминиращата *CEZ*, останалите, приблизително 2000 мВт от инсталираната мощност е собственост на малки локални производители, чиито единичен дял не превишава 3%.

Забележително е да се спомене, че на глава от населението, ЧР се явява най-големият нетен износител на електроенергия в света.

Средно около 65% от годишно произвежданата електрическа енергия в страната е от ТЕЦ на въглища.

Към ЕЕС на ЧР са присъединени две ядрени централи, АЕЦ „Темелин“ (2000 мВт) и АЕЦ „Дуковани“ (2040 мВт). [21, 22] Площадките на двата комплекса са собственост и се експлоатират от *CEZ*.

Бртното производство на електрическа енергия в ЧР, по данни към края на 2011 г., възлиза на 87 560 гВтч, от които дялово: ТЕЦ – 53 928 гВтч (62%); ВЕЦ и ПАВЕЦ – 2835 гВтч (3%); АЕЦ – 28 282 гВтч (32%); ВЕИ – 2515 гВтч (3%). [20]

Електропреносната мрежа е изпълнена чрез линии 440 кВ (3508 км.), 220 кВ (1910 км.) и 110 кВ (83 км.). Включва 26 бр. подстанции 420 кВ, 14 бр. подстанции 245 кВ и 1 бр. подстанция 123 кВ с обща трансформаторна мощност от 19 980 мВтА. [23]

След пълната приватизация на електроразпределението през 2005 г., експлоатацията на регионалните **електроразпределителни мрежи** се осъществява от три електроразпределителни дружества, всяко от които осъществява дейността си в определен регион(и) от територия от страната:

- *ČEZ, a.s.* (осъществява електроразпределителна дейност на територията на Среднобохемски, Пилзенски, Карловарски, Устецки, Либерецки, Краловохрадецки, Пардубицки, Оломоуцки и Моравско-силезски край);
- *E.ON Česká republika* (осъществява електроразпределителна дейност на територията на Южноморавски, Злински и Височински край);
- *PRE Holding group* (Pražská energetika, a.s. (осъществява електроразпределителна дейност на територията на столицата Прага).

Единното управление на ЕЕС на ЧР се осъществява от националния електроенергиен системен оператор – *ČEPS*. Основните дейности на *ČEPS* включват: осигуряване на безопасно, сигурно функциониране и планово развитие на ЕЕС на ЧР, като част от европейските синхронизирани системи за пренос; осигуряване на

управлението и оперативния контрол, преноса на електрическа енергия от производителите до доставчиците; осигуряване на баланс между производството на електроенергия и нейната консумация в реално време; участие в организирането на търгове за разпределяне на наличния преносен капацитет по междусистемните връзки. [24]

За осъществяване на основните дейности, *ČEPS* решава задачи с възрани с прякото предоставяне на системни и електропреносни услуги.

Чрез системните услуги *ČEPS* осигурява необходимото качество и надеждност на снабдяването с електрическа енергия на ниво електропреносна мрежа, както и изпълнението на международните ангажименти и условията за паралелна синхронна работа на ЕЕС на ЧР с електроенергийните системи на другите европейски страни. [25]

Системни услуги включват: [25]

- поддържане на качеството на електроенергията;
- поддържане на баланса на мощностите в реално време;
- възстановяване на електрозахранването при аварии;
- диспечерски контрол.

Чрез електропреносните услуги, *ČEPS* осигурява преноса на електрическа енергия от производителите до районите на потребление в ЧР (вътрешен пренос) и износ/внос от чужбина (трансграничен пренос). [26]

100% от капитала на *ČEPS* е собственост на ЧР, контролиран от Министерството на промишлеността и търговията.

Литература

1. European Energy Regulators. About the European Energy Regulators, 2013, CEER/ACER, <http://www.energy-regulators.eu.>.

2. The European Network of Transmission System Operators for Electricity. ENTSO-E : Member Companies, 2013, ENTSO-E, <https://www.entsoe.eu>.

3. The European Network of Transmission System Operators for Electricity. About ENTSO-E. 2013, ENTSO-E, <https://www.entsoe.eu>.

4. Electricity Act 1989, 2013, <http://www.legislation.gov.uk>.

5. British Electricity Trading and Transmission Arrangements (BETTA), 2013, <http://webarchive.nationalarchives.gov.uk>.

6. Office of Gas and Electricity Markets. Renewables Obligation. 2013, Ofgem, <http://www.ofgem.gov.uk>.

7. Department of Energy & Climate Change. 2013, DECC, <http://www.gov.uk>.

8. Office of Gas and Electricity Markets. About. 2013, Ofgem, <http://www.ofgem.gov.uk>.

9. UK Power. The Big Six Energy Companies. 06.2012, <http://www.ukpower.co.uk>.

10. Compendium of HVDC schemes. CIGRÉ Technical Brochure No. 003. 1987, 03.2013, 194–199 с.

11.<https://www.energy.siemens.com/cms/00000011/de/reused/Documents/h1_conf_etg05_presentation_1313764.pdf>.

12. Howarth, B., Coates, M., Renforth, L., „Fault location techniques for one of the World's longest AC interconnector cables“. 8th IEE International Conference on AC and DC Power Transmission. 2006, 14–18 c.

13. „The Longest AC Subsea Cable in the World“. Major Assets, Manx Electricity Authority. 2008, 03.2012, <http://www.gov.im>.

14. „BritNed begins laying UK-Netherlands marine electricity cable“. сп. Power Engineering. 2009, 03.2013, PE, <http://www.power-eng.com>.

15. Department of Energy & Climate Change. Digest of UK energy statistics' (DUKES), Chapter 5: Electricity. 2012, 117–121 c., 03.2013, DECC, <http://www.gov.uk>.

16. NationalGrid. National Electricity Transmission System (NETS) Seven Year Statement. Chapter 6 – The Transmission System. 2011, NGET, <http://www.nationalgrid.com>.

17. National Grid. Distribution Network Operator (DNO). Companies. 2013, NGET, <http://www.nationalgrid.com>.

18. The Energy Regulatory Office. 2013, ERO, <http://www.eru.cz>.

19. Ministerstvo průmyslu a obchodu České republiky. „Economic assessment of all the long-term costs and benefits for the market and the individual costumer through application of smart metering systems in the Czech Republic power sector“. 2013, 10 c., MPO, <http://www.mpo.cz>.

20. The Energy Regulatory Office. Yearly Report on the Operation of the Czech Electricity Grid for 2011, P., 2012, 6–11 c., ERO, <http://www.eru.cz>.

21. CEZ Croup. The Temelín Nuclear Power Station. 2013, CEZ, <http://www.cez.cz>.

22. CEZ Croup. The Dukovany Nuclear Power Station. 2013, CEZ, <http://www.cez.cz>.

23. ČEPS a.s. Technical infrastructure : Transmission system data. 2013, ČEPS, <http://www.ceps.cz>.

24. ČEPS a.s. Services. 2013, ČEPS, <http://www.ceps.cz>.

25. ČEPS a.s. Services : System Services. 2013, ČEPS, <http://www.ceps.cz>.

26. ČEPS a.s. Services : Transmission Services. 2013, ČEPS, http://www.ceps.cz

СЪСТОЯНИЕ И УПРАВЛЕНИЕ НА ЕЛЕКТРОЕНЕРГИЙНАТА СИСТЕМА НА САЩ

Здравко Ю. Кузманов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и Кис“, Шумен
Катедра „Информационна сигурност“

STATE AND MANAGEMENT OF POWER SYSTEM OF U.S.

Zdravko Y. Kuzmanov

KEY WORDS *United States, power systems, management.*

Пазарните сегменти в електроенергийния сектор на САЩ се регулират от различни държавни институции, някои с препокриващи се функции.

Федералното правителство определя стратегическата политика в сектора чрез *Министерството на енергетиката* (Department of Energy – DOE), политиката по опазване на околната среда чрез *Агенцията за опазване на околната среда* (Environmental Protection Agency) и политиката за защита на потребителите чрез *Федералната търговска комисия* (Federal Trade Commission). Безопасността на атомните електроцентрали се съблюдава от *Комисията за ядрено регулиране* (Nuclear Regulatory Commission). Икономическото регулиране е отговорност на държавата, осъществявана от *Федералната комисия за енергийно регулиране* (Federal Energy Regulatory Commission – FERC). На ниво федерален щат обикновено се извършва чрез щатски регулаторни комисии с относителна самостоятелност.

Пряка отговорност за изпълнението на стратегическата политика в областта на електроенергетиката има Министерството на енергетиката. Ключова роля в това направление е на Службата за електроенергийни доставки и енергийна надеждност (Office of Electricity Delivery and Energy Reliability – OE), влизаща в състава на ведомството. [1]

Регулиране на ниво отделни щати се осъществява от комисии по комунално обслужване (Public Utilities Commissions – PUCs), официалното название и пълномощия на които са различни за всеки щат. В сферата на компетенциите на регионалните власти влизат, по правило, регулирането на търговията (в предела на съответния щат) и разпределението на електроенергията, въпроси относно организацията и дейността на комуналните електроенергийни компании.

САЩ е втората страна в света по производство на електроенергия. [2,3] На територията на Северна Америка се потребява около 20% [4] от общото световно производство на електрическа енергия.

Сумарната инсталирана **генераторна мощност** на електрическите централи в САЩ, по състояние към края на 2011 г., възлиза на 1 050 900 мВт, от които: [4]

- ТЕЦ – 785 900 мВт (74,8%);
- ВЕЦ и ПАВЕЦ – 78 700 мВт (7,5%);

- АЕЦ – 101 400 мВт (9,7%);
- ВЕИ – 64 300 мВт (5,8%);
- Други – 23 700 мВт (2,2%).

На територията на страната функционират повече от 18 000 електрически централи. [4] Около 80% от електроенергията в САЩ се произвежда от частни генериращи компании. Останалата електроенергия се произвежда от федерални агенции като *Tennessee Valley Authority* (производство основно от ядрени и водноелектрически централи), *Bonneville Power Administration* (в тихоокеанския северозапад). Най-големите частни производители се явяват *AES Corporation*, *Duke Energy* (57 700 мВт), *American Electric Power* (38 000 мВт), *Luminant* (15 400 мВт) и др. [5,6,7]

Брутното производство на електрическа енергия в САЩ, по състояние към края на 2011 г., възлиза на 3,856 млрд. кВтч. 68% от произведената електроенергия е от изкопаеми горива (въглища, природен газ и нефт), 37% от които въглища. [4]

От икономикогеографска гледна точка, електроенергетиката на САЩ е разделена на **пет електроенергийни системи,** с относително затворена система за доставка на електроенергия: Източна, Западна, Тексас, Аляска и Квебек. [8]

Тези електроенергийни системи (наречени interconnections) влизат в състава на „Корпорацията за електроенергийна надеждност на Северна Америка“ (North American Electric Reliability Corporation – NERC), в рамките на която се извършва координацията в управлението на отделните структури. *NERC* представлява саморегулируема организация с нестопанска цел, която включва представители на всички сфери в отрасъла: електроенергийни компании, държавни органи и потребители. Към основните функции на *NERC* се отнасят разработка, съгласуване и контрол при прилагането и изпълнението на стандартите за надеждно функциониране на ЕЕС, мониторинг и анализ на проблеми, свързани с надеждността. [8]

Стандартите носят, по правило, препоръчителен характер и не са подкрепени от действителни санкции. В електроенергетиката на САЩ те се явяват задължителни за всички субекти на отрасъла.

Петте ЕЕС и прилежащите им електропреносни мрежи, се управляват от т.нар. Независими системни оператори (Independent System Operator – ISO) и Регионални електропреносни организации (Regional Transmission Organization – RTO).

ISO представлява организация, формирана по нареждане или препоръка на Федералната комисия за енергийно регулиране на доброволен принцип. На управляваната оперативна територия ISO координира, контролира и наблюдава надеждното функциониране на съответната ЕЕС, обикновено в рамките на един щат, но в някои случаи обхваща и няколко съседни щата. [9]

RTO е организация, формирана при одобрението на *FERC*. Функциите и оперативната територия са идентични с тези на *ISO*. Основната разлика между тях се заключава в това, че независимите системни оператори не покриват минимални изисквания, посочени от *FERC*. За да придобие статус на регионална електропреносна организация, всеки независим оператор, трябва да покрива комплекс от минимални изисквания, включващи четири характеристики и седем функции. [10]

Към момента има десет *ISO/RTO* оперираци в Северна Америка: [11]

- *CAISO* (California ISO) – независим оператор на Калифорния;
- *NYISO* (New York ISO) – независим оператор на Ню Йорк;

- *ERCOT* (Electric Reliability Council of Texas) – независим оператор на Тексас, също и Регионален съвет за надеждност;
- *MISO* (Midwest Independent Transmission System Operator) – независим оператор и регионална електропреносна организация на Централна западна част на САЩ и провинция Манитоба, Канада;
- *ISO-NE* (ISO New England) – независим оператор и регионална електропреносна организация на Ню Ингланд;
- *AESO* (Alberta Electric System Operator) – независим оператор на Албърта;
- *OIESO* (Independent Electricity System Operator) – независим оператор на „Хидро Едно“ електропреносна мрежа на Онтарио, Канада;
- *NBSO* (New Brunswick System Operator) – независим оператор на Ню Брунсуик;
- *PJM* (PJM Interconnection) – регионална електропреносна организация на щатовете Делауеър, Илинойс, Индиана, Кентъки, Мериленд, Мичиган, Ню Джърси, Северна Каролина, Охайо, Пенсилвания, Тенеси, Вирджиния, Западна Вирджиния и окръг Колумбия;
- *SPP* (Southwest Power Pool) – регионална електропреносна организация, също и Регионален съвет за надеждност;

Десетте *ISO/RTO* опериращи в Северна Америка образуват „Съвет на Независимите оператори и Регионални електропреносни организации (ISO/RTO Council – IRC). Работата на IRC е насочена към разработване на ефективни процеси, инструменти и методи за подобряване на конкуренцията на пазарите на електроенергия в цяла Северна Америка. [12]

RTO са сходни, но не идентични с регионалните съвети за надеждност (Regional Reliability Councils), организации с нестопанска цел, също влизащи в състава на NERC, отговорни за повишаване на надеждността, сигурността и управлението на общата електроенергийна система в САЩ, Канада и северната част на Баха Калифорния, Мексико. Регионалните съвети за надеждност включват представителства на всички субекти в електроенергетиката на съответния регион.

Източната електроенергийна система обхваща, практически почти цялата източната част на Северна Америка, простираща се от подножието на Скалистите планини до атлантическото крайбрежие, с изключение на основната част от щата Тексас. Явява се най-голямата по площ и брой потребители ЕЕС в Северна Америка. Свързана е в паралелна работа, чрез междусистемни връзки със Западната електроенергийна система, ЕЕС Тексас и системи от северната част на Канада, не влизащи в състава на *NERC*. [13]

В рамките на Източната ЕЕС влизат шест регионални съвета за надеждност:

- *Съвет за надеждност и координация на Флорида* (Florida Reliability Coordinating Council – FRCC), покрива територията на целия Щат Флорида; [14]
- *Централен западен съвет за надеждност* (Midwest Reliability Organization – MRO), покрива щатите Минесота, Северна Дакота и Небраска, части от Монтана, Южна Дакота, Айова, Уисконсин, Горна Пенсилвания – Масачузетс, както и провинциите Саскачеван и Манитоба, Канада. В зоната на MRO се намират четири от шестте междусистемни връзки, свързващи Из-

точната със Западната ЕЕС, както и част от системите в Северна Канада, не влизащи в състава на NERC; [15]

- *Североизточен съвет за електроенергийна координация* (Northeast Power Coordinating Council – NPCC), покрива основната част от Ню Ингланд, щатите Мейн, Върмонт, Ню Хемпшър, Масачузетс, Ню Йорк, Кънектикът, Роуд Айлънд, провинциите Онтарио, Квебек, Ню Брънзуик, Нова Скотия и остров Принц Едуард, Канада. В зоната на NPCC също се намират междусистемни връзки с част от системите в Северна Канада, не влизащи в състава на NERC. По отношение на системното натоварване, NPCC покрива 20% от общото за Източната ЕЕС и 70% от цялото натоварване на Канада. Системата „Хидро-Квебек“[11], обхващаща цялата провинция Квебек, обикновено се счита за част от Източната ЕЕС, въпреки че технически е отделна електроенергийна система. Тя се свързва с NPCC, посредством четири междусистемни връзки високо напрежение; [16]
- *Първи съвет за надеждност* (ReliabilityFirst Corporation – RFC), покрива щатите Ню Джърси, Пенсилвания, Далауеър, Мерилънд, Вирджиния, Западна Вирджиния, Охайо, Мичиган, Кентъки, Тенеси, Индиана, Илинойс, Уисконсин и федерален окръг Колумбия; [17]
- *Корпорация за надеждност SERC* (SERC Reliability Corporation), покрива основната част от Югоизточна Северна Америка, щатите Мисури, Алабама, Тенеси, Северна Каролина, Южна Каролина, Джорджия, Мисисипи, части от Айова, Илинойс, Кентъки, Вирджиния, Оклахома, Арканзас, Луизиана, Тексас и Флорида; [18]
- *Югозападен електроенергиен тръст* (Southwest Power Pool, Inc. – SPP), покрива централната част от Югоизточна Северна Америка, щатите Канзас и Оклахома, части от Ню Мексико, Тексас, Арканзас, Луизиана, Мисури и Небраска. В зоната на SPP се намират две от шестте междусистемни връзки, свързващи Източната със Западната ЕЕС, както и две междусистемни връзки към ECORT, ЕЕС Тексас. [19]

Западната електроенергийна система обхваща, практически цялата западна част на Северна Америка, от подножието на Скалистите планини до западното крайбрежие. Свързана е в паралелна работа, чрез шест междусистемни връзки със Източната ЕЕС, системи от северната част на Канада и северозападната част на Мексико, не влизащи в състава на *NERC*. [20]

В рамките на Западната ЕЕС влиза един регионален съвет за надеждност: *Западен съвет за електроенергийна координация* (Western Electricity Coordinating Council – WECC), покрива щатите Вашингтон, Орегон, Калифорния, Айдахо, Невада, Юта, Аризона, Колорадо, Уайоминг, части от Монтана, Южна Дакота, Ню

[11] Хидро-Квебек е държавна компания, създадена през 1944 г. от правителството на Квебек, със седалище в Монреал. Компанията ръководи производството, преноса и разпределението на електроенергия в цялата провинция Квебек. С над 60 водноелектрически и една атомна електроцентрала, Хидро-Квебек е най-големия производител на електрическа енергия в Канада и една от най-големите производители на електрическа енергия от ходроресурси в света.

Мексико и Тексас в САЩ, [21] провинциите Британска Колумбия и Алберта в Канада, и част от системата на *CFE*[12] в Баха Калифорния, Мексико.

Електроенергийната система Тексас обхваща почти цялата територия на едноименния щат. Свързана е в паралелна работа, чрез две междусистемни връзки високо напрежение с Източната ЕЕС и системи в Мексико, не включени в състава на *NERC*. В рамките на ЕЕС Тексас влиза един регионален съвет за надеждност: *Електроенергиен съвет за надеждност на Тексас* (Electric Reliability Council of Texas – ERCOT). [22]

Електроенергийната система Квебек обхваща, практически цялата провинция Квебек и е свързана в паралелна работа, чрез две междусистемни връзки с Източната ЕЕС. Въпреки, че е функционално отделна електроенергийна система, често се разглежда като част от Източната ЕЕС. За това допринася и факта, че двете системи имат общ съвет за надеждност, NPCC. [23]

Електроенергийната система Аляска обхваща сравнително малка част от едноименния щат и не е свързана в паралелна работа с някоя от другите четири ЕЕС в САЩ. Поради изолирания си характер, често не се причислява към ЕЕС на Северна Америка. В рамките на ЕЕС Аляска влиза един регионален съвет за надеждност: *Съвет за координация на системите в Аляска* (Alaska Systems Coordinating Council – ASCC), асоцииран член на *NERC*. [8]

Около 75% от **разпределението** и продажбите на електроенергия до крайните потребители се извършва от частни компании, а останалата част от държавни и общински компании.

Литература

1. U.S. Department of Energy. 2013, DOE, <http://energy.gov>.

2. Barr, R., China surpasses US as top energy consumer. Associated Press. 16.06.2012.

3. CIA. United States. CIA World Factbook 2009. 16.06.2012, CIA, <http://www.cia.gov>.

4. U.S. Energy Information Administration. Electric Power Annual 2011. 06.2012, EIA, <http://www.eia.gov>.

5. Duke Energy. About. 2013, DE, < http://www.duke-energy.com>.

6. American Electric Power. About. 2013, AEP, < http://www.aep.com>.

7. Luminant. About. 2013, L, <http://www.luminant.com>.

8. North American Electric Reliability Corporation. 2013, NERC, <http://www.nerc.com>.

9. Order No. 888, 24/04/96. Final Rule. 2013, FERC, <http://www.ferc.gov>.

10. Order No. 2000A, 02/25/00. Final Rule. 2013, FERC, <http://www.ferc.gov>.

11. Federal Energy Regulatory Commission. Electric Power Markets: National Overview. 2013, FERC, <http://www.ferc.gov>.

12. ISO/RTO Council, <http://www.isorto.org>.

13. Eastern Interconnection, U.S. Department of Energy, <http://energy.gov>.

[12] Comisión Federal de Electricidad (Федерална електроенергийна комисия), мексиканската държавна електроенергийна компания. Втората най-мощна, с доминираща позиция в електроенергийния сектор на Мексико след Пемекс.

14. Amended and Restated Delegation Agreement Between NERC and FRCC, Exhibit A – FRCC Boundaries, 6/12/2012, NERC, <http://www.nerc.com>.

15. Amended and Restated Delegation Agreement Between NERC and MRO, Exhibit A – Regional Boundaries, 6/25/2012, NERC, <http://www.nerc.com>.

16. Amended and Restated Delegation Agreement Between NERC and NPCC. Exhibit A – Geographic Area. 1/1/2012. NERC, <http://www.nerc.com>.

17. Amended and Restated Delegation Agreement Between NERC and RFC. Exhibit A – Boundaries of Delegation Agreement. 3/11/2013. NERC, <http://www.nerc.com>.

18. Amended and Restated Delegation Agreement Between NERC and SERC. Exhibit A Regional Boundaries. 6/12/2012. NERC, <http://www.nerc.com>.

19. Amended and Restated Delegation Agreement Between NERC and SPP RE. 10/7/2011. NERC, <http://www.nerc.com>.

20. U.S. Department of Energy. Western Interconnection. 2013, DOE, <http://energy.gov>.

Western Area Power Administration. U.S. Department of Energy. 2013, WAPA, <http://ww2.wapa.gov>.

21. Amended and Restated Delegation Agreement Between NERC and WECC. Exhibit A – Regional Boundaries. 3/1/2012, NERC, <http://www.nerc.com>.

22. Amended and Restated Delegation Agreement between NERC and Texas RE, Exhibit A – Regional Boundaries. 10/7/2011. NERC, <http://www.nerc.com>.

23. Northeast Power Coordinating Council Inc., <http://www.npcc.org>.

СЪСТОЯНИЕ И УПРАВЛЕНИЕ НА ЕЛЕКТРОЕНЕРГИЙНАТА СИСТЕМА НА РУСКАТА ФЕДЕРАЦИЯ

Здравко Ю. Кузманов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и Кис“, Шумен
Катедра „Информационна сигурност“

STATE AND MANAGEMENT OF POWER SYSTEM OF THE RUSSIAN FEDERATION

Zdravko Y. Kuzmanov

KEY WORDS *Russian Federation, power systems, management.*

В съответствие с федералния закон за енергетиката на Руската федерация (РФ), държавно регулиране и контрол в сектора се осъществява от правителството, федералните органи на изпълнителната власт и органите на изпълнителната власт в субектите на РФ. [1]

На ниво правителството на РФ държавното регулиране в сферата на електроенергетиката се извършва от Правителствената комисия по въпросите на енергийния комплекс, природно-ресурсен потенциал и енергийна ефективност на икономиката, Правителствената комисията по въпросите на развитието на електроенергетиката и Правителствената комисия за гарантиране сигурността на доставките на електроенергия (федерален щаб).

Основните задачи на *Правителствената комисия по въпросите на енергийния комплекс, природно-ресурсен потенциал и енергийна ефективност на икономиката* са: [2]

- обезпечаване на координираните действия на органите на изпълнителната власт за разработване и реализация на основните направления на държавната политика в сферата на енергетиката;
- разработване на основните направления за усъвършенстване на нормативната база в сферата на енергетиката;
- разглеждане на предложения за структурни реформи в секторите на енергетиката и обезпечаване координираните действия на органите на изпълнителната власт за тяхната реализация;
- разглеждане на предложения, насочени към създаване на условия за формиране и насърчаване на енергийно-ефективна икономика и стимулиране на енергоснабдяването;
- анализ на работата на органите на изпълнителната власт и организации, касаещи развитието на инфраструктурни обекти, необходими за устойчиво развитие и функциониране на енергетиката;
- анализ на реализацията на дългосрочни програми за развитие и инвестиционни програми в енергетиката;
- разглеждане на предложения свързани с въпросите на тарифната политика и ценообразуването в секторите на енергетиката.

Основни задачи на *Правителствена комисията по въпросите на развитието на електроенергетиката* са: [3]

- координиране на дейността на федералните органи на изпълнителната власт и органите на изпълнителната власт в субектите на РФ в областта на електроенергетиката;
- подготовка на съгласувани предложения по приоритетни въпроси свързани с функционирането и развитието на електроенергетиката.

За решаването на тези задачи, Комисията разглежда:

- проекти на нормативни актове свързани с държавната политика в електроенергетиката;
- предложения по програми за дългосрочно развитие и функциониране на електроенергетиката;
- проблеми , касаещи Общия план за изграждане на електроцентрали до 2020 г. и инвестиционните програми на субектите в електроенергетиката, в уставния капитал на които РФ е страна.

През 2012 г. с цел координация на действията за развитие на енергийния комплекс, обезпечаване на промишлеността и екологична сигурност е създадена *Комисия към Президента на РФ по въпросите на стратегическото развитие на енергийния комплекс и екологичната сигурност*. [4]

Основните задачи на Комисията включват:

- обезпечаване на координираните действия на федералните органи на изпълнителната власт и органите на изпълнителната власт в субектите на РФ по разработване и реализация на основните направления на държавната политика в сферата на енергетиката;
- разработване на основните направления за усъвършенстване на правнонормативната база в енергетиката;
- обезпечаване на ефективността и прозрачността в действията на структурните организации в енергетиката с държавно участие;
- разглеждане на предложения за структурни реформи в секторите на енергетиката;
- разглеждане на програми за перспективно развитие на електроенергетиката, дългосрочни програми за развитие на енергийния комплекс и инвестиционни програми;
- разглеждане на предложенията и разработване на мерки, насочени към прилагането на държавната политика в областта на регулирането на цените (тарифообразуване) в енергетиката.

На ниво федерални органи на изпълнителната власт, ключова роля в държавното управление и регулиране на електроенергетиката има *Министерството на енергетиката на Руската федерация* (Министерство энергетики Российской Федерации). Ведомството разработва и прилага държавната политика и правнонормативната уредба в областта на енергетиката, управлява държавната инфраструктура в сферата на производството и потреблението на енергийни ресурси. [5]

Министерството на енергетиката разработва дългосрочните програми за развитие на електроенергетиката, отговаряйки на изискванията за гарантиране на сигурността на РФ, на базата на прогнозата за социално-икономическото развитие на държавата. Утвърждава инвестиционните програми на субектите в електроенергетиката, в които уставния капитал включва участието на държавата, прогнозира възможен недостиг на електроенергия в някои ценови зони на пазара на електроенергия, създава благоприятни условия за капиталовложения и осигурява хармонизиране на процеса по отдаване на обекти и съоръжения от Единната национална (общоросийска) електрическа мрежа (*Единой национальной (общероссийской электрической сети* – ЕНЭС) на териториални преносни организации. [5]

Министерството на икономическото развитие на Руската федерация (Министерство экономического развития Российской Федерации), формира ценовата политика в областта на електроенергетиката. Съвместно с Министерството на енергетиката и Федералната служба по тарифиране разработва и прилага единен подход в регулирането на цените (тарифите) за услугите в електроенергетиката. [6]

Съвместно с Министерството на енергетиката осъществява структурни преобразувания в сектора, с цел намаляване на пречките пред икономическото развитие, насърчаване на ефективността, както и развитието на конкуренцията. Министерството координира работата по намаляване на енергоемкостта на брутния вътрешен продукт на страната.

В областта на конкурентната борба *Федералната антимонополна служба* (Федеральная антимонопольная служба – ФАС России) контролира действията на субектите на пазара на електроенергия, преразпределението на дялове (акции) в уставния капитал на пазара на едро и дребно и тяхната собственост, общата стойност на инсталираните производствени мощности на електроцентралите, включени

в генериращи компании. ФАС също така контролира дейността на администратора на системата за търговия на електроенергийния пазар на едро и спазването на стандартите за оповестяване на информация. [7]

В областта на регулирането на цените (тарифите) и контрола по установяването и изпълнението им отговаря *Федералната служба по тарифиране* (Федеральная служба по тарифам – ФСТ России). ФСТ регулира тарифите за електроенергия, предоставяна от производителите към доставчици, които продават електрическата енергия на потребителите, определя лимити на тарифите за топлинна енергия, произведена в комбиниран цикъл на производство на електрическа и топлинна енергия, арбитрира разногласията между регулировъчните органи от по-ниско ниво, топлоснабдяващите и топлопреносни организации и потребителите. [8]

Органите на изпълнителната власт в субектите на Руската федерация в рамките на тяхната компетентност, утвърждават цените на електрическа и топлинна енергия и контролират тяхното прилагане. Проверяват дейността на доставчиците, координират изграждането на електроенергийни инфраструктурни обекти на съответната територията, създават регионални щабове за гарантиране сигурността на електроснабдяването и обезпечават тяхното функциониране.

Откритото акционерно дружество **„Системен оператор на Единната електроенергийна система“** (Открытое акционерное общество „Системный оператор Единой энергетической системы“ – ОАО „СО ЕЭС“) е специализирана организация, еднолично осъществяваща централизирано оперативно-диспечерско управление на Единната електроенергийна система (ЕЕС) на Руската федерация. [9]

За реализиране на своята дейност ОАО „СО ЕЭС“ решава три групи задачи: [9]

- управление на технологичните режими на работа на обектите от ЕЕС в реално време;
- обезпечаване на перспективното развитие на ЕЕС;
- обезпечаване на единството и ефективната работа на технологичните механизми на пазара на електроенергия.

ОАО „СО ЕЭС“ е най-високото ниво в системата на оперативно-диспечерското управление и изпълнява следните основни функции: [9]

- управление на технологичните режими на работа на обектите в електроенергетиката;
- контрол и наблюдение на установените параметри за надеждно функциониране на ЕЕС и качеството на електроенергията;
- регулиране честотите на електрическия ток, обезпечаване функционирането на системата за автоматично регулиране на честотите и мощността, както и противоаварийната автоматика;
- прогнозиране на обемите на производство и потребление на електроенергия и участие в процесите на формиране на резерв от производствени мощности;
- съгласуване на планово-ремонтно извеждане от експлоатация на обекти от преносната мрежа и производствени мощности на електрическа и топлинна енергия;
- контрол над субектите на електроенергетиката и потребителите на електроенергия за изпълнение на оперативни диспечерски команди и разпореждания, свързани с осъществяване на функциите на системния оператор;

- разработка на оптимални и устойчиви ежедневни графици за работа на електрическите централи и преносната мрежа на ЕЕС;
- организация и управление на паралелните режими на работа на ЕЕС на РФ със системите на съседни държави (Азербайджана, Беларус, Грузия, Казахстан, Киргизтан, Молдова, Монголия, Латвия, Литва, Таджикистан, Узбекистан, Украйна и Естония);
- формиране и въвеждане на технологични изисквания при присъединяване на нови субекти на електроенергетиката към ЕНЭС и териториалните разпределителни мрежи;
- контрол над реализацията на инвестиционни програми на генериращите компании;
- мониторинг на фактическото техническо състояние и нивото на работа на обектите в електроенергетиката.

Към момента структурата на ОАО „СО ЕЭС“ включва: централно диспечерско управление; обединени диспечерски управления (ОДУ) – 7 филиала; регионални диспечерски управления (РДУ) – 59 филиала; 5 представителства (в Брянска, Калужска, Орловска и Псковска област, Република Саха (Якутия), електросистеми, които управляват укрупнени регионални диспечерски управления); дъщерно дружество „Научно-технически център на Единната електроенергийна система“ (*Научно-технический центр Единой энергетической системы*). [9]

100% от капитала на ОАО „СО ЕЭС“, принадлежи на Руската федерация. [9]

От 2012 г. дружеството е включено в списъка на стратегическите предприятия в РФ. [10]

Откритото акционерно дружество „**Федерална електропреносна компания на Единната електроенергийна система“** („Федеральная сетевая компания Единойэнергетической системы“ – ОАО „ФСК ЕЭС“) е създадено в съответствие с програмата за реформиране на електроенергетиката на РФ, като организация пряко отговаряща за управлението на Единната национална (общоросийска) преносна мрежа (ЕНЭС), с цел нейното съхранение и развитие. [11]

Основните направления в дейността на ОАО „ФСК ЕЭС“, включват: [11]

- управление на ЕНЭС;
- предоставяне на услуги към субектите на пазара на електроенергия по пренос на електричество и присъединяване към електрическата мрежа;
- инвестиционна дейност за развитие на ЕНЭС;
- поддръжка в оптимално състояние на електропреносната мрежа;
- технически надзор над състоянието на електропреносните инфраструктурни обекти.

Към момента в структурната организация на ОАО „ФСК ЕЭС“ влизат следните организации, непосредствено предоставящи услуги за пренос на електроенергия и присъединяване към ЕНЭС: „Магистрални електропреносни мрежи“ (МЭС) – 8 филиала; „Предприятия магистрални електропреносни мрежи“ (ПМЭС) – 41 филиала. [11]

79,5% от капитала на ОАО „ФСК ЕЭС“ е собственост на Руската федерация.

От 2012 г. дружеството е включено в списъка на стратегическите предприятия в РФ. [10]

ОАО „ФСК ЕЭС“ заема първо място в света по дължина на електропреносни линии (121,7 хил. км) и трансформаторна мощност (311 хил. МВА) сред публични-

те електропреносни компании. Обектите от електропреносната мрежа са разгърнати на територията на 73 региона на РФ, с обща площ 13,6 млн. кв. км. [12]

Откритото акционерно дружество **„Холдинг МРСК“** (Открытое акционерное общество „Холдинг МРСК“ – ОАО „Холдинг МРСК“) е създадено в резултат на реорганизация и отделяне от състава на ОАО РАО „ЕЕС Росии“. [13]

Основните направления в дейността на дружеството включват управление на мрежите на електроразпределителния комплекс и определяне на стратегиите за неговото развитие. [13]

ОАО „Холдинг МРСК“ обединява междурегионални (МРСК) и регионални електроразпределителни компании (РСК), научно-изследователски, проектно-конструктурски институти и строителни организации. 97 филиала на МРСК/РСК са разгърнати на територията на 69 субекта на Руската федерация. [12]

В структурата на холдинга влизат 11 междурегионални и 5 регионални електроразпределителни компании, включващи повече от 100 филиала и 1694 регионални електроразпределителни мрежи. [12]

В сферата на отговорност на ОАО „Холдинг МРСК“ се експлоатират разпределителни електропроводни линии от различен клас, с номинално работно напрежение от 0,4 до 220 кВ. Общата дължина на електропроводните линии на дружеството възлиза на 2,07 млн. км. По дължина на управляваните линии и количеството на потребители, компанията се явява една от на-големите електроразпределителни организации в света. [12]

Основните **генериращи компании,** производители на електроенергия на пазара в Руската федерация, са: [12]

- 5 генериращи компании на пазара на едро (генерирующих компаний оптового рынка электроэнергии – ОГК), обединяващи най-големите ТЕЦ в РФ;
- ОАО „РусХидро“, обединяващо повечето от най-големите ВЕЦ, а също средните и малки централи (включително каскади);
- 13 териториални генериращи компании (ТГК), обединяващи електрически централи от няколко съседни региона, не влизащи в състава на ОГК и работещи в изолирани електросистеми – предимно ТЕЦ с комбиниран цикъл на производство на електрическа и топлинна енергия;
- ОАО „Концерн Росенергоатом“, обединяващ всички АЕЦ на територията на РФ.

Заедно с ОГК, ТКГ, ОАО „РусХидро“ и ОАО „Концерн Росенергоатом“, към 2012 г., на пазара на електроенергия участват и генериращи компании от група „ЛУКОЙЛ“, ОАО „Татенрго“, ОАО „СИБЕКО“, ОАО „Башкирска генерираща компания“, ОАО „Иркутскенерго“, ОАО „ИНТЕР РАО ЕЕС“ и други по-малки локални производители на електроенергия.

Единната електроенергийна система на Руската федерация се състои от 69 регионални системи, които от своя страна, образуват 7 обединени електроенергийни системи: Изток, Сибир, Урал, Средна Волга, Юг, Център и Северозапад. Всички ЕЕС са свързани посредством междусистемни линии високо напрежение (220-500 кВ) и работят в синхронен режим – паралелно. [9]

Единната ЕЕС е разгърната на територия, която обхваща осем часови зони. Необходимостта от пренос на електроенергия през такава голяма територия, обуславя широкото използване на електропроводни линии високо и свръхвисоко напреже-

ние. Системообразуващата електропреносна мрежа ЕНЭС се състои от електропроводи с номинално напрежение от 220, 330, 500, 750, 1150 кВ. [9]

В състава на Единната ЕЕС влизат около 700 електрически централи с генераторна мощност по-голяма от 5 мВт. Сумарната инсталирана генераторна мощност за 2012 г. възлиза на 223 070,83 мВт, от които дялово: ТЕЦ – 68,1%, ВЕЦ и ПАВЕЦ – 20,6%, АЕЦ – 11,3%. [9]

За Единната ЕЕС на РФ е характерна високата концентрация на мощност към единична електроцентрала. В ТЕЦ се експлоатират серийни енергоблокове с единична мощност 500 и 800 мВт и един блок с мощност от 1200 мВт в ТЕЦ Костромски. Единичната мощност на енергоблоковете в действащите АЕЦ, достига средно 1000 мВт.

Годишно от инсталираните генераторни мощности се произвежда около един милиард кВт/ч електроенергия. За 2012 г. брутната електроенергия произведена в електрическите централи, присъединени към Единната ЕЕС на РФ, възлиза на 1 032,1 млрд. кВт/ч., от които дялово: ТЕЦ – 67,76%, ВЕЦ – 15,05%, АЕЦ – 17, 19%. [9].

Управление на електроенергийните режими на седемте обединени и регионалните системи, разположени на територията на 79 субекта на РФ, се осъществява от филиали на ОАО „СО ЕЭС“, съответно обединени (ОДУ) и регионални (РДУ) диспечерски управления. [9]

В съответствие с принципите за функциониране на единното вертикално оперативно-диспечерско управление, регионалните подразделения на системния оператор са организирани в тристепенна йерархична структура в която влизат: [9]

- Централно диспечерско управление – изпълнителен апарат (гр. Москва);
- 7 Филиала – ОДУ;
- 59 Филиала – РДУ на електроенергийни системи на един или няколко субекта на РФ.

