PROFESSIONAL

Брой 10, година IV, юни 2012



ПРАНЕ НА ПАРИ

ISSN 1314-0574

Мерки срещу финансиране на тероризма и пране на пари • Смартфоните – пробиви и защита • Защита на интелектуалната собственост

Разпространява се безплатно



HDI

Застраховане

www.hdi.bg

ХДИ Застраховане.
Винаги ти помага

Днес застраховката не е каприз, не е лукс и не изисква високи доходи.
Днес застраховката е начин да живеем разумно.

Защото напрегнатото ни ежедневие изисква бързи преценки, много мобилност и малко време за реакция.
Защото не можем да контролираме случайността.

ХДИ Застраховане създаде разнообразие от застрахователни продукти, съобразени с вашето ежедневие.

Ние сме винаги близо до вас в труден момент, винаги на разположение да ви помогнем.
За да може вие да живеете спокойно. Тук и сега.

За повече информация:
тел.: 02/ 930 90 50
факс: 02/ 987 91 67

Централно управление:
София 1000
ул. „Г. С. Раковски" N 99
email: insurance@hdi.bg

СИГУРНОСТ

Макроикономическата стабилност на България - гаранция за икономическа сигурност. 4

Съвременни решения за защита от пожар посредством водна мъгла. 9

ЗАЩИТА НА ИНФОРМАЦИЯТА

Какво е фишинг атака и как да се предпазим. 11

Защитата на лични данни. 14

НАЦИОНАЛНА СИГУРНОСТ

Сирийската кибер-война. 16



Мерки срещу финансиране на тероризма и пране на пари. **19**

Етапи на протичане на терористичната операция. 37

ОХРАНА

Секюрити обков. 28

Средства и устройства за оказване на първа помощ за телохранители и охранители. 44

БИЗНЕС

Смартфоните – пробиви и защита. **30**





Защита на интелектуалната собственост. **34**

СПЕЦИАЛНИ СЛУЖБИ

Снайперските пушки - начин на употреба. 46

ХОБИ

Бенчрест 49

ОРЪЖИЕ

Снайперската винтовка ВССК “Выхлоп”. 50

Мнението на издателския екип не винаги съвпада с мненията на авторите.

PROFESSIONAL

Уважаеми читатели,

В настоящия брой на списание PROFESSIONAL обръщаме специално внимание на мерките срещу финансиране на тероризма и пране на пари в национален и световен мащаб. Не по-малко актуална е темата за употребата, пробивите в сигурността и защитата на смартфоните, които навлязоха в ежедневието ни и осигуряват голяма част от нашите комуникации. Нова за тематиката на списанието ни е защитата на интелектуалната собственост, като понятие и практика в страната. Наред с тези теми сме се опитали да намерим интересни и актуални въпроси, по които да предоставим различна гледна точка и да дадем полезни съвети. Ще се радваме да получим вашите въпроси и идеи за теми в предстоящите броеве на списанието.

ПОЖЕЛАВАМЕ ВИ ПРИЯТНО ЧЕТЕНЕ!

ПРОФИСЕК

ГЛАВЕН РЕДАКТОР - НИКОЛАЙ ЦАПРЕВ
ЗАМ. ГЛАВЕН РЕДАКТОР – АНАТОЛИЙ МЛАДЕНОВ
ОТГОВОРЕН РЕДАКТОР - МАРИЯНА НИКОЛОВА
ОФОРМЛЕНИЕ И ДИЗАЙН – НИКОЛАЙ ИВАНОВ
ПРЕДПЕЧАТНА ПОДГОТОВКА - НИКОЛАЙ ИВАНОВ
КОНСУЛТАНТ - ЦЕЦО ЛОЗАНОВ
ИЗДАТЕЛ - ПРОФИСЕК ЕООД
1407 СОФИЯ, УЛ. “БИГЛА” 16А, ЕТ. 4
TEL/FAX: +359 2 962 05 23, E-MAIL: INFO@PROFISEC.BG
WWW. PROFISEC.BG
photos: SXC, iStockphoto и Dreamstime
ТИРАЖ - 3000 БР.
PRINT - INART VISION

Автор: доц. д-р Антон Т. Маринов

МАКРОИКОНОМИЧЕСКАТА СТАБИЛНОСТ НА БЪЛГАРИЯ - ГАРАНЦИЯ ЗА ИКОНОМИЧЕСКА СИГУРНОСТ

Проблемите на макроикономическата стабилност и икономическата сигурност стават все по-актуални и са обект на изследване от много специалисти, но решаването им е трудно. Анализът на темата е много сложен, тъй като изследваните проблеми са твърде дискусионни, непредвидими и силно динамични. Това налага непрекъснат анализ и търсене на нови начини за решаването им. Ако те не бъдат анализирани своевременно и не се предприемат адекватни и навременни мерки, ще се дестабилизира икономическата и социална сигурност на България.

Макроикономическа стабилност се постига чрез стабилност на цените, високо ниво на заетостта, положителен икономически растеж и външнотърговски баланс. Тези цели не могат да бъдат постигнати при отсъствие на икономическа сигурност, която е гарант за стабилното функциониране на икономиката.

Икономическата сигурност трябва да гарантира независимостта на националната икономика, нейната устойчивост и възможността за непрекъснато обновяване и самоусъвършенстване. Икономическата сигурност има двояко значение - от една страна се явява цел на икономическата политика, а от друга е най-важният елемент на националната сигурност на държавата. Не може да има национална сигурност в слаба и неефективна икономика, както и не може да има национална сигурност и ефективна икономика в едно общество, разкъсвано от социални конфликти.

Дълбоката криза в нашето общество през последните години значително усложнява решаването на проблемите, свързани с отразяването на заплахите за икономическата сигурност.



Макроикономическа стабилност и икономическа сигурност са едни от най-важните цели на икономическата политика и се намират в права корелационна зависимост помежду си.

Икономическата сигурност традиционно е считана за най-важната характеристика на икономиката, която определя нейната способност да се поддържат нормални условия на живот на населението, устойчиво предоставяне на ресурси за икономическо развитие и последователно прилагане на националните интереси. Тя има сложна вътрешна структура, съставена от три важни елемента:

1. Икономическа независимост - способност за контрол на националните ресурси, постигане на такова ниво на ефективност на производството и качеството на брутния вътрешен продукт (БВП), което да гарантира конкурентоспособността на националната икономика и да дава възможност за равноправно участие в световната търговия, вкл. сътрудничество и обмен на научни и технически постижения.

2. Стабилност на националната икономика - защита на собствеността във всичките й форми, създавайки надеждни условия и гаранции за стопанска дейност и контрол на факторите, които могат да дестабилизират икономиката.

3. Способност за самостоятелно развитие и икономически растеж на националната икономика - благоприятен климат за инвестиции и иновации, постоянна модернизация на производството, подобряване на професионалното, образователното и културното равнище на населението и т.н..

Сред показателите за икономическа сигурност могат да бъдат идентифицирани:

- икономически растеж - динамиката и структурата на националното производство и националния доход, отраслова структура на икономиката и динамиката на отделните сектори, инвестиции и т.н.;
- характеристика на природни ресурси, промишления и научно-техническия потенциал на страната;
- характеристика на националната икономика и зависимостта й от външни фактори - инфлация, бюджетен дефицит, влияние на външни икономически фактори, стабилност на националната валута, вътрешния и външния дълг и т.н.;
- качеството на живот - БВП на глава от населението, ниво на неравенството в доходите, предоставяне на стоки и услуги на населението от държавата, брой на икономически активното население, опазване на околната среда и т.н.

За икономическата сигурност сами по себе си отделните икономически показатели, както и техните стойности нямат значение, а значение има тяхното отражение върху икономиката. Например във връзка с вътрешните заплахи такива показатели са: нивото на безработицата, разликата в доходите между най-богатите и най-бедните, темпа на инфлация и т.н.

По отношение на външните заплахи като индикатори могат да се определят: максимално допустим размер на

държавния дълг, положителен или отрицателен външнотърговски баланс, зависимостта на националната икономика от вноса на чужди технологии, компоненти или суровини и т.н.

Критерият за икономическа сигурност е възможността на националната икономика за справяне със заплахите в условията на критични ситуации.

Макроикономическата стабилност има за цел устойчивост на икономиката - стабилност на цените, високо ниво на заетостта, положителен икономически растеж и външнотърговски баланс:

- стабилност на цените - недопускане на увеличаването на цените с над 2-3% годишно (общото ниво на цените). Повишаването на качеството на стоките и вдигането на цената не се отчита като увеличение!;
- високо ниво на заетостта - поддържане на естествено равнище на безработица (3-6%);
- икономически растеж - препоръчително увеличение на БВП с 3-4% годишно при нормални условия, а след криза 6-10%. Това е най-важната задача, а постигането й ще е успех за икономическата политика на всяка страна;
- външнотърговски баланс - поддържане на положително салдо във външната търговия.



За постигане на икономическа сигурност е необходимо изготвяне и въвеждане на времеви план за постигане на целите й, които в по-голямата си част съвпадат с тези на макроикономическата стабилност.

Националната ни икономика не беше пощадена от световната икономическа криза. Тя навлезе в България през експортно ориентираните производства. За периода 2005-2010 година се забелязват преобладаващи положителни стойности на макроикономическите показатели до 2008 г. Стабилният положителен тренд за развитие на икономиката се обърна и тя изпадна в криза. В периода на кризата настъпи и политическа смяна от ляво към дясноцентристко политическо управление. Негативните тенденции при макроиконмическите показатели се запазиха.

При анализа на БВП към края на 2010 г. се забелязва бавен ръст в следствие на възстановяване на икономиките на някои държави-членки от ЕС, които са преобладаващите търговски партньори на България. Ръстът на икономиката отново дойде от експортно ориентираните предприятия от индустриалният сектор, който произвежда около една трета от цялата добавена стойност в България. През втората половина на 2010 годината се наблюдава ръст, достигайки 33,4% в края на същата година, който надминава по стойност предкризисната 2007 г. - 32.3%. Най-силно е свиването му през 2009 г. с 2%, докато при другите два сектора на услуги и земеделие е сравнително по-малко.

Показателят „брутен вътрешен продукт на отработен час" е предназначен да даде общ израз на производителността на националната икономика и на нейната конкурентоспособност. Производителността на труда е важен измерител за достигнатото икономическо равнище. За периода 2005-2010 г. производителността на труда на отработен час нараства средногодишно с 3,0%, като най-висок темп на растеж се наблюдава през 2010 година - около 8 %.

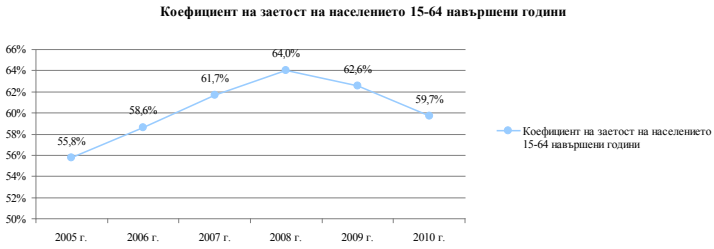
Инвестициите - този показател определя дела на инвестициите в общото производство. Придобиването на капиталови блага определя до голяма степен бъдещото икономическо развитие на държавата, тъй като се увеличават капиталовите запаси както на физическия, така и на човешкия капитал. За периода 2005-2008 г. делът на инвестициите в БВП показва непрекъснато увеличение: от 29,2% през 2005 г. до 46.4% през 2007 година, след което се наблюдава намаление на инвестициите в БВП, като през 2009 г. техният дял е 31,1%, а през 2010 г. е 24,2%. Средният дял на инвестициите в БВП за периода 2005-2010 г. е 34,6%. Повечето инвестиции по време на т. нар. „висок период" са привлечени от секторите „Строителство", „Финанси и търговия", като съществен превес имат недвижимите имоти и строителството. Въпреки значителното свиване на тези сектори, най-големи източници на инвестиции през 2010 г. остават страни от Еврозоната като Холандия, Белгия, Кипър, Гърция и Германия.

Заетостта е също важен показател, който има отношение както към икономическото развитие, така и към качеството на живота и социалното включване, които са сред основните цели на икономическата сигурност. След продължително нарастване на заетостта в България през периода 2005-2008 г., от 2009 г., нейното равнище започва да намалява, като през 2010 г. коефициентът на заетост достига 59,7%, или с 4,3 пункта е по-малък от този през 2008 година. През първото тримесечие на 2011 г. коефициентът на заетост е спаднал още и е 57,3%, а за второто тримесечие на същата година се забелязва леко покачване достигайки 58,2% или 2895,5 хил. души. По този показател през 2010 г. България отстъпва с 4,5 пункта от средната стойност за Европейския съюз. В периода 2009-2010 г. се забелязва намаляване на различието между коефициентите на заетост при мъжете и жените, поради спад в заетостта при мъжете. През 2010 г. коефициентът на заетост на мъжете достига 63,0%, а на жените - 56,4%, като през 2008 година разликата е 9,0 пункта. Намалението на заетостта след 2008 г. се отнася за всички възрастови групи, но в най-голяма степен са засегнати лицата на възраст 25-34 години. През 2010 г. коефициентът на заетост за тази възрастова група е 70,7% и е със 7,5 пункта по-малък от този през 2008 година. Коефициентът на заетост се различава значително според степента на завършеното образование. През 2010 г. заети са 83,8% от

лицата с висше образование на възраст 25-64 навършени години, докато за лицата на същата възраст, завършили основно или по-ниско образование, този дял е два пъти по-нисък - 41.2% - графики 4 и 5.