С цел взаимодействие на ОАО „СО ЕЭС“ със субектите на електроенергетиката, органите на изпълнителната власт в субектите на Руската федерация, териториалните органи на Ростехнадзор, Министерството на извънредните ситуации на РФ (МЧС РФ) в регионалните електроенергийни системи, управлявани от укрупнени диспечерски управления, са създадени представителства на системния оператор в Брянска, Калужска, Орловска и Псковска област, както и в Република Саха (Якутия). [9]

Паралелно с ЕЕС на РФ работят електроенергийните системи на Азербайджана, Беларус, Грузия, Казахстан, Латвия, Литва, Молдова, Монголия, Украйна и Естония. Чрез ЕЕС на Казахстан, електроенергийните системи от Централна Азия, Киргизстан и Узбекистан. Съвместно (несинхронно) с ЕЕС на РФ работи и електроенергийната система на Финландия, влизаща в състава на обединените ЕЕС на Скандинавия, NORDEL. Освен това, паралелно с ЕЕС на Норвегия и Финландия работят отделни генераторни мощности, Колска ТЕЦ, Северо-Западна ТЕЦ, както и Ленинградската енергосистема. [9]

Литература

1. Федеральный закон от 26.03.2003 № 35-ФЗ, Об электроэнергетике.

2. Положение о Правительственной комиссии по вопросам топливно-энергетического комплекса, воспроизводства минерально-сырьевой базы и повышения энергетической эффективности экономики, Утверждено постановлением

Правительства Российской Федерации от 11 февраля 2013 г. №109, <http://www.government.ru>.

3. Положение о Правительственной комиссии по вопросам развития электроэнергетики, Утверждено Постановлением Правительства Российской Федерации от 29 сентября 2008 г. № 726, <http://www.government.ru>.

4. Указ Президента РФ от 15.06.2012 № 859, О Комиссии при Президенте РФ по вопросам развития ТЭК и экологической безопасности, <http://graph.document.kremlin.ru>.

5. Министерство энергетики Российской Федерации, Положение о Министерстве энергетики Российской Федерации, (утв. постановлением Правительства Российской Федерации от 28 мая 2008 г. № 400) (в ред. постановлений Правительства Российской Федерации от 24 марта 2011 г.), <http://minenergo.gov.ru>.

6. Министерство экономического развития Российской Федерации, <http://www.economy.gov.ru>.

7. Федеральная антимонопольная служба, Общие сведения, ФАС, <http://www.fas.gov.ru>.

8. Федеральная служба по тарифам, О ФСТ, <http://www.fstrf.ru>.

9. Системный оператор Единой энергетической системы, ОАО „СО ЕЭС“, <http://so-ups.ru>.

10. Указ Президента РФ от 21.05.2012 № 688 О внесении изменений в перечень стратегических акционерных обществ, утвержденных Указ Президента РФ от 4 августа 2004 г. № 1004, <http://graph.document.kremlin.ru>.

11. Федеральная сетевая компания Единой энергетической системы, ОАО „ФСК ЕЭС“, <http://www.fsk-ees.ru>.

12. Министерство энергетики Российской Федерации, <http://minenergo.gov.ru>.

13. Холдинг МРСК, История компании,< http://www.holding-mrsk.ru>.

УПРАВЛЕНИЕ НА КРИЗИ

Христо Атанасов Десев

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и Кис“, Шумен
Катедра „Организация и управление на тактическите подразделения от полевата артилерия“

CRISIS MANAGEMENT

Hristo Atanasov Desev

Abstract: *The foundation of abilities to manage and respond to different types of crises and emergencies requires the improvement of the methods for planning and crisis management and the implementation of models for decision to allow a qualitative assessment of the results.*

The success in the resolution of a crisis is a possible alternative to the organizational structure which can defend in a most effective way the national interests and has the capacity to integrate, coordinate and address efforts, resources and help towards all citizens in the society.

Key words: *foundation of abilities, prevention, active power management, post-crisis recovery.*

Съвременната среда за сигурност съдържа широк и еволюиращ набор от предизвикателства за сигурността на териториите и населението на държавите. Кризите и конфликтите представляват директна заплаха за сигурността с която управлението на страните трябва да се справи, където и когато е това е необходимо. „*Сигурността чрез управление на кризи*” е основна задача залегнала в Лисабонската стратегия.

В Република България в резултат на това настъпиха редица промени в регламентиращите документи, като Стратегията за Национална сигурност, Националната отбранителна стратегия и др.

Основни положения в тях са прилаганите секторни политики за сигурност: политики по отношение връзката: *човек – природа* и *ресурсната сигурност.*

Управлението на кризи е комплекс от принципи, решения и мероприятия от различен характер, които се изразяват в наблюдаване на рисковите фактори влияещи върху сигурността, анализиране на ситуациите и своевременно предупреждаване за възможни кризи в конкретно време и район.

На територията на страната това са мероприятия по превантивна и непосредствена защита на населението и националното стопанство при природни бедствия, аварии и катастрофи, срещу разпространението на оръжие за масово поразяване, незаконен трафик на оръжие, международен тероризъм и пресичане на терористични действия и по охрана на стратегически обекти.

Овладяването на кризите се постига с провеждането на операции при кризи от невоенен характер, в по-съвременните документи са операции в мирно време.

В най общия случай под операции в отговор на кризи от невоенен характер трябва да разбираме целенасочени действия за предотвратяване, овладяване и ликвидиране на кризи от хуманитарен характер на и извън територията на страната.

Анализът показва, че те се провеждат в мирно време и целят да минимизират щетите върху националното стопанство от природни бедствия и технологични аварии. Основните усилия са насочени към наблюдение на рисковите фактори, прогнозиране на възможните ситуации и ликвидиране на последствията след проявяване на кризата и задействане на ЕСС чрез спомагателни и аварийни дейности и такива по осигуряването на условия за оцеляване.

Редът за провеждане на операциите при кризи от невоенен характер е тясно обвързан с техния вид, характер, динамика на развитие на ситуацията, но дейностите условно могат да се групират в три етапа:

- поддържане в готовност на системите, разработване на сценарии (планове), наблюдение на показателите на уязвимост , обучение и подготовка на силите, обмен на информация;
- анализиране на новопостъпила информация, вземане на кризисно решение (уточняване на плановете), действия по антикризисна превенция, активиране на силите;
- проактивно управление на кризата (основни елементи са действията, предприети от носещите отговорност лица и служби полиция, пожарна, армия, болници, правителство), използването на всички налични ресурси, създаване на екип за бързо и координирано действие, анализ на последиците от кризата, на действията, (не)предприети по време на кризата, и подобряване на структурите за бърза реакция.

Изборът на технология за конкретна на реализацията на модел за управление изисква съответна организационна структура и нейното надграждане, избор на компонентност на действията, разпределение на отговорностите и диагностициране на работата на модела в съответствие на настъпилите изменения.

На тази база могат да се формулират следните цикли на управление:

- мониторинг и анализ на средата - вътрешна и външна;
- обработване на информационните сигнали и оценка на заплахата;
- разработване на хипотези - решения;
- изработване на механизми за избор най-доброто решение и неговата реализация;
- разпределение на избраното решение към изпълнителите, управляващо въздействие върху подсистемите;
- контрол - оценка на настъпилите изменения.

Теоретичните постановки и изследването на опита от практическите действия при управление на кризите от невоенен характер в световен мащаб показват, че може да се модифицира адаптиран модел на кризисно управление. Етапите в този модел имат времеви и ресурсни параметри, които обхващат широки граници на предварителна дейност и след кризисно възстановяване и отразяват различни нива на включване и взаимодействие на органи сили и средства в държавата.

Първият етап е програмираното на управление на кризата:

- превенция;

- създаване на материална и техническа база;
- оценка на рисковете и изготвяне на възможни сценарии на развитие;
- стратегии за интервенция в случай на нужда.

Вторият етап е активното управление на кризата, където основни елементи са:

- вземане на решение за разрешаване на кризата;
- действия на отговорните лица и институции съгласно разработените планове (правителство, МВР, БА, медицински заведения и т.н.т.);
- бързата реакция - съкращаване на времевият диапазон на действие и използването на всички ресурси;
- създаване на екипи за бързо и координирано действие (Task force).

Третият етап в управлението е посткризисен:

- анализ на проведените действия;
- подобряване на структурите за бърза реакция;
- предаване на управлението на други организации.

Този модел съответства на стратегията на ЕС за управление при кризи, която се състои от няколко елемента:

- сценарий на рисковете;
- идентифицирането на екипите и оборудване на държавите членки, за да стане ясно как европейските държави могат да си помогнат помежду си;
- доброволен ангажимент на страните-членки да предоставят екипи и оборудване за съвместна реакция при бедствия. стандартни модули, които могат да се сглобят и да се пуснат в действие там, където са необходими;
- общ транспорт и логистика;
- изграждане на център за реакция при кризи, като целта е да се премине от пасивна към активна регулация на действията.

Основа на превенцията се явява характеризирането на уязвимостите, определяне на обектите, които са потенциална заплаха, оценка и класификация на рисковете за възможните кризи и поддръжка на системата за информация на населението. Същността е съсредоточена върху периодична оценка и управление на риска за обектите, поддържане на нивата на риска под нивата на уязвимост като се въздейства върху предпоставките за възникване на опасности.

Осъществяването на превантивната дейност е пряко свързано с идентифицирането на опасностите и анализирането на обектите, които са потенциално уязвими и са източници на опасни процеси и събития. Голяма част от държавите систематизират тези потенциално опасни обекти с термина “критична инфраструктура” (КИ). Тя е термин, използван от правителствата за описание на активи, които са от съществено значение за функционирането на обществото и икономиката

Съществен момент е търсене и определяне на оценката на отделни обекти в зависимост от тяхната важност към общата система на безопасността в общината и областта. Тя представлява определяне на рейтинг на обектите от КИ в зависимост от степента на тяхното влияние върху цялостното функциониране на живота в региона. Ранговката е по фактори на заплахата обвързани с определен тежестен индекс и се задават предварително като отразяват региона, характера на промишленото производство и икономическата важност на обектите. Оценките могат да са в тристепенна скала и зависят от показателите на оценката. Показателите имат за цел да характеризират:

- вида на производствата;
- структурната важност на обекта;
- заплахите към този обект;
- количество на персонала;
- възможността за справяне с криза самостоятелно;
- мероприятия за ликвидиране на последствията, евентуална стойност на загубите;
- степен на подготвеност на персонала за съдействие и др.

Оценката на риска е основана на измеримостта му. Моделът на интегрирания риск е подчинен на вероятното количество на загубите и е функционално обвързан с честотата на реализация на неблагоприятните събития. Стойностното му изражение е в цената на спасения живот. Количеството на материалните загуби е съобразено с пределната величина, до която обектите са ремонтно пригодни и възможни за възстановяване. Нивото на екологичните загуби е величина на свръхзамърсеност на лито-, хидро- и атмосферата. За сравнение се въвежда потенциалния риск който създава мяра за опасностите, той характеризира пространствено-времевата честота на заплахата, която изобразява максималния риск за поразяване на хора, обекти и екосистеми. Потенциалният риск се явява показател за безопасността на гражданите и основна функция на държавата, поради което трябва да се нормира законодателно.

Ефективното управление на кризи основно зависи от своевременното и компетентно вземане на решение. Приложима е методика за вземане на решение за операцията в няколко стъпки, като са фиксирани целите на етапите, желаният краен резултат, същността на дейностите и евентуалните изпълнители.

Първи етап – Оценка и анализ на ситуацията

Този етап подпомага оценката на риска от операцията, определянето на необходимото количество сили и средства и ангажирането на допълнителни сили, синхронизацията на различните операции. Всеки участник предоставя анализ на информацията от своя ресор и изпълнението на предприетите мерки.

Същност на дейностите:

- Обл. У (или негов представител) определя зоната на аварията, бедствието;
- аналитични групи от експерти (от общините, ОблД ПБЗН) определят нивата на настоящите рискове и промяната в нивата на допустимост;
- формулират се новопоявили се рискове от:
  - наводнения, разширяване на огнища от пожари;
  - повреди по ел., ВиК, газопреносни системи;
  - второстепенни заплахи от химическо заразяване;
  - хуманитарни бедствия;
  - заплахи от проява на тероризъм и мародерство;
- разпределят се групите от участници, при необходимост се създава изнесен щаб в района на бедствието.

Втори етап - Обща оценка на ситуацията

Етапът позволява в първата част да се обобщят изводите за ситуацията, а с втората част насочва екипа към вариантите за провеждане на операцията.

Етапът преминава през стъпките:

- -активиране – активират се обектови и регионални сили, осъществява се окончателната връзка с други агенции и организации, актуализира се информацията и се увеличават разузнавателните усилия;

- оценка – уточнява се времето на събитието, определя се времето до неговата кулминация или преустановяване на активността, набелязват се потенциалните задачи и се определят исканията, насочени към централния щаб (център);
- указания на областния управител – увеличаване на групата (при необходимост), изисквания за външно сътрудничество, времеви график за формиране на решението, необходимост от съдействие, критерии за успех и съображения за поемания риск;
- анализ – извършва се комплексен анализ на възникналата ситуация, в който се преценява съпоставимостта ѝ със ситуации, за които има разработени планове, необходимата им корекция и привеждането им в действие. Тази стъпка може да доведе до приемане на ускорено решение и прилагането му за неутрализиране на ситуацията.

В резултат на този анализ Обл. У може да издаде заповед за извънредно положение, да уточни готовността на силите и средствата и след адаптация да пристъпи към прилагане на предварителен план за провеждане на операцията.

Трети етап: Ориентиране на екипа

Целта на етапа е анализ на задачите, които предстои да се решават, за постигане на успех в специфични условия и ключови фактори.

Същността на дейностите има определена последователност, която може да се променя в зависимост от условията и наличното време. Тя обхваща:

Начало: Областният управител отбелязва основните събития, причинили кризата, необходимостта от преоценка за приложимост и адаптация на съществуващите планове, действията на участниците при ликвидиране на кризата, техните ръководители и координатори.

Условия: Обобщават се нивото, обхватът и динамиката на създалата се ситуация, ключови фактори, налични участници за разрешаване на кризата, заплахи за региона от екологично естество, за граничните райони - възникнали международни ангажименти, състояние на общественото мнение.

Анализ на среда и участници: анализът на средата определя външните условия, при които ще се провежда операцията.

Оценката на участниците се определя от етапа на развитие на кризата, състоянието на силите и средствата, които участват в редуцирането на кризата, тяхното нарастване във времето и възможните действия за овладяване на кризата със собствени, регионални и национални сили.

Анализ на задачата:

- времеви параметри на кризата (времетраене от началото ѝ до евентуален край, време за нарастване на количествата сили и средства, рискове при ограничения във времето);
- район на кризата (изменения в релефа, райони за разполагане на силите, опасни райони);
- участници в овладяване на кризата (количества и техните възможности, модулни способности, рискове за участващите, допустими нива на критични способности);
- изисквания (предпоставки за успех и приоритетни направления);
- ограничения;
- рискове за успеха.

Анализ на елементите от кризата, подлежащи на въздействие: Анализът служи за определяне на действията, от които кризата ще се забави или предотврати, и способностите на силите, които имат най-силно влияние върху бедствието. Редът за извършване на анализ включва: елемента, към който да се въздейства с минимални последствия, кой и с какво може да въздейства (хора и техника), какво трябва да се направи, какви способности да се изграждат в силите за въздействие.

Оценка на условията. Окончателно ОБЛ.У определя целите на операцията, критериите за успех и показателите за постигане на ефективност

Разработването на модела осигурява връзката между създалата се ситуация и желаното крайно състояние на кризата. Основни стъпки в тази дейност се явяват определянето на критичните елементи, върху които трябва да се въздейства, и хронологичното им обвързване с целите на действията.

Четвърти етап: Разработване на план за провеждане на операцията

Целта на етапа е да се определи най-ефективният начин за провеждане на операцията. В преминатите етапи са определени условията за провеждане на дейностите: известни са оценките и анализът на ситуацията, определени са целите на операцията, фиксиран е моделът на операцията и са определени критериите за успех

Пети етап: Прилагане на решението и оценка

Прилагането на плана става със заповед на Обл. У в хода на операцията за поставяне на специфични задачи или при промяна на ситуацията с разпореждания. Този етап периодично диагностицира решението и валидира разработения план за операцията.

Щести етап: Преход

Деескалацията на кризата изисква в посткризисния период управлението на операцията да се предаде на други органи на местна власт, ръководители на нестопански организации и фирми. Постигнатите цели и крайното състояние осигуряват ниския риск и стабилност в района.

Управлението при кризи е сложен процес с много компоненти, които са в основата за постигане на по-голяма ефективност в координацията и взаимодействието на органите в условията на кризи. Дефиниране на приоритетите за осъществяване на ефективна координация и взаимодействие и на тяхна основа извеждане на механизмите, които оказват благоприятно влияние върху ефективността на координацията и взаимодействието в условията на кризи.

В основата на координацията и взаимодействието се застъпват принципи, които трябва да се спазват за постигане на общите цели.

Към тях се отнасят:

- определяне и разграничаване на компетенциите на всеки субект участващ в координацията и взаимодействието;
- необходимост от главно свързващо звено (кризисен щаб) или оторизиран представител на място (ГДПБЗН), към което да текат информационни потоци и йерархичната координация на всеки друг орган с него;
- съгласуване на частни плановете и мероприятия при ясно определяне на възможностите на другите субекти за координация и взаимодействие;
- определяне на границите на организационна и тактическа самостоятелност на органите и участниците;
- самостоятелно делегиране на права за действия по избора на средства;

- основният фокус е насочен към различната подготовка на експертите, които постоянно осъществяване на контрол за паралелното етапно изпълнение на задачите в рамките на координацията.

Стилът Task Force групира човешки, материални и технически ресурси, като участват в екипа - лекари, психолози, икономисти, еколози, политически анализатори и т.н., в зависимост от специфичната проблематика.

Управлението на кризисните комуникации в случай на бедствие обхваща: управление на наличните ресурси под силен натиск, взимане на важни решения при недостатъчна информация, поддържане на рационален и стратегически подход в ситуация с емоционални реакции, справяне с публичните дискусии, обвиненията и критиката към собствените действия.

Информация за обществото следва да се разпространява от служители от структурното звено (екип за комуникация), на което са възложени функции по управлението (кризисен щаб) като изпълнява задачи по осъществяване на комуникациите със средствата за масово осведомяване.

Основни задачи могат да бъдат:

- разработване на приложението към плана на организацията, свързана с управлението на информацията към медиите и висшите ръководители;
- подготовка и предоставяне на ключовите ръководители на организацията информация за обстановката, предприетите към момента действия и въведените режимни мерки в зоната на кризисната ситуация. Тази информация се съгласува с началника на кризисния център и се предоставя на висшите ръководители;
- предоставяне на информация на медиите, други организации (по възприетата комуникационна стратегия) и семействата за пострадали и загинали граждани и служители на организацията, за които има потвърдени данни;
- известява медиите и при необходимост чрез тях обявява телефони за връзка на гражданите с Центъра за управление, като упражнява управлението на този информационен поток;
- изготвя материали за медиите, с основни данни за организацията, ръководните служители, имащи непосредствено отношение към овладяването на кризата, основни новини за развитието на кризата или кризисната ситуация, обстановка и предприетите действия;
- организира провеждането на брифинги и пресконференции.

Управлението и координацията на кризисната комуникация е труден, но неизбежен елемент от операциите за справяне с кризите. Техните широки разновидности предполагат и различни подходи, които трябва да се подготвят предварително.

От изложеното мнение за управлението на кризи следва да се формират няколко извода:

1. Адаптирането на модел за управление на операции от невоенен характер е необходимо да обхваща комплексно дейностите: превенция, активно управление на силите, следкризисно възстановяване и има съществено значение за ефективността на крайните резултати.

2. Разгледаната методика за формиране на решение осигурява възможност за подробна оценка на ситуацията, активиране на сили от ЕСС, обобщаване обхвата на динамиката и ключовите фактори, оптимален избор на алтернатива и своевременно планиране на операцията.

3. Създаването на оперативни способности, чрез изграждане на интегрирани, високо подготвени екипи от специалисти със съвременни технически средства и възможности за действие върху цялата територия на страната ще позволи активно въздействие върху факторите на кризата в ескалационния етап ще намали щетите и ще улесни следкризисното възстановяване.

Литература:

1. Георгиева, Кр.: "Нови стратегии за реакция при кризи в Европа", публична лекция от 01-11-2010г. в хотел "Шератон".
2. Манев, М. Процедури за управление на кризи, С., ВЖ, кн. 5, 2001.
3. Ръководство за комуникацията на публичните органи при терористични кризи "SAFE-COMMS", 2011.
4. Стратегическа концепция за отбрана и сигурността на държавите членки на НАТО. Лисабонска стратегия.
5. Стандарт ISO/IES 31010-2009. Risk management - Risk assessment techniques.

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ГРАЖДАНИТЕ НА РЕПУБЛИКА БЪЛГАРИЯ

Сашо С. Евлогиев

Национален военен университет „В. Левски", Факултет „Артилерия, ПВО и КИС", гр. Шумен, Република България

PERSONAL DATA PROTECTION SITIZEN OF THE REPUBLIC OF BULGARIA

Sasho S. Evlogiev

ABSTRACT: Personal data means data which relate to a living individual who can be identified from those data, or from those data and other information. Personal data protection is one of the fundamental human rights of all citizens and is grounded in the Universal Declaration of Human Rights. Personal data protection is provided by one or more independent Bulgarian state authorities having control of the compliance with the Law on Personal Data Protection, adopted by each member state of the Council of Europe. These independent authorities and the Ministry of Interior in particular, are responsible for the implementation of the regulations asserted by the EU Legal Framework and the Bulgarian Legal Framework in the field of Personal Data Protection.

KEY WORDS: personal data, personal data protection, actions to protect personal data.

Личните данни на всеки български гражданин представляват съвкупност от информация за физическо лице, чрез която лицето може да се идентифицира пряко или непряко. Информацията за лицето съдържа един или няколко специфични признаци, които по обективен, безспорен и категоричен начин позволяват неговото посочване или разкриване. Информацията позволява съхраняване, обработване и разпространяване чрез определен идентификационен номер. Идентификационният номер на информацията за физическото лице е единствен и неповторим.

Защитата на личните данни е едно от основните човешки права на личността, както правото на живот, правото на свобода, правото на труд, правото на личен живот и други. Основните човешки права и свободи са залегнали във Всеобща декларация за защита правата на човека. Тези права и свободи при никакви обстоятелства не могат да бъдат упражнявани в противоречие с целите и принципите на Организацията на Обединените нации (ООН).

Проблемът за защита на личните данни е изключително актуален поради това, че от една страна всеки човек има право на защита на личните данни, като неотменно човешко право, а от друга непрекъснато нарастващия обем от информация, включително и личните данни и техния обмен в международен и национален мащаб. Като член на Европейския съюз Република България признава и приема да развива съюза между народите на страните членки на основата на мирното съвместно съществуване и на общи ценности, каквито са човешките права и свободи.

Като съзнава своето духовно и морално наследство, съюзът на страните от европейското семейство се основава на неделимите и универсални ценности на човешко достойнство, свобода, равенство и солидарност; той почива на принципа на демокрацията и на принципа на правовата държава. Той поставя човека в центъра на своята дейност, като учредява гражданството на Съюза и създава пространство на свобода, сигурност и правосъдие.

Съюзът допринася за съхраняването и развитието на тези общи ценности при зачитане многообразието на културите и традициите на европейските народи, както и националната идентичност на държавите-членки и организацията на техните публични власти на национално, регионално и местно равнище; той се стреми да насърчава балансирано и устойчиво развитие и гарантира свободното движение на хора, услуги, стоки и капитали, както и свободата на установяване.

За тази цел е необходимо да се засили защитата на основните права в светлината на развитието на обществото, на социалния прогрес, на научните и технологични постижения като те се включат в Харта, която ги прави по-видими.

При съблюдаване на компетенциите и задачите на Съюза, както и принципа на субсидиарност, настоящата Харта потвърждава отново правата, които произтичат по-специално от общите за държавите-членки конституционни традиции и международни задължения, както и от Европейската конвенция за защита на правата на човека и основните свободи, от приетите от Съюза и от Съвета на Европа социални харти, от практиката на Съда на Европейския съюз и на Европейския съд по правата на човека [2].

Ползването от тези права поражда отговорности и задължения на всяка държава, както спрямо другите държави-членки, така и спрямо човешката общност и бъдещите поколения. В чл. 8 на Хартата е записано, че 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.

Голямото значение и сериозността на проблема за защита на личните данни се потвърждава и от факта, че в Европейския парламент и Съветът на Европейския съюз е приета Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни. В нея се отчита, че:

- Общността подпомага, гарантиране на икономически и социален напредък чрез общи действия с цел премахване на бариерите, които разделят Европа, насърчаване на непрекъснато подобряване на условията на живот на европейските народи, запазване и укрепване на мира и свободата и насърчаване на демокрацията спазвайки основните права, признати в конституциите и законодателството на държавите-членки и в Европейската конвенция за защита на правата на човека и основните свободи;

- системите за обработка на данни са създадени с цел да служат на хората;

- независимо от националността или местожителството на физическите лица, е необходимо да се зачитат техните основни права и свободи и по-конкретно правото на личен живот, да допринасят за икономическия и социален прогрес, развитието на търговията и благосъстоянието на хората;

- създаването и функционирането на вътрешен пазар, в който е гарантирано свободното движение на стоки, хора, услуги и капитали, изисква не само личните данни да могат да се предават от една държава-членка в друга, но и основните права и свободи на лицата да бъдат гарантирани;

- в Общността все по-често се прибягва до обработване на лични данни в различни сфери на икономическия и социален живот на базата на напредъкът на информационните технологии;

- икономическата и социалната интеграция, произтичаща от създаването и функционирането на вътрешния пазар ще доведе безусловно до съществено увеличение на трансграничните потоци от лични данни между всички участници в икономическия и социален живот в държавите-членки;

- обменът на лични данни между предприятия, установени в различните държави-членки, се развива;

- националните власти в отделните държави-членки са призовани, по силата на правото на Общността, да си сътрудничат и обменят лични данни с цел да изпълняват своите задължения или да осъществят задачи от името на орган на друга държава-членка в контекста на пространство без вътрешни граници, което съставлява вътрешния пазар;

- засилването на научно-техническото сътрудничество и координираното въвеждане в Общността на нови далекосъобщителни мрежи изисква и улеснява трансграничните потоци от лични данни;

- различните степени на защита на правата и свободите на лицата при обработването на лични данни, разрешено в държавите-членки, могат да предотвратят предаването на данни от територията на една държава-членка до територията на друга държава-членка; тези различия могат да се превърнат в препятствие за осъществяването на множество икономически дейности на равнище Общност, да нарушат конкуренцията и да възпрепятстват органите на властта при изпълнението на техните отговорности съгласно правото на Общността;

- различието в степента на защита се дължи на съществуването на голямо многообразие от национални законови, подзаконови и административни разпоредби;

- с цел да се премахнат препятствията пред потоците от лични данни, степента на защита на правата и свободите на лицата при обработването на такива данни трябва да бъде еднаква във всички държави-членки;

- целта, която е от първостепенно значение за вътрешния пазар е трансграничният поток от лични данни да бъде регламентиран по последователен начин и в съответствие с целта на вътрешния пазар; това не може да се постигне единствено с усилията на държавите-членки, поради различията, които съществуват понастоящем между съответните закони на държавите-членки, и на потребността от съгласуване на законодателствата на държавите-членки;

- необходимо е да се предприемат действия на равнище Общност с цел сближаване на законодателствата в тази област;

- при еднаква защита, произтичаща от сближаването на националните законодателства, държавите-членки няма да могат да възпрепятстват свободното движение на лични данни помежду си, основавайки се на защитата на правата и свободите на лицата, и по-конкретно на правото им на личен живот;

- държавите-членки ще имат известна свобода на действие, която би могла да се използва от икономическите и социални партньори, следователно държавите-членки ще могат да конкретизират в своето национално законодателство общите условия, които определят законосъобразността на обработването на данни;

- държавите-членки се стремят да подобрят защитата, осигурена понастоящем от тяхното законодателство, като имат предвид, че в рамките на тази свобода на действие и в съответствие с правото на Общността биха могли да възникнат несъответствия при прилагането на директивата, което би оказало влияние върху движението на данни в дадена държава-членка и в Общността;

- предмет на националните законодателства, отнасящи се до обработването на данни е осигуряване спазването на основните права и свободи на Европейската конвенция за защита на правата на човека и основните свободи, както и общите принципи на правото на Общността;

- сближаването на тези законодателства не трябва да доведе до намаляване степента на защита, която те осигуряват, а обратно - да има за цел гарантиране на висока степен на защита в Общността;

- принципите на защита на правата и свободите на лицата и по-конкретно правото на личен живот, които се съдържат в директивата, дават съдържание и разширяват принципите, съдържащи се в Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на данни от 28 януари 1981 г.;

- принципите на защита трябва да се прилагат за всякакво обработване на лични данни, извършвано от всяко лице, чиято дейност се урежда от правото на Общността;

- трябва да се изключи обработването на данни, извършвано от физическо лице при упражняване на дейности, които са изключително лични или домашни, например кореспонденция и поддържане на адресни указатели;

- дейностите, които се отнасят до обществената сигурност, отбраната, държавната сигурност или дейностите на държавата в областта на наказателното право, са извън приложното поле на правото на Общността;

- обработването на лични данни е необходимо за гарантиране на икономическото благосъстояние на държавите и не попада в приложното поле на настоящата директива, когато това обработване се отнася до въпроси, свързани с държавната сигурност;

- поради значимостта на развитието в рамките на информационното общество, на техниките, използвани за улавяне, предаване, манипулиране, запис, съхранение и предаване на звук и картина, отнасящи се до физическите лица, настоящата директива следва да се прилага в пълна сила за обработването на такива данни;

- обработката на такива данни се обхваща от директивата, само ако тя е автоматизирана или ако обработваните данни се съдържат или са предназначени да се съдържат във файлова система, структурирана съгласно определени критерии, отнасящи се до лица, с цел осигуряване на лесен достъп до лични данни;

- обработването на звук и картина, например при видео- наблюдение, не попада в приложното поле на настоящата директива при условие че то се извършва за целите на обществената сигурност, отбраната, националната сигурност или при държавни дейности, свързани с областта на наказателното право или с други дейности, които не попадат в приложното поле на правото на Общността;

- обработването на звук и картина, извършвано за целите на журналистическа дейност или на литературно или художествено изразяване, и по-конкретно в областта на аудиовизията;

- с оглед да се гарантира, че лицата няма да бъдат лишени от защитата, която им се полага по силата на настоящата директива, всяко обработване на лични данни в Общността се извършва в съответствие със законодателството на една от държавите-членки и обработването се извършва под ръководството на администратор, установен в дадена държава-членка;

- когато на територията на няколко държави-членки е установен единединствен администратор, конкретно чрез дъщерни дружества, той трябва да гарантира за да се избегне всякакво заобикаляне на националните правила, че всеки от клоновете изпълнява задълженията, наложени му от националното законодателство по отношение на неговата дейност;

- когато обработването на данни се извършва от лице, установено в трета страна, това не трябва да възпрепятства защитата на лицата; в тези случаи обработването следва да се урежда от законите на държавата-членка, в която се намират средствата, използвани за обработването на данни, и следва да има гаранции за действително спазване на правата и задълженията;

- настоящата директива не накърнява правилата за териториалност, приложими в наказателното право;

- държавите-членки ще определят по-точно в приеманите от тях закони или при въвеждане в действие на мерките, при които обработването на данни е законосъобразно; държавите-членки, независимо от общите правила, могат да предвидят специални условия за обработването на данни, отнасящи се до конкретни сектори и до различните категории данни;

- държавите-членки са оправомощени да гарантират прилагането на защитата на лицата, както чрез общ закон за защита на лицата при обработването на лични данни, така и чрез секторни закони, например закони, отнасящи се до статистическите институти;

- принципите на защита трябва да бъдат отразени, от една страна, в задълженията, наложени на лицата, държавните органи, предприятията, агенциите и другите

органи, отговорни за обработването, както по отношение на качеството на данните, техническата надеждност, уведомяването на надзорния орган и обстоятелствата, при които може да се извършва подобна обработка, и от друга страна, в правата, предоставени на лицата, чиито данни са подложени на обработване, да бъдат уведомявани за извършването на такава обработка, да имат достъп до данните, да могат да поискат поправка и дори да възразят срещу обработването на данни при определени обстоятелства;

- принципите на защита трябва да се прилагат за всяка информация, отнасяща се до идентифицирано лице или подлежащо на идентификация лице; за да се определи дали едно лице подлежи на идентификация, следва да се разглежда съвкупността от всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице с цел идентифицирането на даденото лице;

- защитата на лицата трябва да се отнася в еднаква степен до автоматизираната обработка на данни и до ръчната им обработка; обхватът на тази защита не трябва да зависи от използваните техники, защото в противен случай това би създало сериозен риск от заобикаляне на закона; директивата обхваща само файловите системи, а не неструктурираните досиета; съдържанието на файловата система трябва да бъде структурирано според конкретни критерии, отнасящи се до лица, позволяващи лесен достъп до личните данни;

- всяко обработване на лични данни трябва да бъде законосъобразно и почтено по отношение на съответните лица; данните трябва да бъдат достатъчни, релевантни и да не бъдат прекомерни по отношение на целите, за които се обработват; целите трябва да бъдат ясно формулирани и законосъобразни и трябва да бъдат установени при събирането на данни; целите на обработването, последващи събирането, не трябва да бъдат несъвместими с целите, определени първоначално;

- обработването на лични данни с историческа, статистическа или научна цел не се разглежда като несъвместимо с целите, за които тези данни са събирани, при условие че държавата-членка даде подходящи гаранции; гаранциите трябва да попречат на използването на данни в подкрепа на мерки или решения, отнасящи се до дадено лице;

- за да бъде законосъобразно, обработването на лични данни трябва да се извършва със съгласието на съответното физическо лице или да бъде необходимо за сключване или изпълнение на договор, задължителен за съответното физическо лице, да бъде законово задължение, или за изпълнение на дадена задача, която е от обществен интерес, необходима за упражняване на публична власт, или да бъде в законен интерес на физическо или юридическо лице, при условие че интересите или правата и свободите на съответното физическо лице нямат преимущество;

- националното законодателство следва да определи дали администраторът, изпълняващ тази задача в интерес на обществото или упражняващ публична власт, трябва да бъде държавна администрация, физическо или юридическо лице, подчинено на публичното или на частно право, например професионална асоциация;

- данни, които по своя характер могат да нарушат основните свободи или личния живот, не могат да бъдат обработвани, освен ако съответното физическо лице не даде изричното си съгласие за това; например, когато обработването на тези данни се извършва за цели, свързани със здравословно състояние, от лица, които са задължени да пазят професионална тайна, или в хода на законосъобразна дейност

на някои дружества или фондации, чиято цел е да се позволи упражняването на основните свободи;

- държавите-членки могат да предвидят ограничения по отношение на правата на достъп и на информация и на някои задължения на администратора, доколкото те са необходими за гарантиране на националната сигурност, отбраната, обществената сигурност или на важни икономически или финансови интереси на държава-членка или на Съюза, както и за наказателно разследване, преследване и искове, свързани с нарушение на етиката при регламентираните професии;

- опростяването или освобождаването от задължението за уведомление не освобождава администратора от нито едно от другите му задължения, произтичащи от настоящата директива.

Спазвайки поетите международни ангажименти, като страна от Европейското семейство, Република България изразява своя непрекъснат стремеж към хармонизиране на националното законодателство с европейското международно публично право и стриктно спазване на поетите договорености. Защитата на личните данни се извършва на основата на изпълнението на разпоредбите на Закона за защита на личните данни от януари 2002 г.

Този закон урежда защитата на правата на физическите лица при обработването на личните им данни. Целта на закона е гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните. Законът се прилага за обработването на лични данни, както с автоматични средства, така и с неавтоматични средства, когато тези данни съставляват или са предназначени да съставляват част от регистър.

Този закон се прилага за обработването на лични данни, когато администраторът на лични данни е установен на територията на Република България и обработва лични данни във връзка със своята дейност или не е установен на територията на Република България, но е задължен да прилага този закон по силата на международното публично право или не е установен на територията на държава - членка на Европейския съюз, както и в друга държава - членка на Европейското икономическо пространство, но за целите на обработването използва средства, разположени на българска територия, освен когато тези средства се използват само за транзитни цели; в този случай администраторът трябва да посочи представител, установен на територията на Република България, без това да го освобождава от отговорност.

Доколкото в специален закон не е предвидено друго, този закон се прилага и за обработването на лични данни за целите на отбраната на страната, националната сигурност, опазването на обществения ред и противодействието на престъпността, наказателното производство и изпълнението на наказанията.

Когато в рамките на полицейско или съдебно сътрудничество данни са получени от или са предоставени на държава - членка на Европейския съюз, или органи или информационни системи, създадени въз основа на Договора за създаването на Европейския съюз или на Договора за функциониране на Европейския съюз, те се обработват при условията и по реда на този закон. Обработването на данните в този случай се извършва под контрола на съответния държавен орган.

Условията и редът за обработването на единен граждански номер (ЕГН) и на други идентификационни номера с общо приложение се уреждат в специални закони.

Личните данни трябва да се обработват законосъобразно и добросъвестно; да се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели; допълнително обработване на личните данни за исторически, статистически или научни цели е допустимо, при условие че администраторът осигури подходяща защита, като гарантира, че данните не се обработват за други цели с изключение на случаите, изрично предвидени в този закон.

По закон личните данни трябва да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват; да бъдат точни и при необходимост да се актуализират; да се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват; да се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват. Личните данни, които ще се съхраняват за по-дълъг период за исторически, статистически или научни цели, се поддържат във вид, непозволяващ идентифицирането на физическите лица.

Личните данни могат да бъдат обработвани допълнително за друга цел, различна от целта, за която са събрани, когато това обработване е съвместимо с целта, за която са били събрани данните и съществува основание, предвидено в закон, за обработване на данните за тази друга цел.

В законът са посочени кой е администратор на лични данни, какви са неговите права и задължения при обработването на лични данни. Законодателят е предвидил Комисия за защита на личните данни, която е независим държавен орган. „Комисията“ осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни (ЗЗЛД). Тя съдейства за провеждането на държавната политика в областта на защита на личните данни и е юридическо лице на бюджетна издръжка със седалище София и е първостепенен разпоредител с бюджет. Комисията е колегиален орган и се състои от председател и 4 членове. Членовете на комисията и председателят й се избират от Народното събрание по предложение на Министерския съвет за срок 5 години и могат да бъдат преизбирани за още един мандат.

В ЗЗЛД, глава четвърта, са посочени необходимите технически и организационни мерки, за защита на данните от случайно или незаконно унищожаване, от случайна загуба, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване. По закон администраторът на лични данни определя срокове за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаване на личните данни. Предвидени са специални мерки за защита, когато обработването включва предаване на данните по електронен път. Мерките са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени. Мерките и сроковете се определят с инструкция на администратора на лични данни, а „Комисията“ определя с наредба минималното ниво на технически и организационни мерки, както и допустимия вид защита. Наредбата се обнародва в „Държавен вестник“ [5].

Забранено е обработването на лични данни, когато те разкриват расов или етнически произход; политически, религиозни или философски убеждения, членство

в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели; отнасят се до здравето, сексуалния живот или до човешкия геном.

В заключение е необходимо да се посочи, че защитата на личните данни на гражданите на всяка демократична държава е основно човешко право, залегнало в редица фундаментални международни документа, определящи основните правата и свободи на човека, а тяхното съблюдаване е задължение на националните парламенти съгласно конституциите на държавите. Спазването на основните човешки права гарантира изграждането на един нов свят – свят, в който хората ще се радват на свобода на словото и убежденията си, ще бъдат свободни от страх и лишения като най-съкровения стремеж на човека, изграден на основата на уважение, защита на личното достойнство, свят без граници за свободно движение на стоки, хора и услуги.

Литература:

1. Общо събрание на ООН. Всеобща декларация за правата на човека. 1948.
2. Европейски парламент, Харта на основните права на Европейския съюз. Л. 2010.
3. Европейски парламент, Съвет на Европейския съюз. Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.Б., 1995.
4. Съвет на Европа. Конвенция 108 за защита на лицата при автоматизирана обработка на лични данни. Л., 1981.
5. Закон за защита на личните данни, ДВ бр. 1 от 2002, изм. и доп. ДВ бр.15 от 2013, С.

ИНФОРМАЦИОННА СИГУРНОСТ

СТАТИСТИЧЕСКИ МОДЕЛ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО НА ЗАПЛАХИТЕ ЗА КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ[1]

Атанас И. Начев **Станимир К. Железов**

Шуменски университет „Епископ Константин Преславски”,
E-mail: anatchev@abv.bg E-mail: stanzhelezov@yahoo.com

A STATISTICS MODEL FOR ASSESSING THE IMPACT OF THREATS TO THE COMPUTER SYSTEMS AND NETWORKS

Atanas I. Nachev **Stanimir K. Zhelezov**

ABSTRACT: *The specific features of the information protection systems in the computer systems and networks require the development of non-trivial methods for their analysis and assessment. Attempts for solutions in this area are given in this paper.*

KEY WORDS: *Computer Systems and Technologies, Networks, Model, Statistical Model, Information security.*

Нека бъде разгледана компютърна система (мрежа), която може да бъде подложена на въздействието на n заплахи. Времето между възникването на две заплахи от конкретен тип е случайна величина с произволен закон на разпределение.

Загубите, които възникват при настъпване на *i*-та заплаха са z_i.

В указаните условия ще се определи ефективността на системата за защита. За целта ще бъде обозначена посредством p_i вероятността за възникване на *i*-та, $i = \overline{1,n}$, заплаха и ще се вземе предвид факта, че възникването на *i*-та, $i = \overline{1,n}$, заплаха води до загуби z_i.

Общите загуби от възникнали заплахи заплахи ще се определят като $\overline{W} = \sum_{i=1}^{n} \overline{W} = \sum_{i=1}^{n} \Delta w_i \, (1 - P_i) \cdot$

Използването на аналитични модели за решаване на така дефинирания проблем е свързано с ограничения, като:

- трудно може да се отчете въздействието на различните заплахи, когато количествата на възникването им за определен период от време представляват случайни величини с различни закони на разпределение;

[1] Статията е частично финансирана от Фонд научни изследвания към Шуменски университет по проект РД-08-250/2013

- с редица ограничения може да се определи влиянието на едновременните възниквания на две и повече заплахи;

Използването на методите на статистическото моделиране (метод на Монте-Карло) [1, 2] позволява да се избегнат посочените недостатъци.

За формулиране на случайните величини със зададен закон на разпределение ще използваме генерирането на случайни числа с равномерен закон на разпределение в интервала [0, 1]. Процедурата на преобразуване на случайното число ξ_i равномерно разпределено в този интервал в случайно число x_i със зададен закон на разпределение f(x) се свежда до решаване относително $\mathbf{X_i}$ на интегралното уравнение от вида:

$$\xi_i = \int_0^{x_i} f(x)dx \qquad (1)$$

За формиране на случайни числа със зададен закон на разпределение се използват следните съотношения [1]:

експоненциално разпределение с интензивност **λ:**

$$x_i = -\frac{1}{\lambda}\ln \xi \,. \qquad (2)$$

нормално разпределение с математическо очакване **a** и дисперсия σ^2:

$$x_i = a + \sigma Z_i;$$
$$Z_i = \sum_{i=1}^{12}\xi_i - 6 \qquad (3)$$

логаритмически нормално разпределение с параметър **σ**:

$$x_i = e^{\left(\frac{a+\sigma Z_i}{m}\right)}; \qquad (4)$$
$$m = \lg e = 0{,}4343...$$

разпределение на Ерланг с параметър n и β:

$$x_i = -\frac{1}{2}\ln(\xi_1\xi_2\xi_3...\xi_n) \qquad (5)$$

разпределение на Вейбул: α - мащабен параметър, k – параметър, определящ асиметричността на ексцеса:

$$x_i = \sqrt[k]{-\frac{1}{\alpha}\ln \xi_i} \qquad (6)$$

хиперекспоненциално разпределение с параметри:

$\lambda_1,....,\lambda_k;$
$c_1,.....c_k;$ x_i се изчислява при $k \le 4$

За всички горе приведени съотношения ξ е случайна величина равномерно разпределена в интервала [0, 1].

Разглежданият статистически модел за оценка на въздействието на заплахите за компютърните системи и мрежи е представен със структурната схема, изобразена на фиг.1. Тя включва: въвеждане на изходните данни (бл. 1); задаване на изходните условия за моделиране (бл. 2 – бл. 3); непосредствено моделиране на възникването на заплахи (бл. 6-бл. 15); проверка на зададените условия за количеството цикли (ЦМ) на моделиране (бл. 15); определяне на общия брой „възникналите" заплахи (бл. 16 – бл. 19); определяне на вероятностите на възникване на съответните заплахи, загубите, „възникнали" от всяка една заплаха и общите загуби от „възникналите" заплахи. За реализацията на статистическия модел са дефинирани следните броячи: броячи $M_i, i=\overline{1,n}$ на „възникналите" конкретни въздействия; брояч N на общия брой на „възникналите" смущаващи въздействия; брояч $ЦМ$ на количеството цикли на моделиране.

За определяне на момента на възникване на конкретна заплаха последователно се генерират n случайни числа с равномерен закон на разпределение в интервала [0, 1] – бл. 7. След генерирането на $i-$то, $i=\overline{1,n}$, число се определя момента τ_i, $i=\overline{1,n}$ на възникване $i-$то, $i=\overline{1,n}$, смущаващото въздействие, в зависимост от закона на разпределение на това време (бл. 8). Решение за това кое е „реално възникналото" въздействие се приема по минималното време от съвкупността получени стойности $\{\tau_i\}; i=\overline{1n}$ - бл. 11. На основание на взетото решение за типа на настъпилата заплаха се увеличава с единица съдържанието на съответния брояч M_i, $i=\overline{1,n}$.

При условие, че се окаже, че са получени равни стойности на две или повече времена, т. е. $\tau_i = \tau_j = ...$ се приема решение за едновременно настъпване две или повече заплахи, като при това се увеличава е единица съдържанието съответни на броячите $M_i = M_j = ...$ (бл. 13), като се отчита факта, че съдържанието на един от броячите вече е увеличен на единица при изпълнението на бл. 12.

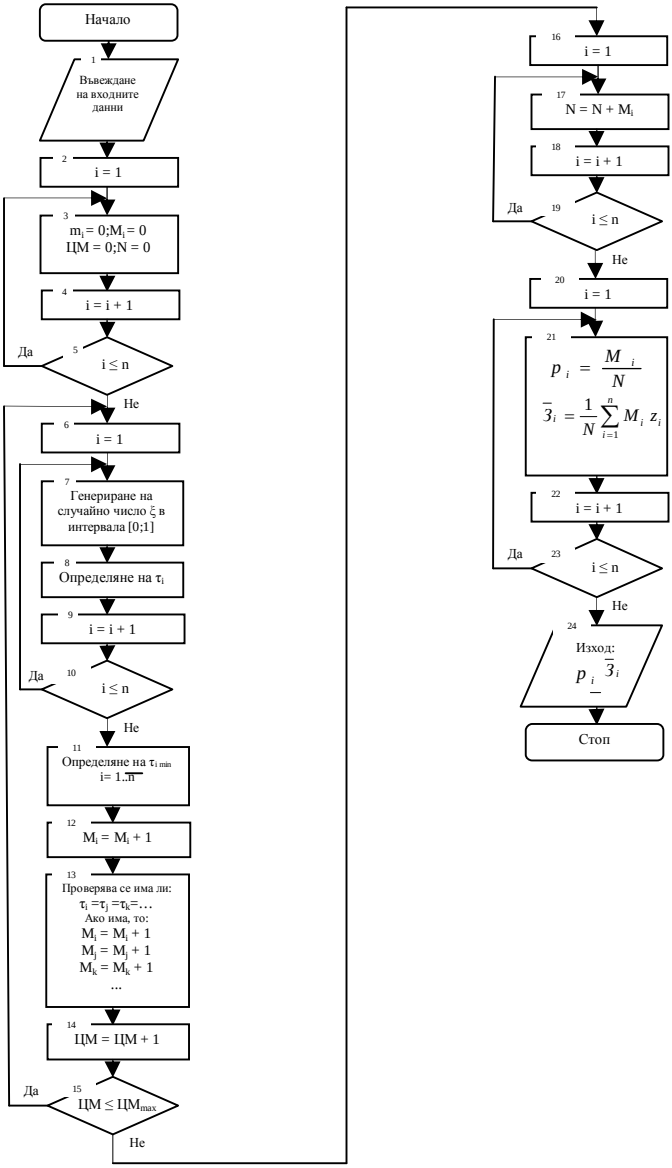
Вероятността p_i, че при възникване на заплаха тя ще е от $i-mu; i=\overline{1n}$ тип се определя по съдържанието на броячите M_i, $i=\overline{1,n}$ и N:

$$p_i = \frac{M_i}{N}, \tag{7}$$

Загубите Δw_i, които настъпват с настъпването $i-$та заплаха, ще се определят в съответствие с вероятността на възникването й, т.е.

$$\Delta w_i = p_i z_i = \frac{M_i}{N} z_i, \tag{8}$$

където z_i са относителните загуби, причинени от $i-$ та заплаха.


Начало
1
Въвеждане на входните данни
2
i = 1
3
$m_i = 0; M_i = 0$
ЦМ = 0; N = 0
4
i = i + 1
5
i ≤ n
Да
Не
6
i = 1
7
Генериране на случайно число ξ в интервала [0;1]
8
Определяне на τ_i
9
i = i + 1
10
i ≤ n
Да
Не
11
Определяне на $\tau_{i\,min}$
i= 1..n
12
$M_i = M_i + 1$
13
Проверява се има ли:
$\tau_i = \tau_j = \tau_k = \ldots$
Ако има, то:
$M_i = M_i + 1$
$M_j = M_j + 1$
$M_k = M_k + 1$
...
14
ЦМ = ЦМ + 1
15
ЦМ ≤ $ЦМ_{max}$
Да
Не
16
i = 1
17
$N = N + M_i$
18
i = i + 1
19
i ≤ n
Да
Не
20
i = 1
21
$p_i = \frac{M_i}{N}$
$\overline{3}_i = \frac{1}{N}\sum_{i=1}^{n} M_i z_i$
22
i = i + 1
23
i ≤ n
Да
Не
24
Изход:
p_i $\overline{3}_i$
Стоп

Фиг. 1

Общите загуби, причинени от всички *n* заплахи, при условия на тяхната независимост и адитивност на последствията от тях ще се определят като:

$$\overline{З}_i = \sum_{i=1}^{n} \Delta w_i = \frac{1}{N} \sum_{i=1}^{n} M_i z_i .$$

Предвид на (7) горният израз може да се запише и като:

$$\overline{З} = \sum_{i=1}^{n} \overline{З_i} . \qquad (9)$$

Литература

1. Бусленко, Н. П., Моделирование сложных систем, Москва, Наука, 1968.

2. Начев, А. И., Структурнофункционална надеждност на компютърни мрежи, Военно издателство, София, 2002.

СВИВАЩ ГЕНЕРАТОР НА ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ, ФОРМИРАНИ ЧРЕЗ НЕЛИНЕЙНИ ФУНКЦИИ

Борислав Й. Беджев[1], Цветослав Ст. Цанков[2], Лилия Ан. Станева[3]

[1] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, bedzhev@abv.bg
[2] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, hitar@abv.bg
[3] Бургаски университет „Проф. д-р Асен Златаров”, Факултет по технически науки, anest_bg@bitex.bg

SHRINKING GENERATOR OF PSEUDORANDOM SEQUENCES, FORMED BY NONLINEAR FUNCTIONS

Borislav Y. Bedzhev, Tsvetoslav St. Tsankov, Lilia An. Staneva

Abstract: *Generators of pseudo-random sequences (PRSs) have a very important role for stream and block ciphers, because they influence essentially on the crypto resistance. With regard in the paper a variant of the well known shrinking generator is presented. It is based on the positive features of the PRSs, formed by nonlinear mathematical functions, which provide a very high resistance to the present crypto attacks.*

Key words: *stream and block ciphers, pseudo-random sequences, shrinking generator*

Този доклад е подкрепен по Проект BG051PO001-3.3.06-0003 “Изграждане и устойчиво развитие на докторанти, постдокторанти и млади учени в областта на

природните, техническите и математическите науки". Проектът се осъществява с финансовата подкрепа на Оперативна програма „Развитие на човешките ресурси", съфинансирана от Европейския социален фонд на Европейския съюз.

Увод

Псевдослучайните последователности (*ПСП*) намират голямо приложение в различни области на науката и техниката, основните, от които са: анализ на системи и процеси по метода Монте-Карло, планиране на експерименти, синтезиране на сложни шумоподобни комуникационни сигнали, криптографска защита на информацията. В сферата на криптографската защита на информацията ПСП обаче имат особено важна роля, тъй като те се използват като гамиращи (маскиращи) последователности при поточните шифри и за формиране на така наречените субституционни кутии при блоковите шифри, при което от тях пряко зависи устойчивостта на системите към опитите за неоторизиран достъп до техните ресурси. По тази причина ПСП трябва да отговарят следните изисквания [1], [2], [3], [4], [5], [6]:

(И1) периодът $\boldsymbol{N}$ на ПСП трябва да бъде изключително голям;

(И2) в рамките на периода всички възможни групи от $\boldsymbol{k}$ на брой последователни символи (единични символи, двойки от символи, тройки от символи, ..., $\boldsymbol{k}$-тици от символи) трябва да имат практически равномерно разпределение за всички стойности на $\boldsymbol{k}$ в диапазона $k = 1, 2, 3, ..., s$;

(И3) да притежават висока устойчивост към известните криптоатаки;

(И4) техническата им реализация да не е сложна и скъпа.

За съжаление изброените изисквания са взаимно противоречиви, защото, ако структурата на поточния шифър е опростена, за да се осигури висока скорост и ниска цена на генератора на ПСП, тогава криптоустойчивостта е ниска. Например, класическите бързи и евтини преместващи регистри с линейни обратни връзки (*ПОРЛВ*, *Linear Feedback Shift Registers – LFSRs*) са уязвими от така наречената криптоатака на *Берлекемп-Меси* (*Berlekamp–Massey*) [1], [2], [3]. Както е известно, тази атака е реализуема, ако на криптоаналитика са известни $2\boldsymbol{n}$ последователни бита от гамиращата (маскиращата) последователност като тук $\boldsymbol{n}$ е броят на тригерите в ПРЛОВ.

С цел едновременно удовлетворяване на горепосочените изисквания в началото на 90-те години на миналия век беше предложена така наречената доктрина на *Голич* (*Golic*) [1], [4]. Основната идея на този подход е изграждането на криптографски устойчиви генератори на ПСП чрез комбиниране по някакъв подходящ начин на бързи, евтини и технически надеждни компоненти, включително ПРЛОВ. В резултат бяха предложени няколко нови архитектури на генератори на ПСП като например сумиращият генератор, свиващият генератор и *N*-адичният преместващ регистър с обратна връзка с пренос (*N*-ПРОВП, *N*-adic Feedback with Carry Shift Register - *N*-FCSR) [1], [2], [4], [5]. Отчитайки положителните им свойства, тези генератори на ПСП бяха интензивно изследвани през последните десет години [4], [5], [6], [7], [8], [9], [10], [11], [12], [13]. При тези изследвания обаче основно внимание е отделено на генератори, изградени от компоненти като ПРЛОВ и *N*-ПРОВП, описвани математически с линейни функции, които са най-уязвими от криптоатаката на Берлекемп-Меси и нейните разновидности (например Клапер и Горески (A. Klapper, M. Goresky) са модифицирали този подход с цел ефективна криптоатака на *N*-ПРОВП).

Предвид на изложеното естествено възниква въпросът дали е възможно да се повиши криптоустойчивостта на генераторите на ПСП, ако се комбинират по-сложни, но и с по-добра криптоустойчивост компоненти. Отговорът на този въпрос е положителен и се обосновава по-нататък в доклада.

Докладът е структуриран както следва. Първо се припомня принципът на работа на свиващия генератор (*СГ*). След това се обосновава възможността за повишаване на криптоустойчивостта на СГ в резултат на използване на ПСП, формирани чрез нелинейни функции, които са най-устойчиви към известните криптоатаки. Накрая се обсъжда практическото приложение на производните структури на СГ, предложени в доклада.

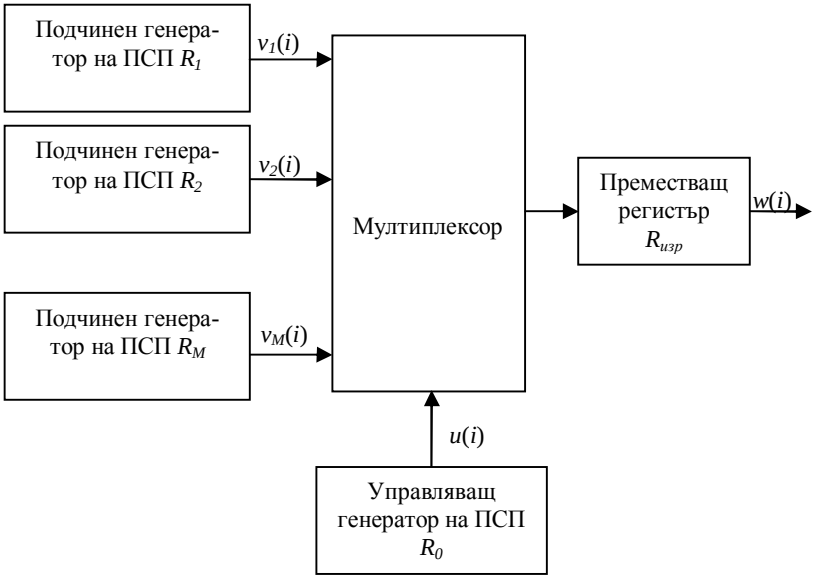
Свиващ генератор на псевдослучайни последователности, формирани чрез нелинейни функции

Обобщената структура на СГ на ПСП има вида, показан на фиг. 1 [1], [2], [4], [7], [8], [11]. Както се вижда, СГ се състои от $\boldsymbol{M}$ на брой подчинени генератори на ПСП $R_1, R_2, ..., R_M$, един управляващ генератор на ПСП R_0, изравняващ преместващ регистър $R_{изр}$ и мултиплексор. При това всички генератори на ПСП работят едновременно под управлението на общ тактов сигнал, който не е показан на фиг. 1. ПСП, формирани от генераторите, са съставени от символите

(1) $$u(i) \in \{0,1,...,M\},\ i = 1,2,....,$$

(2) $$v_j(i) \in \{0,1,...,p\},\ j = 1,2,...,M,\ i = 1,2,....$$

Тук $u(i)$ е $\boldsymbol{i}$-тият елемент на ПСП, формирана от управляващия генератор R_0, а $v_j(i)$ е $\boldsymbol{i}$-тият елемент на $\boldsymbol{j}$-тата ПСП, формирана от $\boldsymbol{j}$-тия подчинен генератор R_j.



Фиг. 1: *Обобщена структура на свиващ генератор на ПСП*

Елементите на управляващата ПСП задават адресите на мултиплексора. По тази причина, ако по време на ***i***-тия такт от работата на СГ е изпълнено условието:

(3) $$u(i) = j,\ \ j = 1, 2, ..., M,\ \ i = 1, 2, ...$$

тогава мултиплексорът пропуска към изхода на СГ символа $v_j(i)$ на ***j***-тата ПСП (т.е. $w(i) = v_j(i)$). Ако в същия такт е изпълнено условието:

(4) $$u(i) = 0,\ \ i = 1, 2, ...$$

тогава мултиплексорът не пропуска към изхода на СГ какъвто и да е символ (т.е. не се формира символът $w(i)$).

От изложеното се вижда, че изходната ПСП $\{w(i)\}_{i=1}^{\infty}$ на СГ е едновременно свита и разбъркана последователност, съставена от елементите на подчинените ПСП $\{v_1(i)\}_{i=1}^{\infty}$, $\{v_2(i)\}_{i=1}^{\infty}$, ..., $\{v_M(i)\}_{i=1}^{\infty}$. Тъй в някои тактове от време липсват символи, за да не се наруши равномерността на процеса на шифриране преди изхода на СГ е включен изравняващ преместващ регистър $R_{изр}$ като тактовите импулси за въвеждане на символи в него са с малко по – висока честота в сравнение с тактовите импулси за извеждане на символи.

Следва да се отбележи, че в оригиналния си вид СГ [1], [2], [4] съдържа само един подчинен генератор (т. е. $M = 1$). В тази ситуация изходната ПСП $\{w(i)\}_{i=1}^{\infty}$ на СГ е свита версия на ПСП $\{v_1(i)\}_{i=1}^{\infty}$, формирана от подчинения генератор R_1. В общия случай, когато $M > 1$, свиващият генератор всъщност е свиващ - мултиплексиращ генератор [7], [8].

Доказано е, че изходната ПСП $\{w(i)\}_{i=1}^{\infty}$ на СГ притежава следните положителни свойства [1], [2], [4], [7], [8].

Първо, ако периодите $N_0, N_1, N_2, ..., N_M$ на ПСП на управляващия и подчинените генератори са взаимно прости числа, тогава периодът $N_{CГ}$ на изходната ПСП $\{w(i)\}_{i=1}^{\infty}$ на СГ е:

(5) $$N_{CГ} = N_{0(\neq 0)} \cdot \prod_{i=0}^{M} N_i$$

като тук $N_{0(\neq 0)}$ е броят на елементите, различни от 0, в един период на управляващата ПСП $\{u(i)\}_{i=1}^{\infty}$.

От (5) се вижда, че дори при малки стойности на ***M*** и при използване на *N*-ПРОВП и/или ПРЛОВ в качеството на управляващ и/или подчинени регистри, периодът $N_{CГ}$ на изходната ПСП $\{w(i)\}_{i=1}^{\infty}$ на СГ достига изключително големи стойности, т. е. удовлетворява се изискването (И1).

Второ, еквивалентната линейна сложност (*ЕЛС*) при използване на *N*-ПРОВП и/или ПРЛОВ в качеството на управляващ и/или подчинени регистри също е много голяма. Така например, ако управляващият и подчинените регистри са ПРЛОВ, формиращи линейни рекурентни последователности с максимален период (*M*-последователности, maximal length sequences - *M*-sequences) над крайните алгеб-

рични полета $GF(2)$ и $GF(p)$ (*Galois Field – GF, полета на Галоа*) съответно, тогава ЕЛС $n_{СГ}$ на СГ е в границите [7]:

$$\frac{(p-1)p^{n_0-1}}{2}\prod_{i=1}^{p-1}n_i < n_{СГ} \le (p-1)p^{n_0-1}\prod_{i=1}^{p-1}n_i \ . \quad (6)$$

Тук $n_0, n_1, n_2, ..., n_M$ е броят на тригерите в управляващия и подчинените ПРЛОВ съответно.

ЕЛС изразява количествено криптоустойчивостта на ПСП и се обяснява по следния начин. Първо е необходимо да се отчете, че всяка последователност, формирана от автоматичен (електронен) генератор, в крайна сметка е периодична и е съставена от краен брой символи (т. е. азбуката на последователността е ограничена). Второ, ако броят на символите на ПСП е произволно просто число, тогава като се използват символите на интересуващата ни ПСП чрез последователно прилагане на атаката на Берлекемп-Меси, се построява така нареченият еквивалентен ПРЛОВ, формиращ същата ПСП. Ето защо ЕЛС на интересуващата ни ПСП се измерва чрез броя на тригерите $n_{екв}$ в еквивалентния ПРЛОВ, тъй като атаката на Берлекемп-Меси може да се приложи успешно само ако на криптоаналитика са известни $2n_{екв}$ последователни символа от атакуваната ПСП. При това времето за изчисления е от порядъка на $O(n_{екв}^2)$.

В светлината на изложеното и от (6) се вижда, че дори при $M=1$ СГ може да има ЕЛС $n_{екв} > 2^{128}$, което прави атаката на Берлекемп-Меси практически неприложима в момента. Следователно, дори СГ с проста структура имат много висока криптоустойчивост, т. е. СГ удовлетворяват и изискванията (И3) и (И4).

Все пак, като се отчитат непрекъснато нарастващите изчислителни възможности на компютърната техника, естествено възниква въпросът дали е възможно да се повиши още повече криптоустойчивостта на СГ на ПСП, ако се използват по-сложни, но и с по-голяма ЕЛС, управляващи и подчинени генератори.

За да се даде отговор на този въпрос чрез компютърно моделиране [14] в средата на Матлаб беше проведено изследване на схемата от фиг. 1 при следните условия.

Първо, броят на подчинените регистри беше ограничен до стойностите $M=1,2,4$.

Второ, като управляващи генератори бяха използвани генератори на така наречените бент-последователности с дължини (периоди):

$$N_0 \in \left\{2^4-1=15, 3^4-1=80, 2^8-1=255,\ 5^4-1=624\right\}. \quad (7)$$

Подчинените генератори бяха реализирани чрез ПРЛОВ, формиращи M – последователности с дължини (периоди)

$$N_j \in \left\{2^7-1=127,\ 2^9-1=511,\ 2^{11}-1=2047, 2^{13}-1=8191\right\}, j=1,2,3,4 . \quad (8)$$

Въведените ограничения произтичат от необходимостта да се спазват изискванията (И1), (И2), (И3), (И4).

Както е известно, бент-последователностите представляват семейства от последователности, които се формират по правилото [15], [16], [17]:

(9) $s_j(i) = f\left[tr_1^n(\beta_0.\alpha^i), tr_1^n(\beta_1.\alpha^i),..., tr_1^n(\beta_{m-1}.\alpha^i)\right] + \vec{j}^T.\vec{X} + tr_1^n(\sigma.\alpha^i)$.

Тук са използвани следните означения:

1) $s_j(i), j = 0,1,...,K-1,\ i = 0,1,...,N-1$ е ***i***-тият елемент от ***j***-тата бент-последователност от семейството;

2) $N = p^n - 1$ е дължината на бент-последователностите от семейството като ***p*** е произволно просто число, а ***n***, ***m*** и ***k*** са цели положителни числа, свързани със съотношенията:

(10) $n = 2m = 4k \cap p = 2;\ n = 2m \cap p \neq 2$;

3) ***K*** е броят на бент-последователностите в семейството $K = p^m = p^{n/2}$;

4) α е примитивен елемент на крайното алгебрично поле $GF(p^n)$ [18];

5) $\beta_0, \beta_1,..., \beta_{m-1}$ са базис на $GF(p^m)$ над $GF(p)$; най-просто е да се вземе:

(11) $\beta_0 = \beta^0 = 1, \beta_1 = \beta^1,..., \beta_{m-1} = \beta^{m-1}$,

(12) $\beta = \alpha^d, d = p^m + 1$

е примитивен елемент на крайното алгебрично поле $GF(p^m)$;

6) $\sigma \in GF(p^n)/GF(p^m)$; най-просто е да се приеме $\sigma = \alpha$;

7) $\vec{j}^T$ е следният вектор-ред („Т" означава матрична транспозиция):

(13) $\vec{j}^T = (a_0, a_1,..., a_{m-1})$,

(14) $j = a_0 + a_1.p + ... + a_{m-1}.p^{m-1}, 0 \le a_s \le p-1, s = 0,1,..., p-1$

е поредният номер на бент-последователността в семейството;

8) $\vec{X}^T$ е следният вектор-ред:

(15) $\vec{X}^T = (x_0, x_1,..., x_{m-1})$;

9) $f(x_0, x_1,..., x_{m-1})$ е бент-функция, съпоставяща на елементите на $GF(p^m)$ елементите на $GF(p)$; най-просто е да се приеме, че:

(16) $f(x_0, x_1,..., x_{m-1}) = x_0.x_{m/2} + x_1.x_{m/2+1} + ... + x_{m/2-1}.x_{m-1}$,

(17) $x_0 = tr_1^n(\beta_0.\alpha^i), x_1 = tr_1^n(\beta_1.\alpha^i),..., x_{m-1} = tr_1^n(\beta_{m-1}.\alpha^i)$;

10) в (17) $tr_1^n(\gamma)$ е следата (*the trace*) на елемента $\gamma \in GF(p^n)$ в $GF(p)$ [18]:

(18) $tr_1^n(\gamma) = \gamma^{p^0} + \gamma^{p^1} + ... + \gamma^{p^{n-1}}$.

Във връзка с гореизложеното, следва да се акцентира върху следните факти.

Първо, формула (16) е представяне на бент-функцията $f(x_0, x_1,..., x_{m-1})$ под формата на квадратична булева функция. Всъщност бент-последователностите са въведени именно поради факта, че се формират чрез нелинейни булеви функции и по тази причина те имат много висока ЕЛС [15], [16], [17]. По – конкретно, в [17] са доказани долна и горна граници за ЕЛС на бинарните бент-последователности (т. е. когато броят на символите в азбуката на бент-последователностите е $p = 2$), които се илюстрират от Табл. 1 [17].

Таблица 1

Граници на ЕЛС на бинарните бент-последователности

n (ЕЛС на класически *M*-последователности)	долна граница на ЕЛС на бент-последователностите	ЕЛС на конкретни реализирани бент-последователности	горна граница на ЕЛС на бент-последователностите
8	20	-	32
12	202	232	232
16	1 416	-	1 808
20	10 334	-	14 204
24	16 804	-	114 512

Както се вижда, ЕЛС на бинарните бент-последователности е десетки и дори стотици пъти по-голяма от ЕЛС на класическите бинарни *M*-последователности със същата дължина (период) $N = 2^n - 1$.

Второ, бент-последователностите, освен на изискванията (И1) и (И3), отговарят и на изискването (И2) (макар и за по-малки стойности на $\boldsymbol{s}$ в сравнение с *M*-последователностите със същия период).

Трето, бент-последователностите се реализират практически по-трудно в сравнение с *M*-последователностите със същия период, но бързият напредък в развитието на електронните интегрални схеми (*ИС*), съчетан с намаляване на техните цени отслабва много съществено значението на този недостатък. По-конкретно, схемата от фиг. 1 може да се реализира с $\boldsymbol{M}$ на брой PIC процесора, като всеки PIC процесор е генератор на една управляваща или подчинена ПСП. При този подход конкретната електрическа схема има проста структура и се изгражда чрез евтини, надеждни и бързодействащи ИС.

Направените чрез компютърно моделиране [14] в средата на Матлаб изследвания на схемата от фиг. 1 показаха, че СГ на ПСП, формирани чрез бент-функции, отговарят на изискванията (И1), (И2), (И3) и (И4) и могат да намерят приложение в съвременни системи за криптографска защита на информацията.

Заключение

В доклада е предложена производна структура на СГ, при която управляващата ПСП е формирана чрез нелинейна функция. В резултат на това ЕЛС на изходната ПСП на СГ много съществено нараства при напълно приемливо от практическа гледна точка увеличаване на сложността и цената на СГ.

Практическата приложимост на обоснования в доклада вариант на построение на СГ е проверена чрез компютърно моделиране в средата на Матлаб. Резултатите от моделирането показват, че изходната ПСП на СГ освен много висока ЕЛС се характеризира и с много голям период и с практически равномерно разпределение на всички възможни групи от $\boldsymbol{k}$ на брой последователни символи в относително широк диапазон от стойности на $\boldsymbol{k}$.

Предвид на демонстрираните положителни качества, предложената производна структура на СГ може да намери приложение в поточните и блоковите шифри, предназначени за защита на информацията в съвременните компютърни бази от данни.

Литература:

[1] P. van Oorshot, A. Menezes and S. Vanstone, “Handbook of Applied Cryptography,” CRC Press, 1997.

[2] R. Rueppel, “Analysis and Design of Stream Siphers,” Springer Verlag, N. Y., 1986.

[3] S. Golomb, G. Gong, “Signal design for good correlation,” Cambridge University Press – 2005

[4] D. Coppersmith, H. Krawczyk, Y. Mansour, “The Shrinking Generator,” Proceedings of Crypto 93, Springer-Verlag, 1994., pp. 22-39

[5] A. Klapper, M. Goresky, “*2*-adic Shift Register. Fast Software Encryption,” Second International Workshop. (Lecture Notes in Computer Science, vol. 950, Springer Verlag, N. Y., 1994.) pp.174-178

[6] Zh. N. Tasheva, B. Y. Bedzhev, V. A. Mutkov, “An Shrinking Data Encryption Algorithm with *p*-adic Feedback with Carry Shift Register,” XII International Symposium of Theoretical Electrical Engineering ISTET 03, Warsaw, Poland, 6-9 July, 2003., Conference Proceedings, vol.II, pp. 397–400.

[7] T. Tashev, B. Bedzhev, Zh. Tasheva, “The Linear Complexity of the LFSR Based Generalized Shrinking-Multiplexing Generator,” XLII International Conference on Information, Communication and Energy Systems and Technologies, ICEST 2007, 24 - 27 June 2007, Ohrid, Macedonia

[8] T. Tashev, B. Bedzhev, Zh. Tasheva, “The Generalized Shrinking-Multiplexing Generator,” International Conference on Computer Systems and Technologies - CompSysTech’07, June 22-26, 2007, Bulgaria

[9] T. Tashev, „The Period of the LFSR Based Generalized Shrinking-Multiplexing Generator,” International Conference on Computer Systems and Technologies - CompSysTech’07, June 22-26, 2007, Bulgaria.

[10] Zh. Tasheva, B. Bedzhev, B. Stoyanov, “N-adic Summation-Shrinking Generator. Basic properties and empirical evidences,” Cryptology ePrint Archive, Co-Editors: Mihir Bellare, UCSD Christian Cachin, IBM Zurich, Accepted and posted with Number 2005/068, http://eprint.iacr.org/2005/068.pdf.

[11] Zh. Tasheva, B. Bedzhev, B. Stoyanov, “P-adic Shrinking–Multiplexing Generator,” IEEE Third International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS’2005, September 5-7, 2005 Sofia, Bulgaria, 2005.

[12] B. Stoyanov, A. Milev and A. Nachev, “Research on the Self-Shrinking 2-Adic Cryptographic Generator,” *Journal of Communication and Computer*, ISSN 1548-7709, USA, Volume 7, No.11 (Serial No.72), November 2010

[13] A. T. Tasheva, Zh. N. Tasheva, and A. P. Milev, “Generalization of the Self-Shrinking Generator in the Galois Field GF(p^n),” *Hindawi Publishing Corporation - Advances in Artificial Intelligence*, Volume 2011, Article ID 464971

[14] J. Soto, “Statistical Testing of Random Number Generators,” http://csrc.nist.gov/rng/.

[15] J. D. Olsen. R. A. Scholtz. and L. R. Welch. “Bent-function sequences,” *IEEE Trans. Infirm. Theory*, vol. IT-28, pp. 858-864, Nov. 1982.

[16] P. V. Kumar, “On Bent Sequences and Generalized Bent Functions,” Ph.D. dissertation, Elec. Eng. Dept., Univ. Southern Calif., Los Angeles, Aug. 1983.

[17] P. V. Kumar and R. A. Scholtz, “Bounds on the Linear Span of Bent Sequences,” *IEEE Trans. Infirm. Theory*, vol. IT - 29, No. 6, pp. 854-862, Nov. 1983.

[18] R. Lidl, H. Niederreiter, “Finite Fields,” Addison – Wesley Publishing Company, London, England, 1983.

МЕТОД ЗА ПРИЛОЖЕНИЕ НА СИГНАЛИ С ВИСОКА СТРУКТУРНА СЛОЖНОСТ В РАДИОЛОКАЦИОННИ СИСТЕМИ

Борислав Й. Беджев[1], Цветослав Ст. Цанков[2], Лилия Ан. Станева[3]

[1] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, bedzhev@abv.bg
[2] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, hitar@abv.bg
[3] Бургаски университет „Проф. д-р Асен Златаров”, Факултет по технически науки, anest_bg@bitex.bg

A METHOD FOR APPLICATION OF SIGNALS WITH HIGH STRUCTURAL COMPLEXITY IN THE RADAR SYSTEMS

Borislav Y. Bedzhev, Tsvetoslav St. Tsankov, Lilia An. Staneva

Abstract: *At present the problem for protection the communication systems against different outer and inner threats has a great practical importance. With regard a method for application of signals with high structural complexity in the radar systems is presented. The method allows the practical usage of signals with very low probability for interception, providing simultaneously a very high resolution of the radar signals.*

Key words: *signals with high structural complexity, radar systems, signal processing*

Този доклад е подкрепен по Проект BG051PO001-3.3.06-0003 “Изграждане и устойчиво развитие на докторанти, постдокторанти и млади учени в областта на природните, техническите и математическите науки”. Проектът се осъществява с финансовата подкрепа на Оперативна програма „Развитие на човешките ресурси”, съфинансирана от Европейския социален фонд на Европейския съюз.

Увод

На съвременния етап проблемът за надеждна защита на комуникационните системи срещу различни вътрешни и външни заплахи, произтичащи от опитите за неоторизиран достъп до техните ресурси, има голямо практическо значение. Един ефективен метод за неговото решаване е използването на широколентови сигнали с малка спектрална плътност и висока структурна сложност [1], [2], [3]. Положителните страни на метода произтичат от следните обстоятелства. Първо, малката спектрална плътност маскира използваните в комуникационната система сигнали на

фона на смущенията и в резултат те са практически неоткриваеми за радиотехническото разузнаване на различни криминални или терористични групи. Второ, високата структурна сложност затруднява изключително много имитацията на сигналите, което съществено ограничава възможностите за претоварване или радиоелектронно подаване на атакуваните комуникационни системи.

При практическото използване на посочения метод за защита на комуникационните системи обаче възникват следните проблеми [1], [3].

Първо, методът изисква прилагането на сложни методи за разширяване на спектъра на сигналите и за тяхната обработка.

Второ, сигналите с висока структурна сложност в недостатъчна степен отговарят на изискванията, които произтичат от необходимостта за максимално ефективно използване на ограничения природен ресурс – електромагнитния спектър. По-конкретно сигналите, използвани в съвременните комуникационни системи, трябва да осигуряват:

(И1) висока разделителна способност по разстояние, позволяваща разделна обработка на сигналите, преминали по различни пътища, тъй като в противен случай възниква самосмущаване, при което ехото на предхождащите символи се наслагва върху пристигащите в момента символи от съобщенията;

(И2) възможност за едновременна работа на много потребители при допустимо ниво на взаимните смущения.