Заетост за периода 2005-2010 г. - абсолютен брой



Заетост за периода 2005-2010 г. - в проценти

Нормата на безработица е един от основните показатели за икономическата сигурност, тъй като липсата на заетост е сред главните причини за бедност и социално изключване. Анализирайки пазара на труда за изследвания период става ясно, че през 2008 г. тенденцията за намаляване се обръща и започва да се покачва. През 2008 г. безработицата в България достига най-ниското си равнище за последните 15 години - 5,7%, като през следващата година тя започва да се покачва и през 2010 г. коефициентът на безработица достига 10,3%, като за второто тримесечие на 2011 г. вече е 11,2% или около 370 хиляди души с тенденция за покачване. Анализирайки данните за месечната норма на безработица става ясно, че още през 2008 г. пазарът на труда започва да отразява кризисните импулси. Увеличението на безработицата през последните две години е по-голямо при мъжете в сравнение с жените - коефициентът на безработица при мъжете нараства от 5,5% през 2008 г. на 10,9% през 2010 г., а на жените - съответно от 5,8 на 9,5%, което се потвърждава и от данните за заетостта. Въпреки че от 2009 г. коефициентът на безработица в България започва да расте, през същата година той е с 2,1 пункта по-нисък от средния за ЕС-27, докато през август 2011 г. тенденцията вече е обратна - безработицата в ЕС е достигнала 9,5%, а в България е сред страните с най-голямо повишение - 11,7% . През периода 2005-2010 г. коефициентът на младежка безработица (15-24 години) отбелязва най-големи изменения в сравнение с останалите възрастови групи. През 2008 г. той достига най-ниското си равнище - 12,7%, или с 10,5 пункта по-малко в сравнение с 2010 г., където се покачва до застрашителните 23,2%. Увеличението на безработицата засяга най-съществено хората с по-ниско образование. През 2010 г. коефициентът на безработица за лицата с основно или по-ниско образование на възраст 25-64 навършени години е 21,7%, за завършилите средно образование е 8,3%, а за лицата с висше образование - 4,3%.

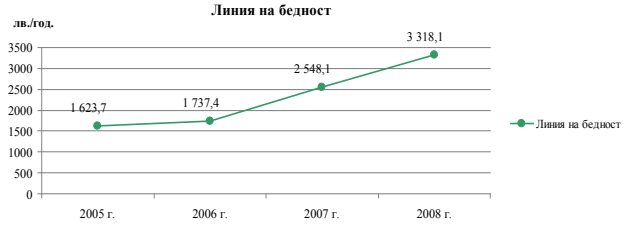
Кризата продължава да оказва сериозно влияние върху благосъстоянието на домакинствата, т.е. това е нейната социална цена. Ниските трудови доходи и свитото кредитиране намаляват потреблението, увеличават задлъжнялостта и лошите кредити. Наблюдаваната смяна на посоката към консервативна кредитна политика е фактор, който няма да позволи на домакинствата да достигнат равнищата на потребление от преди кризисния период през следващите 2-3 години, като същевременно задлъжнялостта им нараства.

Неравенство в разпределението на доходите S80/20 оценява ефектът от провежданата социална политика по отношение на бедните слоеве от населението. В България доходите се разпределят твърде неравномерно - 20% от най-богатите хора получават 6 пъти повече от 20-те процента от най-бедните в страната. През периода 2005-2008 г. не се наблюдават съществени изменения в поляризацията на населението. Това може да се обясни с обстоятелството, че линията на бедност постоянно нараства, а равнището на бедност почти се запазва за периода при равни други условия. С други думи, наблюдава се повишаване на доходите както на богатите, така и на бедните слоеве от населението, а съотношението между тях приблизително се запазва.

При анализа на доходите на населението и линията на бедността се забелязва, че разликата между тях се свива през годините на изследвания период, което означава, че има общо обедняване на населението, и още по-висок ръст на бедността през последните години, както и появата на феномена „работещи бедняци" - графики 9, 10 и 11.



Годишен доход на лице за периода 2005-2010 г.



Линия на бедност за периода 2005-2008 г.



Равнище на бедност за периода 2005-2008 г.

Най-големият дял бедни се състои от тези останали без работа, което поставя сериозни предизвикателства пред цялостното благосъстояние на страната. При анализа на структурата на доходите в страната става ясно, че тенденцията за нарастване на трудовите възнаграждения като част от всички доходи е изключително слаба, за сметка на доходите от пенсии, което е алогично и води в бъдеще до заплахи за икономическата сигурност и пенсионната система. Тенденцията от предходния анализ е, че делът на заетите намалява, а се увеличава делът на безработните и пенсионерите. Прогнозите на демографската статистика в бъдеще са за постоянно нарастване на населението в надтрудоспособна и намаляващо в трудоспособна възраст. Обедняването, от друга страна, оказва сериозен натиск върху демографския ръст и не благоприятства възпроизводствените процеси в обществото, като допълнително натоварва пенсионната система, водейки до нейната бъдеща задлъжнялост и фалит.

Ефектът от икономическата криза оказа положително влияние върху темповете на инфлация в България, които обаче отново са по-високи спрямо изискванията на Маастрихтските критерии с от 8% до 1,4 % през различните години на изследвания период. Освен, че тя нараства повече от доходите и влошава благосъстоянието на домакинствата, високите цени се отразяват и на размера на лихвения процент по кредитите, тъй като оказват влияние върху рисковата премия в страната. В условията на валутен борд Българската народна банка (БНБ) не разполага с инструментариум за определяне на основния лихвен процент (ОЛП), т.е. не може да влияе върху темповете на инфлация. В такъв случай съществува реална опасност от стагфлация, при положение че инфлацията продължи да расте в съчетание със спад на БВП, което може да предизвика поредната заплаха пред икономическата сигурност. Ръстът на реалния доход е единствения ефективен подход за преодоляването на тази тенденция.

България отчита стабилно намаляване на държавния дълг от 2005 г. до 2008 г., като продължава да поддържа нива от 14,6% за 2009 г. и 16,2% 2010 г., следвана само от Люксембург и Естония. За сравнение средната задлъжнялост на Европейския съюз (ЕС) през 2009 г. достига почти 80% и надхвърля Маастрихтските критерии с близо 20%. В резултат на следваната благоразумна фискална политика през последните години, и въпреки дефицитите от последните две, се очаква България да запази позицията си сред трите страни с най-нисък държавен дълг, оставайки в рамките до 20% от БВП в следващите две години. Въпреки, че България не бележи сериозни отклонения от референтните стойности по този показател, за разлика от други страни в Еврозоната като Гърция и Ирландия, индикаторите за фискалната дисциплина за изследвания период се влошиха, което доведе до отлагане присъединяването ни към „чакалнята" на Еврозоната.



Държавен дълг за периода 2005-2010 г.

За изследвания период бюджетният баланс на България показва идентична тенденция като повечето от анализираните макропоказатели - от излишък - 1,8% от БВП в края на 2008 г. достигна до 3,9% дефицит през 2009 г. и лекото му намаляване до 3,6% (дефицит) в края на 2010 г. като следствие на рестриктивната политика на правителството. Излизайки извън параметрите на критериите за фискална стабилност, България отложи влизането си в чакалнята на Валутно-курсовия механизъм II



Бюджетен баланс за периода 2007-2010 г.