На съвременния етап първият проблем, свързан с прилагането на сложни методи за разширяване на спектъра на сигналите и за тяхната обработка, практически е решен в резултат на огромния прогрес в разработката и производството на електронните градивни елементи и снижаването на техните цени.

В момента обаче вторият проблем е все още далече от окончателно решение [2], [3]. По тази причина в доклада се обосновава метод за преодоляване на недостатъците на сигналите с висока структурна сложност, произтичащи от недостатъчното им съответствие на изискванията (И1) и (И2). По-конкретно, по-нататък в доклада се доказва, че висока разделителна способност по разстояние може да се осигури чрез използването на специален несъгласуван филтър в приемника на комуникационната система. Същевременно е показано, че е възможно този важен положителен резултат да бъде постигнат при известно влошаване на отношението сигнал/шум, което е напълно приемливо от практическа гледна точка. По тези причини методът е особено ценен за радиолокационните и радионавигационните системи, където проблемът за постигане на висока разделителна способност по разстояние е много важен [2].

Докладът е структуриран както следва. Първо се обосновава метод за постигане на висока разделителна способност по разстояние чрез несъгласувана обработка на приетите сигнали. След това са представени резултатите от експериментално изследване, проведено по метода на компютърното моделиране, които потвърждават коректността на предложения метод. Накрая са направени някои основни изводи по доклада.

Метод за приложение на сигнали с висока структурна сложност в радиолокационни системи

Идеята за постигане на висока разделителна способност по разстояние чрез несъгласувана обработка на приетите сигнали може да се проследи 30 – 40 години

назад във времето [3]. В настоящия доклад обаче тя ще бъде разгледана по начин, съчетаващ едновременно краткост и математическа строгост. Единствените ограничение, които се приемат, са следните.

Първо, в комуникационната система се прилагат цифрови методи за обработка на сигналите.

Второ, в комуникационната система се използват периодични сигнали.

Следва да се отбележи, че първото допускане напълно съответства на съвременното състояние на техниката и технологиите, а второто допускане е характерно за много комуникационни системи и особено за радиолокационните и радионавигационните системи.

При посочените ограничения приетият сигнал може да се опише математически със следния полином:

$$u_{np}(x) = u_{N-1}x^{N-1} + u_{N-2}x^{N-2} + \ldots + u_1 x + u_0 \quad (1)$$

Формула (1) се обосновава по следния начин [1], [3]. В комуникационната система се използват сложни широколентови сигнали с период (продължителност, дължина) ***N***, които представляват редици от следващи един след друг елементарни импулси (чипове) с продължителност τ_u . Приетият сигнал се преобразува в цифров вид с интервал на дискретизация:

$$\tau_\partial \approx \tau_u \,. \quad (2)$$

В резултат на това от всеки елементарен импулс (чип) на приетия сигнал се получава по един отчет и се формира следната последователност от отчети $\{u_0, u_1, ..., u_{N-2}, u_{N-1}\}$. Всеки отчет $u_i, i = 0,1,...,N-1$ е комплексно число, чиято големина и фазов ъгъл изразяват амплитудата и началната фаза на ***i***-тия елементарен импулс (чип), т. е. отчетите $u_i, i = 0,1,...,N-1$ представляват комплексните амплитуди (обвиващи) на елементарните импулси (чипове). В тази ситуация променливата $\boldsymbol{x}$ в (1) има физическия смисъл на задръжка на елементарните импулси на един тактов интервал τ_∂ По-конкретно, едночленът $u_1 x$ означава, че елементарният импулс с комплексна амплитуда u_1 следва на интервал τ_∂ от елементарния импулс с комплексна амплитуда u_0 . От своя страна, едночленът $u_2 x^2$ означава, че елементарният импулс с комплексна амплитуда u_2 следва на интервал τ_∂ от елементарния импулс с комплексна амплитуда u_1 и на интервал $2\tau_\partial$ от елементарния импулс с комплексна амплитуда u_0 . Напълно аналогичен е физическият смисъл и на останалите едночлени $u_3 x^3, u_4 x^4, ..., u_{N-2}x^{N-2}, u_{N-1}x^{N-1}$ в (1).

След приемането на сигнала (1), в приемниците се изчислява неговата цифрова периодична автокорелационна функция (*ПАКФ*), тъй като в теорията на оптималното приемане е доказано, че тази процедура максимизира отношението сигнал/шум на изхода на приемника, ако смущенията представляват адитивен бял шум, което е най – често срещаният в практиката случай [1], [2], [3]. В конкретния случай ПАКФ на цифровия сигнал (1) се описва с формулата [2]:

$$Q_{uu}(x) = \left(u_{N-1}x^{N-1} + u_{N-2}x^{N-2} + \ldots + u_1 x + u_0\right) \times \left(u^*_{N-1}x^{-(N-1)} + u^*_{N-2}x^{-(N-2)} + \ldots + u^*_1 x^{-1} + u^*_0\right) \mod(x^N - 1) \quad (3)$$

Тук са използвани следните означения.

Първо, $Q_{uu}(x)$ означава ПАКФ на приетия цифров сигнал.

Второ, символът „*" показва *комплексно спрягане*.

Трето, изразът $\mathrm{mod}(x^N - 1)$, показва, че $\boldsymbol{x}$ не е произволна променлива, тъй като тя може да приеме само стойности, представляващи $\boldsymbol{N}$-ти корен от единицата, т.е.:

$$x = e^{j\frac{2\pi}{N}l},\ l = 0,1,...,N-1. \quad (4)$$

Като се отчете това обстоятелство, се вижда, че като се дават на $\boldsymbol{x}$ в (1) последователно стойностите от (4) за $l = 0,1,...,N-1$ ще се получат $\boldsymbol{N}$ константи $C_l, l = 0,1,...,N-1$, които в общия случай са комплексни числа:

$$C_l = u_{N-1}\left(e^{j\frac{2\pi}{N}l}\right)^{N-1} + u_{N-2}\left(e^{j\frac{2\pi}{N}l}\right)^{N-2} + ... + u_1\left(e^{j\frac{2\pi}{N}l}\right) + u_0,\ l = 0,1,...,N-1, \quad (5)$$

Редицата от константи $C_l, l = 0,1,...,N-1$ обаче представлява *право дискретно преобразование на Фурие* (*ДПФ*) на цифровия сигнал (приетата последователност) $\{u_0, u_1, ..., u_{N-2}, u_{N-1}\}$.

Следва да се отбележи, че ако в (3) се направи заместването $z = x$ тогава:

$$U_{сф}(z) = u^*_{N-1}z^{-(N-1)} + u^*_{N-2}z^{-(N-2)} + ... + u^*_1 z^{-1} + u^*_0 \quad (6)$$

представлява $\boldsymbol{z}$-преобразованието на импулсната реакция на съгласувания с излъчения сигнал приемен филтър.

От (4), (5) и (6) произтича следният *Метод за несъгласуваната цифрова обработка на сигналите* в приемниците на комуникационните системи, осигуряващ постигането на максимално възможната разделителна способност по разстояние при зададена стойност на продължителността τ_u на елементарните импулси, формиращи конкретен сложен широколентов сигнал.

Първо, приетите ехо-сигнали се преобразуват в цифров вид. При това, ако се пренебрегнат изкривяванията, породени от шумовете и смущенията, може да се приеме, че:

$$u(i) = u_i,\ i = 0,1,...,N-1, \quad (7)$$

като тук $u(i)$ е $\boldsymbol{i}$-тият елементарен импулс (чип) от излъчения сигнал.

Второ, следва да се забележи, че в най – обща ситуация след разкриване на скобите в (3) и привеждане на подобните едночлени, резултатът е

$$Q_{uu}(x) = q_{N-1}x^{N-1} + q_{N-2}x^{N-2} + ... + q_1 x + q_0 \mod(x^N - 1). \quad (8)$$

Тук коефициентът q_0 е така наречения основен (главен) лист (пик) на ПАКФ, който е продукт на кохерентното натрупване на цялата енергия на приетия сигнал. Всъщност откриването и различаването на конкретен приет сигнал става въз основа на q_0 [1], [3].

Другите коефициенти $q_1, q_2, ..., q_{N-1}$ в (8) представляват страничните листа (пикове) на ПАКФ и те влошават разделителната способност по разстояние на комуникационната система. Действително, нека на входа на приемника постъпват

два различни сигнала като времевата разлика между тях е по – малка от $N.\tau_u$. Тогава главният лист на ПАКФ на втория сигнал ще се смеси със страничните листа на ПАКФ на първия сигнал, както и обратното - главният лист на ПАКФ на първия сигнал ще се смеси със страничните листа на ПАКФ на втория сигнал. С други думи, ненулевите странични листа на ПАКФ на сигналите представляват адитивен шум, който в редица случаи съществено влошава разделителната способност по разстояние на комуникационните системи.

От този анализ следва важният извод, че максимално възможната разделителна способност по разстояние Δd_m за една комуникационна система

(9) $$\Delta d_m = c.\tau_u ,$$

може да се постигне, ако по някакъв начин се отстранят всички странични листа на ПАКФ.

Следва да се отбележи, че константата $\boldsymbol{c}$ в (9) е скоростта на разпространение на електромагнитните сигнали (в радиолокационните системи е необходимо $\boldsymbol{c}$ да се замени с $c/2$ тъй като сигналите два пъти изминават разстоянието до целта).

Следователно, ако оптималният приемен филтър се замени с неоптимален, така че да са изпълнени едновременно следните $\boldsymbol{N}$ уравнения

(10) $$C_l.D_l^* = q_0,\ l = 0,1,...,N-1,$$

като тук $\{C_0, C_1,..., C_{N-2}, C_{N-1}\}$ е ДПФ-спектърът на приетия сигнал, а $\{D_0, D_1,..., D_{N-2}, D_{N-1}\}$ е ДПФ-спектърът на импулсната реакция на несъгласувания приемен филтър, тогава страничните листа на ПАКФ ще бъдат елиминирани и ще се постигне максимално възможната разделителна способност по разстояние.

Както е известно, $\{C_0, C_1,..., C_{N-2}, C_{N-1}\}$ и $\{D_0, D_1,..., D_{N-2}, D_{N-1}\}$ е прието да се наричат честотни предавателни характеристики на съгласувания и несъгласувания цифров филтър съответно.

Всъщност, ако предварително се изчислят отчетите $C_l, l = 0,1,...,N-1$ по формула (5), тогава от уравненията (10) могат да се определят отчетите $D_l, l = 0,1,...,N-1$

(11) $$D_l = \left(\frac{q_0}{C_l}\right)^*,\ l = 0,1,...,N-1.$$

Трето, използвайки последователността $\{D_0, D_1,..., D_{N-2}, D_{N-1}\}$ чрез *обратното дискретно преобразование на Фурие* (*ОДПФ*) могат да се изчислят отчетите на импулсната реакция на несъгласувания филтър, т.е.:

(12) $$v_l = \frac{1}{N}\left\{D_{N-1}\left(e^{-j\frac{2\pi}{N}l}\right)^{N-1} + D_{N-2}\left(e^{-j\frac{2\pi}{N}l}\right)^{N-2} + \right.$$
$$\left. + ... + D_1\left(e^{-j\frac{2\pi}{N}l}\right) + D_0\right\},\ l = 0,1,...,N-1$$

което позволява желания несъгласуван приемен филтър да бъде реализиран практически.

Следва да се отбележи, че правото и обратното дискретни преобразувания на Фурие могат да се изчислят лесно като матрични произведения:

(13) $\{C_0, C_1, ..., C_{N-2}, C_{N-1}\} = F.\{u_0, u_1, ..., u_{N-2}, u_{N-1}\}^T$,

(14) $\{v_0, v_1, ..., v_{N-2}, v_{N-1}\} = F^{-1}.\{D_0, D_1, ..., D_{N-2}, D_{N-1}\}^T$.

При това матриците F и F^{-1} се определят както следва:

(15) $$F = \begin{bmatrix} w^{0.0} & w^{0.1} & ... & w^{0.(N-1)} \\ w^{1.0} & w^{1.1} & ... & w^{1.(N-1)} \\ ... & ... & ... & ... \\ w^{(N-1).0} & w^{(N-1).1} & ... & w^{(N-1).(N-1)} \end{bmatrix},$$

(16) $$F^{-1} = \frac{1}{N}\begin{bmatrix} (1/w)^{0.0} & (1/w)^{0.1} & ... & (1/w)^{0.(N-1)} \\ (1/w)^{1.0} & (1/w)^{1.1} & ... & (1/w)^{1.(N-1)} \\ ... & ... & ... & ... \\ (1/w)^{(N-1).0} & (1/w)^{(N-1).1} & ... & (1/w)^{(N-1).(N-1)} \end{bmatrix},$$

като тук е използвано означението

(17) $$w = e^{j\frac{2\pi}{N}}.$$

За проверка на изчисленията се използва матричното равенство

(18) $$F \otimes F^{-1} = \begin{bmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{bmatrix}.$$

Следва да се отбележи, че за да се постигне максимална скритост на сигналите по отношение на радиотехническото разузнаване на различни криминални или терористични групи не се използва амплитудна модулация, при което всички отчети на излъчените сигнали имат някаква стандартна амплитуда U_{mu}, която без намаляване на общността на анализа може да се счита за $U_{mu} = 1[V]$. В тази ситуация може да се приеме, че

(19) $$q_0 = N,$$

при което числителят q_0 в (11) и коефициентът $1/N$ в (16) могат да се заменят с 1.

Коректността на обоснования метод за несъгласуваната цифрова обработка на сигналите в приемниците, осигуряващ постигането на максимално възможната разделителна способност по разстояние, беше проверена чрез компютърно моделиране в средата на Матлаб при предположение, че в комуникационната система се използват така наречените бент-сигнали.

Както е известно, бент-сигналите са фазово манипулирани (ФМ) сигнали като законът на фазовата манипулация се задава чрез бент-последователности, които се

отличават с много висока структурна сложност и именно това е причината те да бъдат разработени в началото на 80-те години на миналия век [4], [5], [6].

Бент-последователностите представляват семейства от последователности, които се формират по правилото [4], [5], [6]:

(20) $s_j(i) = f\left[tr_1^n(\beta_0.\alpha^i), tr_1^n(\beta_1.\alpha^i), ..., tr_1^n(\beta_{m-1}.\alpha^i)\right] + \vec{j}^T.\vec{X} + tr_1^n(\sigma.\alpha^i)$.

Тук са използвани следните означения:

1) $s_j(i), j = 0,1,...,K-1,\ i = 0,1,...,N-1$ е ***i***-тият елемент от ***j***-тата бент-последователност от семейството;

2) $N = p^n - 1$ е дължината на бент-последователностите от семейството като ***p*** е произволно просто число, а ***n***, ***m*** и ***k*** са цели положителни числа, свързани със съотношенията:

(21) $$n = 2m = 4k \cap p = 2;\ n = 2m \cap p \neq 2;$$

3) ***K*** е броят на бент-последователностите в семейството $K = p^m = p^{n/2}$;

4) α е примитивен елемент на крайното алгебрично поле $GF(p^n)$;

5) $\beta_0, \beta_1, ..., \beta_{m-1}$ са базис на $GF(p^m)$ над $GF(p)$ като $\beta = \alpha^d, d = p^m + 1$ е примитивен елемент на крайното алгебрично поле $GF(p^m)$;

6) $\sigma \in GF(p^n)/GF(p^m)$;

7) скаларното произведение $\vec{j}^T\vec{X}$ („T" означава матрична транспозиция) определя номера на бент-последователностите в семейството;

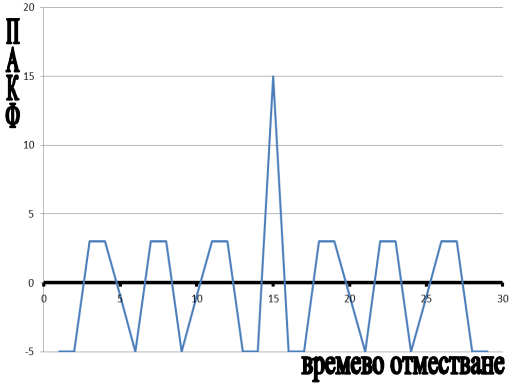
8) $f(x_0, x_1, ..., x_{m-1})$ е бент-функция, съпоставяща на елементите на $GF(p^m)$ елементите на $GF(p)$.

На базата на синтезираното по формула (20) семейство от бент-последователности, се формират елементарните импулси (чиповете) на съответните ФМ сигнали:

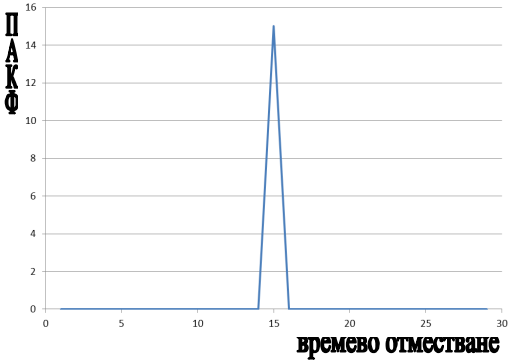
(22) $$u_j(i) = w^{s_j(i)},$$

като тук $u_j(i), j = 0,1,...,K-1,\ i = 0,1,...,N-1$ е комплексната амплитуда на ***i***-тия елементарен импулс (чип) от ***j***-тия бент-сигнал от семейството ФМ сигнали, а ***w*** е ***p***-ти корен от единицата.

Следва да се отбележи, че компютърното моделиране потвърди напълно коректността на обоснования в доклада метод за несъгласуваната цифрова обработка на сигналите. Това се илюстрира от фиг. 1 и фиг. 2, където са показани ПАКФ на бинарен бент-сигнал (т. е. $p = 2,\ w = -1$ в (22)) с дължина (период) $N = 2^4 - 1 = 15$ при използване на съгласуван (фиг. 1) и несъгласуван филтър (фиг. 2).



Фиг. 1. *ПАКФ на бинарен бент-сигнал при използване на съгласуван филтър*



Фиг. 2. *ПАКФ на бинарен бент-сигнал при използване на несъгласуван филтър*

Както се вижда от фиг. 1 и фиг. 2, използването на обоснования в доклада метод за несъгласуваната цифрова обработка на сигналите позволява напълно да се елиминират страничните листа на ПАКФ.

Заключение

В доклада е обоснован метод за реализиране на максимално възможната разделителна способност по разстояние на комуникационните системи чрез несъгласувана обработка на приетите сигнали.

Коректността на предложения метод е доказана чрез експериментално изследване, проведено по метода на компютърното моделиране. При моделирането са използвани ФМ сигнали с много висока структурна сложност (бент-сигнали), осигуряваща висока степен на защита срещу опитите за неоторизиран достъп до ресурсите на комуникационните системи.

Предвид на демонстрираните положителни качества, методът може да намери приложение в радиолокационните и радионавигационните системи, където проблемът за постигане на висока разделителна способност по разстояние е много важен.

Литература:

[1] Л. Е. Варакин, "Системы связи с шумоподобными сигналами," Москва, Радио и связь, 1985. – 384 с.

[2] S. Golomb, G. Gong, "Signal design for good correlation," Cambridge University Press – 2005

[3] В. П. Ипатов, "Периодические дискретные сигналы с оптимальными корреляционными свойствами," Москва, Радио и связь, 1992. – 152 с.

[4] J. D. Olsen. R. A. Scholtz. and L. R. Welch. "Bent-function sequences," *IEEE Trans. Infirm. Theory*, vol. IT-28, pp. 858-864, Nov. 1982.

[5] P. V. Kumar, "On Bent Sequences and Generalized Bent Functions," Ph.D. dissertation, Elec. Eng. Dept., Univ. Southern Calif., Los Angeles, Aug. 1983.

[6] P. V. Kumar and R. A. Scholtz, "Bounds on the Linear Span of Bent Sequences," *IEEE Trans. Infirm. Theory*, vol. IT - 29, No. 6, pp. 854-862, Nov. 1983.

СОФТУЕРНИ ПРОДУКТИ ЗА СТЕГАНАЛИЗ [1]

Станимир С. Станев

Шуменски университет „Епископ Константин Преславски"

STEGANALYTIC SOFTWARE PRODUCTS

Stanimir S. Stanev

Bishop Konstantin Preslavski University of Shumen

Abstract: *The paper deals with the popular steganalytic software products, accessible through the Internet to help the law enforcement and intelligence/counter-intelligence computer forensics examiners when conducting an examination of the storage media. The purpose and main features of the most popular commercial products for steganalysis are shown. The results of comparing the features of the most popular programs through coefficients of determination are marked.*

Key words: *steganology, computer steganography, network steganography, social engeneering, computer forensics.*

От средата на първото десетилетие на XXI век в информационната сигурност се използва терминът **стеганология,** обхващащ два смислово противоположни компонента - стеганография и стеганализ [1]. **Стеганографията** е изкуство, съвкуп-

[1] Разработката е частично финасирана от проект РД 08 – 250/14.03.2013 г., от фонда „ Научни изследвания" на Шуменския Университет „ Епископ Константин Преславски".

ност от технически умения и научно-приложна област за начините за скриване на факта на предаване (наличие) на информация [2]. Целта на стеганографията е скриването на информация в явен набор от данни по начин, който не би позволил откриването й в явните. Сега под стеганография най- често се разбира скриването на информация в компютърни файлове чрез специално програмно осигуряване. **Стеганализът** обединява методи и технологии за откриване на секретни стеганографски комуникации. Той се прилага при ком-пютърни съдебни разследвания, при проследяване на криминални дейности в Интернет и при събиране на доказателства за разследвания, особено на анти-социални елементи. Освен това, стеганализът се използва за усъвършенстване на сигурността на стего средствата чрез оценка и идентификация на техните слабости. По аналогия с криптологията, специалистите в областта на стеганализа се наричат **стеганалитици. Стегоатака** е всеки опит да се открие, извлече или да се унищожи скрито чрез стеганография съобщение [3].

Целта на настоящата работа е анализ на популярни софтуерни стегана-литични средства от гледна точка на практическата дейност при разследването на стегоинциденти. Тя не е обзор на всички достъпни средства, а само на продукти за откриване на факта на наличие на стегофайлове. Това е основната цел на стеганализа и по този начин се унищожава главното предимство на стеганогра-фията – скрития стегоканал за комуникация.

Повечето от известните методите за стеганализ се базират на откриване на следи от използвани стегопродукти. Доказано е, че всяка използвана стегопрограма оставя характерни цифрови отпечатъци в стегофайловете - т.нар. сигнатури. Много от програмите за стеганализ разчитат на разкриването на тези сигнатури чрез сравняването им с такива, събрани в специални бази от данни, подобно на антивирусните приложения и системите за откриване на нахлуване (IDS) .

Друг стеганалитичен подход изследва отклоненията на разследваната мултимедийна информация- стегофайла, от неговия очакван модел. Статис-тическите методи за стеганализ използват множество статистически характеристи, като оценка на ентропията, коефициенти на кореляция, вероятност на поява и зависимости между елементите на последователностите, условни разпределения, различимост на разпределенията по критерия Хи-квадрат и много други.Най- елементарните тестове оценяват корелационните зависимости на елементите на контейнерите, в които могат да се вграждат скритите съобщения. Извършени са много изследвания в областта на т.н. универсално сляпо откриване на стеганогра-фия (“universal blind detection”), наричано още откриване на базата на аномалии (anomaly-based detection). За откриването на скрита информация, особено в режим на реално време, стеганалитикът трябва да разполага с големи изчислителни ресурси.

Първите публикации в областта на стеганализа датират от края на 90-те години на миналия век, а сега техният брой е много голям. В тях се разглеждат различни подходи, методи и алгоритми за стеганализ [4, 5]. Днес повечето методи се базират на сигнатурите, но се разработват и системи за стеганализ чрез детек-тиране на аномалии [5]. Те са достатъчно точни и надеждни както и „сигнатур-ните” системи, но са по-гъвкави и приспособени бързо да отговорят на изисква-нията за откриване на нови стегометоди.

Практиката показава, че много стеганалитични програми работят по-добре, ако е налична ключова информация за типа на използваните стегоалгоритми. Откриването на стегопрограми на заподозрян компютър дават основание да се мисли, че на

този компютър има и стегофайлове. Типът на намерената стегопро-грама влияе на подхода за последващия стеганализ.

През 2008 в Internet има вече над 1500 стеганографски програми, и само 80 за стеганализ, днес техния брой е много по- голям. Съществуват много източници с обзор на достъпните стеганографски програми, например [6, 7, 8, 9]. У нас опит в това отношение е [10]. Внедрени са 7 поколения стего-програми, но подробни описания и анализи има само на тези от първите поколения, които едва ли сега вече някой ще рискува да използва. Интересно е да се отбележи, че в Internet има публикувани малко оригинални руски стегопрограми , например FoxSecret 1.00 (freeware - 5,7 MB), ImageSpyer2 (freeware - 13,9 MB), StegoG2 for TC, RedJPEG XT (freeware - 3,7 MB), DarcCryptTC, а е трудно да се намери руска стеганалитична програма [13]. В публикациите относно достъпния софтуер обаче не се използват количествени критерии за сравняване на техните качества [8,10]. В [8] 111 стеганографски програми се анализират само по типа на стегофайловете, в които скриват съобщения, и по достъпността им (сред тях 30 са open source, 27 са със статут на freeware, 22 - shareware , 8 са комерсиални) и само 8 - за стеганализ.

Желаещите да използват достъпните в Интернет стегопрограми обаче трябва да са наясно, че вероятността за откриване на скрити с тях съобщения от компетентните органи е почти 100%. Стегопрограмите, които имат приемлива надеждност в това отношение, са с голяма изчислителна сложност за кодиране на данни в реално време, и освен това обема на скритите съобщения не надвишава 3-4 % от размера на контейнера. Такива програми едва ли се предоставят за публично ползване.

Една от първите програми за стеганализ, цитирана като средство за експерименти от много изследователи, е **Stegdetect*** (със статут на freeware) на Нилс Провос (Niels Provos) от 2001 год. [11,12]. Тя използва статистически анализ, базиран на хи- квадрат **(χ^2)** тестове и може да открива данни в JPEG изображения, вградени с стегопрограми като F5, Invisible Secrets, JPHide and JPSeek, JPHide и JSteg, Outguess 01.3b, appendiX, Camouflage и Steghide. Дава добри резултати, когато скритото съобщение има размер над 10 % от този на контейнера. **Chi-Square*** е популярна програма, разработената от Guillermito през 2004 г. Тя реа-лизира статистически атаки срещу bmp. стего, генерирано от Steghide и DIIT [13]. **StegSpy***открива следи от програмите Hiderman, JPHIde and Seek, Masker, JPegX, Invisible Secrets. Едва ли звучи сериозно използването днес на такива програми при наличие на по-добри комерсиални програми.

На пазара има достъпни различни стеганалични инструменти като 2Mosaic, StirMark Benchmark, PhotoTitle и др. Те откриват информация, вградена в стегофайловете чрез стегопрограмите Jsteg-shell, JPhide, Outguess 0.13b, Invisible Secrets, F5, appendX, Camouflage, Hiderman, JPHIde&Seek, Masker, и JpegX. Тези програми могат да премахнат скрити съобщения от всеки графичен контейнер, с два метода - Break apart и Resample. **2Mosaic** (автор Fabien Petitcolas) премахва съобщение от всеки контейнер - изображение с метода Break apart. Този метод разбива подозрителното стегоизображение на десетки или стотици части. **StirMark Benchmark** премахва съобщение от всеки контейнер- изображение чрез метода Resample. **Photo Title** премахва съобщение от всеки контейнер- изображение чрез Break apart.

По договор с американските ВВС, компанията WetStone Technologies Inc. е разработила една от първите комерсиални стеганалитични програми за правителствени органи - **Stego Suite** (цената й е 1995 долара), за откриване на стего без предва-

рително да се знае стегоалгоритъма, по метода " blind anomaly-based de-tection ". Открива съобщения в изображения и аудиофайлове и използва речник за извличането им. Stego Suite се състои от три продукта. **Stego Watch** е стега-нографския инструмент, който търси скрито съдържание в цифрови изображения или аудио файлове. **Stego Analyst** е анализатор на графични и аудио файлове. Интегриран е със Stego Watch, за да предостави по-подробен анализ на подоз-рителни файлове. Има 9 стегоалгоритъма за детектиране. **Stego Break** открива паролата за отваряне на контейнера чрез т.н. „атаки- речник". Освен това **Stego Suite** позволява да се унищожат данните, скрити по метода LSB, чрез промяна на младшите разряди на всеки байт на мултимедийния стегофайл, в нулева стойност без промяна на качеството на контейнера [14].

Софтуерът Gargoyle Investigator (цена 1195 долара)(старо название Stego Detect) на същата компанията може да се използва за откриването на стегопрогра-ми. Gargoyle има колекция от данни, съдържаща данни за над 10 000 типа вреден софтуер. В нея има база данни Steganography Program Dataset с хеш набори за над 625 известни стеганографски програми [15]. WetStone Technologies се занимава и с обучение на кадри и стегозащита на правителствени учреждения.

Програмата Forensic Toolkit на компанията AccessData и програмата EnCase на компанията Guidance Software използват хешовете на програмата HashKeeper на Maresware и National Software Reference Library за търсене на използваните програми.

Американската фирма Backbone Security е световен лидер в продажбите на стеганалитичен софтуер.Тя доставя продукти на правителства и специални служби в много държави. Постоянно се актуализира и разширява най- голямата в света достъпна комерсиална база от данни за стеганографски сигнатурни отпечатъци Steganography Application Fingerprint Database (**SAFDB**) [16], създадена от изследователския център на фирмата - Steganography Analysis and Research Center (SARC). През 2005 г. той е разработил работещ прототип за откриване на опитите на „къртици" да получат или използват стегопрограми. Първият вариант на StegAlyzerAS откривал наличието на повече от 15000 артифакта, свързани с 230 стеганографски програми, чрез сканирането на файлове или „арестувани" компютри за отпечатъци. Той проверява за съвпадение изчислените от него хеш- стойности на файловете, с тези от набор от известни хеш- стойности на файлове от стегоприложения, съхранени в базата от данни SAFDB. Съвпадението означава, че с висока вероятност в изследвания файл има артефакт за използвана стего-програма. Автоматичният инструмент за откриване на сигнатури - Steganography Analyzer Signature Scanner (StegAlyzerSS) в началото откриваше присъствието на 27 уникални сигнатури на стегопрограми. Сега Backbone Security доставя четири продукта- StegAlyzerAS, StegAlyzerSS, StegAlyzerRTS и StegAlyzerFS разработени на базата на хибриден подход за откриване използването на стегоприложения. Те са с варианти за 32- и 64- битови компютри. Според фирмата те могат да открият използването на стеганография от „инсайдери".

Пакетът **StegAlyzerAS** (Steganography Analyzer Artifact Scanner) дава възможност за сканиране на цялата файлова система или отделни директории за подозрителна медия. За разлика от други известни изследващи инструменти, StegAlyzerAS може да извършва автоматично или ръчно търсене в регистрите на Windows, за да определи дали някои ключове от регистрите могат да се свържат

със артефакти от стеганографски приложения. Програмата позволява на криминалистите да сканират подозрителните носители на информация за наличие на известни „отпечатъци” (fingerprints, or hash values) на повече от 1175 стего-програми. Тази програма позволява да се определят подозрителни файлове чрез значенията на хеш-функциите на стегоприложенията, получени с CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Тези хешове се съхраняват в базата от данни SAFDB. Известните ключове на регистрите се определят с помощта на базата от данни за ключове на регистрите -Registry Artifact Key Database (**RAKDB**). Тази база е единствената достъпна стенографска база от данни за такива ключове [18].

Програмният продукт **StegAlyzerSS** (Steganography Analyzer Signature Scanner) (цена 1495 долара) е предназначен за криминалистки компютърни раз-следвания. Програмата сканира подозрителни контейнери за наличието на 55 из-вестни комбинации от байтове или известни сигнатури, които са останали във файловете и се отнасят към популярни стегопрограми. Той може да възстановява и скритата информация чрез автоматичен алгоритъм за извличане на данни. StegAlyzerSS разширява възможностите на сигнатурния анализ благодарение на метода сляп стеганализ (“blind detection”) [19]. Този продукт е признат от института Defense Cyber Crime Institute (DCCI) и изследователската лаборатория CyberScience Laboratory (CSL), за ефективно решение за откриване на файлове, които съдържат скрити данни.

Според много специалисти, **StegAlyzerRTS** (Steganography Analyzer Real-Time Scanner) е най-добрият в момента в света достъпен на пазара стеганалитичен програмно-апаратен комплекс за мрежова сигурност.Той е предназначен да открива в режим на реално време стеганографски приложения и техните сиг-натури. Работи в режим “drop-in, turn-key”, който не влияе на пропусната способност на мрежата (100 Mb или 1Gb). Комплексът позволява да се открие кога инсайдер зарежда (сваля) стегоприложения, чрез сравняване на значенията на хеш- функции или цифрови "отпечатъци” на файлове,с базата от данни SAFDB. Ком-плексът StegAlyzerRTS позволява да се определи инсайдерско използване на стеганографски програми чрез сканиране на файлове на входа и изхода на мрежата, за наличие на повече от 55 известни сигнатури на стегоприложения. StegAlyzerRTS открива кражба на конфиденциална информация, скрита в безобидни на пръв поглед файлове, които се изпращат на външни получатели по електронна поща или изпращане към общо достъпен сайт [20].

StegAlyzerFS е стеганалитичен продукт от категорията Computer Forensic Field Triage Products . Той може да направи за няколко минути бърза предварителна сортировка на полетата на подозрителни файлове директно в заподозрените компютри, за да открие скрита стегоинформация още на мястото на инцидента, което не може да се извърши от други продукти. Работи с популярните файлови системи ext2, ext3, ReiserFS, XFS, FAT, FAT32, NTFS, ISO и други, поддържани от Linux kernel 2.6.32. Установява наличието на хеш-функции от 1175 стегоприложения и 55 известни сигнатури на стегоприложения [17].

Сегашната версия на посочената база от данни, SAFDB v3.16, е неделима част от посочените четири продукта на фирмата. Съдържа файлове, артефакти или значения на хеш-функции свързани с повече от 1175 стего-приложения [17] .

Стеганалитичният софтуер **Ben-4D** прави бързо и точно идентифициране на стегофайлове в набор от файлове, чрез използване на разпределение според закона

на Бенфорд. Открива следи от JPHSWin, LSB, Invisible Secrets v4.0, Fuse, Uses JPEGSnoop [21].

StegSecret е стеганалитичен продукт с отворен код, базиран на java-мултиплатформа. Позволява откриването в различни цифрови среди на скрита информация чрез стеготехниките EOF, LSB, DCT и програми Camouflage V1.2.1, ThePicture v2, JPEGXv2.1.1, PGE (Pretty Good Envelope) v1.0, appendX, steganography v1.6.5, PlainView, DataStash v1.5 dataStealth v1.0. Използва базата от данни BDAS v0.1 (Steganography Tools Fingerprint DataBase) за откриване на повече от 40 стегопрограми [22].

Програмата **Steg_IDS** обединява стеганалитични програми с цел създаване на комплексна система за откриване на стегоатаки (SIDS). Съдържа 4 модула - Snort, Parse Snort , Crawler, и Stegdetect. Използва статистически тестове да разкрият стегосъдържание, и да определят с каква програма са направени [23].

В много университети в света се работи активно по разработване на стеганалитични продукти.Интересна форма за развитие на методите за стеганализ от млади изследователи е периодично провежданото международно състезание по стеганализ **BOSS** (Break our steganography system). Целта на състезанието е разби-ването на специално разработения за целта стегометод HUGO [24]. Този метод е най-устойчив срещу стегоатаки чрез най- добрия в момента стеганалитичен метод SPAM, разработен от екипа на една от най-известните специалисти по стеганология проф. Jesica Fridrich от SUNNY Bingham University, NY. Този екип е световен университетски лидер в областта на стеганалитичните изследвания. Един от резултатите е разкриването на слабостта на HUGO по отношение на метода 1D за предотвратяване на стеганализа. През през юни 2011 г. състезанието е спечелено от студентския отбор на проф. Fridrich с коефицент на откриваемост K_{sa}=0,82, а на второ място с K_{sa}=0,73 е британския отбор Queen с водачи Dr. Fatih Kurugollu и Gokhan Gul [25].

Друга университетска форма е Virtual Steganographic Laboratory (**VSL**) - средство за тестване и настройка на стеганографски и стеганалитични методи [26]. Институтът за сигурност на технологиите в Dartmouth College е разработил софтуер за откриване на скрити данни в графични файлове с помощта на статистически модели, които са независими от формата на изображението или техниката на стеганография. Тази програма е в състояние да открие наличието на скрити съобщения с ефективност 0,65 [27].

В лаборатория „Компютърна сигурност" на Шуменския университет са направени над 1600 експеримента за определяне на ефективността на откриване върху база данни от по 100 контейнера- изображения тип BMP и JPG. За сравнителна оценка на програмите за стеганализ бе предложен критерий за ефективност- коефицент $\mathbf{K_{sa}}$:

$$\mathbf{K_{sa} = N_f / N_t},$$

където N_f е броят на стего файловете, в които стгоаналитичната прог-рама е открила скрито съобщение, а N_t е общият брой на тестваните стего файлове.

Проведени са по 100 експеримента с всеки от избраните контейнери и с всяка от стеганалитичните програми, отбелязани със * по-горе. Експериментите с **StegDetect** (модул **xsteg**) със скрити със стегопрограмата Invisile Secrets в JPG-контейнери, съобщения с разширения .txt и .jpg, показват значения на този коефициент K_{sa}=1 , при опция в xsteg, sensitive= 1. Резултатите от анализа със същата

програма на .jpg стегофайлове, но с получени с програмата JPhide, при sensitive=1, е $K_{sa}=0,13$ за текстови съобщения и $K_{sa}= 0,48$ за .jpg съобщения. При sensitive=10 съответно те са $K_{sa}=0,96$ и $K_{sa}=0,81$.

Програмата **StegSpy** има ефективност- $K_{sa}=0,53$ при анализа на .bmp стегофайлове, получени с Invisile Secrets вградени текстови и .bmp съобщения, и $K_{sa}=0,39$, за същите съобщения и контейнери при използване на програмата StegoMagic. При опитите за анализ на .jpg стегофайлове с вградени .txt и .jpg съобщения, резултатите са много по-слаби – съответно $K_{sa}=0,06$, и $K_{sa}=0,02$-$0,03$. Програмата **Chi- Square** има $K_{sa}=1$ при анализа на .bmp стегофайлове с вградени .txt и .bmp съобщения.

Следователно ефективността на откриване зависи от програмата, с която е скрито съобщението и от типа на файла - контейнер. В някои случаи при един и същи размер и формат на контейнера и една и съща скрита информация, не винаги се открива нейното наличие. Програмите StegDetect и Chi-square са по-ефективни от програмата StegSpy при търсене на информация в стего файлове, и по бързодействието при намиране на информация. Тестваните програми се справят най-добре с откриването на информация, вградена с програмата Invisible Secrets.