От анализа на данните на търговския ни баланс се вижда подобрение и свиване на търговския дефицит от 12,315 милр. лева през 2008 г. на 3,919 милр. лева през 2010 г. Това подобрение на търговския баланс се изразява в стопяване на дефицита от 17,8% от БВП през 2008 г. до 5,7% през 2010 г., което се дължи на леко покачване на износа и силно свиване на вноса поради икономическата криза.

При анализа на сивата икономика се забелязва спад от 40,4% от БВП през 2006 г. до 37,5% през 2009 г. и лек ръст през 2010 г. - 37,7%, като покачването е резултат от рестриктивните мерки на правителството в следствие на икономическата криза. За изследвания период България си остава страна с голям дял на сивата икономика. Тя е трета от 37 страни след Латвия и Естония . Според друго национално изследване делът на сивата икономика според бизнеса за 2010 г. е 48,6%, докато населението посочва още по-висок дял - 58% . За изследвания период сивата икономика в държавите от Европа е на нива средно от 22%, като структура й е идентична в различните държави - графика 17.



Графика 17 Размер на сивата икономика за периода 2005-2010 г.



От една страна по време на криза сивата икономика може да служи като буфер и да носи ползи, а не само негативи, но от друга страна тя се явява заплаха за икономическата сигурност и развитието на страната ни. По тази причина сивата икономика трябва да се наблюдава и изследва непрекъснато, за да може да се контролира в допустими граници и да се провежда адекватна икономическа политика.

Кризата доказа факта, че спада на БВП води след себе си забавяне темпа на инфлация, но разликата между замразените доходи и растящите цени, може да доведе до по-нататъшно обедняване и диспропорции в сравнение с другите държави-членки на ЕС. Ефектът на ниската заетост съчетан с ниски доходи може само да затвърди позиционирането на страната ни измежду най-бедните в ЕС. Такива страни по дефиниция страдат до голяма степен от социална поляризация.

Друга тенденция е, че освен младите хора, нискоквалифицираните лица и малцинствените етнически групи са сериозно заплашени от безработица и изпадане под прага на бедност.

За да има макроикономическа стабилност и икономическа сигурност е необходимо да има нормативно обвързване на заплащането с производителността на труда и на пенсионната възраст с продължителността на живота, както и разумни публични финанси и балансиран валутен курс, които са от огромно значение за малка и отворена икономика като българската.

Целите на икономическата политика трябва да са насочени към висока производителност на труда, конкурентоспособна продукция, икономически растеж и повишаване благосъстоянието на населението.

Все пак, някои от правителствените мерки, насочени към пазара на труда и осигурителната тежест, наред с програми за квалификация и преквалификация на безработните лица, повлияха положително на трудовия пазар и бизнес климата в страната ни, но явно недостатъчно.

Един от възможните варианти за постигане на макроикономическа стабилност и икономическа сигурност е присъединяването ни към Еврозоната и Пакта за финансова стабилност, за което се изисква още работа за постигане на Маастрихтските критерии.

Забелязва се тенденция, че държавите-членки на ЕС стават много предпазливи и консервативни относно присъединяването към Еврозоната и Пакта за финансова стабилност на държави-членки от периферията на ЕС. От друга страна, те изтъкват и неикономическите си притеснения, свързани с организирана престъпност, сивата икономика, нива на корупция и др., отколкото неизпълнението на конвергентни критерии.

Друг вариант за постигане на макроикономическа стабилност и икономическа сигурност е да се изгради система от количествени макроикономически показатели (индикатори), които позволяват ранно предупреждение за приближаваща заплаха към националната икономика и предприемането на мерки за предотвратяването ѝ.

При определяне на стойностите на макроикономическите показатели задължително трябва се взимат под внимание:

- максимално допустимото ниво на спад в икономическата дейност;
- максимално допустимото намаление на нивото на качеството на живот на населението като цяло;
- максимално допустимото ниво на спестяване на разходи за поддържане и възпроизвеждане на природните ресурси, отвъд което има риск от необратимо унищожаване на елементи на околната среда.

Най-висока степен на икономическа сигурност би се постигнала, ако пълният набор от показатели е в рамките на допустимите граници и подържането на нивото на един индикатор не е за сметка на другите.

Липсата на икономическа сигурност в националната икономика води до: загуба на способностите ѝ за динамично и самостоятелно развитие, конкурентоспособност на външните и вътрешния пазари, експанзия на чуждестранни и транснационални компании, появяват се социални язви като корупция и престъпност, кражба на национално богатство и др.

За постигането на макроикономическа стабилност и икономическа сигурност няма универсални рецепти. В една държава определена група мерки може да имат ефект, но другаде да нямат, така, че трябва да се подхожда индивидуално.

Не винаги предписаните мерки дават желаните резултати поради причини свързани със заобикалящата среда, което налага да се анализират непрекъснато и да се търсят нови решения на възникналите проблеми, за да могат те да бъдат решени.

От настоящия анализ можем да направим два основни извода:

1. Икономическата сигурност на страната следва да гарантира на първо място ефективност на икономиката, т.е. тя трябва да се защитава въз основа на висока производителност, качество на продукта и т.н.

2. Икономическата сигурност на държавата трябва да се регулира и поддържа от цялата система на държавните институции, както и от всички структури на икономиката.

Всичко това налага изграждането на ефективна стратегия за икономическо развитие с устойчиво нарастване на БВП, постигане на пълна заетост, отсъствие на инфлация и справедливо разпределение на доходите. Осигуряването на макроикономическа стабилност и икономическа сигурност е гаранция за независимостта на страната, условие за стабилност, икономическа ефективност и повишено благосъстояние. Те трябва да са национален приоритет номер едно. Това е цел, към която се стремят всички правителства по света.

СЪВРЕМЕННИ РЕШЕНИЯ ЗА ЗАЩИТА ОТ ПОЖАР ПОСРЕДСТВОМ ВОДНА МЪГЛА

Синхрон-С, специализирана в проектиране и изграждане на противопожарни системи, предлага надеждни решения за защита от пожар, които са успешно приложими както в помещения с присъствие на хора, така и в промишлени обекти с наличие на сложно производствено оборудване. Решенията са базирани на иновативния метод за потушаване и контролиране на пожари посредством инсталации с водна мъгла.

Интелигентно използване на водата като гасителен агент

Основната характеристика на водата като гасителен агент, върху която се базира механизма на пожарогасене при традиционните спринклерни системи е охлаждащият ефект, който се получава в резултат на абсорбираната енергия от огъня. Водната мъгла използва същия метод, но благодарение на преобразуването на водата в пара, охлаждащият ефект е седем пъти по-голям, а консумацията на вода може да бъде намалена с 90% спрямо обикновените спринклерни системи.