Постоянно развиващите се стегометоди отправят нови предизвикателства към стеганалитиците и компютърните следователи [28]. Универсални инструменти, които могат да открият и класифицират стеганографска активност все още се намират в стадий на начално разработване. И се реализира следващ цикъл както при криптографията - стеганализът помага да се открият скрити съобщения, но също така показва на създателите на нови алгоритми за стеганография как да избегнат откриването на такива съобщения.

Литература:

1. Cox I., L.Matthew, J. Miller,J. Bloom,J. Fridrich and T. Kalker. Digital Watermarking and Steganography.Second Edition. Elsevier, Morgan-Kaufmann publishers, 2008. ISBN 978-0-12-372585-1.

2. Аграновский, А., А. Балакин , В. Грибунин и С. Сапожников. Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга, 2009. ISBN 978-5-9502-0401-2.

3. Станев,С. и В.Галяев. Семантична еквивалентност на основните термини на ком-пютърната стеганология в българските, английските и руските научни публикации. В:Трудове на Международна научна конференция MATTEX2012, Шумен, 2012. (под печат).

4. Nissar, A. and A. Mir. Classification of steganalysis techniques: A study. Digital Signal Processing, 20 (2010), 1758-1770.

5. Kessler,G. An Overview of Steganography for the Computer Forensics Examiner . [онлайн].[прегледано 1.05.2013].http://www.garykessler.net/library/fsc_stego.html.

6. Neil F.Johnson.Steganography software.[онлайн].[прегледан 22.04.2013]. http://www.jjtc.com/Steganography/tools.html.

7. Network Steganography Tools.[онлайн]. [прегледан 20.04.2013]. http:// stegano. net/ tools.html.

8. Hayati, P.,V.Potdar and E. Chang.A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator.[онлайн]. [прегледан 20.05.2013]. http:

//www.pedramhayati.com/images/docs/survey_of_steganography_and_steganalytic_tools .pdf.

9. Барсуков, В. и А. Шувалов. Ещё раз о “стеганографии” – самой современной из древнейших наук. [онлайн]. [прегледан 20.04.2013].http://www.ess.ru/sites/ default/ files/files/articles/2004/02/2004_02_04.pdf

10. Стоянова, В. Сравнителен анализ на устойчивостта в някои стеганографски алгоритми. В: Сборник трудове на научна конференция „Зашитата на личните данни в контекста на информационната сигурност”.ФАПВОКИС на НВУ, Шумен , 2013 (под печат).

11. Provos, N. and P. Honeyman. Detecting Steganographic Content on the Internet. Univ. Michigan, Ann Arbor, Tech. Rep. CITI 01-la, 2001. [онлайн]. [прегледан 15.05.2012].http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

12. Provos, N. OutGuess - universal steganography. 2004, http://www.outguess.org

13. Ibrahim,A. Steganalysis in Computer Forensics.[онлайн].[прегледан 20.03.2013]. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1009&context=adf

13. Стеганография. [онлайн]. [прегледан 21.03.2013]. http://rusteganography.narod.ru/

14.Wetstone Technologies inc.[онлайн].[прегледан 20.04.2013].http://www. Wetstonetech. com/product/stego-suite/; http://www.htt.co.in/wetstone/Stego-Suite.htm.

15. Gargoyle Investigator Enterprise Module (GEM).[онлайн].[прегледан 20.04. 2013]. http://www. htt.co.in/wetstone/ Gargoyle -Investigator-Enterprise-Module.htm.

16. Backbone Security Expands World's Largest Digital Steganography Database. [онлайн] . [прегледан 20.05.2013] . http://www. backbonesecurity.com/ SteganographyDatabase1175Applications.aspx.

17.StegAlyzerAS. [онлайн]. [прегледан 20.05.2013].http://www.sarc-wv.com/ products /stegalyzeras/learn_more.aspx .;http://www.sarc-wv.com/products/.

18. [онлайн]. [прегледан 14.05.2013]. http://www.forensicmall.ru/cat/back-bonesecu rity/stegalyzerss/ ; http://www.sarc-wv.com/stegalyzerss.aspx.

19. StegAlyzerSS. [онлайн]. [прегледан 8.05.2013]. http://www.sarcwv.com/products /stegalyzerss/learn_more.aspx.

20. StegAlyzerRTS.[онлайн].[прегледан 5.05.2013]. http://www.sarcwv.com/products /stegalyzerrts/learn_more.aspx.

21. Ben-4D.[онлайн].[прегледан 23.05.2013]. http://ben4dstegdetect.sourceforge.net/.

22. Stegsecret. [онлайн].[прегледан 21.05.2013]. http://stegsecret.sourceforge.net/.

23. Steg_IDS. [онлайн]. http://www.securityknox.com/Steg_project.pdf

24. HUGO.[онлайн].[прегледан 21.05.2013]. http://www.agents.cz/boss/.

25. BOSS. [онлайн].[прегледан 21.05.2013]. http://www.csit.qub.ac.uk.

26. VSL.[онлайн].[прегледан 2.05.2013]. http://vsl.sourceforge.net/.

27. Institute ISTS.[онлайн].[прегледан 21.05.2013]. http://www.ists.dartmouth.edu/ projects/ archives/ddi.html.

28. Computer Forensics, Cybercrime and Steganography Resources Website, Steganography & Data Hiding - Articles, Links, and Whitepapers page. [онлайн]. [прегледан 22.05.2013]. http://www.forensics.nl/steganography.

СТЕГАНОГРАФСКИТЕ МЕТОДИ И ЛИЧНИТЕ ДАННИ – АСПЕКТИ НА АТАКИ И ЗАЩИТА[1]

Станимир С. Станев, Христо А. Христов

Шуменски университет „Епископ Константин Преславски"

STEGANOGRAPHIC METHODS AND PRIVACY- ASPECTS OF ATTACKS AND PROTECTION

Stanimir S. Stanev, Hristo A. Hristov

Bishop Konstantin Preslavski University of Shumen

Abstract: *The paper reveals the possibility of using the methods of computer and network steganography by insiders to create hidden leakage of sensitive private information from organizations, and the challenges on the security services. The possible variant of insider's activities is discussed. Based on the analysis of those threats some countermeasures in the security policy are proposed.*

Key words: *steganology, computer steganography, network steganography, social engineering, privacy.*

Информацията за личните данни, обработвана от информационните системи, може да са обект на посегателства от фирми и престъпни групировки. За целите си те използват различни методи, включително и нови информационни технологии за проучвателните дейности, информационни атаки, информационни и психологически въздействия [1]. Едно от ефикасните направления за създаване на скрити канали за изтичане на такава информация е стеганографията- съвкупност от методи и средства, които имат една обща цел- скриването на самия факт на съществуване на тайна информация в различни среди [2]. Класическата стеганография предлага много методи за скриване (симпатични мастила, микроточки, тайни канали, холография, и др.) [3]. Днес техни наследници са методите на компютърната и мрежовата стеганография - направления на информационната сигурност, изучаващи проблемите на скриване на информация в явна информационна среда, създавана от компютърните системи и мрежи. Стегопрограми могат да се прилагат както за целите на защитата на данните, така и за незаконно извличане на чувствителна за хората информация [3].

Защитата на правата на физическите лица при обработването на личните данни е ангажимент на всяка организация у нас, вменена от Закона за защита на личните данни [4]. Основните мерки за защита на тази информация в държавните структури се базират на съответните закони, наредби и правилници [5]. Разглеждането на аспектите на тази защита в частния сектор, и преди всичко на борбата срещу нови-

[1] Разработката е частично финансирана от фонд „Научни изследвания" на Шуменския университет „Епископ К. Преславски" по проект РД 08-250 / 14.03.2013.

те методи за информационна престъпност, на практика не е обсъждана достатъчно. Трябва да се отбележи, че за защита на информацията си и за контра-разузнаване, западните фирми отделят до 20 % от чистата си печалба. За съжаление практиката показва, че методите и средствата на разузнаването винаги изпреварват средствата за защита [1].

Лични данни са всяка информация за физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или специфични признаци, които са свързани с неговата физическа, физиологична, генетична, психическа, психологическа, икономическа, културна или социална идентичност [4]. В [6] е разработен частен модел относно заплахите за личните данни на базата на редица документи , в това число и на законите за защита на личните данни.

Сигурността на личните данни е **състояние на защитеност** на тези данни, характеризиращо се със способността на потребителите, техническите средства и информационните технологии да осигурят конфиденциалност, цялостност и достъпност на такива данни при тяхната обработка в информационните системи [6]. Лични данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии, както и данни, отнасящи се до здравето, сексуалния живот и човешкия геном на съответното физическо лице, се наричат още **чувствителни данни**. Тези данни по принцип са забранени за обработка освен в случаите, изрично предвидени в закона. В организациите на основание чл. 23 от Закона администраторите на лични данни предприемат необходимите технически и организационни мерки за защита на данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Те са длъжни да вземат специални мерки за защита, когато обработването включва предаване на данните по електронен път. С наредбата [7] се определя минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. Тази защита в мрежите на фирмите и организациите от изграждането на ефективно противодействие на съществуващите несанкциониран достъп е актуален, но много труден и нерешен проблем.

Целта на настоящата разработка е да се посочат както аспекти на заплахите от използването на компютърната стеганография за предаване на лични данни от вътрешни за дадена организация нарушители, така и на защита от такива средства. Актуалността на темата е свързана с отговорностите на службите за фирмена сигурност и на администраторите на лични данни (т.нар. „лица по защита на личните данни“) при възможности за използване на стеганографските методи за скрито извличане на информация за лични данни от организациите и фирмите .

Службите за сигурност извършват огромна работа по защита на своите компютърни мрежи от външни атаки и разузнаване. Заедно с ежедневната дейност за спиране на нежелани трафици, вируси, зловреден софтуер, и други несанкционирани опити за достъп до тях, тези служби трябва да имат предвид и вътрешни нарушители, използващи дигитални носители за секретно разпространяване на информация извън охранявания от мрежите периметър. Вътрешните заплахи са особено трудно разрешим проблем, защото има толкова много начини вътрешните зложелатели в организацията (т.н. „инсайдери”, от англ. insiders) да откраднат информация от нейната мрежа. Проблемът с тези заплахи е толкова актуален, че

той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List), на Американският съвет за из-следване на сигурността на информационните системи – INFOSEC. Това е списък на най-трудните и най-критичните предизвикателства в INFOSEC изследванията, които трябва да бъдат решени за разработването и внедряването на надеждни системи за правителството на САЩ. „Инсайдерите" са напълно наясно за стойността на информацията, с която те работят въз основа на ежедневната си дейност. Като резултат, вътрешните кражби на чувствителна информация, се увеличават с обезпокоителни темпове, за целта инсайдерите може да използват всяка от повечето от 1500 стеганографски приложения, достъпни в Интернет като безплатен или Shareware софтуер. Повечето средства за мрежова сигурност и системи за предотвратяването на загуба на данни не откриват употребата на стеганография от вътрешни служители [8].

Ролята на защитниците и наблюдателите, още от публикуваната през 1983 год. статия на Симънс с „проблема на затворниците" Алис и Боб [9], е все още повече обект на теоретични изследвания, отколкото на практическо приложение.

В настоящата разработка на базата на този сценарий с участието на Алис и Боб, с цел изследване на проблема за възможните стеганографски канали за изтичане на лични данни и практическа насоченост на разработката, е предложен хипотетичен модел на **атаката** на разузнавателната служба на организация „Б", с използване на стеганографски методи срещу организация „А" (фиг.1). Организация „Б" е инициатор на незаконно посегателство върху лични данни. Управлението на тази компания поставя задача на разузнавателното си звено от службата за фирмена сигурност, да придобие конфиденциални лични данни от организация „А". Изрично е поставено условието задачата да бъде изпълнена в условия на пълна конспиративност, без атакуваната организация да узнае за изтичането на информацията. Разузнавателното звено на „Б" възлага изпълнението на задачата на своя служител-агент Боб.

От направеното предварително проучване Боб установява, че желаните лични данни в организацията „А" са защитени с надеждно функционираща система за информационна сигурност, изключваща несанкциониран външен достъп към компютърните й ресурси. Поради това, за изпълнение на тази задача, Боб решава да вербова служител на фирма „А", имащ естествен достъп до желаната разузнавателна информация на база заемана длъжност. След осъщественото изучаване на личния състав на „А", Боб вербува на компроматна основа служител от тази организация - Алис, която отговаря на това условие [10].

След вербовката Алис и Боб започват поетапно да изпълняват задачата за разузнавателното звено на „Б".

Информацията, която Алис трябва да предостави на Боб, е определена за конфиденциална за атакуваната фирма, поради което тя е достъпна само в зоната за обработка на лични данни на организацията „А", с функциониращ режим на достъп. Сведенията, получени от Алис, потвърждават наличието на „твърда" политика за компютърна и мрежова сигурност в „А" [2], и наличието на специализирана стегопрограма от типа на StegAlyzerRTS [11] в защитната стена на компания „А" (фиг.1). Предвид съществуващата опасност от разкриване на вербуваният агент Алис, ако тя използва традиционните канали за изнасяне на лична информация от зоната за обработка на тези данни, Боб търси и намира слабост в системата за сигурност на „А". Това е разрешението за служителите на „А" да използват не само

служебните компютри, контролирани от администратора по сигурността на мрежата на фирма „А”- Вили, но и лични компютри и мобилни апарати за безжична връзка с глобалната мрежа Интернет. Боб решава да приложи стеганографски способи за решаване на задачата. Той преценява, че използването на мрежова стеганография в защитената мрежа на „А” от агент като Алис, с недобра квалификация като компютърен специалист, би било неудачно поради по- сложния за целта софтуер [11].

Боб осигурява на Алис специално разработената от специалистите на „Б” стеганографска програма „ST” за вграждане на скрити съобщения в мултимедийни носещи файлове (т.н. контейнери) , набор от подходящи контейнери и стегоключ (в случая това е съвкупност от правила за установяване на връзка между двамата абонати , вида и парола на използваната програма , начина за вграждане в един или няколко контейнера и др.), като и адреса на определен от Боб Web сайт („тайник”), където Алис трябва да изпрати стегограмата със скритата информация. За да не бъде разкрита предварително от Вили за подготовката си за непозволена дейност, Алис може да получи тази информация от облака- компютри с общи ресурси в Интернет пространството, позволяващи тяхното общо ползване от Алис и Боб (фиг. 1).

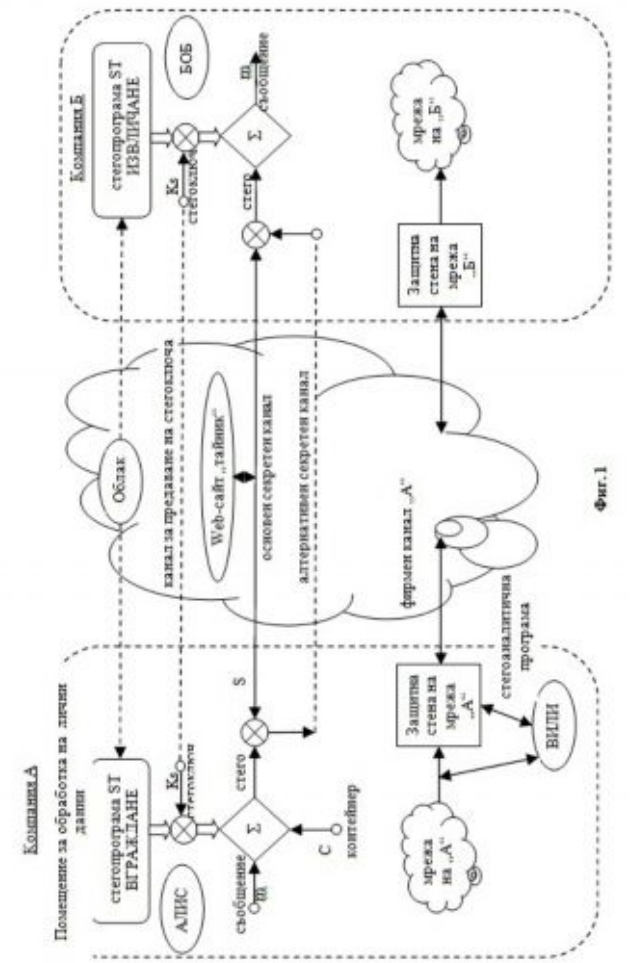
Основният секретен канал се установява чрез предаване на стегофайла чрез безжичната мрежа до „тайника”. Алтернативен секретен канал може да бъде изграден чрез изнасяне на стего във вид на безобиден мултимедиен файл на физически носител. Този вариант обаче е много по- рисков за Алис.

Чрез представената схема (фиг.1) се онагледява последователността от действия на Алис за предаване на конфиденциалната информация .След добиване на необходимата конфиденциална информация, Алис изтегля в личния си компютър стегопрограмата и файла - контейнер и използвайки тези средства, преобразува информацията в стегосъобщение. Възможно е Алис да използва и алгоритъм за разпръснато вграждане в контейнер/контейнери и реализация на стегометод за вграждане на псевдослучаен принцип [12]. Алис изпраща стегофайла от своя личен компютър чрез безжична мрежа, нямаща нищо общо с мрежата на „А”, до посочения от Боб Web сайт - „тайник”. От него впоследствие Боб изтегля стегофайла, чрез уговорените стеганографски средства извлича желаната конфиденциална информация и я предоставя на централата на „Б”.

След всяко изпращане на стегограма, Алис изтрива всички компрометиращи я файлове от своя личен компютър. Преди всеки нов сеанс тя отново изтегля необходимите й средства от „облака”.

Този сценарий разкрива как на практика чрез използване на методите на стеганографията е възможно конспиративно да бъде извлечена разузнавателна информация от дадена организация (включително и лични данни), осигуряващо минимизиране на възможностите за нейното разкриване от службите за сигурност на атакуваната организация.

Разкриването на канала за изтичане на конфиденциална информация е основна задача на фирмената служба за сигурност на „А” с цел пресичане на престъпната дейност. Нейна отговорност е и организиране на ефективно противодействие на съществуващите възможности за използване на стеганографските методи за скрито извличане/изтичане на конфиденциална персонална информация от организацията.



Фиг. 1

Противодействието на стеганографските методи кореспондира пряко с политиката за сигурност на атакуваната организация. Политика за IT-сигурност включва множество правила, които определят как организацията защитава важната си информация в няколко направления- организационни, административни, технически и програмни [2].За постигане на желаната надеждност и ефективност, задължително условие е съчетанието на горепосочените мерки с класически оперативни мерки за противодействие [10].

Детайлното разглеждане на мерките за сигурност излиза извън рамките на дадената разработка, тук могат да се маркират някои от тях, като ограничаване на комуникациите , заглушаване с генератор на бял шум на зоната, в която се обработват личните данни, ограничаване ползването на мобилни телефони, ограниче-

ване и контрол на достъпа до Интернет, създаване на проксисървър. В политиката за IT- сигурност на организацията могат да бъдат включени правила за забрана на внасянето, тегленето и ползването на криптиращи и стеганографски програми за лични цели без разрешението на системния администратор; забрана за достъп до интернет на компютри, в които се обработва чувствителна информация на организацията; забрана за презапис на данни върху информационни носители; забрана за ползване в зоните за сигурност на компютри с достъп до Интернет, извън компютърната мрежа на компанията; стеганализ на всички изходящи по официалния мрежов канал на организацията мултимедийни обекти, или тяхното „зашумяване" чрез вграждане на специални стеганалитични съобщения, с цел унищожаване на евентуално вградена секретна информация, и др.

Фиг. 2

Допълнително към тези мерки трябва да се отбележи и възможността за **стеганографска защита на личните данни**, противоположна на разгледаната до тук стегоатака. Стеганографски методи вече се прилагат за защита на авторско право на фотографии, картини, музика и др. Това са т.н. цифрови водни знаци (digital watermarks). Овен това подобни методи се прилагат за създаването на цифрови пръстови отпечатъци (digital fingerprints), вграждащи диагнози, резултати от медицински изследвания и лични данни в изображения от скенери, ехографи, коронарография и др. [13]. Тези методи могат с успех да се приложат и за защита на личните данни. За целта звената в организациите, които обработват с компютри лични данни, трябва да разполагат със съответните стегопродукти и да вграждат персоналните данни на всеки човек, например в негова лична цифрова снимка (фиг. 2) [14]. Това много ще затрудни инсайдери като Алис да намерят тази информация, тъй като със стегоключовете за разкриването ѝ боравят само съответните служители от отделите за човешки ресурси.

Но и най-съвършените методи не могат да дадат гаранция за абсолютната защитеност на информацията. Голямо практическо значение има изследването на социологическите аспекти на нарушенията, в това число и мотивите, движещи

„инсайдерите". Компютърните престъпления се извършват от хората, а не от компютрите, и даже и да се приеме като аксиома тезата „Проблема на защита на информацията е най-напред проблем на човешките ресурси", и при наличие на правилна кадрова политика, проблема остава нерешен. Не е възможно да се подбере абсолютно верен на ръководството на организацията персонал, а освен това, могат да се допускат и случайни, неумишлени нарушения.

Задачата се свежда до построяване на система със зададено ниво на надеждност, от предварително известни, ненадеждни от гледна точка на защитата на информацията, елементи. Но тази задача не се решава във вакуум, а при наличието на външно, понякога доста мощно, въздействие, състоящо се от разузнавателната дейност на противник. За решаване на тази задача, свързана със защитата на информацията, трябва добре да се познават видовете разузнавания, техните методи, особено нелегалните разузнавателни методи за добиване на секретна информация [7]. Общоизвестно е, че техническите средства не могат да се контролират на 100%, затова е необходимо и съчетаното прилагане на оперативни мерки за противодействие, свързани с осигуряване на оперативен контрол на поведението и действията на служителите с цел проверка на тяхната лоялност и установяване на признаци за подготовка и използване на стеганографски продукти [15]. Предложените в разработката направления за противодействие на злонамереното използване на стеганографски методи са само началото на конкретни разработки в тази област.

Литература

1. Дворянкин, С. Компьютерные технологии обеспечения безопасности оперативных аудиоданных в условиях информационно-технического противодействия. Дисертация. Москва: 2000.

2. Станев, С, С. Железов. Компютърна и мрежова сигурност. Шумен: Университетско издателство, 2002.

3. Zielinska, E., W. Mazurczyk, K. Szczypiorski. The Advent of Steganography in Computing Environments. In: Computing Research Repository (CoRR), abs /1202.5289, arXiv.org E-print Archive, Cornell University, Ithaca, NY (USA), published on 23 February 2012. [онлайн]. [прегледан 2.04.2013]. http://arxiv.org/ftp/arxiv/papers/1202/1202.5289.pdf .

4. Закон за защита на личните данни. http://lex.bg/laws/ldoc/2135426048.

[онлайн]. [прегледано 10.04.2013].

5. Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация. [онлайн]. [прегледано 20.04.2013]. http://www. dans.bg/ images/ stories/ promzak/naredba_ais_mrezhi-06122012.pdf .

6. Частная модель угроз безопасности персональных данных в информационной системе персональных данных.[онлайн].[прегледано20.04.2013]. http://dehack.ru/PDn/dokumenty.

7. Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. [онлайн]. [прегледан 2.04.2013]. http://ciela.net/FreeStateGazette/ OpenDocument.aspx?id = 2135836487.

8. Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. [прегледано 20.04.2013]. http://www.sarc-wv.com/news/press_releases/2013/steganography_insider_threat.aspx

9. Simmons, G. The Prisoners' Problem and the Subliminal Channel. Advances in Cryptology: Proceeding in Crypto. CRYPTO'83,1983, pp. 51-67.

10. Асенов, Кипров. Теория на контраразузнаването. София: Труд, 2002.

11. Steganography Analyzer Real-Time Scanner. [онлайн]. [прегледано 20.04.2013]. http://www.sarc-wv.com/products/stegalyzerrts/learn_more.aspx

12. Беджев, Б., С. Йорданов и др. Приложение на линейните рекурентни последователности над крайни полета при синтеза на сложни широколентови сигнали. Научна конференция, Русе, 2012.

13. Li,M., R. Poovendrana and S.Narayananb. Protecting patient privacy against unauthorized release of medical images in a group communication environment . [онлайн]. [прегледано 20.05.2013]. http://www.ncbi.nlm.nih.gov/pubmed/15893452 .

14.http://volgastars.ru/chapman/chapman.html. [онлайн]. [прегледано 2013].

15. Христов, Х. Особености на организацията и управлението на оперативното противодействие на посегателства срещу фирмената сигурност. В: Сборник трудове на юбилейна научна конференция „10 години от създаването на НВУ „В. Левски", 2012, Том 4 (под печат).

СТЕГАНОГРАФСКИ МЕТОДИ В МРЕЖОВИЯ СЛОЙ НА OSI МОДЕЛА[1]

Станимир Стоянов Станев Христо Иванов Параскевов
Станимир Станчев Станев

Шуменски университет „Епископ Константин Преславски"

STEGANOGRAFIC METHODS IN NETWORK LAYER OF THE OSI MODEL

Stanimir Stoyanov Stanev Hristo Ivanov Paraskevov
Stanimir Stanchev Stanev

ABSTRACT: *The paper deals with the options of using stego methods by protocols at network level for forming covert data transmission channels. Some characteristics of these channels have been proposed. Directions for protection of network stegano-graphic methods leaks have been pointed out.*

KEY WORDS: *Steganology, network steganography, covert cnannels,information hiding.*

Един от аспектите на информационната сигурност е скриването на информацията. Интернет и компютърните мрежи откриха нови възможности за скрита връзка.

[1] Разработката е частично финансирана от фонд „Научни изследвания" на Шуменския университет „Епископ К. Преславски" по проект РД 08-250 / 14.03.2013.

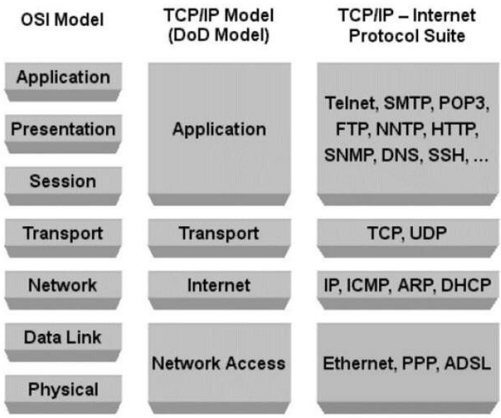
Секретни съобщения може да бъдат скрити не само в безобидни на пръв поглед мултимедийни файлове, като е при компютърната стеганография, но и в елементите за управление на комуникационните протоколи и в резултатите от изменение в логиката на протоколите и създаване на скрити канали. Този термин в контекста на компютърните системи за пръв път е публикуван през 1973 год. в САЩ, а през 1985 год. отново се появява в публикация на американското Министерство на отбраната [1]. От началото на настоящия век алтернативно се из-ползва и терминът мрежова стеганография. Мрежовата стеганография (наричана още протоколна) е вид високотехнологична стеганография, в която за носители на секретни данни се използват мрежовите протоколи на седемслойния модел на взаимодействие на отворени системи OSI (фиг. 1). При нея стегометодите се прилагат към динамични обекти – протоколните единици PDU (Protocol Data Unit) на съответния мрежови протокол. PDU са определени в спецификациите на съответния протокол - формата на техните полета, тяхната семантика, допустимата големина, последователност на предаване на отделните протоколни единици, обработване и др.

Мрежовото ниво от OSI модела формира структурата на данните и осигурява обмена на информация между обектите на транспортния слой. Протоколите на физическия и канален слой са локални, защото се отнасят само към едно от ребрата на графа, описващ комуникационната мрежа (между два съседни мрежови възли). За разлика от протоколите на първите два слоя на OSI модела, протоколите на мрежовия слой са глобални, защото се реализират в подмрежата като цяло и са тясно свързани с топологията ѝ [3].

Фиг. 1. Протоколни характеристики, използвани за мрежова стеганография, свързани с OSI модела

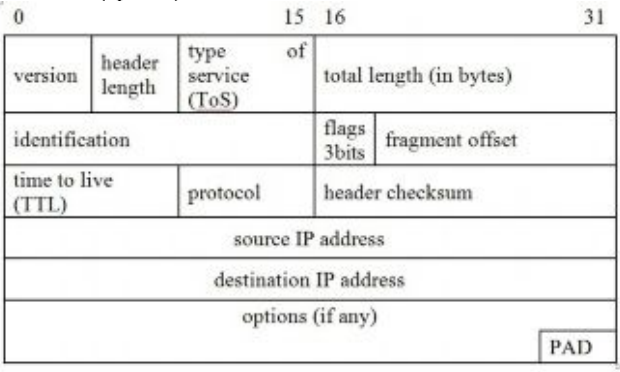
Мрежовият слой има стратегически управляващи функции, като основна негова задача е да определи маршрута на пакетите от подателя към получателя им. За целта в междинните възли (рутерите) на подмрежата се използват алгоритми за оптимално маршрутизиране на базата на метрика (комплексен показател за определяне на маршрут). В локалните компютърни мрежи с общ (споделен) канал маршрутизирането е просто и почти липсва. За да не се получат задръствания в мрежата от много на брой пакети, мрежовият слой се занимава и с контрол на натовare-

ността на подмрежата. Осигурява се стабилна и гъвкава среда за взаимодействие на различни подмрежи [3] (фиг.2).



Фиг. 2. Сравнение на OSI модела с протоколния стек TCP/IP

Има множество публикации, прилагащи стеганографски методи, използващи полета от заглавната част на IP пакета. Причината за това многообразие е, че в заглавната част на IP има полета, чиято модификация не би попречила на нормалната комуникация [4](фиг. 3).



Фиг. 3. Заглавна част на IP пакет

Полето Type of Service е предназначено да определи начина на обработване на дейтаграмата. То предлага възможност за стеганография, защото съвременните реализации на мрежовите устройства игнорират стойностите в това поле. Обичайните стойности във всички битове са 0 и следователно ако стойностите са различни от 0, то по всяка вероятност има намеса в тях [5]. Това е сравнително бърз начин за установяване на стеганографско предаване, както и за неговото компрометиране.

Полета Identification, Flags (DF и MF) и fragment offset са свързани едно с друго и могат да се прилагат за стеганографско предаване в случаите, когато флагът DF е

установен в 1. Ако не е разрешена фрагментация то стойностите в полетата Identification и Fragment Offset, могат да бъдат заместени с желана информация [5].

Полето Header CheckSum, може да се използва за стеганографски цели в два аспекта. Ако се извърши нарочна промяна в друго поле, като Options, ще се наложи преизчисляване на стойността. Някои разработки предлагат да се впише стойност, която е грешна, което ще доведе до повторно предаване [6].

Полето Options е незадължително и също е възможно да се използва за стеганографско предаване. Полето PAD е допълващо заглавната част до 32 кратно. Запълването обикновено е с 0, но за стеганографско предаване може да се използват и други стойности.

В доклада е разгледан вариант за скрито предаване на данни с използване на полето TTL. Въпреки, че предназначението на това поле традиционно не е за комуникация с помощта на подходящо кодиране от страна на изпращача в това поле може да се запише информация, която по-късно да бъде успешно декодирана от получателя. Преминаването на пакета по различни пътища до получателя и през мрежови устройства, като рутери и защитни стени, променя стойността на TTL, но въпреки това може да се определи интервал на „очаквана" стойност.

Последствията от това са две. Първо скритият канал трябва да се подбере по такъв начин, че промяната на стойността на TTL да бъде в интервала на „очакваната" стойност. На второ място капацитета на скритият канал зависи от естествената вариация на TTL. За целта е направен анализ на стойността на TTL в Internet и е предложена кодираща схема, която да направи измененията на TTL „естествени".

Както е известно TTL ограничава живота на IP пакета по време на предаване с цел да не се „наводни" трафика с пакети, които не са достигнали до местоназначението си. Стойността на TTL се определя от изпращача и се декрементира от всеки мрежов елемент, като рутери и защитни стени, през цялото протежение на пътя на пакета. Пакетът се отхвърля, ако стойността му е нула и той все още не достигнал получателя си. Използването директно на полето с цел да се кодират определени стойности би било много подозрително, тъй като има установени първоначални „нормални" стойности. Драстичната промяна на стойността би могла да доведе до две евентуални състояния: увеличение – неопределено време за преминаване на пакета и намаление – евентуално недостигане до получателя на пакета. Кодирането на скритата информация директно в TTL ще изисква да се знае на колко хопа е далеч подателя, а това може да се променя в зависимост от маршрутизирането.

Предлага се скритата информация да се представя посредством ниски и високи стойности на TTL, като ниските стойности се на TTL кодират 0, а високите 1. Ниските и високите стойности на TTL са две конкретни стойности избрани на база на анализ на явния поток. За високи стойности на TTL се разбират или първоначалните или прихванатите като обичайни за комуникацията. Ниските стойности са високите минус едно. Декрементирането на TTL по подразбиране елиминира риска пакетите да останат в примка на маршрутизирането, а и вероятността пакетите да достигнат своя получател е много висока. Традиционните операционни системи използват начални стойности на TTL най-малко 64, като броя на хоповете между два хоста в Internet обикновено е по-малък от 32.

Получателят наблюдава поток с пакети с две различни стойности на TTL и декодира пакетите с по-висока стойност като 1-бит и пакети с по-ниска като 0. Преди получателят да започне декодирането той се нуждае от двете различни стойности.

Поради тази причина подателя не следва да изпрати дълги последователности само от нула или единица.

При анализа на потоците от пакети между изпращачите и получателите се наблюдава малка вариация на “обикновената” стойност на TTL, но все пак присъства в потоците. Това означава, че за предаване на скрито съобщение между изпращач и получател може да се очаква канал без шум, т.е. с малки отклонения от “обичайните” стойности за TTL. Малките отклонения могат да се дължат на промени в пътя на пакетите, в следствие маршрутизирането. В този случай приемника ще декодира няколко бита некоректно, но след адаптиране към новата ситуация ще установи нови стойности на ниски и високи стойности на TTL.

Друг въпрос е загубата на пакети и пренареждане. Известно е, че TCP предоставя надежден трансфер, но от друга страна UDP пакетите могат да издържат на загуби на пакети и пренареждане. За да се осигури надеждно предаване могат да се използват добре известни техники като кодове за корекция на грешки, сегментиране и препредаване.

Без възникнали грешки капацитета на скритият канал е един бит на пакет, предаден в явния канал. Със скорост от стотици пакети за секунда, скоростта на предаване на скритият канал е стотици бита за секунда в рамките на един явен канал. Няколко явни потоци могат да се използват паралелно за увеличаване на капацитета.

В мрежовата стеганография, както и при компютърната, е важно да се сравняват отделните стегометоди по тяхната ефективност, т.е. какво количество данни може да се предава с една протоколна единица. Оценката на скрити канали в зависимост от тяхното действие може да се извършва чрез броя на скритите битове в една протоколна единица, или чрез броя PDU за бит/байт за „пространствените” канали и броят битове за секунда или броя на секундите за предаване на бит/байт за „времевите” канали. Скритите канали може да се характеризират още с техния механизъм за синхронизиране (има или няма), възможностите за мултиплексиране на скритите потоци от данни или за разликите между каналите за управление и каналите за данни [1].

В мрежовата стеганография трябва да се използват поне два параметъра на качеството на скритите канали – правоподобност и устойчивост. Правоподобността (аналогично на незабележимостта в компютърната стеганография) означава, че скритият канал трябва да бъде невидим както за компютърните системи, така и за потребителите им. Използването на скрит канал не трябва да оказва влияние на нормалната работа на носещия протокол и също да не предизвиква очевидни аномалии на качествата на носителя в приемащата мрежа.

Устойчивостта означава надеждност на скрития канал. Той трябва да има средства за откриване и коригиране на грешки, които да се справят с проблемите на латентността и задръстванията. Надеждността не трябва да зависи от последователността, маршрута и времето за доставката на пакетите (протоколните единици) [1].

Естествено е да се вземат мерки и за защита от използването на мрежовите протоколи от инсайдери за предаване на чувствителна информация.

Много от техниките, прилагащи се в IP хедъра за стеганографско предаване могат да бъдат елиминирани чрез прилагане на стандарти за стойностите в заглавните полета и уплътненията, чрез пренаписване на тези полета.

На практика обаче, ограничените възможности за обработка на активен надзирател могат да попречат на тяхното пълно премахване. За да се премахне скритият

канал с използване на TTL, надзирателят трябва да зададе една и съща стойност за всички пакети. Тази еднаква стойност може да бъде най-малката, която се наблюдава в потока. Тъй като надзирателят не винаги може да бъде „близо" до изпращача пълно манипулиране на стойността за целия поток не може да бъде извършено, като по този начин скритият канал не може да се елиминира напълно, но може да влоши капацитета поради добавянето на шум.

Част от най- общите мерки срещу скритите канали, които се формират на ниво TCP/IP са:

- използване на средства за блокиране на IP - спуфинга;
- използване на мрежови анализатори, които са в състояние да открият незавършени или провалени TCP съединения;
- рутиране на целия TCP трафик през прокси устройство, което да установи TCP съединение до получателя от източника, но от собствен доверен генератор на реда на предаване на пакетите;
- създаване на база от еталони за TCP трафик и наблюдаване на наличието на аномалии при предаването.

В [7] е предложен интересен вариант на скрито предаване на информация на ниво TCP/IP, който може да преодолее предложените защитни подходи. Той подлежи на експериментална проверка в бъдеща разработка.

Способите за реализация на скрити канали за предаване на данни чрез мрежова стеганография на ниво мрежов слой на модела OSI продължават да се развиват. Тяхното детайлно познаване ще подпомогне защитата от използването им за неправомерен достъп до лични данни извън зоните за тяхната обработка.

Литература:

1. Smeets, M. and M. Koot. Covert Channels. Research Report for RP1, University of Amsterdam, 2006.[онлайн]. [прегледан 15.o5.2013]. http://www.findthatpdf. com/ search-117858924-hPDF/download-documents-covert-channels-research-report.pdf.htm

2. T. Handel,T. and M. Sandford. Hiding data in the OSI network model. In: Proceedings of the First International Workshop on Information Hiding, p. 23–38, 1996.

3. Wolf,M. Covert Channels in LAN Protocols. In: Proceedings of the Workshop on Local Area Network Security (LANSEC), pp. 91–101, 1989.

4. J. Postel,J. Internet Protocol, RFC 0791, IETF, Sept. 1981. http://www.ietf. org/rfc / rfc0791.txt.

5. Ahsan,K. and D. Kundur. Practical data hiding in TCP/IP. In:Proceedings ACM Workshop on Multimedia Security, December 2002.

6. Postel,J. Transmission Control Protocol. RFC 0793. IETF, Sept. 1981. [онлайн] . [прегледан 11.05.2013].http://www.ietf.org/rfc/rfc0793.txt.

7. Алексеев, А. и В. Орлов. Скрытая передача информации в сегментах TCP. В: Стеганографические и криптографические методы защиты информации (Учебное пособие). Самара, ИУНЛ ПГУТИ , 2010 . 330 с. ISBN 978-5-904029-12-8.

СРАВНИТЕЛЕН АНАЛИЗ НА ЗЛОНАМЕРЕНИ УЕББАЗИРАНИ АТАКИ

Жанета Николова Ташева*, Петър Красенов Боянов**

**Национален Военен Университет "В. Левски", Факултет „Артилерия, ПВО и КИС", ул. „Карел Шкорпил" 1 , 9700 Шумен, България, e-mail: zh.tasheva@mail.bg*
***ШУ „Епископ К. Преславски", Факултет по технически науки, ул."Университетска" 115, 9700 Шумен, България, e-mail: peshoaikido@abv.bg*

A COMPARATIVE ANALYSIS OF MALICIOUS WEB-BASED ATTACKS

ZHANETA NIKOLOVA TASHEVA, PETAR KRASENOV BOYANOV

ABSTRACT: *The web-based attacks cause some damages to the computer and network resources. The most dangerous web-based attacks are XSS, SQL Injection and Parameter/Form Tampering attacks that are totally illustrated and explained in this paper. In addition different examples of these attacks are made and some security mechanisms for several web-based attacks are presented.*

KEY WORDS: *XSS, CSS, SQL Injection, Parameter Tampering, Security, Vulnerability.*

1. Въведение

Повечето уеб приложения осигуряват и предоставят интерфейс между крайните потребители и уеб сървърите. Това е осъществено чрез множество от уеб страници, които са генерирани на уеб сървъра или съдържат в себе си скрипт, който трябва да бъде изпълнен динамично в уеб браузъра на крайния потребител. В практиката повечето големи корпорации и организации използват Web 2.0 [5] технологии с цел подобряване на производителността на своите бизнес процеси и услуги. За съжаление, тези нови уеб технологии са изключително уязвими към различни злонамерени кибератаки [1], [2], [3], [5], [7], [8], [10], [11], [12], [13], [16].

В редица предишни научни трудове са показани различни методологии и таксономии на уеб-базирани атаки с цел изясняване на действието на злонамерената атака. Целта на този доклад е да се направи сравнителен анализ на най-актуалните злонамерени уеб-базирани атаки и заедно с това да предостави определени мерки за защита от злонамерени уеб-приложения [3], [5], [7], [9], [14], [16], [17].

Този доклад е структуриран по следния начин. В раздел 2 са представени и сравнени предишни научни разработки и решения на уеб-базирани атаки. В раздел 3 е илюстрирана методологията на най-злонамерените уеббазирани атаки. Резултатите от изследването са показани в раздел 4. Изводите и бъдещата работа са представени в раздел 5.

2. Предишни научни разработки и решения на уеббазирани атаки

Различни начини и етапи, с които крайния потребител бива компрометиран и атакуван от злонамерен софтуер са изяснени от Eshete [3]. Етапите на кибератаката са:

1) Посещение на злонамерената, компрометирана уеб-страница.

2) Зареждане на отдалечена страница.
3) Допълнително пренасочване на страницата.
4) Навлизане в Exploit (внедряване на злонамерен софтуерен код) сървър и прилагане на ”експлойт”.
5) Пренасочване към сървър за злонамерен софтуер с цел автоматично изтегляне и инсталиране на злонамерения софтуер в устройството на крайния потребител.

Процесът на инжектиране на SQL атаката е показан от Amitab [1]. По време на този процес атакуващият имплементира злонамерена SQL заявка, с която кибер престъпникът може после да заобиколни контрола за автентификацията, като по този начин може да копира, модифицира или изтрие важна конфиденциална информация. Атаката Cross-Site Scripting (XSS) е описана от Shalini и Usha [17], като е представено и собствено решение за защита от тази уеб-базирана атака. Сравнение на различните методи за събиране на дигитални доказателства с цел разследване на дадената уеббазирана атака са направени от Parate и Nirkhi [10]. Различните начини за откриване и защита от уебатаки чрез използването на специализирани софтуерни филтри са илюстрирани от Royal и Walia [15]. Различни техники за ранно откриване на уеб-базирани атаки и различни скриптове за защита от тях са показани от Klein [8]. Някои политики на сигурност за защита от неоторизиран достъп до мрежовите ресурси са имплементирани от Purdila и Terzis [13]. Направено е и описание на начина на действие на виртуалната машина и пясъчната кутия (sandbox) с цел избягване на нежелани кибератаки. Четири широко разпространени аспекта на уеббазираните атаки, като сигурност в уебсървъра, съдържанието на потребителя, рекламирането и hird-party приспособления, са разгледани от Provos, McNamee, Mavrommatis, Wang и Modadugu [12].

3. Злонамерени уеббазирани атаки

В практиката са известни следните видове злонамерени уеб-базирани атаки:

- SQL Injection [1], [5], [8], [9].
- Cross Site Scripting (XSS или CSS) [1], [4], [6], [17];
- Invalidated Input [11], [12], [13], [14].
- Parameter/Form Tampering [2], [4], [8], [9], [13].
- Directory Traversal [1], [5], [8], [9], [10], [11], [12].
- Security Misconfiguration [3], [4], [6], [9], [11].
- Injection Flaws [12], [13], [14].
- Command Injection [10]-[15].
- File Injection [8], [9] - [14].
- Information Leakage [1], [13], [14].
- Cookie Poisoning [2], [3], [4], [5], [7].
- Denial of Service (DoS) [1], [7] - [9].
- Buffer overflow [9], [10], [11].
- Malicious File Execution [8], [9], [13].
- Authentication Hijacking and Management [1], [2], [5], [7], [9].
- Broken Account Management [1], [5], [9], [11], [12], [13].

Кибератаките, които причиняват най-големи щети на компютърните и мрежовите ресурси, са Cross Site Scripting, SQL Injection, Parameter Tampering, Cookie Poisoning,

Database server attacks, Web Server attacks, Buffer Overflow [1], [4]. [5], [8], [9], [11], [14], [15], [16], [17]. Затова по-надолу са пояснени някои от тези уеб-базирани атаки.

Фалшифициране на параметъра/формуляра (Parameter/Form Tampering) е вид уеб-базирана атака, която има възможност да подправи параметрите, които се обменят между крайния потребител и сървърната част, с цел да се променят потребителските данни или друга конфиденциални информация. На фиг. 1 е показана имплементация на този вид атака като компрометираните нови стойности са заградени в червен цвят. По този начин, ако, примерно, искате да си прегледате състоянието в сметката, може вместо това да изтриете друга важна информация [1], [5], [6], [9], [11], [12], [13],[14], [15], [16].

Фиг. 1. Атака с фалшифициране на параметъра

SQL Injection атаките използват множество от злонамерени SQL заявки с цел директно манипулиране на базата от данни. За да осъществи достъп до базата от данни, атакуващият използва уязвими уеб-приложения, с които да може да преодолее защитните механизми и по този начин да получи пълен и директен достъп до важна конфиденциална информация. Щетите, които причиняват SQL Injection атаките, са [1], [3], [4], [7], [8], [9], [11], [12], [13], [14], [17]:

- Изтриване или разрушаване на важна конфиденциална информация.
- Фалшифициране на различните привилегии на достъп до базата от данни.
- Модифициране на записите в базата от данни.
- Подправяне на самоличността на потребителя.

На фиг. 2 е показана проста SQL Injection атака. На езика на SQL, тази SQL Injection заявка представлява следният програмен фрагмент:

Select Count (*) From Hosts Where UserName='Ivan' or 1=1 --' AND Password='1234567890'. С тази проста заявка се инжектира SQL Injection атаката и атакуващият придобива достъп до ресурсите в базата от данни [1], [2], [3], [5], [13].

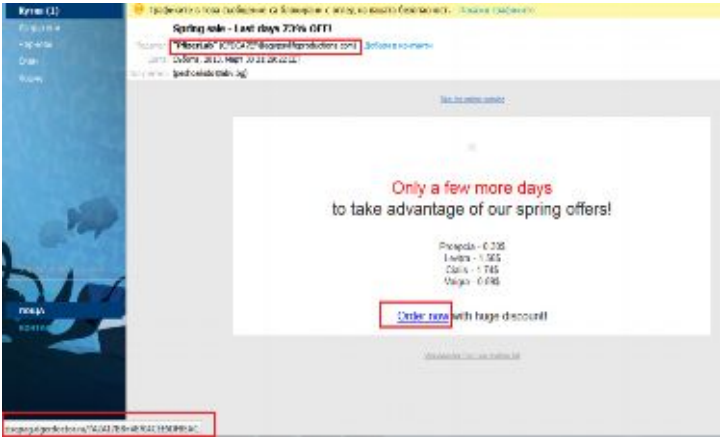
Фиг. 2. SQL Injection атака

Атаките на скриптове в кръстосани сайтове (Cross-Site Scripting - "CSS" или "XSS") използват основно уязвимости и слабости в динамично генерираните уебстраници. Благодарение на тези слабости кибер престъпниците "инжектират" злонамерен потребителски скрипт в дадена уеб-страница с цел другите потребители да отворят тази уеб-страница и да се заразят от нея [17].

В практиката основно се използват шест подтипа на тази атака. Тези подтипове са [17]:

- **Атака на скриптове в кръстосани сайтове чрез електронна поща;**
- **Атака на скриптове в кръстосани сайтове чрез откраднване на потребителските "бисквитки";**
- **Атака на скриптове в кръстосани сайтове чрез изпращане на неоторизирана заявка;**
- **Атака на скриптове в кръстосани сайтове чрез публикуване в блогове;**
- **Атака на скриптове в кръстосани сайтове чрез полета от коментари;**
- **Атака на скриптове в кръстосани сайтове чрез натискане на подправени уеб-бутони.**

На фиг. 3 е показано приложение на подтипа - **атака на скриптове в кръстосани сайтове чрез електронна поща (Cross-Site Scripting Attack via E-mail).** Единствената стъпка, която трябва да се направи, е да се натисне върху текста „Order now" и по този начин потребителят става жертва на XSS атаката. За предпазване, потребителят е необходимо първо да обърне внимание на електронната поща на подателя, след това да разгледа адреса на линка и чак тогава, ако прецени, да натисне съответния линк**.**



Фиг. 3. Атака на скриптове в кръстосани сайтове чрез електронна поща (Cross-Site Scripting Attack via E-mail)

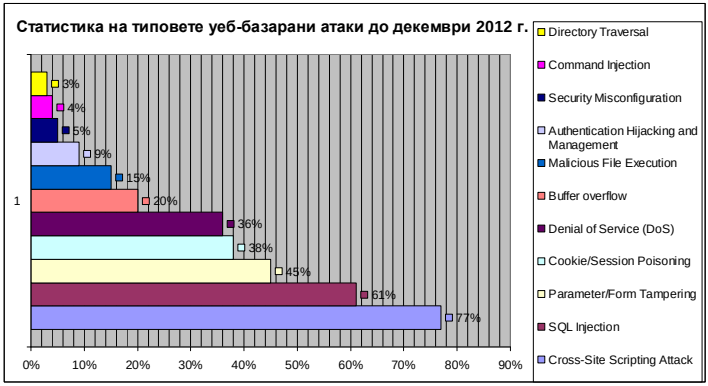
На фиг. 4 е показана атака на скриптове в кръстосани сайтове чрез натискане на подправени уеб-бутони. От фигурата се разбира, че няма разлика дали ще се натисне бутона „**Continue**" или се избере текста "**Click here to Continue for free**". Това е направено с цел да се излъжат обикновените потребители и като резултат е

възможно да претърпят сериозни щети със своите компютърни и мрежови ресурси след натискането на тези линкове.

Фиг. 4. Атака на скриптове в кръстосани сайтове чрез натискане на подправени уеббутони

4. Резултати от изследването

На фиг. 5 е обобщена статистиката на най-злонамерените и разпространени уеб-базирани атаки до декември 2012 г. [3], [5], [7]. От получените резултати се вижда, че атаките, които причиняват най-значителни щети на големите компании и крайните потребители, са Cross Site Scripting (XSS или CSS), Parameter/Form Tampering, SQL Injection и Cookie/Session Poisoning и DoS.



Фиг. 5. Обща статистика на най-злонамерените и разпространени уеб-базирани атаки до декември 2012 г.

В практиката съществуват различни методи за защита от отделните уеб-базирани атаки. За защита от SQL Injection атака е желателно да се използват следните методи [1], [4], [5], [7], [8], [9], [13], [15], [17]:

- разделяне уеб сървъра и сървъра с базата от данни на различни места;
- следене на трафика в базата от данни чрез технологиите IDS и IPS;
- ограничаване на входната потребителска дължина при автентификация в базата от данни;
- създаване на модифицирани съобщения за грешка и др.

За защита от XSS атака е желателно да се използват следните методи [17]:

- кодиране на входните и изходните данни, както и филтрация на входните мета символи;
- прилагане и използване на уеб-базирана защитна стена с цел предотвратяване изпълнението на злонамерен код;
- не винаги е необходимо да се има доверие на протокола HTTPS и др.

5. Изводи и бъдещи задачи

С развитие на новите технологии киберпрестъпниците са успели да усъвършенстват своите атаки с цел неоторизиран достъп до различни компютърни и мрежови ресурси. Уеббазираните атаки причиняват огромни щети на различни компании, корпорации и крайни потребители, като годишно общата загуба се равнява на 500 милиарда долара [3], [5], [7]. Всички системни администратори, както и уебразработчици трябва да изграждат стабилни защитни механизми от всякакви злонамерени уеб-базирани атаки. Бъдещата ни работа ще бъде свързана с изграждане на уеб-базирана защитна стена с цел филтриране на входно-изходния трафик на крайния потребител.

Литература:

[1] Amitab k., “Comparison of SQL injection detection techniques which uses chi-square test”, “International journal of engineering science”, 2011.

[2] Brunner M., "Integrated Honeypot Based Malware Collection and Analysis.", Der Fernuniversit, at in Hagen, Fakultät für Mathematik und Informatik, 2012.

[3] Crist J., “Web based attacks”, SANS Institute Infosec Reading Room, 2007

[4] Eshete B., “Effective Analysis, Characterization, and Detection of Malicious Web Pages”, Fondazione Bruno Kessler, Trento, Italy, 2013.

[5] Fossi M., Gerry E., Kevin H., Eric J., Trevor M., Téo A., Joseph Blackbird et al. "Symantec Internet security threat report: Trends for 2010'." Volume 16, Published April 2011.

[6] Frankel M. A., “Web 2.0 Vulnerabilities”, Doctoral dissertation, John Jay College of Criminal Justice of the City University of New York , 2008

[7] Global Threat Trends, ESET, January 2013.

[8] Klein D., “Defending against the wily surfer-web-based attacks and defenses”. In Proceedings of the USENIX Workshop on Intrusion Detection and Network Monitoring, Santa Clara, California, USA, April 9–12, 1999.

[9] Likaris P., & Jung E., “Leveraging Google Safe Browsing to Characterize Web-based Attacks”, Dept. of Computer Science the University of Iowa Iowa City, IA 52242, 2009.

[10] Parate M. S., & Nirkhi M. S., „A Review of Network Forensics Techniques for the Analysis of Web Based Attack”, International Journal of Advanced Computer Research, Volume-2 Number-4 Issue-6 December-2012.

[11] Park J., & Noh B., „Web Attack Detection: Classifying Parameter Information according to Dynamic Web page”, International Journal of Web Services Practices, 2(1-2), 68-74, 2006.

[12] Provos N., McNamee D., Mavrommatis P., Wang K., & Modadugu N., “The ghost in the browser analysis of web-based malware”, In Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets (pp. 4-4), 2007.

[13] Purdila O., & Terzis A., "A Dynamic Browser Containment Environment for Countering Web-based Malware", Department of Computer Science, Politehnica University of Bucharest, 2009.
[14] Raza, M., Iqbal, M., Sharif, M., & Haider, W, „A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences Journal, 19(4), 439-444, 2012.
[15] Royal m. R., & Walia d. P. S., „Detecting and preventing web attacks by filters", International Journal of Enterprise Computing and Business, 2, 2230-8849, 2012.
[16] Tang S., "Towards Secure Web Browsing", (Doctoral dissertation, University of Illinois), 2011.
[17] Shalini S., & Usha S., „Prevention of Cross-Site Scripting Attacks (XSS) On Web Applications In the Client Side", International Journal of Computer Science, Vol. 8, Issue 4, No 1, July 2011.

СРАВНИТЕЛЕН АНАЛИЗ НА УСТОЙЧИВОСТТА В НЯКОИ СТЕГАНОГРАФСКИ АЛГОРИТМИ

Веселка Т. Стоянова

Национален военен университет "В. Левски", Факултет "Артилерия, ПВО и КИС", катедра „Комуникационна и компютърна техника"
veselka_tr@abv.bg

A COMPARATIVE ANALYSIS OF RESISTENCE OF SOME STEGANOS ALGORITHMS

Veselka T. Stoyanova

veselka_tr@abv.bg,

National Military University, Faculty of Artillery, AAD and KIS, 1 Karel Shkorpil Str., 9700 Shumen, Bulgaria

Abstract*: In this paper a comparative analysis of resistance of modern steganos algorithms to various attacks are given, the main principles of construction of steganographic systems of information introduction into the spatial area and the area of transformation are considered. The criteria of estimation of resistance of steganos algorithms are determined.*

KEY WORDS: *digital steganography, steganos algorithums, LSB, cryptography*

Динамичните промени в нашия живот и в областта на технологиите оказват съществено влияние върху непрекъснато развитие на комуникациите и нараства-

щото желание на обществото за повече нововъведения в информационните технологии. На дневен ред излиза необходимостта от сигурна защита и надеждно управление при обмена данни.

Актуален проблем е възможността да се предава конфиденциална или защитена информация, която да не бъде променяна по време на трансфера ú. Съществува необходимост от защитена комуникация, като потребителите на световната мрежа наред с криптографските средства за защита на предаваната информация използват и стеганографски подходи. За да скрият самия факт за осъществяването на обмен на данни по комуникационния канал, участниците в него използват възможностите на известните стеганографски методи ,като предпазват информацията си от увреждане от атакуващи програми или неоторизирани потребители.

За да може да бъде направен избор на алгоритъм за стеганография за определено приложение е необходимо ясно да се разграничат плюсовете и минусите на всеки един от тях. Основен фактор за това е определянето на конкретни показатели, по които да се оценяват алгоритмите.

Критерии за избор на метод за скриване на информация в изображения са:

- незабележимост;
- устойчивост по отношение на опитите за премахване на скритата информация;
- устойчивост на модификации;
- възможност за вграждане на относителен обем информация;
- секретност.

На български език има ограничен кръг публикации, в които авторите използват термини, повлияни от източниците, които авторите са използвали в изследванията си[2].

Целта на настоящата работа е да сравни някой от популярните стеганографските алгоритми по един от горните критерии, а именно устойчивост на модификации и атаки.

Според някои специалисти основно изискване към стегосистемата е устойчивост срещу активни и пасивни противници. Устойчивост означава съобщението да бъде устойчиво към деформации в процеса на предаване, даже и след компресиране [1]. Друго тълкуване за устойчивост на стеганографски алгоритъм е вероятността за успешно възстановяване на скритото съобщение след въздействие върху обекта носител като е реализирана някакъв вид атака.

Устойчивостта на модификации при реалната комуникация се реализира като съществуват външни фактори, които оказват влияние върху предаваните данни. Злонамерени страни или случайни шумове могат да променят изпращаните файлове и така скритото съобщение да се загуби.

В нашето съвремие най-разпространеният метод в стеганографията се явява LSB-метода, т.е. метод за замяната на най-младшия значещ бит. Предимствата на подхода са простота при неговата реализация и голям размер на данните за прикриване (голям размер на вместимостта) до 37,5 % от размера на носителя. Този метод има и сериозен недостатък, а именно при побитовото разглеждане на изображението лесно може да се установи факта за наличие на скрито съобщение.

В резултат на анализа на стотици изображения, направено от авторите [17], става ясно, че при тях много често се срещат дълги серии от еднакви битове и практически, кое и да е изображение съдържа серии от минимум 14 еднакви бито-

ве. В случай, че в най-младшия бит на изображението се вмъкне информация, тази закономерност се нарушава.

Метод за вмъкване на скритите съобщения основаващ се на промяната на цвета на пикселите в зависимост от тяхната яркост предлагат M.Kitter, F. Jordan, F.Bossen [3]. Те предлагат вграждането на съобщението да се извършва в изображения с RGB кодиране. Вграждането се изпълнява в канала на синия цвят, понеже човешкото зрение е най-малко чувствително към него. Извличането на бита от получателя се осъществява без наличието при него на изходното изображение, т.е. слепешката. Това се получава като се предсказва стойността на изходния, немодифициран пиксел на базата на неговите съседни. Установено е, че алгоритъмът е устойчив на много от известните атаки: нискочестотна филтрация на изображението, неговата компресия е в съответствие с алгоритъма на JPEG.

Предимството на този метод е, че изменението стойността на цвета на всеки пиксел зависи от неговата яркост, затова в този случай е затруднено използването на статистическия стегоанализ. Недостатъка му е, че в процеса на възстановяване на скритото съобщение при неправилна оценка на изходната стойност на немодифицирания пиксел, при предсказването му на база съседите пиксели, може да се възстанови с грешка и предаваното съобщение също да бъде объркано.

W. Bender, D.Gruhl, N.Morimoto, A.Lu [4] предлагат алгоритъм, основан на копирането на блокове от случайно избрани текстурни области в друга имаща сходни статистически характеристики. Това води до появата в изображението на напълно еднакви блокове. Те могат да бъдат намерени по следния начин:

1. Анализ на автокорелационната функция на стегоизображението и местоположението на нейните пикове.
2. Промяна на изображението в съответствие с тези пикове и изчисляване на изображението от неговите променени копия.
3. Разликата в местоположението на копираните блокове трябва да е близка до нулата. Затова може да се избере праг и по-малки по абсолютна стойност от този праг величини се приемат за търсените блокове.

Така както копията на блоковете са единични, то тяхното изменение ще е еднакво при преобразованието на цялото изображение. Ако се направи размера на блоковете достатъчно голям, алгоритъмът ще бъде устойчив по отношение към болшинството от негеометрични изкривявания. При експериментите е установена устойчивост на алгоритъма към филтрации, компресия, ротацията (завъртането) на изображението.

Друг популярен метод за вграждането на съобщения, е използването на различните особености на форматите на данните, като използващите компресирането със загубата на данни (напр. JPEG). Този метод (за разлика от LSB) е по устойчив към геометрични преобразования и откритите канали за предаване, тъй като има възможност да варира в широк диапазон качеството на компресираното изображение, в следствие на което е не възможно да се определи произхода на изкривяванията.

В [18] се разглежда метод за вмъкване на цифров воден знак в графичен файл, компресиране с алгоритъма на JPEG с използването на ефекта на пространственото маскиране. Предложения алгоритъм работи с областта на преобразованията и може да се прилага в режим на реално време (за обработката на 24 битови изображения с размер 512x512 пиксела).

За постигане на бързодействие на алгоритъма [18] авторите препоръчват да не се използват многото операции свързани с JPEG компресията, такива като право и обратно дискретно косинусово преобразование (DCT) или квантуване на коефициентите.

Алгоритмите за скриване на данните в областта на преобразованията са описани в [5-8], а за вълновите преобразования в [9-16]. За първи път DCT за скриване на информацията е описана в [5]. DCT се прилага към цялото изображение. Обикновено стего носителя (cover image) се разделят на блокове с размер 8x8 пиксела. Дискретно косинусовото преобразование се прилага за всеки блок и за резултата се получава матрица от коефициентите на DCT също с размерност 8x8. Алгоритмите за скриване на данни в пространствената област вмъкват и цифров воден знак (ЦВЗ) в оригиналното изображение [4,19,20]. Предимство се явява, че за вмъкването на цифров воден знак в изображенията няма необходимост да се изпълняват изчисления на обемистите линейни преобразования. Цифровите водни знаци се вмъкват за сметка на манипулацията на яркостта или цветовите компоненти.

В табл. 1 са представени в табличен вид предимствата и недостатъците на методите, които разглеждам в тази статия получени от анализа на съответната литература. Всеки метод може да бива описан в съответните алгоритми, в които се прилага като в световната практика са налице проекти, които подобряват даден показател, а в същото време друг бива неглижиран и има нужда от доработване и усъвършенстване.

Таблица 1

Метод	Предимство	Недостатък
LSB	Простота при реализация и относително голям размер на данните за прикриване	Лесно установяване на скритото съобщение, заради побитовото представяне.
M.Kitter, F. Jordan, F.Bossen	Изменението стойността на цвета на всеки пиксел зависи от неговата яркост, затова в този случай е затруднено използването на статистическия стегоанализ	При възстановяване на съобщението има вероятност да се възстанови с грешка и предаваното съобщение да бъде объркано поради неправилна оценка на немодифицирания пиксел
W. Bender, D.Gruhl, N.Morimoto, A.Lu	Копиране на блокове от случайно избрани текстурни области в други имащ сходни. Това води до появата в изображението на напълно еднакви блокове	Засичане чрез: Анализ на автокорелационната функция, промяна на изображението в съответствие с пиковете и
Метод използващ на форматите на данните	Устойчив на геометрични преобразования	Невъзможност определянето произхода на изкривяванията

Като се има предвид това, че има още много на брой методи и съответните алгоритми за изследване, таблицата може да бъде доразвита и обогатена с анализа на параметрите им.

Заключение:

Анализът на устойчивостта на стеганографските алгоритми показва, че всеки един от тях има недостатъци. Именно затова създаването на устойчив алгоритъм с достатъчна степен на стабилност към различните преобразования и средства за противопоставяне на статистическия и зрителния стегоанализ е от голямо значение. LSB е сравнително неустойчив метод, въпреки възможността за вмъкване на значителен обем от данни, докато DCT е със средна устойчив. Идеалният стеганографски алгоритъм би имал голяма незабележимост, голям обем на вграждане данни, независимост от файловия формат и съответно неподозрителен обем, отлична устойчивост на стегоанализ и модификации

Литература

[1] Станев, С., Галяев, В. Семантична еквивалентност на основните термини на компютърната стеганология в българските, английските и руските научни публикации. Международна научна конференция MATTEX2012, Шумен 2012. (под печат).

[2] Ташева А., Ж.Ташева, Система за скриване на конфиденциална информация чрез комбинирано използване на криптографски и стеганографски методи, Трудове на „Хемус-2012", Пловдив , 2012

[3] Kitter M., Jordan F., Bossen F. Digital signature of color image using amplitude modulation, Proceedings of SPIE: Security and Watermarking of Multimedia Content II,1999, B.3667

[4] W. Bender, D.Gruhl, N.Morimoto, A.Lu/ Techniques for Data Hiding, IBM Systems Journal.-1996-B.35

[5] Koch E., Zhao J., Towards Robust and Hidden Image Copyright Labeling, IEEE Workshop on Nonlinear Signal and Image Processing, 1995, P.123-132

[6] Hsu C., Wu J.L., Hidden digital watermarks in images, IEEE Transactions on Image Processing, 1999, P.58-68

[7] Cox I., Kilian J., Leighton T., Shamoon T., Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, 1997, P.1673-1687

[8] Fridrich J., Combining low – frequency and spread spectrum watermarking , Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption, 1998, P.2-12

[9] Barni M., Bartolini F., Capellini V. et al, A DWT-based technique for spatio-frequency masking of digital signatures, Proceedings of the 11 th SPIE Annual Symposium, Electronic Imaging'99, Securityand Watermarking of Multimedia Contents, 1999, B. 3657

[10] Lewis A. S., Knowles G. Image compression using the 2-d wavelet transform, IEEE Transactions on Image Processing,1992, P244-250

[11] C.-S Lu, H.-Y.M. Liao, Oblivious watermarking using generalized Gaussian , Proceedings of the 7th International Conference on Fuzzy Theory and Technology, 2000, P. 260-263.

[12] C.-S Lu, S.-K. Huang, C.-J. Sze, H.-Y.M.Liao, A New Watermarking Technique Multimedia Protection, 2000, CRC Press

[13] C.-S. Lu, H.-Y.M.Liao, S.-K. Huang, C.-J. Sze, Cocktail watermarking on images, 1999, P.333-357

[14] C.-S. Lu, H.-Y.M.Liao, S.-K. Huang, C.-J. Sze, Highly robust image watermarking using complementary modulations, Proceedings of the 2th International Information Security Workshops,1999, P.136-153

[15] A.B. Watson, G.Y. Yang, J.A. Solomon, J. Villasenor, Visibility of wavelet quantization noise, IEEE Transactions on Image Processing, 1997, P.1164-1175

[16] Podilchuk C.I., Zeng W., Digital image watermarking using visual models, Proceedings of the 2th SPIE Human Vision and Electronic Imaging Conference,1997, P100-111.

[17] Алиев А.Т. О применении стеганографического метода LSB к болышим областям монотонной заливки//Вести, Дагестан,Гос.тех.ун-та-2004г.- Т.4 №4 (22).- с.67-72

[18] Luo W., Heileman G.L. A fast and robust labeling methods for JPEG imagen, IEEE Journal on Selected Areas of Communications , 1998g

[19]Langelaar G., Lagendijk R., Biemond J., Robust labeling methods for copy protection of images, proc. Of SPIE Storage and Retrieval for Image and Video Databases V. , 1997, B.3022

[20] Darmstaedter V., Delaigle J.F, Quisquater J., Macq B. , Low cost spatial watermarking, Computers and Graphics,1998, P.417-423.

АСПЕКТИ НА ПОВЕРИТЕЛНОСТТА НА ДАННИТЕ В ОБЛАЧНИЯ КОМПЮТИНГ

Димитър Т. Дойчинов

Национален Военен Университет "В. Левски",
Факултет „Артилерия, ПВО и КИС", ул. „Карел Шкорпил" 1, Шумен,
e-mail: d.doychinov@nvu.bg

ASPECTS OF DATA PRIVACY IN CLOUD COMPUTING

Dimitar T. Doychinov

ABSTRACT: The purpose of this paper is to review same aspects of data privacy when data are in cloud storage.

KEY WORDS: personal data, cloud computing, data storage, privacy.

Преди няколко години хората пренасяха документите си на дискети, след това премина на флаш памети. Облачния компютинг дава възможност за достъп и обработка на информация, съхранявана на отдалечени сървъри, като се използват всякакви устройства с възможност за достъп до Интернет, включително и смартфони.

Модела облачен компютинг променя начина, по който се управлява информацията, особено когато се отнася за обработването на лични данни. Крайните потребители имат достъп до облачни услуги, без да е необходимо да имат на експертни познания на основната технология. Това е ключова характеристика на облачния

компютинг, чието предимство е намаляването на разходите чрез споделяне на компютърни ресурси и дисково пространство. Тези нови характеристики имат пряко въздействие върху IT бюджет и разходите за притежание, но също така водят до проблеми на традиционната сигурност, доверие и механизми за защита на личните данни.

Без информация за физическото местоположение на сървъра или как се обработват личните данни, крайните потребители ползват облачните услуги без никаква информация за извършващите се процеси. Данни в облака са по-лесни за манипулиране, но също е и по-лесно да се изгуби контрола над тях. Например, съхраняването на личните данни на сървър някъде в киберпространството може да представлява сериозна заплаха за личната неприкосновеност. Използването на облачния компютинг повдига редица въпроси на сигурността и неприкосновеността на личния живот. Може ли да се доверим на доставчиците на облачни услуги? Сървърите им достатъчно ли са надеждни? Какво се случва, ако данните се губят? Неприкосновеността на личния живот и обвързването с определен доставчик? Трудно ли ще е преминаването към друг доставчик?

Неприкосновеността на личния живот става все по-важна в света на Интернет. По принцип се приема, че е отдадено дължимо внимание на неприкосновеността на личния живот, което насърчава доверието на потребителите и икономическото развитие. Въпреки това, сигурността, управлението и контрола на лични данни в облачния компютинг представлява огромно предизвикателство за всички заинтересовани страни, включващо както юридически, така и търговски затруднения.

Има няколко стъпки, които могат и трябва да бъдат предприети, за да си гарантираме сигурността на корпоративните данни при преминаването към облачните услуги.

Въпросът за поверителността на данните е на челно място на съзнанието на всички. Всяка организация има правното задължение да гарантира неприкосновеността на личния живот на своите служители и клиенти.

Законите забраняват някои данни да бъдат използвани за друго, освен за целта, за която са били събрани. Вие не можете да събирате данни за здравето на служителите си например и след това да я използвате за да определите на пушачите по-високи застрахователни премии. Също така, не можете да споделяте някои данни с трети страни. В света на облачния компютинг това става много по-трудно, тъй като сега има трета страна, оперираща и и управляваща вашата инфраструктура. По своята същност доставчик на облачни услуги ще има достъп до вашите данни.

Събиране и съхраняване на данни в облака и е подчинено на законовите изисквания на една или повече разпоредби. Трябва да сте сигурни, че доставчикът защитава неприкосновеността на данните по подходящ начин. Както данните, събрани в рамките на вашата организация, така и събраните данни в облака трябва да се използват само за целта, за която първоначално се събират. Ако лицето уточни, че данните се използват само за една цел, това му желание трябва да бъде спазено.

Споразуменията за поверителност често посочват, че хората имат достъп до своите данни и те могат да бъдат изтривани или променяни. Ако данните са в облака, изискванията за поверителност все още се прилагат и предприятието трябва да осигури тази възможност в рамките на същия срок, както ако данните се съхраняваха на място. Ако достъпа до данните може да се осъществи само от персонала

на доставчика на облачни услуги, трябва да сте уверени, че те могат да изпълнят тази задача при необходимост.

При сключването на типов договор, вие ще сте бъдете ограничени до това, което доставчикът на облачни услуги е посочил като условия. Дори и със специализиран договор, доставчикът може да се опита да се ограничи контрола над данните, за да се гарантира на своите клиенти единен подход. Това намалява разходите на доставчика, както и необходимостта да има специализиран персонал под ръка. Ако е необходим пълен контрол над данните, това трябва да е упоменато изрично в договора, за да се бъдещи проблеми с доставчика на облачни услуги.

Има редица доставчици на облачни услуги, които се специализират в различни пазари и приспособят своите услуги за тях. Това вероятно ще става по-често срещано явление в предстоящите години. Например, доставчиците на облачни услуги, които предлагат услуги в областта на здравеопазването ще бъдат обвързани от съответните разпоредби.

Местоположение на данните

Всеки бизнес с уеб присъствие или лица, които публикуват в социалните мрежи записва данни върху един или повече сървъри, които в действителност могат да се намери навсякъде. Независимо дали публикувате лична информация във Facebook, или актуализирате бизнес връзки на LinkedIn, тези данни ще се съхраняват някъде. Тъй като бизнесът върви към използване и възприемане на доставчици на облачни услуги, местонахождението на тези данни ще става все по-важно поради поверителността данните, правни или регулаторни изисквания.

Глобалните компании трябва да гарантират, че всички услуги, разположени в облака се използват в съответствие със законовите и подзаконовите актове в съответното място за служителите, чуждестранни дъщерни дружества или трети страни. Законодателството на отделните страни се различава значително, така че дори и собствените служители на компанията, които ползват услугата, трябва да са наясно със законите, които се отнасят до тях в тяхното местоположение.

Дъщерни дружества в други региони могат да имат малко по-различни закони, за които трябва да се вземат под внимание, дори и ако те са в една и съща област. Някои чуждестранни дъщерни дружества могат да нямат никакви проблеми със споделянето на данни с един регион, но не и с друг. Добавянето на доставчик на облачни услуги към всичко това, усложнява още повече нещата.

Основното място за съхранение на данните и всички резервни места трябва да се знаят, за да се гарантира, че тези закони и разпоредби са спазени. Често резервните места за съхранение на данните трябва да бъдат точно определени.

Законите за защита на данните на страни-членки на Европейския съюз (ЕС), както и други региони, са изключително сложни и имат редица окончателни изисквания. Трансферът на лични данни извън тези региони трябва да се извършва по много специфични начини. Например, ЕС изисква администратора на лични данни да информира хората, че данните им ще бъдат изпратени и обработени в район извън ЕС. Администратора на данни и крайния получател също трябва да имат предварително одобрени от органа по защита на данните договори. Трудността на този процес е в зависимост от региона, които се обработват данните. САЩ и ЕС имат реципрочно споразумение и на за получателя от САЩ е необходимо само сам да сертифицира своите процедури за обработка данни и регистрира в американското министерство на търговията.

Трябва да сте уверени, че всички доставчици на облачни услуги, които използвате и са извън вашата юрисдикция, разполагат с подходящи мерки за сигурност. Това включва техните основно и резервно места за съхранение на данни, както и на всички междинни местоположения, ако данните се прехвърлят между юрисдикции.

С въвеждането на данните си върху сървър на трета страна, независимо дали е доставчик на облачни услуги, или не, вие доверявате данните си на тях. Трябва да сте уверени, че съществува необходимата сигурност за вашите нужди и тя отговаря на всички правни и регулаторни изисквания. Процедурите на доставчикът трябва да съответстват на местните закони в региона, където се намира сървъра. Ако сте сключили договор с фирма, в Съединените щати, но те съхраняват данните на даден сървър в ЕС, най-вероятно ще трябва да спазва законите на ЕС, ако искате да прехвърляте данни в и от системата.

Тези закони могат да бъдат по-обременителни, ако сървърът се хоства в някои региони като Китай, където законите могат да позволяват на местната власт неограничен достъп до данните, независимо от неговата чувствителност. Криптирането на данните може да бъде ограничен (или забранено), ако не може да се гарантира възможността на местните власти да го дешифрират при необходимост.

Пазарът на доставка на облачни услуги се разширява, но все още има само ограничен брой участници, които могат да предложат хостинг на данни и приложения в голям мащаб. Това може да принуди компаниите да възложат някои или всички хостинг услуги на друга компания, вероятно в друг регион. Преди да сключите споразумение, трябва да сте запознати с всички договори с подизпълнители и да извършите съответните проверки за сигурност на тях.

Някои доставчици на облачни услуги неизбежно ще фалират или преустановят работа. Достъпа до вашите данни незабавно се превръща в проблем. В зависимост от това къде се намира сървърът, това може да се наложи да мине през друга юрисдикция, за да получите данните си, а данните могат да бъдат предмет на съвсем различни правила за достъп.

Вторично използване на данни

В зависимост от вида доставчик на облачни услуги, ще трябва да решите дали достъп до вашите данни ще имат доставчикът, или други лица. Използването на данните ви може да се стане без вашето знание поради конфигурационни грешки от страна на доставчика. В зависимост от чувствителността на вашите данни, може да желаете в договора ви да се включи клауза, забраняваща или поне ограничава достъпа на доставчика на облачни услуги до тези данни.

Данните, които съхранявате в облака могат да са конфиденциални или да съдържат лични данни, на които трябва да се осигури защитеността. Доставчикът на облачни услуги вероятно има пълен достъп до тези данни, за да може да поддържа и управлява своите сървъри. Вие трябва да сте сигурни, че с този достъп не се злоупотребява по никакъв начин. Въпреки, че договорът може да ви защитава законово, вие също така ще трябва да сте уверени, че мерките за сигурност от страна на доставчика гарантират откриването на неоторизиран достъп до вашите данни.

Възстановяване след катастрофи

Вие не можете да преувеличите значението на осигуряването на непрекъснатост на дейността ви като предприятие и възстановяването след катастрофи. От гледна точка на възстановяването след катастрофи, трябва да се обмислят няколко възможни сценария: доставчикът на облачни услуги може да фалира или центърът

им за съхранение на данни да стане негоден. Основният проблем при първия сценарий е да си получите данни обратно и преместването на вашите облачните приложения към друг доставчик. Това трябва да се бъдат обмисли, преди разполагането в облак. Вие също така трябва да защити вашите интереси, като си осигурите редовни резервни копия на данните.