Вместо изпускането на вода върху пожара, системите с водна мъгла въздействат чрез голямо количество пара. Те разпръскват водата във вид на водна мъгла, съдържаща капки с микроразмери и могат да произведат около 8 000 капки със същото количество вода, което типичните спринклерни системи биха използвали, за да произведат една единствена капка. Това многократно увеличава повърхностната площ на водата и е причина за големия охлаждащ ефект и бързото отнемане на кислорода от горивния процес. Това прави системите с водна мъгла едни от най-ефективните съществуващи противопожарни системи, базирани на гасителния агент вода.

Принцип на работа на системите с водна мъгла

Системите с водна мъгла атакуват пожара по три начина: охлаждане, отнемане на кислорода („задушаващ” ефект) и блокиране на топлопредаването към съседните запалими предмети. В режим на изчакване системата поддържа налягане от около 20 бара. Когато температурата надвиши предварително зададена стойност, чувствителният на топлина елемент в спринклерната глава се стопява. В този момент се активира автоматично помпена система, водата се придвижва от резервоар до колектор с високо налягане, откъдето се разпределя до съответните секции посредством селекторни вентили. Разпръскването на водата става през микродюзи под високо налягане (около 120 бара), благодарение на което се образува водна мъгла. Активират се само дюзите със стопени ампули, което означава, че системата се задейства само над зоната с повишена температура. Водната мъгла обгръща цялата рискова зона и тъй като е отличен охлаждащ агент настъпва бързо отнемане на топлинната енергия на горивния процес. Това понижава температурата в огнището на пожара и също така блокира топлопредаването, като по този начин топлината не уврежда предметите, намиращи се в близост до източника на пожар. Отделно от това топлината преобразува водната мъгла в пара, която заема 1700 пъти повече обем. Парата буквално „изсмуква” кислорода от помещението и „задушава“пожара. По-нататъшно повторно запалване е невъзможно.

Ефективно решение за защита от пожари клас A, B и C

Уникалността на системите с водна мъгла е комбинирането на гасителния ефект при газовите и конвенционалните спринклерни системи. Те съчетават предимствата на двата типа системи и същевременно избягват недостатъците им. Затова системите с водна мъгла са успешно приложими, както в обществени сгради с присъствие на хора, така и в производствени обекти. Те са напълно безвредни за хората и с много по-голяма безопасност за сградата, имуществото и оборудването.

Системите с водна мъгла често са предпочитани в зони, където трябва да се избегнат щети вследствие на водата като гасителен агент. Тъй като системите с водна мъгла използват много по-малко количество вода и в много по-ниска концентрация в сравнение с конвенционалните спринклерни системи, много малка е вероятността да причинят повреда в сложното електрическо и електронно оборудване. В промишлени условия значителната редукция на щетите от изпускане на гасителния агент е от голямо значение, тъй като те могат да бъдат по-опасни отколкото щетите причинени от пожара. Много важно е също така производството да бъде възстановено бързо. Дълъг период на прекъсване на работата означава голям риск от загуба на пазари, което често води до дългосрочен негативен икономически ефект, надхвърлящ загубите от самия пожар. Опитът показва, че само 4 от 10 предприятия успяват да стартират производството си отново след голям пожар.

Системите с водна мъгла са особено ценни за архитектурни и исторически сгради, библиотеки или архиви, чието ценно и уникално имущество не е устойчиво на гасителни агенти, като вода или синтетични газове. Водната мъгла е толкова фина, че не причинява щети на имуществото. Тя е ефективно решение и за защита от пожар в тежки производствени условия с голям риск от възникване на пожар, каквито са леярските цехове. Въпреки, че парата охлажда помещението много по-бързо, вероятността да се получи термичен шок за разтопения метал е минимална, за разлика от изсипването „като из ведро” на студена вода, характерно за обикновените спринклери.

При противопожарната защита на високи сгради, системите с водна мъгла също предлагат няколко предимства. Инсталациите са с малък размер, не изискват голямо пространство за разполагането им и могат да бъдат интегрирани в сложни и тесни конструкции. Също така отличните охлаждащи характеристики ги правят идеални за защита на стъклени фасади. Триизмерният охлаждащ ефект премахва риска от термичен шок и счупване, което може да се получи при конвенционалните спринклерни системи. Други възможности, които могат да бъдат реализирани със системите с водна мъгла, които често са и единственото решение за противопожарна защита са пътни тунели, кабелни канали, шахти, роторни турбини, трансформаторни подстанции и др.

Освен изброените технологични предимства, много важно за успешната работа на системите е професионалното изпълнение и взаимодействието на всеки един етап от реализирането им. Задълбоченият анализ на проектните изисквания, правилната оценка на риска, качественото проектиране, монтиране и поддържане на системите, както и отговорното отношение към обучението на обслужващия персонал са критично важни за правилното действие на системите. Прилагайки този метод на работа, фирма Синхрон-С има успешно реализирани проекти с водна мъгла, сред които е рудодобивното предприятие Асарел Медет. Фирмата е първата и единствената в страната, сертифицирана за изграждане на системи с водна мъгла. Решенията на компанията отговарят на най-високите изисквания на стандартите, приети в тази област.

Защита на Живота и Имуществото

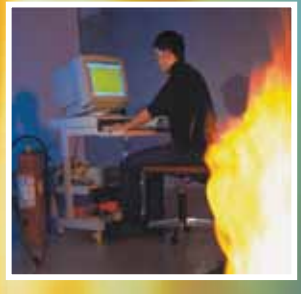












® СИНХРОН С ООД

ПОЖАРНА БЕЗОПАСНОСТ

ПРОЕКТИРАНЕ • УЗАКОНЯВАНЕ • ИЗГРАЖДАНЕ

- СПРИНКЛЕРНИ ПОЖАРОГАСИТЕЛНИ СИСТЕМИ
- СИСТЕМИ ЗА ПОЖАРОГАСЕНЕ С ВОДНА МЪГЛА
- СИСТЕМИ ЗА ПОЖАРОГАСЕНЕ С ПРАХ И ПЯНА
- СИСТЕМИ ЗА ПОЖАРОГАСЕНЕ С ГАЗ
- СИСТЕМИ ЗА ПРЕВЕНЦИЯ ЧРЕЗ РЕДУКЦИЯ НА O_2
- СИСТЕМИ ЗА ПОЖАРОИЗВЕСТЯВАНЕ







Партньори:
SIEMENS, LPG, Rolland, Tyco

СИНХРОН-С ООД: България, София 1504 , ул. Кракра 19А
Тел.: (02) 944 14 04, Моб. тел.: 0884 852 708, Факс: (02) 946 12 15
E-mail: synchron-s@synchron-s.com, Website: www.synchron-s.com

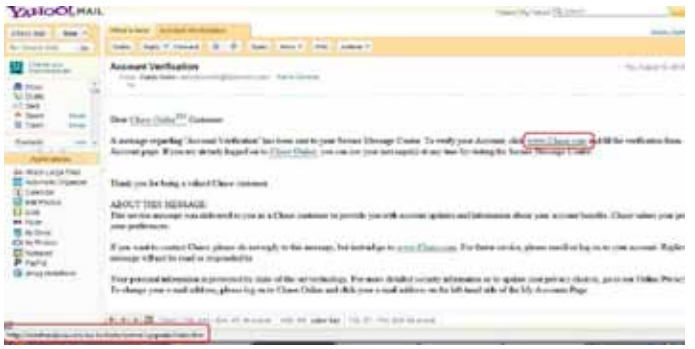
Автор: Огнян Глушков, www.safety.bg

КАКВО Е ФИШИНГ АТАКА И КАК ДА СЕ ПРЕДПАЗИМ

Фишинг атаките са най-разпространената форма на интернет измама. По всяко време много от най-главните финансови институции по света са цел на подобни измами. Фишинг атаките целят да подмамят хората да предоставят важна лична информация, най-често подробности по кредитни карти и банкови сметки.