Подгответе план за действие при инциденти, когато се преместват данните си в облака и обновявайте този планът регулярно. Пазарните фактори и други обстоятелства се променят доста бързо. Има редица случаи, в които центровете за данни са претърпявали катастрофална прекъсване на работата си, което е довело до загуба или прекъсване на услугите на много уеб сайтове и дейности:

- Пожар в център за данни в Грийн Бей, Уисконсин, през 2009 г. е довело до прекъсване на някои хоствани сайтове за до 10 дни.
- Прекъсване във Фишер Плаза (Сиатъл) през юли 2009 г засегна много сайтове, включително Travel Bing.
- Експлозията в The Plant datacenter в Хюстън през 2008 г. доведе близо 9000 клиенти офлайн за няколко дни.
- Rackspace US Inc. имаше прекъсване в техния център в Далас през 2009 г., който продължи малко по-малко от час.
- 365 Main Datacenter имаше прекъсвания през 2007 г., които се отразиха на Craigslist, Yelp и др.
- Google претърпя прекъсване на захранването в център за съхранение на данни поради грешка при софтуерен ъпгрейд през февруари на 2009 г., което доведе до загуба на пощенската услуга за много клиенти.

В зависимост от нивото на подготвеност, някои от тези събития могат да са просто неудобство или непосредствена заплаха за бизнеса ви. Малките фирми са по-уязвими, поради по-малкият им опит и ресурси. Прекъсването на работата им може сериозно да наруши функционирането на техния бизнес.

Както можете да видите от списъка с инциденти, това не са само физически проблеми, дължащи се на повреди в електричеството или охлаждащите системи провали, но също така и софтуерни грешки, които могат да доведат до прекъсване на работата на центъра за съхранение на данни. Хакерска атака тип „отказ на услуга“ срещу определени уеб сайтове може да засегне и Вашия сайт поради изчерпване на пропускателната способност на канала, ако атакуваният сайт се хоства в същия център за данни.

Нарушения на сигурността

Вашите приложения или данни могат да бъдат компрометирани или нарушени, докато се съхраняват в облака. В такъв случай, ще бъдете уведомени от системите на доставчика на облачни услуги или по друг начин.

Трябва да сте наясно с политика за оповестяване на доставчикът на облачни услуги и да разбирате колко бързо те ще разкрият нарушението. Повечето държави имат законови разпоредби, изискващи собственика на данни да уведоми лицата, ако личните им данни са компрометирани по някакъв начин. Тези закони изискват да сте сигурни, че ще бъдете информиран незабавно за всяко нарушение.

Алтернативно, ако вие откриете пробив във вашите данни, може да се наложи да уведомите доставчикът на облачни услуги, тъй като това би могло да има последици за другите им клиенти. Най-вероятно ще споделяте оборудването с едно или

повече предприятия. В зависимост от степента на нарушение това може да повлияе на някои от тях. Наличието на взаимно договорен план за действие при инцидент ще гарантира, че и двете страни ще могат да смекчат последиците от нарушението.

Литература:

1. Cavoukian, A., & Abrams, S. T. (2010). Privacy by Design: essential for organizational accountability and strong business practices. www.globalprivacy.it/Allegati_Web/57C2B8AA758546A0B76D5668F5CF5E16.pdf
2. ENISA. (2009). Cloud Computing Security Risk Assessment. www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
3. IDC Predictions 2011: Welcome to the New Mainstream. www.idc.com/research/predictions11/downloads/IDCPredictions2011_WelcometotheNewMainstream.pdf
4. V. Winkler, Securing the Cloud, Syngress, 2011.

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ – ПРАВНА РАМКА В ЕВРОПЕЙСКИЯ СЪЮЗ

Христо А. Ангелов

PERSONAL DATA PROTECTION – EU LEGAL FRAMEWORK

Hristo A. Angelov

EU Legal framework - Directive 95/46/EC of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Regulation (EC) No 45/2001 of the EP and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Key words: data protection, EU, directive, regulation, legal framework

В края на българския Закон за защита на личните данни (ЗЗЛД) са споменати релевантните актове на Европейския съюз (ЕС) в областта на защитата на личните данни. Това са на първо място Директива 95/46/ЕО на Европейския парламент (ЕП) и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, както и Регламент 45/2001/ЕО на ЕП и на Съвета от 18 декември 2000 година за защита на физическите лица по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни. Освен това съществуват и няколко свързани с въпроса решения на Европейската комисия (ЕК).

Но освен тези нормативни актове, съществуват и други, които макар и неспоменати в ЗЗЛД имат отношение към проблема за защита на личните данни. Настоящият доклад цели да хвърли повече светлина и върху тези нормативни актове. Това са Директива 2002/58/ЕО на ЕП и на Съвета относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации; Директива 2006/24/ЕО на ЕП и на Съвета за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58; Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси.

Преди да се пристъпи към разглеждането на отделните нормативни актове на ЕС в областта на защитата на личните данни, следва да се направи уточнението за тяхното значение за националното право. Тяхната роля зависи от техния вид. Регламентите имат пряко действие и са директно приложими, без нужда да бъдат

опосредени от национални нормативни актове. Директивите са актове, които „полагат" целите, които трябва да бъдат постигнати, като всяка държава преценява по какъв начин (включително с какъв вътрешен акт) да постигне тези цели.

Директива 95/46/ЕО на Европейския парламент (ЕП) и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (наричана по нататък Директива 95/46 за личните данни) дава основната правна рамка на защитата на личните данни в ЕС. Тя е транспонирана в българския ЗЗЛД. В структурно отношение се състои от 72 съображения за приемането ѝ и 34 члена. В съображенията например се изтъква, че създаването и функционирането на вътрешния пазар неминуемо ще доведе до нужда от трансгранично прехвърляне на лични данни и съответно до риск за неправомерно разкриване на лични данни. Изтъква се също така, че системите за обработка на данни са създадени с цел улесняване на този процес, но следва да се държи сметка за основните права и свободи и по-конкретно правото на личен живот.

Нуждата от действия на общностно ниво може да бъде обяснена с различното ниво на защита на личните данни в различните държави. Така дадена държава, в която личните данни са защитени по един достатъчно сериозен начин може да възрази на искането на друга държава за прехвърляне на данни с аргумента, че в тази друга страна информацията вече няма да бъде така добре защитена и може да стане обект на различни посегателства. За да се избегнат такива ситуации, които ще попречат на изграждането на единен пазар, ЕС си поставя за цел да създаде една правна рамка, която да очертае границите на защита на личните данни. Чрез директивата се дава минимумът защита на данните, която всяка държава трябва да осигури. Целта е уеднаквяване на националните законодателства.

Обработването на звук и картина при едно видео-наблюдение, свързано с опазване на обществената сигурност, отбраната или националната сигурност не попада в обхвата на Директива 95/46 за личните данни. Що се отнася до обработването на звук и картина, извършвано за целите на журналистическата дейност или за нуждите на литературно произведение – тук влизат в колизия принципите за свобода на словото и за защита на личния живот, като се предвиждат изключения от прилагането на Директивата за личните данни.

Приложното поле на Директивата за личните данни е очертано в чл. 3 – настоящата директива се прилага към пълната или частична обработка на лични данни с автоматизирани средства, както и към обработката със средства, които не са автоматизирани, на лични данни, съставляващи част от файлова система, или които са предназначени да съставляват част от файлова система.

Проекция на този текст виждаме в чл. 1 (3) на българския ЗЗЛД, който се прилага за обработването на лични данни с автоматични средства или с неавтоматични средства, когато тези данни съставляват или са предназначени да съставляват част от регистър.

Както стана дума по-горе, директивите са нормативни актове, които само дават насоката, в която държавите членки следва да действат, и целите, които трябва да бъдат постигнати. В такъв смисъл следва да се тълкува и чл. 5 от Директивата за личните данни, съгласно който държавите сами и в границите, дадени от директивата, определят критериите за това дали дадена обработка на лични данни е законна или не. По-нататък в директивата са дадени и конкретни критерии за законосъобразност и допустимост на обработването на личните данни. Тези критерии са

залегнали и в родния ЗЗЛД – съгласие на физическото лице, чиито данни се обработват, изпълнение от администратора на нормативно задължение.

Предаването на лични данни на трети страни (които не са държави членки) също трябва да е съобразено със степента на защита, които тези страни осигуряват по отношение на личните данни. Съответните текстове, транспониращи изискванията на директивата в тази посока, се съдържат в чл. 36а и сл. ЗЗЛД. Предоставянето на лични данни в държава членка на Европейския съюз, както и в друга държава членка на Европейското икономическо пространство, се извършва свободно при спазване на изискванията на този закон. Предоставяне на лични данни в **трета държава** се допуска само ако тя осигурява адекватно ниво на защита на личните данни на своя територия. Преценката на адекватността на нивото на защита на личните данни в трета държава се извършва от Комисията за защита на личните данни, като се вземат предвид всички обстоятелства, свързани с действието или съвкупността от действията по предоставянето на данните, включително характера на данните, целта и продължителността на обработването им, правната им уредба и мерките за сигурност, осигурени в третата държава.

Разпоредбите на Директивата за личните данни намират място в националното законодателство чрез разпоредбите на ЗЗЛД, като не е нужно да се спираме на всяка от тях по отделно. Интерес представлява редът за защита на правата на лицата.

Текстът от Директивата за личните данни, посветен на средствата за правна защита – чл. 22 – по един недостатъчно ясен начин (поне в българския превод) определя формите за защита на физическите лица. В разпоредбата се казва: „Без това да засяга и да е административно средство за правна защита, което може да бъде предвидено, *inter alia*, пред надзорния орган, посочен в член 28, преди сезиране на съдебен орган, държавите членки предвиждат правото на всяко лице на правна защита за всяко нарушение на правата, гарантирани от националното право, приложимо към въпросната обработка."

Българският ЗЗЛД съдържа уредба на въпроса за правната защита на лицата в глава седма, озаглавена Обжалване на действия на администратора на лични данни. В двата члена (чл. 38 и чл. 39 ЗЗЛД) са представени двете форми на защита – защита по административен и по съдебен ред. По административен ред правната закрила се осъществява пред Комисията за защита на личните данни (българският надзорен орган по смисъл на чл. 28 от Директивата за личните данни). При нарушаване на правата му по ЗЗЛД всяко физическо лице има право да сезира Комисията за защита на личните данни в едногодишен срок от узнаване на нарушението, но не по-късно от пет години от извършването му. Комисията се произнася в 30-дневен срок от сезирането с решение, като може да даде задължителни предписания, да определи срок за отстраняване на нарушението или да наложи административно наказание.

Комисията за защита на личните данни изпраща копие от решението си и на физическото лице, като то може да го обжалва по реда на Административнопроцесуалния кодекс в двуседмичен срок от получаването му. Чрез въвеждането на този ред за обжалване се изпълняват изискванията на Директивата за личните данни по отношение на правото на всяко лице на правна защита пред националния надзорен орган. Частта на разпоредбата – „без това да засяга и да е административно средство за правна защита" на практика не се изпълнява, защото обжалването пред Комисията за защита на личните данни е точно административният ред за защита на

правата на лицата. Що се отнася до сезирането на съдебен орган – чл. 39 ЗЗЛД е посветен на съдебния ред за защита.

При нарушаване на правата му по ЗЗЛД всяко физическо лице може да обжалва действия и актове на администратора по съдебен ред пред съответния административен съд или пред Върховния административен съд по общите правила за подсъдност, като то може да иска обезщетение за претърпените от него вреди вследствие на неправомерно обработване на лични данни от страна на администратора.

Може да бъде направен избор между сезиране по административен или по съдебен ред, като ограничение в тази насока е висящо производство пред Комисията – ал. 4 на чл. 39 - физическото лице не може да сезира съда, ако има висящо производство пред комисията за същото нарушение или нейно решение относно същото нарушение е обжалвано и няма влязло в сила решение на съда. По искане на физическото лице комисията удостоверява липсата на висящо производство пред нея по същия спор.

В края на ЗЗЛД се съдържат разпоредбите за санкциите, които се налагат за нарушаване на разпоредбите му. В Директивата за личните данни е предвидено, че държавите членки вземат подходящи мерки, за да гарантират пълното прилагане на разпоредбите на настоящата директива и в частност определят санкциите, които се налагат в случай на нарушаване на разпоредбите й.

Освен Директивата за личните данни следва да бъде разгледан и Регламент 45/2001/ЕО на ЕП и на Съвета от 18 декември 2000 година за защита на физическите лица по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (наричан по-нататък Регламент 45/2001).

В съответствие с него институциите и органите на ЕС следва да защитават основните права и свободи на физическите лица спрямо обработката на лични данни. Същевременно институциите на ЕС не трябва да ограничават или забраняват свободното движение на лични данни помежду си или до получатели, спрямо които се прилага националното право на държавите членки. А както вече стана дума, в националното право е транспонирана **Директива 95/46/ЕО** за личните данни.

Европейски надзорен орган по защита на данните, създаден с Регламент 45/2001, наблюдава и контролира прилагането на разпоредбите на настоящия регламент по отношение на всички операции по обработка на лични данни, извършвани от институция или орган на Общността.

Европейският надзорен орган по защита на данните се назначава с общо съгласие от Европейския парламент и Съвета за срок от пет години въз основа на съставен от Комисията списък след публично отправена покана за представяне на кандидатури. По същата процедура и за същия срок се назначава помощник надзорен орган, който подпомага надзорния орган в изпълнението на неговите задължения и действа като негов заместник, когато надзорният орган отсъства или е възпрепятстван да изпълнява задълженията си.

Става дума за едноличен орган, като лицата измежду които се избира той са лица, чиято „независимост не подлежи на съмнение и за които е признато, че притежават необходимите опит и умения, за да изпълняват функциите на Европейски надзорен орган по защита на данните". Критерий за този избор според Регламент 45/2001 е фактът, че даденото лице е работило или работи в някой от националните

надзорни органи по защита на личните данни (например в българската Комисия за защита на личните данни).

Регламент 45/2001 дава собствена, автономна квалификация на някои от използваните в него понятия. Само пример в тази насока са определенията за контролиращ орган, а именно „институцията или органът на Общността, Генералната дирекция, звеното или всяка друга организационна структура, която самостоятелно или съвместно с други определя целите и средствата за обработка на лични данни", както и за трета страна – „физическо или юридическо лице, обществен орган, агенция или орган, различен от субекта на данни, контролиращия орган, обработващото лице и лицата, които са упълномощени да обработват данните под прекия контрол на контролиращия орган или обработващото лице". „Получател" означава физическо или юридическо лице, публична власт, агенция или друг орган, пред който се разкриват данните, независимо дали той е или не е трета страна. Органите, които могат да получават данни в рамките на конкретно следствие не се считат за получатели.

На практика Регламент 45/2001 не съдържа „нови" разрешения, а разширява приложението на съществуващите изисквания и спрямо обработката на лични данни от институции на ЕС. Нуждата от регламент в тази материя се обяснява със спецификата на отношенията, в които участват институции на Общността.

От изрично неспоменатите в ЗЗЛД релевантни актове на Съюза следва да бъде разгледана Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации).

Съобразно изложеното в съображенията към тази директива интернет преобръща традиционните пазарни структури, като осигурява обща глобална инфраструктура за доставка на широк обхват от електронни комуникационни услуги. Публично достъпните електронни комуникационни услуги чрез Интернет разкриват нови възможности за потребителите, но също нови рискове за техните лични данни и неприкосновеност на личния им живот. По-нататък съображенията продължават с аргумента, че по отношение на публичните комуникационни мрежи, трябва да се изготвят специфични законови, подзаконови и технически разпоредби, за да се защитят основните права и свободи на физическите лица и легитимните интереси на юридическите лица, като се има предвид увеличаващата се способност за автоматизирано съхранение и обработка на данни за абонати и потребители.

Доставчиците на услуги трябва да вземат подходящи мерки, за да гарантират сигурността на техните услуги, ако е необходимо заедно с доставчика на мрежата, и да информират абонатите за всякакви особени рискове от нарушаване на сигурността на мрежата. Такива рискове могат да се получат при електронните комуникационни услуги през открита мрежа, каквато е Интернет или аналогови мобилни телефони. Особено важно е за абонати и потребители на такива услуги да бъдат напълно информирани от техния доставчик на услуга за съществуващите рискове относно сигурността, които са извън обхвата на възможностите за отстраняване от доставчика на услуга. Доставчици на услуги, които предлагат публично достъпни електронни комуникационни услуги чрез Интернет, трябва да информират потребители и абонати за мерките, които те могат да вземат, за да защитят сигурността на техните съобщения, например чрез използване на специални типове софтуер или кодирани технологии.

Целта на Директивата за правото на неприкосновеност на личния живот и електронни комуникации е да хармонизира разпоредбите на държавите членки, необходими за осигуряване на еквивалентно ниво на защита на основни права и свободи – правото на неприкосновеност на личния живот по отношение на обработката на лични данни в електронно-комуникационния сектор и да се осигури свободно движение на такива данни и оборудване за електронни съобщения и услуги в Общността.

Държавите членки гарантират конфиденциалност на съобщенията и свързания трафик на данни през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, чрез националното си законодателство. Поспециално те забраняват **слушане, записване, съхранение и други видове подслушване или наблюдение** на съобщения и свързаните данни за трафика без съгласието на заинтересованите потребители. Разбира се, допустими са изключения, например когато става дума за националната сигурност.

В Директива 2002/58/ЕО също се използват специфични термини – например „данни за местонахождение" - всякакви данни, обработени в електронни комуникационни мрежи, показващи **географското местоположение** на терминалното оборудване **на потребителя** на публично достъпни електронни комуникационни услуги. Засягат се въпроси не само на строго личните данни на потребителя, но и на данни, свързани например с неговото местоположение.

Дадена е дефиниция и на термина „повикване" - връзка, установена посредством публично достъпна телефонна услуга, позволяваща двустранна комуникация в реално време.

Друга директива, регулираща въпроса за защитата на личните данни, е Директива 2006/24/ЕО на ЕП и на Съвета за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58.

Освен че изменя Директивата за правото на неприкосновеност на личния живот и електронни комуникации, Директива 2006/24/ЕО има за цел да хармонизира разпоредбите на държавите членки, свързани със задълженията на доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи по отношение **запазването на някои данни**, които са създадени или обработени от тях, за да се гарантира, **че данните са достъпни за разследването, разкриването и преследването на сериозни престъпления**, както те са определени в националното право на всяка държава членка.

Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, има за цел да осигури високо ниво на защита на основните права и свободи на физическите лица с акцент, поставен върху правото им на неприкосновеност на личния живот във връзка с обработването на лични данни в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси.

Правната рамка на защита на личните данни в ЕС се съдържа в различни нормативни актове – основно в няколко директиви и един регламент. Чрез използването на общностните средства за регулация се постига така нужната хармонизация на законодателствата на отделните държави членки. Така защитата на личните данни е еднакво гарантирана във всяка от тях.

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ

Христо А. Ангелов

PERSONAL DATA PROTECTION AND CYBERCRIMES

Hristo A. Angelov

Abstract: This report addresses the subject in two ways. On the one hand, it aims to cast light on the relationship between cybercrimes and personal data protection. On the other, it explores cyber-security policy. Cybercrimes refers to crimes that involves a computer and a network. This report includes also information about EU-policy in the area of cybercrimes.

Key words: data protection, privacy, cybercrime

Личните данни могат да бъдат обект на различни престъпления, при които се използва компютърна система и връзка с глобалната мрежа. Обект на такива престъпления могат да бъдат не само личните данни, в смисъл на данни на физически лица, но също така и чувствителна информация и данни за дейността на различни юридически лица – например търговски дружества.

Посредством използването на новите технологии може да се стигне и до нерегламентиран достъп до класифицирана информация по смисъла на т. 6 на § 1 от ДР на Закона за защита на класифицираната информация (ЗЗКИ), а именно „разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата ѝ или до загубване на такава информация."

Според същата т. 6 „за нерегламентиран достъп се счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това."

Съгласно чл. 1, ал. 3 от Закона за защита на личните данни (ЗЗЛД), същият се прилага за обработването на данни с **автоматични средства** или с неавтоматични средства, когато тези данни съставляват или са предназначени да съставляват част от регистър. Автоматични средства представляват и компютърните системи, чрез които се обработват лични данни.

Обработване на лични данни е „всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване." - т. 1 от § 1 на ДР на ЗЗЛД

В настоящия доклад са разгледани формите на престъпна дейност, при които се използват компютърни системи и интернет. При тази група престъпления обект на посегателство могат да бъдат и лични данни по смисъла на ЗЗЛД.

Компютърните престъпления – престъпленията при които се използват като средство компютърни системи или имат за обект посегателство върху такива системи, могат да бъдат класифицирани в следните групи[1]:

- компютърни престъпления против неприкосновеността на кореспонденцията и на информацията в електронна форма (чл. 171 и чл. 319д НК);
- компютърни престъпления против икономическите отношения (чл. 319а, чл. 319б, чл. 319в, чл. 216, ал. 3-6, чл. 212а, чл. 246, ал. 3 НК);
- компютърни престъпления против интелектуалната собственост (чл. 172а НК);
- компютърни престъпления, свързани със създаването, предоставянето или разпространението на произведения с незаконно или неморално съдържание (чл. 159 НК);
- други компютърни престъпления (чл. 313, чл. 319г и чл. 319е НК).

От така изброените групи компютърни престъпления ни интересуват тези, при които лични данни или друг тип информация са обект на престъпното посегателство. На първо място могат да се разгледат престъпленията срещу неприкосновеността на кореспонденцията. Съгласно чл. 171 НК, който:

1. отвори, подправи, скрие или унищожи чуждо писмо, телеграма, запечатани книжа пакет или други подобни;

2. вземе чуждо, макар и отворено писмо или телеграма с цел да узнае тяхното съдържание или пък със същата цел предаде другиму чуждо писмо или телеграма;

3. **узнае неадресирано до него съобщение, изпратено по електронен път**, или отклони от адресата му такова съобщение, се наказва с лишаване от свобода до една година или с глоба от сто до триста лева.

При нарушаване на неприкосновеността на кореспонденцията лесно може да бъдат узнати чужди лични данни, включително и когато съобщението е изпратено по електронен път.

Възможно е чуждите лични данни да бъдат придобити и при атакуване на трафик-данни – чл. 171а НК - противозаконното придобиване, разкриване или разпространяване на трафични данни, каквито се събират, обработват, съхраняват или използват съгласно Закона за електронните съобщения, се наказва с лишаване от свобода до три години или пробация.

Новата гл. 9а от Особената част на НК е озаглавена Компютърни престъпления. Въпреки че в повечето от текстовете в тази глава се говори общо за компютърни данни (с малки изключения – вж по-долу анализа на чл. 319д НК), безспорно тези компютърни данни могат да представляват и лични данни, както и класифицирана информация. Затова, говорейки за посегателства срещу компютърни данни изобщо, следва да държим сметка, че обект на тази група престъпления могат да бъдат лични данни или друг тип защитена от закона информация.

В чл. 319а НК се казва, че се наказва този, който „копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова.”. Когато деянието е извършено от две или повече лица при предварително сговаряне, както и при повторност, наказанието е по-тежко.

[1] Дацов, П. Договорите в областта на интелектуалната собственост и компютърните престъпления, сп. Теза, бр. 1, 2011 г., с. 83

Предвидени са и квалифицирани състави, ако деянието е извършено по отношение на информация, представляваща държавна или друга защитена от закон тайна, а също така и ако са настъпили тежки последици.

Копираните лични данни (ако приемем че обект на престъпното посегателство са именно такива данни) могат да бъдат използвани за извършване на други престъпления.

Освен копиране спрямо компютърни данни могат да се извършват и други действия, които при определени обстоятелства са обществеоопасни. Затова държи сметка чл. 319б НК. Съгласно този текст който без разрешение на лицето, което администрира или ползва компютърна система, добави, промени, изтрие или унищожи компютърна програма или компютърни данни, в немаловажни случаи, се наказва с лишаване от свобода до една година или глоба до две хиляди лева. Особена опасност представлява това престъпно посегателство, когато се добавят, променят или изтриват лични данни или класифицирана информация. В някои случаи е възможно унищожената информация да не може да бъде възстановена или нейното възстановяване да коства много средства и усилия.

Квалифициращи обстоятелства са значителните вреди или настъпили други тежки последици, както и специфичната цел на извършителя – имотната облага. По тежко наказуемо е и деянието, ако е извършено по отношение на данни, които се дават по силата на закон, по електронен път или на магнитен, електронен, оптичен или друг носител.

На следващо място следва да бъде споменат чл. 319д НК - който разпространи пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва **разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна**, се наказва с лишаване от свобода до една година. За деяние, извършено с користна цел, или ако с него са причинени значителни вреди или са настъпили други тежки последици, наказанието е лишаване от свобода до три години.

При деяния, квалифицирани по чл. 319д НК виждаме, че посегателството срещу и разкриването на лични данни, както и на информация, представляваща държавна или друга тайна, е въздигнато в елемент от състава на престъплението – в условие за съставомерност на деянието.

Съгласно чл. 319д НК наказва се този който, разпространи пароли и кодове за достъп до компютърна система или до компютърни данни. Дефиниции на понятията се съдържат в чл. 93, т. 21 и т. 22 от НК. "Компютърна система" е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява **автоматична обработка на данни**. "Компютърни данни" е всяко представяне на факти, информация или понятия във форма, поддаваща се на **автоматична обработка**, включително компютърни програми.

Както по-горе беше казано, ЗЗЛД се прилага за данни, обработвани автоматично (включително чрез компютърна система), така и с неавтоматични средства, при условие, че така обработените данни съставляват или са предназначени да съставляват част от регистър.

В чл. 319д НК е поставено и изискването вследствие на разпространението на паролите и кодовете за достъп да е последвало разкриване на лични данни или на информация, представляваща държавна или друга защитена от закон тайна.

Чл. 319г НК касае наказуемостта на въвеждането на компютърен вирус в дадена компютърна система. Съгласно т. 27 на чл. 93 НК "Компютърен вирус" е компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите компютърните системи лица и е предназначена за привеждане на компютърни системи или компютърни мрежи в нежелани от ползващите ги състояния или в осъществяване на нежелани резултати.

Такъв „нежелан резултат" по смисъла на закона може да бъде и „изтичането" на лични данни или друга информация от дадена компютърна система, като това става против волята или по често без знанието на ползващите системата.

В чл. 319г НК се предвижда наказание и за лица, които въведат друга компютърна програма, която е предназначена за нарушаване на дейността на компютърна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква. Тук също неоторизираното узнаване, заличаване, изтриване и копиране на данни може да бъде извършено по отношение на лични данни.

Квалифицирането на дадено деяние може да бъде затруднено поради известното сходство между отделните текстове от гл. Компютърни престъпления. В чл. 319а и 319б НК се говори за копиране и изтриване и други действия, извършени спрямо компютърни данни. В чл. 319г (1) се криминализира въвеждането на компютърен вирус в компютърна система. Във втората алинея на чл. 319г за престъпление се обявява извършеното без необходимо разрешение въвеждане на компютърна програма, чрез която се извършва манипулиране на компютърни данни. Самият компютърен вирус по дефиницията, дадена в закона, също е компютърна програма. На практика едно деяние може да бъде квалифицирано по всеки един от тези текстове. Защото лицето, което осъществява нерегламентиран достъп до компютърна система и извършва действия спрямо данните в нея най-често използва някаква компютърна програма, а въведеният вирус също представлява компютърна програма. Така се стига до ситуация, в която трябва да се извърши трудна преценка по кой от текстовете да бъде квалифицирано деянието.

По-стабилна основа за безспорно квалифициране дава чл. 319д НК, касаещ узнаване, заличаване и други действия спрямо лични данни или информация, представляваща държавна или друга пазена от закон тайна.

Друго посегателство, което може да засегне и лични данни, запазени в компютърна система, е деянието по чл. 216, ал. 3 НК – който унищожи или повреди чуждо имущество, като осъществи нерегламентиран достъп до компютър от значение за предприятие, учреждение, юридическо или физическо лицесе наказва с лишаване от свобода от една до шест години и глоба до десет хиляди лева. В случая става дума за механично унищожаване на компютърна система, в която могат да се съдържат всякакъв вид данни.

Доколкото може да касае и лични данни, които да бъдат манипулирани и да въведат някого в заблуждение, следва да се спомене и компютърната измама – текста на чл. 212а НК, предвиждащ наказание за този, който с цел да набави за себе си или за другиго облага възбуди или поддържа заблуждение у някого внесе, измени, изтрие или заличи компютърни данни или използва чужд електронен подпис и с това причини на него или на другиго вреда. Съгласно ал. 2 същото наказание се налага и на този, който, без да има право, внесе, измени, изтрие или заличи компютърни данни, за да получи нещо, което не му се следва.

В цитираната вече статия е предложена и още една, строго теоретична класификация на компютърните престъпления.[2] Тя обхваща осем групи:

1) престъпления, които засягат националната сигурност (тук се включват разпространение на незаконна информация чрез Интернет като инструкции за направа на бомби, производство на наркотици или терористични действия);

2) престъпления, които засягат интересите на ненавършилите пълнолетие (порнографията, детското насилие, някои форми на маркетинг чрез Интернет);

3) престъпления, които нарушават човешкото достойнство (разпространение на материали чрез Интернет, които провокират омраза или расова дискриминация);

4) престъпления срещу икономическата сигурност (компютърна измама, злоупотреба с кредитни карти);

5) престъпления срещу информационната сигурност (хакерство);

6) престъпления, които засягат неприкосновеността на кореспонденцията и информацията в електронна форма (неоторизирано разпространение или използване на лични данни);

7) престъпления, които увреждат репутацията и доброто име на дадено лице (клевета чрез Интернет или компютърни мрежи);

8) престъпления срещу интелектуалната собственост (софтуерно и други форми на пиратство).

След разглеждането на чисто националните измерения на въпроса с компютърните престъпления и връзката им със защитата на личните данни, следва да бъде обърнато внимание на международните аспекти на проблема, както и да бъдат обсъдени действията на ниво Европейски съюз.

Конвенцията за престъпленията в кибернетичното пространство приета на 109 заседание на Комитета на министрите на Съвета на Европа, създава своеобразен стандарт в областта на наказването на компютърните престъпления като дава определения на най-разпространените понятия – компютърна система, компютърни данни, доставчик на услуги, данни за трафик.

Освен това в конвенцията са предвидени и мерки, които трябва да бъдат взети на национално равнище, както в областта на материалното право, така и в областта на процесуалното право. Описани са възможните правонарушения срещу тайната, неприкосновеността и възможността за ползване на компютърни данни и системи – осъществяване на незаконен достъп; незаконното прихващане на компютърни данни; посегателството срещу такива данни, изразяващо се в увреждане, изтриване, разстройване, изменяне и заличаването им, както и други посегателства срещу компютърни системи. Компютърната фалшификация и компютърната измама също следва да бъдат въведени в националното наказателно право като вид престъпления.

Предвидени са и конкретни мерки в областта на наказателно-процесуалното право, за да се обезпечи ефективното преследване и наказване на подобен тип деяния. Само един пример в тази посока - чл. 16 предвижда задължение за всяка държава да приеме необходимите законодателни мерки, за да даде възможност на компетентните си органи да наредят или да осигурят по друг начин бързото запазване на уточнените компютърни данни, включително данните за трафика, които се съхраняват в дадена компютърна система.

[2] Пак там, с. 94

Интересно е определението на понятието „данни за абоната", използвано в цитираната конвенция. Изразът "данни за абоната" означава всички сведения, съдържащи се под формата на компютърни данни или под всякаква друга форма, притежавани от доставчик на услуги, и отнасящи се до потребителите на неговите услуги, **различни** от данните за трафика или за съдържанието, и даващи възможност да се установи:

а. използвания тип на комуникационната услуга, техническите мерки, взети по отношение на нея, както и времетраенето на услугата ;

б. **самоличността на потребителя, неговият пощенски адрес или адрес по местонахождение , телефонен номер или всеки друг номер за достъп до него**, сведения за сметката и заплащането, съществуващо на основата на договор или споразумение за услугата,

в. всяка друга информация относно местонахождението на инсталационния сайт на комуникационното съоръжение, съществуваща на основата на договор или споразумение за услугата.

Става дума за личните данни на абоната, които администраторът на лични данни, доставчик на интернет услуги следва да предоставя на компетентните разследващи органи.

Освен на международно ниво, уредба на компютърните престъпления се съдържа и на ниво Европейски съюз. Наказателноправната уредба на ЕС за борба срещу компютърната престъпност се отличава с някои характерни особености.[3]

Първата особеност – хармонизираното на националните наказателно правни системи преследва постигането на няколко цели – по-голяма ефективност при осъществяване на наказателното преследване за разглежданите престъпления, борба срещу организираната престъпност и тероризма (включително кибертероризма), избягване на свръхкриминализацията в разглежданата област.

Втората особеност[4] е нужната от терминологични уточнения. Употребяваните термини са различни – компютърна престъпност, кибернетична престъпност, престъпност на високите технологии, свързана с компютрите престъпност. Нужно е уеднаквяване и използване на един и същ термин в нормативните актове на ЕС. Компютърна престъпност в тесен смисъл на думата означава престъпност, която е била невъзможна при отсъствието на новите технологии.

Друга особеност е диференцирането на съдържанието на основните използвани понятия. Освен това се създават стандарти за криминализиране на определени форми на поведение,както и се въвежда диференциране на наказателната отговорност. Общата тенденция е европеизиране на националното наказателно право.

В обобщение – личните данни, както и друга „чувствителна" информация лесно могат да бъдат засегнати от различни форми на престъпна дейност при които се използват новите технологии. Става дума за т. нар. компютърна престъпност. В националното право, под влияние на европейското и международното право, се съдържа уредба на подобен тип деяния. За да се постигне ефективно противодействие е нужно единодействие на компетентните национални органи.

[3] По-подробно за особеностите вж. Панайотов П., Наказателното право на ЕС и българското наказателно право, С 2012 г., с 161

[4] Пак там, с. 162

ОСНОВНИТЕ ПРАВА НА ГРАЖДАНИТЕ В СВЕТЛИНАТА НА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА

Христо А. Ангелов

FUNDAMENTAL RIGHTS IN THE LIGHT OF SPECIAL INVESTIGATION TECHNIQUES

Hristo A. Angelov

Abstract: The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any unlawful interference in his private or family affairs and against encroachments on his honour, dignity and reputation. No one shall be followed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law.

Key words: fundamental rights, special investigation techniques

Личният живот на гражданите е неприкосновен. Това основно право е закрепено в Конституцията на Република България (КРБ), в сила от 13.07.1991 г. обн. ДВ. бр.56 от 13 Юли 1991г., посл. изм. ДВ. бр.12 от 6 Февруари 2007г.

Гражданите имат право на защита срещу незаконна намеса в личния и семейния им живот и срещу посегателство върху тяхната чест, достойнство и добро име. Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие **освен в предвидените от закона случаи**. Свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени. Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления. Тези права са закрепени в чл. 32 и 34 от КРБ.

Освен основни, тези права могат да бъдат наречени още конституционни, защото се съдържат в Конституцията. Те са заложени в КРБ, защото представляват минимума защита на гражданите, минимума права, който те трябва да притежават. Цитираните текстове представляват конституционната основа на нормативната уредба за защитата на личните данни на гражданите. Тя е доразвита в Закона за защита на личните данни (ЗЗЛД) обн. ДВ. бр.1 от 4 Януари 2002г, изм. и доп. ДВ. бр.15 от 15 Февруари 2013г.

Тези основни права имат свои граници и влизат в колизия с други ценности, които също трябва да бъдат пазени. Така например в името на националната сигурност, или пък за разкриване или предотвратяване на тежки престъпления тази лична неприкосновеност (а също така и неприкосновеността на личните данни в широк смисъл на думата) може да бъде нарушена, като това следва да стане в предвидените в закона случаи и по предвидения в закона ред и процедура. Подробно разписаните правила, по които се извършва навлизането в личната сфера, има за цел предотвратяване на злоупотребата с получената информация.

Така например задържането и изземването на кореспонденция в досъдебното производство се извършват по искане на прокурора с разрешение на съдия от съответния първоинстанционен съд или от първоинстанционния съд, в района на който се извършва действието. Нарушаването на неприкосновеността на кореспонденцията се допуска само когато това се налага за разкриване или предотвратяване на тежки престъпления.

Настоящият доклад разглежда едно от предвидените в законите изключения от принципа за неприкосновеност – специалните разузнавателни средства. Уредба на специалните разузнавателни средства (СРС) се съдържа в Наказателно-процесуалния кодекс (НПК) обн. ДВ. бр.86 от 28 Октомври 2005г.,доп. ДВ. бр.17 от 21 Февруари 2013г. и в Закона за специалните разузнавателни средства (ЗСРС) обн. ДВ. бр.95 от 21 Октомври 1997г.,доп. ДВ. бр.17 от 21 Февруари 2013г.

Органите на досъдебното производство могат да използват специални разузнавателни средства: технически средства - електронни и механични съоръжения и вещества, които служат за документиране на дейността на контролираните лица и обекти, и оперативни способи - наблюдение, подслушване, проследяване, проникване, белязване и проверка на кореспонденция и компютърна информация, контролирана доставка, доверителна сделка и разследване чрез служител под прикритие.

Престъпленията, за чието разследване е допустимо използването на СРС, са лимитативно изброени в чл. 172, ал. 2 НПК. Такива са например част от престъпленията по гл. втора Престъпления против личността – раздели „Убийство", „Телесна повреда", „Отвличане и противозаконно лишаване от свобода", „Принуда", „Разврат" и „Трафик на хора"; цялата гл. пета „Престъпления против собствеността" без „Злоупотребата на доверие" и т. н.

По отношение разследването на същите лимитативно изброени престъпления доставчиците на компютърно-информационни услуги са длъжни да подпомагат съда и органите на досъдебното производство при събирането и записването на компютърни информационни данни чрез прилагане на специални технически средства.

Законодателят е преценил, че за разкриването на тези престъпления е допустимо навлизане в личното пространство на гражданите, както и се позволява обработване от компетентните органи на придобитата информация. Всичко това следва да става по определения в закона ред.

За използване на СРС в досъдебно производство се подава писмено мотивирано искане до съда от наблюдаващия прокурор, като искането трябва да съдържа информация за престъплението, за разследването на което се налага използването на специални разузнавателни средства и описание на извършените до момента действия и резултатите от тях.

Освен това в искането се съдържат данни за лицата или обектите, спрямо които ще се прилагат СРС, оперативните способи, които следва да се приложат и срока на използването.

Разрешението за използване на СРС се дава предварително от председателя на окръжния съд или от изрично оправомощен от него заместник-председател, а ако се касае за военнослужещи, разрешението се дава от председателя на съответния военен съд. Ако се касае за дела, подсъдни на специализирания наказателен съд, използването на СРС се разрешава предварително от неговия председател или от изрично оправомощен от него заместник-председател.

Специалните разузнавателни средства се прилагат от съответните структури на Министерството на вътрешните работи или на Държавната агенция "Национална сигурност" по реда на ЗСРС. Писменото разпореждане за прилагане на СРС се дава от министъра на вътрешните работи или от писмено оправомощен от него заместник-министър, съответно председателят на Държавна агенция "Национална сигурност" (писмено оправомощен от него заместник-председател).

При използване на СРС веществените доказателствени средства се изготвят в два екземпляра като в срок до 24 часа от изготвянето им се изпращат запечатани съответно на прокурора, поискал разрешението, и на съда, дал разрешението. Този специален ред за изпращане на веществените доказателствени средства има за цел опазване на събраната информация от възможна злоупотреба и предотвратяване на „изтичането" на лични данни на лицата, спрямо които са приложени СРС. Когато данните, събрани от използването на СРС могат да бъдат използвани и за доказване на друго тежко умишлено престъпление, е допустимо веществените доказателствени средства, закрепящи информацията, добита посредством СРС, да бъдат изготвени и в повече от два екземпляра, които да бъдат приложени по съответните дела.

СРС по смисъла на едноименния закон са техническите средства и оперативните способи за тяхното прилагане, които се използват за изготвяне на веществени доказателствени средства – кинозаписи, видеозаписи, звукозаписи, фотоснимки и белязани предмети. Оперативни способи са наблюдението, подслушването, проследяването, проникването, белязването и проверката на кореспонденцията и компютризираната информация, контролираната доставка, доверителната сделка и разследването чрез служител под прикритие. Техническите средства за изготвяне на веществени доказателствени средства са електронни и механични съоръжения, както и вещества, които служат за документиране на дейността на контролирани лица и обекти.

В ЗСРС отново са уточнени случаите, в които е допустимо временно да „се ограничават неприкосновеността на личността и жилището и тайната на кореспонденцията и на другите съобщения." – чл. 1, ал. 2 ЗСРС. Това е допусимо в случаите, когато това се налага за предотвратяване и разкриване на тежки престъпления по реда на Наказателно-процесуалния кодекс, когато необходимите данни не могат да бъдат събрани по друг начин. Освен това в чл. 4 ЗСРС изрично е посочено, че „по реда на този закон специалните разузнавателни средства могат да се използват и по отношение на дейности, свързани със защитата на националната сигурност".

Отделните оперативни способи и тяхното съдържание са описани в ЗСРС. При наблюдението зрително и чрез технически средства, се разкриват и документират различни страни от дейността и поведението на лица и обекти при тяхното движение, пребиваване на различни места или при изменения в конкретната обстановка, а при подслушването чрез използване на технически средства, слухово или по друг начин се усвоява устна, телефонна или електронна комуникация на контролирани лица. При проследяването - зрително и чрез използване на технически средства, се установява, разкрива и документира движението на контролирани лица. Добитата по този начин информация служи за изготвянето на съответните веществени доказателствени средства. Но освен полезна за разкриването на престъпления информация, чрез използването на тези способи е възможно да бъдат добити и други лични данни.

Затова и в случаите, когато събраната информация не се използва за изготвяне на веществени доказателствени средства, органът, дал разрешението за използване на СРС, разпорежда нейното унищожаване.

При проникването като оперативен способ се установяват фактически данни, намиращи се в помещения, и вещи, ползвани от контролирани лица. При белязването чрез използване на технически средства и вещества се поставят белези на предмети и вещи за установяване на **тяхното движение**, придобиване или мястото на съхранението им. При проверката на кореспонденцията чрез използване на химически вещества и технически средства се установяват **съдържанието и адресатите на кореспонденцията** на контролирани лица и обекти.

Когато се проследява движението на предмети и вещи, косвено може да се съди за местоположението и на контролираните лица. Затова държи сметка и Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации). В нея се използва и терминът „данни за местонахождение" - всякакви данни, обработени в електронни комуникационни мрежи, показващи географското местоположение на терминалното оборудване на потребителя на публично достъпни електронни комуникационни услуги. Директивата за правото на неприкосновеност на личния живот и електронни комуникации изисква по-задълбочен анализ, който излиза извън рамките на настоящата тема и може да бъде предмет на друга разработка, посветена на въпросите за правото на ЕС в областта на защитата на личните данни.

Нейното споменаване е свързано с възможността да се следи местонахождението на лицата, ползващи съвременни технологии под формата на мобилни устройства, таблети и компютри. Данните за местонахождението също могат да бъдат счетени за особен вид лични данни. Затова и СРС, които са свързани с локализирането на лица и предмети, се явяват свързани с въпроса за защита на неприкосновеността на личния живот.

Още по-ясно тази връзка проличава при оперативния способ проверка на кореспонденцията, при което се установяват съдържанието и адресатите на кореспонденцията. Информацията за адресатите на кореспонденцията очертава кръга лица, с които контролираното лице осъществява контакти, а по съдържанието на кореспонденцията може да се съди за сферата на интереси на даденото лице.

Останалите оперативни способи са контролираната доставка, доверителната сделка и служителят под прикритие. Контролираната доставка се прилага от разузнавателния орган и се използва от разследващия орган в кръга на компетентността му при непрекъснат контрол на територията на Република България или друга държава в рамките на международното сътрудничество и се изразява във внасяне, изнасяне, пренасяне или транзитно превозване през територията на Република България от контролираното лице на вещ - предмет на престъпление, за да се разкрият участниците в трансгранично престъпление.

Казаното за проследяването на вещи и предмети важи и за контролираната доставка. Що се отнася до последния оперативен способ – доверителната сделка – по смисъла на ЗСРС доверителната сделка се използва от служителя под прикритие и се изразява в сключването на привидна продажба или друг вид сделка с вещ с цел да се спечели доверието на другата страна, която участва в сделката.

Последният оперативен способ е служителят под прикритие. Той е служител от компетентните служби по Закона за Министерството на вътрешните работи, Закона за отбраната и въоръжените сили или от Националната разузнавателна служба, оправомощен да установи или поддържа контакти с контролирано лице, за да **получи или разкрие информация** за извършването на тежко умишлено престъпление и за организацията на престъпната дейност.

Реда за използване на СРС, даден в НПК е подробно доразвит в ЗСРС. СРС могат да се използват по отношение на лица за които са получени данни и има основание да се предполага, че подготвят, извършват или са извършили тежки престъпления. Възможно е да бъдат приложени СРС и спрямо лица, които макар и да не извършват престъпна дейност, чрез действията си подпомагат други лица, които я извършват. СРС могат да се използват и по отношение на лица и обекти, свързани с националната сигурност.

По-интересните моменти около процедурата по разрешаването на използването на СРС са свързани с лимитативното изброяване на имащите право да искат прилагане на СРС и да използват събраните чрез тях данни. Това са Главна дирекция "Борба с организираната престъпност", Главна дирекция "Национална полиция", Главна дирекция "Гранична полиция", дирекция "Вътрешна сигурност", областните дирекции на Министерството на вътрешните работи, специализираните дирекции - **с изключение на дирекция "Технически операции"**, териториалните дирекции и самостоятелните териториални отдели на Държавна агенция "Национална сигурност".

Специализирана дирекция „Технически операции" към Държавна агенция „Национална сигурност", която осъществява прилагане на СРС, не би могла да изисква такова прилагане, защото това ще означава една и съща структура от една страна да иска използването на СРС, а от друга страна да изпълнява това искане, което може да доведе до недостатъчен контрол върху използването им и до опасност от злоупотреба с лични данни на контролираните лица.

Искане за използване на СРС могат да отправят и службите "Военна информация" и "Военна полиция" към министъра на отбраната, Националната разузнавателна служба, както и окръжните прокуратури за престъпления свързани с т. нар. купуване и продаване на гласове.

Съобразно чл. 175, ал. 5 НПК прилагането на СРС се преустановява във следните случаи:

- когато е постигната предвидената цел;
- когато прилагането на СРС не дава резултати;
- при изтичане на срока за разрешението;
- при опасност от разкриване на оперативните способи;
- в случаите, когато прилагането на оперативните способи стане невъзможно;
- когато възникне опасност за живота или здравето на служителя под прикритие или на неговите възходящи, низходящи, братя, сестри, съпруг или лица, с които се намира в особено близки отношения, когато опасността произтича от възложените задачи.

При преустановяване прилагането на специалните разузнавателни средства незабавно се уведомява писмено и мотивирано органа, дал разрешението. В случаите, когато събраната информация не се използва за изготвяне на веществени доказателствени средства, той разпорежда **нейното унищожаване**.

Подробни правила за това как следва да се процедира с информацията, добита при използването на СРС, са разписани в едноименния закон. Това се налага от факта, че използването на събраните данни, включително и лични, е един от „критичните" моменти по отношение на това дали навлизането в личната сфера на лицето в името на някакви по-висши ценности няма да се трансформира във форма на злоупотреба с лична информация.

Резултатите от прилагането на СРС се отразяват на хартиен или друг носител от съответния орган на структурата, осъществяваща прякото прилагане на оперативните способи – например специализирана дирекция „Технически операции" към ДАНС. Незабавно след изготвянето носителят се изпраща на органа, направил искането за използване на специалното разузнавателно средство – вж. по-горе кои органи могат да отправят такова искане.

Веществените доказателствени средства, получени при използване на СРС, се изготвят в два екземпляра от структурата, която е осъществила прилагането им. Те се отразяват и в протокол и се изпращат на органа, който е изискал прилагането на СРС. В този протокол се отразяват искането, решението и разпореждането за използване. Той съдържа също така информация за времето и мястото на прилагането на специалните разузнавателни средства, видовете използвани оперативни способи и технически средства, **получените данни за контролираните лица** и обекти, текстовото възпроизвеждане на съдържанието на веществено доказателствено средство. В протокола следва да се отразят също и условията, при които са възприети резултатите от ползването.

Добитата информация, която не се използва за изготвяне на веществени доказателствени средства, независимо дали представлява **класифицирана информация**, се унищожава от структурите, които са възложили и осъществили използването на СРС в 10-дневен срок от прекратяване на прилагането на специалното разузнавателно средство. Унищожаването се извършва от тричленна комисия в състав, определен от ръководителя на структурата, за което се изготвя протокол.

В чл. 32 и 33 от ЗСРС са дадени още няколко законови гаранции за предотвратяването на злоупотребата със СРС. Резултатите, получени чрез СРС, не могат да бъдат използвани за друго, освен за предотвратяване, разкриване и доказване на престъпления при условията и по реда, посочени в закона. Лицата, на които са станали известни факти и сведения за СРС, както и за събраните данни, са длъжни да не ги разгласяват.

Освен това Народното събрание чрез комисия, определена с правилника за организацията и дейността му, осъществява парламентарен контрол и наблюдение на процедурите по разрешаване, прилагане и използване на СРС, съхраняването и унищожаването на получената чрез тях информация, както и за защита **на правата и свободите на гражданите** срещу незаконосъобразното използване на специални разузнавателни средства.

Законовата рамка, създадена да регулира използването на СРС, цели да постави ясни граници, в които е допустимо навлизането в личната зона на неприкосновеност на всеки гражданин. Съвременните условия на живот налагат известен компромис с основните права в името на защита на по-висши ценности. Само добросъвестното прилагане на законовите правила, съчетано с някаква форма на външен надзор могат да гарантират, че използването на СРС ще бъде именно за защита на тези ценности.

ТЕРОРИЗЪМ. ПРИЗНАЦИ ЗА ПОДГОТОВКА НА ТЕРОРИСТИЧЕН АКТ

Калоян Н. Димитров **Свилен В. Господинов**

Национален военен университет "В. Левски",
Факултет "Артилерия, ПВО и КИС",
075kl@mail.bg

TERRORISM. SIGNS OF PREPARATION

Kaloyan N. Dimitrov **Svilen V. Gospodinov**

ABSTRACT: The report presents the main stages of the planning and preparation of terrorists attacks. Prior signs such as residence, transport, finance, activities, and signs supporting terrorist activity.

Keywords: planning, financing, residence, transport, fake documents, money, signs and activity.

Общоприетите дефиниции на тероризма визират актовете на насилие, които са предназначени да създават - страх, преднамерено се прицелват в безопасността на гражданите и се извършват с идеологически цели.

Така например в книгата си „Тероризъм: История и генезис", Г. Стоянов определя тероризма като „организирана или индивидуална дейност за нанасяне на телесни повреди, за прилагане на насилие и задържане на хора, отвличане на моторни превозни средства или оказване на психологически натиск чрез заплаха с насилие с цел удовлетворяване на конкретни политически искания и най-вече отслабване и дестабилизиране на съществуващото държавно управление." [1]

По своята същност тероризма представлява сложно социално – политическо явление, свързано със същността на обществото и възникнал от неговите противоречия, засилващ се с тяхното задълбочаване.

Терористични актове са определени криминални деяния, срещу личността и собствеността, които - „като се има предвид характера или контекста им" - могат сериозно да навредят на дадена страна или на международна организация, в която са извършени с цел: сериозно сплашване на населението; или незаконно изискващи от дадено правителство или международна организация да извърши или да се въздържи от извършването на дадено действие; или сериозно дестабилизиране или разрушаване на фундаменталните политически, конституционни, икономически или социални структури на страната или международна организация.

Болшинството от терористичните актове се извършват от предварително създадени, обучени, оборудвани със съвременно въоръжение и екипировка и добре финансирани терористични групи. Терористичната група представлява „обединение на двама или по-вече души, имащи общи цели (извършване на терористични актове), с определена йерархия между тях. Терористичните групи се формират предимно на идеологическа основа. Болшинството от участниците в тях

са фанатично предани на идеите за изпълнение на поставените цели, и са готови да пожертват живота си за тях.“ [2].

Изследователите на тероризма не са се обединили около едно единствено определение за терориста характеризиращо моралния, физическия и идеологическия му профил. В основата на всяка една терористична акция стоят личности ръководени от различни идеологически или морални подбуди. Терористичните операции се планират, организират и провеждат от хора, действащи сами или като част от група. Подготовката на терористична атака може да бъде много сложна, професионална и да отнеме дълъг период от време или може да бъде по-малко професионална и по-спонтанна.

За подготовката на дадена атака терористите трябва да предприемат действия, като събиране на разузнавателни сведения, обучение и движение на хора, пари и оръжия. Тези действия могат да бъдат забелязани от органите на реда или цивилното население. Ранните предшестващи признаци могат да помогнат да се разпознае вероятната подготовка на терористична атака.[3]

Терористичните организации, мрежи или отделни хора могат да използват определени места, като офиси, къщи, складове и др., за да се срещат или подготвят определени дейности. Има случаи в които, къщи под наем са били използвани като „убежища" или като „фабрики за бомби". Често това се извършва по възможно най-дискретния начин. Дейности в това отношение, които могат да привлекат вниманието на службите за борба с тероризма или на отделни граждани, могат да бъдат:

- Редовна смяна на жителите;
- Дълго отсъствие на жителите;
- Необичайна смесица от жители;
- Домът се използва като място за срещи;
- Необичайно използване на гаражи или др. помещения под наем;
- Необичайни дейности в странни часове на деня;
- Необичаен боклук.

Организацията и провеждането на всеки терористичен акт е свързано с придвижване на участниците в нея, както и с транспортирането на експлозиви и оръжия. Това важи особено за периода на последните приготовления, когато хора и консумативи заемат местоположението си за извършване на терористичен акт, което може да бъде последната възможност за намеса. [4]

В по-вечето от случаите, терористите използват различни превозни средства за осъществяване на конкретната атака, за наблюдение на „мишената“ на атаката или за оттегляне на участниците в нея след извършването и.

Признаци за иползването на различни автомобили за подобни цели могат да бъдат:

- използване на превозно средство като място за наблюдение;
- табелки с чуждестранни номера;
- паркиране в един и същ район за дълъг период от време;
- изоставено превозно средство;
- наемане на превозно средство с фалшиви документи;
- кражба на превозно средство с лого на дадена компания;
- модификация на превозно средство, с цел подобряване на габаритните му характеристики или увеличаване на товароносимостта му. [6]

За подготовка и осъществяване на терористична атака, терористите се нуждаят от съществени финансови средства. Анализът на знаковите терористични атаки през последните десетилетия, показва тенденция към изразходване на все по-големи суми за тяхното извършване. Като примери :

- Лондонската транспортна система 7 Юли , 2005г. -18256 лева;
- Мадрид, влаковете атентати 11 мар 2004г. -15000 лева;
- Истанбул, камиони бомби 15 и 20 ноември 2003г.-26000 лева;
- Атентатите в Бали 12 октомври 2002г.- 75000 лева; [7]

Финансирането на тероризма – това е дейност, насочена към предоставяне или събиране на средства (в това число и парични) с цел последващото им използване за подготовка и извършване на терористичени актове от отделни терористи или терористични организации.

Освен за прякото организиране и извършване на терористични атаки, са нужни и текущи средства за задоволяване на ежедневните нуждите на терористите и техните семейства - ползването на коли, наем на жилища, осигуряване на средства за комуникация, оръжия или експлозиви и др.

Начините за сдобиване с необходимите финансови средства могат да бъдат нелегални и легални. Към нелегалните могат да бъдат причислени:

- търговия с наркотици;
- незаконно добиване и търговия със скъпоценни камъни и злато добивани в зоната на водените въоръжени конфликти;
- търговия с хора, отвличане на хора, принуждаване към проституция;
- измами с използване на кредитни карти и мобилни телефони;
- производство и продажба на фалшиви стоки и фалшиви пари;
- изнудване и др.

Легални източници на финансови средства могат да бъдат:

- благотворителна дейност;
- постъпления от Комитета за поддръжка на Афганистан;
- вносно-износни операции;
- машинации с ценообразуването на вносни/износни стоки;
- доходи от такси, ресторанти и др;
- печалби от банки, строителни фирми, туристически агентства, играли домове, казина и др.

За да поддържат анонимността си, терористите могат да използват фалшиви или откраднати кредитни карти.

Характерни признаци за подобно незаконно придобиване на средства с цел финансиране на терористична дейност са:

- Притежание или харчене на значителни суми пари в брой;
- Необичайни финансови транзакции;
- Притежание или харчене на големи суми чуждестранна валута;
- Извършване на измама със социалния осигурителен номер или финансова документация;
- кражби от магазин, грабежи, отвличания, търговия с наркотици и опойващи вещества и др.; [6]

За прикриване самоличността на терористите могат да се използват фалшиви документи, паспорти, шофьорски книжки, кредитни карти и др. Развитието на съвременните технологии и наличието на достатъчно финанси в терористичните

групи и организации им позволяват изработкатана достатъчно добре фалшифицирани документи, които по нищо не остъпват на оригиналните. Не са изключение и случайте в които поради липса на средства или време документите са с лошо качество, което позволява бързо и лесно да бъдат разпознати и съответните лица да бъдат задържани преди или в хода на извършване на терористичния акт.

От особено значение за реализацията на всеки терористичен акт е набавянето на различни средства за непосредственото му осъществяване. Средства за провеждане на терористичната дейност са всички онези, които могат да бъдат използвани от терористите според конкретните цели на всеки отделен терористичен акт.

Под средства за провеждане на терористични акции трябва да се разбират всички устройства, прибори, апарати, машини и вещества, които се използват от терористите за решаване на стоящите пред тях задачи. Бурното развитие на научно-техническият прогрес през последните десетилетия позволява създаването на нови видове оръжия, на нови способи за тероризъм, което съществено разширява мащабите на дейността на различните организации и групи и открива принципно нови възможности за провеждане на терористични акции.

Снабдяването на терористите, със средства за провеждане на терористична дейност, се осъществява по два начина: чрез създаване на нови средства, специално предназначени за изпълнение на терористични задачи и чрез приспособяване за техните потребности на технически средства, използвани в други сфери на човешката дейност.

Средствата за терористични актове могат да бъдат изготвени в промишлени условия или саморъчно направени от терористите, като последните могат да бъдат и продукти на високи технологии.

По предназначение, принципи на действие и способи за прилагане, техническите средства, използвани в терористичната дейност, са разнообразни. Често едни и същи средства могат да бъдат употребени за постигане на различни престъпни цели. Според критериите „решавани задачи" и „характер на въздействие върху обекта" се открояват три групи средства:

- средства за физическо въздействие върху хора;
- средства за въздействие върху материални обекти;
- средства за психологическо въздействие върху съзнанието и поведението на хората.

Снабдяването с подобни средства може да се осъществи по най-различни начини. Те варират от кражбата на оръжия, покупка на експлозиви, амуниции и средства за комуникация, както и придобиване на униформи, ключове или ключови символи в зависимост от конкретния замисъл. Някои от материалите се намират и доставят много трудно, докато други могат да бъдат закупени от обикновени или специализирани магазини.

Факти които могат да бъдат признаци за подготовка на терористичен акт могат са:

- Намиране на карти, скици или подробен план на потенциалните мишени;
- Ръководства за летене или разписания;
- Снимки или видеоматериали на обекти и сгради;
- Помощни средства за навигация и наблюдение;
- Материали за направа на експлозиви, като прекис, изкуствени торове, амоняк;
- Материали за изработване на импровизирани експлозивни устройства, като батерии, електронни схеми, халогенни крушки и др.

- Военни или химически ръководства;
- Ръководства за изработване на бомби;
- Наличие на различни мобилни телефони или предплатени карти;
- Незаконно притежавани оръжия,бронежилетки, амуниции и/или експлозиви;
- Кодово разговорни таблици за шифриране и дешифриране на съобщения;
- Униформи (полицейски, военни, болнични) и др.; [5]

Осъществяването на всяка една терористична операция се съпровожда от щателна предварителна подготовка. Ако терористи са избрали специфична мишена, зоната на мишената най-вероятно ще бъде наблюдавана по време на фазата на планиране на операцията. Това се прави с цел определяне на силните страни, слабостите и броя на членовете на персонала. Наблюдението може да продължи до момента точно преди атаката, което дава на терористите най-актуална информация за целта. За тази цел могат да бъдат използвани различни средства като камери, водене на бележки, анотации и карти и използване на бинокъл.

Членове на терористична група могат да се опитат да получат информация или сведения за критична инфраструктура с цел подготовка и провеждане на терористичен акт. Опити за извличане на информация могат да бъдат направени по електронната поща, телефона, факса или лично.

След извършването на атаката, атентаторът или терористът имат две възможности:

- да се оттеглят от района на атентата (съгласно предварително обмислен план);
- да извършат самоубийство, унищожавайки хората намиращи се в близост до обекта за атака.

Анализът на терористичната дейност в края на XX и началото на XXI век показва че терористите използват все по съвременни средства за извършване на своята дейност и въпреки че бяха постигнати определени успехи в борбата срещу него в световен мащаб, все още терористичната заплаха е реална опасност за човечеството.

В развитието на тероризма през последните няколко десетилетия се забелязват редица по-вече или по-малко отчетливи тенденции, изучаването на които има важно значение за осмислянето на ролята на съвременния тероризъм като глобална заплаха за човечеството, както и за разработването на ефикасни мерки борбата с него.

Независимо от някои различия, специалистите по проблемите на тероризма се обединяват около мнението че развитието му през новото хилядолетие ще се характеризира със [2]:

- Разширяване на географията на терористичната дейност в световен мащаб и неговата интернационализация;
- Повишаване на нивото на организираност на терористичната дейност, създаване на нови крупни терористични формирования с развита инфраструктура;
- Засилване на връзката на тероризма с организираната престъпност;
- Увеличаване на ръста на финасовото и материално-техническото осигуряване на терористичните организации;
- Стремеж към придобиване и използване на оръжия за масово поразяване;
- Активно използване от терористите на съвременните информационни технологии и средства за свръзка;
- Разработване и усъвършенстване на нови форми и методи, насочени към разширяване на мащабите и последствията от терористичната дейност и увеличаването на количеството на жертвите от терористичните актове.

Литература:
1. Стоянов Г., Тероризъм: История и генезис, ВИ, София, 2003 г.
2. Досев Н., Сандев Г., Тероризъм и противодействие, Шумен, 2007 г.
3. Трифонов Т., Същност и съдържание на терористичната дейност, София, 1997 г.
4. www.terrorism-research.com/
5. www.start.umd.edu/gtd/
6. www.rt.com/tags/terrorism/
7. www.fatfgafi.org/media/fatf/documents/reports/Terrorist Financing

СИГУРНОСТ НА FACEBOOK

Иван М. Николов, Петко Г. Мутафчиев, Стойко Т. Тодоров

petko_mutafchiev@abv.bg, opelx20dtl@gmail.com, sers@abv.bg

FACEBOOK SAFETY

Ivan M. Nikolov, Petko G. Mutafchiev, Stoiko T. Todorov

ABSTRACT: *The social networks are being constantly used nowadays. They offer fun and easy communication but we forgot about the dangers in our private security. However we can optimize the privacy settings to maximize our protection.*

KEY WORDS: *security, safety, Facebook, settings, privacy*

Социалните мрежи са нещо чудесно – изумителен начин за общуване, който може да ви позволи да поддържате контакти с хора от цялото земно кълбо. Разбира се, би било чудесно, ако всеки един от тях е добронамерен и благоразположен към вас, но за съжаление реалността подсказва друго.

Измежду многобройните социални мрежи като Twitter или Google+ най-утвърдена към момента в България е Facebook с над 2,5 милиона потребители. Facebook предлага достатъчно добри политики по сигурност за да може да се предотвратят злоупотреби с личната информация. На първо място използваният протокол е https, който предоставя криптирана комуникация и защитава самоличността в мрежата на уеб сървъра. Всички останали действия по сигурността са въпрос на правилното конфигуриране на настройките и личната култура на потребителя.

Facebook наскоро направи промяна на интерфейса като е акцентирано именно на настройките по сигурността като е изнесен нов бутон в непосредствена близост до бутона "Home", който представлява пряк път до основните опции за поверителност. Споделянето на лична информация в интернет е опасно само по себе си, но с помощта на тези настройки е добре информацията за нас да бъде видима само за група хора, които наистина познаваме в реалния свят. А как различните групи хора виждат как изглежда профилът ни може да се провери от функцията "View as". Сега тя е подоб-

рена и можем да изберем не просто група или тип абонати, а да посочим конкретен наш приятел и да наблюдаваме какво би виждал той на нашия Timeline.

Фиг. 1. Пряк път с бързи настройки

Регистърът на дейността е основно редактиран. В предната версия на тази настройка ни се показваше дневник с дълъг списък от активности, като всички бяха събрани на едно място и разграничени единствено по време, което е объркващо и трудно за анализ. Сега всички статуси са разделени по снимки, коментари, харесвания, статуси на другите, приложения, приятели, новини, групи, абонаменти, събития, въпроси, търсене и изобщо всичко, което може да правите във Facebook. Наличните филтри се променят според вида активност, която разглеждате. Освен това, Activity Log позволява да ревизирате вашият Timeline, което ще ви даде ясна представа дали в него се съдържа нещо социално уличаващо ви или пък нещо неудобно, което ще ви злепостави.

Вече е въведен т.нар. Request Removal Tool, който служи да премахнете себе си от постове/статуси, в които сте тагнати. Въпрос на организация е, но е изключително полезно да се управляват нашите приятели чрез списъци. Това е един от най-силните инструменти на Facebook. Всеки списък може да бъде с обособено ниво на поверителност. Когато споделяме нещо чрез списъците много лесно контролираме кой да вижда поста ни. Също така списъците са много удобни ако искаме да останем видими единствено като офлайн за чата.

Фиг. 2. Поверителност по избор

Въобще всички инструменти за към момента максимално лесни за употреба и са предоставени достатъчно голям набор от възможности потребителя да филтрира или защити своята информация. Но въпреки взетите мерки даден акаунт може да бъде следен от "бисквитките", които се използват от браузъра. Например ако на-

тиснем бутона "Like" на някоя картинка от някой сайт, чрез "бисквитките" се разбира, че харесаната снимка трябва да се покаже на стената на точно нашия акаунт. За да избегнем този проблем можем да използваме интернет браузър с многопотребителско използване (Google Chrome например). Създаваме си потребителски профил 1, който ще ползваме за нормално интернет сърфиране, на който забраняваме да се приемат бисквитки от Facebook. На профил 2 задаваме настройка да се блокират всички бисквитки, с изключение на тези от Facebook и така когато искаме да споделим нещо копираме страницата от профил 1 на профил 2 и тогава натискаме "Like". Междувременно ако в профил 1 натиснем бутона за харесване, просто ще ни се отвори диалоговия прозорец за вход във Facebook.

Най-големият проблем е, че неопитните потребители често попадат в капани или се отнасят небрежно към своята поверителност. Има сайтове, на които изскачащ диалогов прозорец наподобяващ например интерфейса на чата подканва потребителя да напише името и паролата си поради настъпила техническа неизправност. След като злонамереното лице притежава данните за вписване на потребителя може практически да прави всякакви злоупотреби. Има регистрирани случаи когато от откраднати по този начин акаунти се изпращат съобщения на приятели на жертвата, в които се съобщава, че има нужда спешно от пари, които да бъдат изпратени някъде. От друга страна някои потребители не се отнасят отговорно към информацията, която оставят. Пример: потребителят съобщава, че цялото семейство напускат града за седмица. Много хора, къде познати от реалния свят, къде приятели само от някоя от Facebook игрите, виждат това и е налице предпоставка да бъде извършен грабеж на жилището на нищо неподозиращият потребител.

Помнете, че в интернет нищо не е напълно частно. Акаунтите могат да се хакнат, хората правят снимки на екраните ви без да подозирате, самоличността на човека отсреща никога не е ясна. Ползвайте ограничен кръг от близки, които да могат да виждат профила ви.

Литература:

[1] http://www.socialbakers.com/
[2] FACEBOOK TIMELINE - LIFEHACK.BG - 2013Г. ОТ ХРИСТО СТОЯНОВ
[3] http://technews.bg/article-17445.html#.UaY-4NgjHFx

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА PC ПОТРЕБИТЕЛИТЕ

Петко Г. Мутафчиев, Иван М. Николов, Стойко Т. Тодоров

petko_mutafchiev@abv.bg, opelx20dtl@gmail.com, sers@abv.bg

INFORMATION SECURITY OF PC USERS

Petko G. Mutafchiev, Ivan M. Nikolov, Stoiko T. Todorov

ABSTRACT: *This publication is about the kind of hacker attacks and the ways of defence against them. There are some advices from us and tricks for successful building of strong security. We took a look at offline and online security threads.*

KEY WORDS: *security, information, attacks, hackers, passwords, encryption, network*

В днешно време въпросът за защита на информацията е все по-актуален поради масовостта на интернета и снижаването на подготовката на обикновения потребител. Ще разгледаме начините за защита на личните ни данни от практическа гледна точка при целенасочени опити за извличане на информацията ни.

Като начало съвсем накратко ще спомена методите за разбиване на пароли, използвани от хакерите и официални софтуери за забравени пароли. Първият вид е "грубата сила" (brute-force), при който атакуващият изпраща множество заявки към сървъра с различни двойки от име и парола, с цел да налучка някоя правилна комбинация. Това е изключително мощен метод. Друг вид атака е "речниковата" (dictionary). При нея хакера използва brute-force техники за обхождане на големи и изчерпателни списъци от познати думи (речници) в опит да открие съвпадение с паролата. Ако паролата е сложна и е над 7 символа с букви, цифри и специални символи, несъдържаща познати думи, фрази или комбинации за пароли, тази атака е безобидна. Нейното предимство е, че може бързо да постигне успех при разбиване на лесна парола, каквато обаче поставят повече от потребителите. За разлика, brute-force атаките може да се проточат със седмици, но успеха им е в пъти поголям. Използват се и крипто-анализиращи атаки. Целта е разбиване на криптиращия алгоритъм. За разлика от другите атаки тази е по сложна и комплексна, е необходимо да се приложат задълбочени знания по криптография и математика. За да се противодейства на тази атака и необходимо да се използват тествани алгоритми, внедрявани коректно.

Най-базовите и също така най-лесно преодолимите методи за защита са поставянето на пароли. Напредналите потребители могат да преодолеят повечето пароли, но това в никакъв случай не означава, че те не са необходими. Първото нещо което можем да направим е да зададем парола на BIOS-а. Методите за премахването и са няколко, като един от тях е премахване на батерията на BIOS, а другия - използване на универсална фабрична парола за даден тип BIOS, например за AWARD BIOS. Като препоръка е необходимо компютъра да има заключване на капака или поне стикер за да се избегне чужда интервенция. Второто нещо, което е необходимо да направим е да поставим парола на операционната ни система. Като

правило паролите трябва да бъдат поне 8 символа, съчетаващи букви и цифри за да не бъдат разбивани бързо от хакерски софтуер. Добре е да ползваме различни пароли и да ги сменяме периодично. В Windows Guest акаунта е по-сигурно да бъде изключен. При Windows XP администратора по подразбиране е без парола и трябва да му бъде зададена. Това е сериозен пропуск и може да бъде проникнато в операционната система чрез него. В Windows Vista, 7 и 8 този проблем е решен чрез по подразбиране забранения администраторски акаунт. По-защитените операционни системи са Unix базираните като дистрибуциите на Linux и Mac OS. Концепцията им е, че се работи с ограничен потребител и за определени действия се използва супер потребителя root с неограничени права. Един от начините за преодоляване на паролата на Windows е чрез използване на софтуер като Kon-Boot, който стартира Windows, заобикаляйки паролата му. Други начини за достъп до данните са стартиране на Mini Windows XP или 7, Mini Linux и др.

Другите фактори за успешна базова защита е използването на добра антивирусна и анти-шпионска програма и външен Firewall, който е по-сигурен от вградения в Windows. Ъпдейтите на Windows "запушват" дупките в сигурността. Също така трябва да спрем Remote Assistance и Remote Desktop. Тези услуги може да се използват от недоброжелатели за отдалечен достъп до системата.

Най-елементарният начин за спиране на любопитни погледи е скриването на папки и файлове, но това е твърде несериозно дори и за деца. Криптирането на информацията е най-надеждния начин за защита. В днешно време методите за криптиране и декриптиране се развиват с бурни темпове. Има голямо разнообразие от софтуер за тази цел, но трябва да внимаваме, защото на част от този софтуер защитата може да бъде доста наивна. Например, ако се използва парола за декриптиране, тя може да бъде записана в явен некриптиран вид в регистрите. Това можем да тестваме като пуснем претърсване за паролата. Вградения софтуер в Windows Vista, 7 и 8 - BitLocker Drive Encryption позволява криптиране както на отделни файлове и папки, така и на цели дялове. Декриптиращият ключ се пази на външен носител като флашка и както е логично - не е желателна загубата му. Криптиране на информацията се поддържа от някои e-mail клиенти. Електронните пощи като АБВ използват парола за оторизация на достъпа и данните се предават чрез интернет протоколи. Точно тук е слабото звено - процеса на пренос на данните по протокола. Хакери могат да засекат пакетите, формиращи мрежовия поток и да откраднат данните. За тази цел са въведени защитени мрежови протоколи с криптиран пренос на информация. Пример за такъв протокол е HTTPS, който е защитен HTTP, който е най-масово използваният. Препоръчително е използването на електронни пощи със защитен протокол. Има, разбира се, и други решения за криптиране на информация. Повечето програми за компресиране на файлове имат функция за защита на архивирания файл с парола. Неудобството на този подход е, че ако често се налага да работим с тези файлове, всеки път трябва да разкомпресираме и след това на ново да компресираме информацията. Донякъде WinRAR решава този проблем, чрез възможност за работа директно в архива. Ако изпращаме файлове през мрежата, подобно решение е удачно. Първо, защото информацията е защитена с парола, и второ - получателят на файла не трябва да притежава и програмата за криптиране. Един от най-сигурните архиви е rar-а. Паролата на rar архив се разбива за много дълго време, а в повечето случаи е практически невъзможно. За разлика от rar, zip архива е един от най-лесно пробиваемите. Често това става за секунди.

На хора с много пароли препоръчваме създаването на текстов файл, където да бъдат съхранени, и неговото архивиране с парола чрез WinRAR в rar архив. Така можем да помним само една единствена парола.

Следващият елемент на защитата е мрежовата защита. Задължително достъпа до компютъра трябва да се осъществява чрез парола. Известна доза защита, най-вече от вируси, предоставя влизането в интернет посредством виртуална машина. Най-добрия софтуер за виртуализация е VMware. Ако се зарази виртуалната машина не се заразява компютъра. Разбира се не е добре да се работи с важни данни под вуртуална машина. Най-сигурният начин за предаване на мрежови данни е използването на частна виртуална мрежа (VPN). Цялата информация е криптирана, включително и данните за подателя, което прави почти невъзможно някой да прихване изпращаната информация. За тази цел трябва да се инсталира на компютрите VPN клиент за да комуникират помежду си.

Широко разпространение днес имат Wi-Fi мрежите. Тяхна особеност е, че използват криптиращи методи за пренос на информацията. Основният проблем е, че повечето криптиращи протоколи като WEP, WPA, TKIP, 802.11g могат да бъдат разбити бързо и лесно от хакери, като дори има създадени специални хардуерни устройства за тази цел. Вредите от това могат да варират от кражба на интернет достъп до кражба на поверителна информация. Най-защитен е протоколът WPA2, а най-непробиваемият метод за криптиране е AES, за разлика от TKIP. Стандарта WPS (Wi-Fi Protected Setup) е създаден, за да се улесни настройката и да гарантира сигурността на безжична домашна мрежа. Характерното за него е наличието на 8-цифров PIN код, който е уникален за всяко безжично устройство и не може да се променя. Открита е опасна уязвимост в PIN кода на WPS. Обикновено, за да се налучка кодът, трябва да се пробват десетки милиони комбинации, което изисква огромно време. Дупката в WPS съкращава броя на комбинациите до 11 хиляди. Някои рутери имат защита, така че при наличието на много заявки за PIN кодове, спират WPS за няколко минути (WPS Lock). Това забавя съвсем малко атаката. Единствената адекватна защита е спирането на WPS, но някои рутери не поддържат такава опция. Тогава следва да направим update на фърмуера и ако не се появи опцията - евентуално да използваме неофициален такъв. Паролата е добре да е над 13 символа и да не съдържа думи. Защитата трябва да е WPA2 (AES).

Важен елемент от защитата е настройката на браузърите. Желателно е да не се запазват пароли за сайтове, защото има софтуер, който е способен да ги измъкне. Периодично може да се изтриват бисквитките и хронологията.

Последно, но не на последно място - за изтриване на информация, която не искаме да бъде възстановена от специализиран софтуер в Windows трябва да използваме външен софтуер като Eraser. В Mac OS има опция Secure Empty Trash, а в Linux - команда "shred -u", изписана в терминал или командна линия. Ако държим информацията да не може да бъде възстановена дори от разследващи институции като ФБР и ЦРУ, в Mac OS инструмента Disk Utility има опции за многократно запълване на секторите на твърдия диск с нули или случайни нули и единици. В Windows и Linux няма подобен инструмент и трябва да се прави запълване с нули с външен софтуер. При 35 цикъла на запълване, който може да отнеме седмица и повече имаме 100% гаранция, че никой вече не е в състояние, чрез специални алгоритми или определяне намагнитеността на плочата на хард диска, да възстанови данните.

Защитата на информацията е изключително важно мероприятие и изисква комплексен подход, съобразяване с множество технически и човешки фактори. Редовно трябва да се проучват пробивите в сигурността и да се изучават новостите в тази сфера.

Литература:

[1] http://technews.bg/article-414.html#.UaBuVb2-2ig
[2] http://pcworld.bg/369_zashtita_na_informaciyata&page=1
[3] https://ssd.eff.org

НАУЧНА КОНФЕРЕНЦИЯ 2013

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

СБОРНИК НАУЧНИ ТРУДОВЕ

Българска. Издание първо. Тираж 50

Предпечатна подготовка - Факултет „Артилерия, ПВО и КИС“ - Шумен