Как работят фишинг атаките?

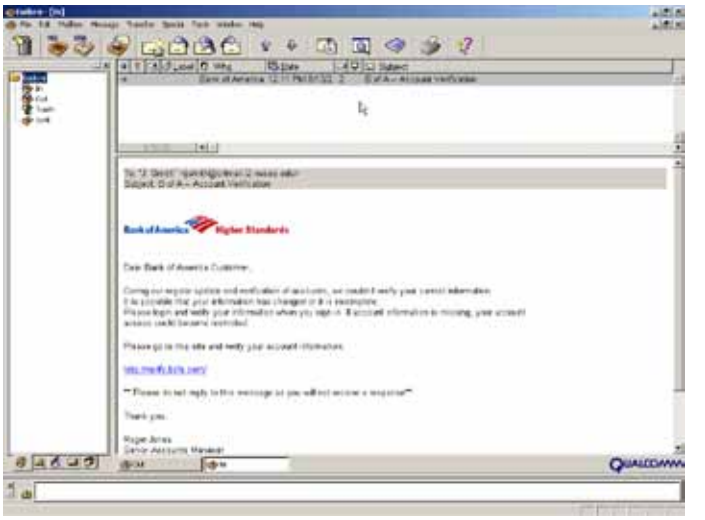
За да успеят да убедят хората да предоставят финансовата си информация, измамниците изпращат имейл, който е пълно копие на имейлите на избраната компания. Най-често измамниците създават и подобен уебсайт. Фалшивият сайт може да бъде почти идентичен с този на компанията.



Получателите на този имейл, са помолени да отворят даден хиперлинк, който отваря фалшивия уебсайт. След това от потърпевшите се иска да въведат лична информация (най-често данни от банкова сметка, адрес и телефон). Често се изисква и въвеждане на данните им за вход в оригиналния сайт. Въведената във фалшивия сайт информация се запазва и измамниците могат да я използват.

Друг вариант на измамата е подобна форма за въвеждане на информация, в самия имейл. Потърпевшите са помолени да въведат потребителското си име и парола, както и номера на банковата им сметка. Възможно е измамниците да се опитат да ви подлъжат да свалите троянски кон на компютъра си, от приложение в имейла. След това този вирус събира и изпраща личната ви информация на престъпниците.

Подобни имейли се изпращат на голям брой потребители, като измамниците се надяват да подлъжат малка част от потърпевшите. Най-вероятно получателя дори няма да бъде клиент на избраната от престъпниците институция. Въпреки това те се надяват, че поне малък брой хора ще имат сметки в нея и няма да са запознати с подобни измами.



Този вид измама е много изгоден за престъпниците, дори и много малък процент получатели да станат жертви.

Как измамниците използват събраната информация?

Престъпниците могат да използват събраната информация по няколко начина:

Кражба на банкова сметка

След като са събрали нужната информация, измамниците могат директно да имат достъп до банковата сметка на потърпевшия. След това могат да извършват транзакции, да пренасочват средства към други сметки и да издават чекове. Най-често престъпниците сменят паролата, за да не може потърпевшия да влезе в сметката си.

Използване на кредитни карти



Ако измамниците са откраднали информация за кредитна карта, те могат да плащат стоки за сметка на собственика на картата.

Кражба на самоличността

Ако престъпниците са събрали достатъчно лична информация, могат напълно да откраднат самоличността на потърпевшия. След това могат да извършват криминални дела от името на пострадалия. Кражбата на самоличността може да има дългосрочни последици. Понякога на потърпевшите са необходими години да изчистят името си, разрешат възникналите правни проблеми и да изплатят дълговете си.

Общи характеристики на фишинг измамите:

Нежелани искания за лична инфорамция.

Смисълът на фишинг атаките е потребителя сам да предостави личната си информация. Ако получите имейл от банка или друга институция, която иска да отворите страница и да въведете лична информация, подходете със силно подозрение. Банките НИКОГА не искат лична информация и информация за сметките ви по този начин.

Съдържанието изглежда правдоподобно.

Фишинг измамите са създадени да правят илюзията, че са изпратени от истинска институция. Имейлите могат да съдържат идентично лого и стил, като истинската компания. За да се засили усещането за истинност дори някои от хиперлинковете в имейла водят до истинската страница на институцията. Но този, който води към формата за попълване на информация, препраща към фалшивият уебсайт.

Маскирани хиперлинкове и изпращач.

Линковете във фишинг измамите са маскирани, така че да изглежда все едно препращат към сайта на реалната организация. Адреса на изпращача също изглежда, че идва от домейна на институцията.

Имейлът се състои от картинка, която е хиперлинк.

Някой измамни имейли представляват картинка. Лошото е, че където и по нея да цъкнете, ще бъдете препратени към фалшивия уебсайт.

Общи поздрави.

Понеже се изпращат до много хора, измамните имейли съдържат общи поздрави („Скъпи клиент на …", „Скъпи картодържател" и тн.). Ако някоя институция имаше нужда да се свърже със свой клиент за потвърждаване на подобна информация, най-вероятно щеше да се обърне към него поименно, но както вече споменахме финансовите компании никога не се свързват по този начин с клиентите си.

Многобройни уловки, насърчаващи получателя да предприеме действие.

Във фишинг имейлите е обяснено, че е необходимо потребителят да въведе личната си информация. Екипът на SAFETY.BG е изготвил списък на най-честите уловки, използвани в такива имейли:

Акаунтът на потребителя трябва да бъде потвърден, заради обновяване в системата за сигурност.

Акаунтът на потребителя може да бъде спрян, ако личната информация не е въведена за определено време.

Засечена е подозрителна активност с акаунта на потребителя и той трябва спешно да предостави информацията.

Рутинни процедури за сигурност изискват потребителя да потвърди личната си информация.

Какво да правите, ако получите подобен е-мейл?

- НЕ отваряйте хиперлинковете в съдържанието.
- НЕ предоставяйте лична информация.
- НЕ отговаряйте на имейла и не опитвайте да осъществите контакт с изпращача.
- НЕ въвеждайте информация в фалшивия уебсайт, ако той се е отворил.
- НЕ отваряйте прикачени в имейла файлове.
- Изтрийте имейла.

Какво да правите, ако вече сте били подмамен да въведете лична информация?

Ако вече сте предоставили личната си информация на измамниците, трябва незабавно да се свържете с институцията, от чието име е изпратен имейлът. Важно е да действате бързо, за да запазите банковите си сметки и лична информация. Обадете се на полицията.

Как да се предпазите от фишинг атаки?

Ако имате съмнения относно имейл, изпратен от някоя институция, свържете се директно с нея за потвърждение.

Не кликайте върху линкове в подозрителни имейли. Най-добре ръчно въведете адреса на институцията.

Ако предоставяте лична информация, се убедете че уебсайта е сигурен.

Използвайте антивирусен софтуер.

Обновявайте браузера и операционната си система редовно.

ЛЕМА ТРЕЙДИНГ

ТЕЛЕКОМУНИКАЦИОНЕН ИНЖЕНЕРИНГ

Структурно-кабелни системи
Телефонни централи и мрежи
Сигнално-охранителни системи
Системи за контрол на достъпа
Системи за видеонаблюдение
Пожаро-известителни системи
Спътникови системи и приложения
Интеграция на мрежи за глас, данни и видео
Безжични мрежи и приложения









www.lematrading-bg.com

Автор: инж. Румен Добрев

ЗАЩИТАТА НА ЛИЧНИ ДАННИ

Хартата на основните права на гражданите в Европейския съюз е изработена в периода декември 1999 – октомври 2000 от конвент[1], състоящ се от 62 члена. Тя е необвързваща и няма правна сила, а само препоръчителен характер. Макар да няма задължителен характер, Хартата очертава общата воля на гражданите на ЕС да бъдат гарантирани много по-широк кръг от права освен тези, заложени в Европейската конвенция за правата на човека и основните свободи.

Хартата е включена в Договора за създаване на конституция за Европа (вторият дял на Конституцията). Ако договорът бъде ратифициран, това ще придаде на Хартата задължителен характер. Тогава нейното прилагане би било задължително, както за институциите, органите и агенциите на Съюза, така и за държавите-членки, в случаите, когато прилагат Европейското законодателство.

Хартата представлява своеобразен "каталог на правата", където за първи път в един текст са обединени гражданските, политическите, икономическите и социалните права. Тя се състои от преамбюл и 7 части, в които отделните права са обединени по теми – всяка от частите има свое "заглавие" (тема):

Част I - Достойнство

Част II - Свободи

Част III - Равенство

Част IV - Солидарност

Част V - Граждански права

Част VI - Правосъдие

Част VII - Общи разпоредби при тълкуването и прилагането на хартата

Хартата включва граждански и политически права, които са защитени от Европейската конвенция за правата на човека и основните свободи, но редом с тях са включени и допълнителни области, като:

- социални права на работниците;
- защита на околната среда;
- право на добро управление;
- защита на личните данни;
- биоетика и др.

Защита на личните данни

Директива 95/46/ЕО на Европейския парламент и на Съвета на Европа от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни е основният документ, регламентиращ правилата в тази област. Тя въвежда подзаконова уредба, която цели да установи баланс между високата степен на защита на личния живот на физическите лица и свободното движение на лични данни в Европейския съюз (ЕС). За тази цел, директивата определя стриктни ограничения при събирането и използването на лични данни и изисква във всяка държава-членка да бъде създаден независим национален орган, който да отговаря за защитата на личните данни.

Директивата се прилага към данните, обработвани



чрез автоматизирани средства (напр. компютърна база данни на клиенти), както и към данните, които са включени или които ще бъдат включени в неавтоматизирано досие (традиционни хартиени досиета), а не се прилага към обработването на данни от физическо лице при упражняването на изключително лични или домашни дейности или при упражняването на дейности, които не влизат в приложното поле на общностното право, като обществената сигурност, отбраната и държавната сигурност.

Директивата цели да защити правата и свободите на физическите лица, доколкото се отнася до обработването на лични данни, като установява ръководни принципи за законосъобразност на операциите по обработването. Тези принципи се отнасят до:

- качеството на данните: личните данни трябва по-специално да бъдат обработвани по справедлив и законосъобразен начин и да се събират за определени, ясни и законни цели. Освен това те трябва да бъдат точни и ако е необходимо, да се актуализират;

- узаконяване на операциите по обработване на данни: обработването на лични данни може да се извършва само ако съответното физическо лице е дало недвусмислено своето съгласие за това или обработването на данни е необходимо:

- за изпълнението на договор, по който съответното физическо лице е страна; или

- за спазването на правно задължение, чийто субект е администраторът; или

- за да бъдат защитени жизненоважни интереси на

съответното физическо лице; или

о за изпълнението на задача, която се осъществява в обществен интерес; или

о за целите на законните интереси, преследвани от администратора;

При използване на лични данни е необходимо:

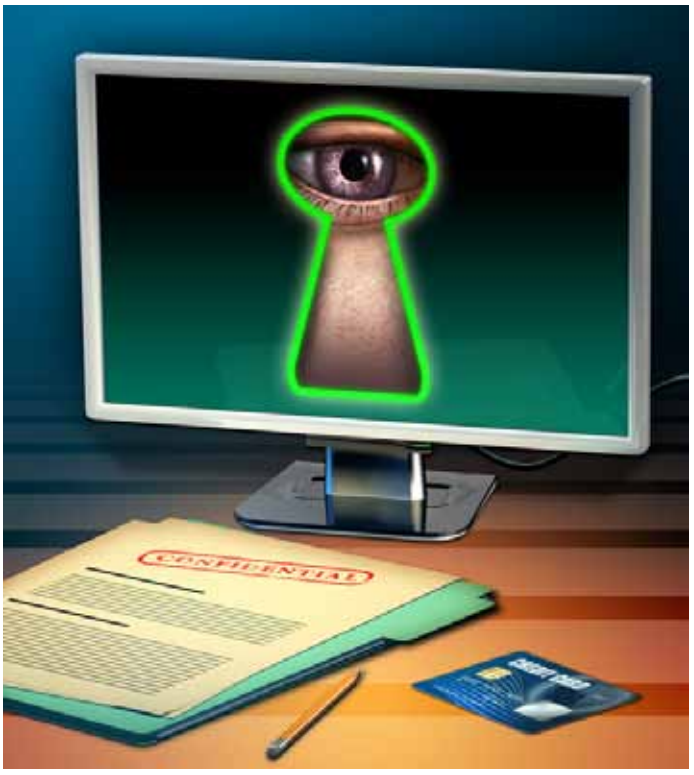
о прилагане на специални категории обработване, т.е трябва да се забрани обработването на лични данни, разкриващи расов или етнически произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи, както и обработването на данни, свързани със здравословното състояние и половия живот. Тази разпоредба не се прилага, например когато обработването на данни е необходимо за защита на жизнените интереси на съответното физическо лице или за целите на профилактичната медицина и поставянето на медицинска диагноза;

о информирането на физическите лица, засегнати от обработването на данни: някои видове сведения (самоличността на администратора, целта на обработването, получателите на данни и пр.) трябва да бъдат предоставени от администратора на физическото лице, от което той събира данните, които го засягат;

о право на достъп на тези лица до данните: всяко засегнато лице трябва да има право да получи от администратора:

- потвърждение за това, дали отнасящи се до него данни се обработват и съобщение относно данните, които се обработват;
- поправяне, изтриване или блокиране на данни, чиято обработка не е в съответствие с разпоредбите на настоящата директива, и по-конкретно поради непълнота или неточност на самите данни - както и уведомяване за тези изменения на третите лица, на които са били съобщени данните;
- право на възражение при обработването на лични данни: съответното физическо лице трябва да има право на възражение, въз основа на законови основания във връзка с обработването на личните му данни. То също така трябва да може да възрази, с молба или безплатно, срещу обработването на личните данни, когато се очаква да бъдат обработени за целите на директен маркетинг. Най-накрая то трябва да бъде уведомено, преди личните данни да бъдат разкрити на трети страни, както и изрично да ползва правото на възражение срещу подобно разкриване;

За да се спазват поверителният характер и надеждност на обработването на лични данни е необходимо всяко лице, действащо под ръководството на администратора или на обработващия данни, включително самият обработващ, които имат достъп до тях, да ги обработват само по указание на администратора. От друга страна, администраторът задължително прилага подходящи мерки за защита на личните данни срещу случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп.



Всяко лице е необходимо да разполага с правна защита при нарушение на правата, гарантирани от националното право, приложимо към въпросната обработка. Освен това лицата, които са понесли вреди в резултат на неправомерна операция по обработка на личните им данни, имат право да получат обезщетение за понесените вреди.

Предаването на лични данни от държава-членка към трета държава е разрешено при подходяща степен на защита. В замяна на това то не може да бъде извършвано към трета страна, в която няма такова равнище на защита, освен при изрично изброени изключения.

Директивата предвижда разработването на национални и общностни кодекси за поведение, които имат за цел да допринесат за правилното прилагане на националните и общностни разпоредби. Всяка държава-членка предвижда на нейната територия един или повече независими държавни органи да отговарят за контрола на прилагането на разпоредбите, приети от държавите-членки, съгласно настоящата директива.

Как в България се защитават личните данни? Какво се случва с тях? Каква е правната рамка у нас и какви права имаме по отношение на личната си информация – четете в следващите броеве на списанието!

Автор: д-р, инж. Милен Иванов

СИРИЙСКАТА КИБЕР-ВОЙНА

Интернет е първата медия в историята, която поддържа групи и разговори по едно и също време. Докато телефонът дава на обществото платформата „един-към-един“, телевизиите, списанията, радиото, книгите дават платформата „един-към-много“, интернет създава платформата много-към-много. Като средство за комуникация и споделяне, интернет се оказва изключително мощна сила, която е изключително трудно да бъде контролирана.

Все по-често държави и корпорации се опитват да я обуздаят, да впрегнат потенциала й в рамките на сигурността и правните норми, които съществуват извън мрежата. Това обаче, се оказва непостижимо дори и за най-мощните организации на планетата, именно защото интернет е нещо повече от просто технология - това е култура.

Интернет има две основни характеристики. Едната е възможността хората да общуват свободно, а втората е възможността да се свържат с останалата част на света. Ако през 1996 г., първото надеждно в световен мащаб проучване на използването на Интернет преброява около шестнадесет милиона потребители, то днес има над петстотин милиона. В момента има около седем процента от общия брой на населението на планетата, свързани към интернет. Въпреки, че използването на интернет се разраства бързо, две трети от планетата все още ще бъде извън кибер пространството до края на това десетилетие. Това показва, че скоростта на дифузията е изключителна. В интернет, всеки носител на информация след като веднъж е преобразуван в цифрова форма може да бъде свързан, комбиниран и обединен с друга информация и така да се получи ново знание (вярно или манипулативно). Следователно, тя е единственото и най-важно средство, което може да оказва най-голямо въздействие на глобалното общество, след като толкова голям процент от населението на света има и ще има достъп до него.

Социалните медии са широко използвани по време на бунтовете в арабските страни през последните години, но все пак това не е еднопосочно предимство. Активистите успяват да насърчат създаването на глобална култура на онлайн действия и да накарат света да осъзнае силата на интернет. Блогъри и активисти се превръщат в национални герои. Те стават основен двигател за организиране на протести, лобиране от името на лишените от свобода и изпращане на новини към външния свят от страните, където достъпът на журналисти е ограничен. Бунтовете в арабските държави разчитат на две основни оръжия: решителността на протестиращите и ролята на отдушник на натрупаното напрежение в социалните медии. Ако се изследват тенденциите в социалните медии, може да се установи, че Сирия има безпрецедентно присъствие в тях от март 2011 г. насам.

Сирийската държава налага фактически монопол върху медиите след баасисткия военен преврат през 1963 г. Но сателитните телевизионни станции, както и появата на „Ал-Джазира” и последвалите на пан-арабски новинарски канали разбиват монопола на режима. Интернет също се очертава като безспорен източник на новини. Бунтът в Сирия върви ръка за ръка със социалните медии. Сирийското правителство също се възползва от силата на интернет, заедно с действията на армията на улиците, за да се справи с активистите-бунтовници. Сирийците използват няколко инструмента за достъп до сайтове на социални медии, като Facebook и YouTube, които са блокирани във вътрешността на страната. Тези инструменти, обаче, не позволяват проследяване на активисти, така че правителството на Ассад, в крайна сметка деблокира достъпа до двата портала. Скоро след това официалните държавни агенции започват да стартират Distributed Denial of Service (DDOS) - атаки от специално създадена фалшива страница във Facebook, за да откраднат пароли за достъп на опозиционните ак-



тивисти. Освен това, според данни на опозицията, силите за сигурност са използвани за изтезания срещу задържани противници на Ассад, за да получат пароли за техните Facebook и и-мейл акаунти. Сирия, освен това подкрепя мрежа от хакери, които създават Сирийската електронна армия (Syrian Electronic Army (SEA), която стартира атаки срещу сирийски опоненти и други обекти, включително и спрямо интернет-страницата на телевизия „Ал Джазира".



Сирийското правителство изгражда система за наблюдение през 2011 г., която е предназначена да контролира електронната поща и използването на интернет. Оборудването за наблюдение на тази система е произведено от Hewlett Packard Co. и NetApp Inc., и двете са базирани в САЩ компании. Оборудването на стойност повече от 7,2 милиона долара е продадено на Сирия, чрез базираната в Италия компания, наречена Area SpA. Германската Utimaco Safeware AG (САЩ) и регистрираната в Париж Qosmos SA също участват със свои технологии в проекта. Европейските санкции за забрана на износ на технологии срещу Сирия не успяват да попречат на тези продажби, тъй като те са приети през декември 2011 г. Освен това, Иран също помага на сирийския режим, като обучава държавните служители, ангажирани с извършването на контрол и наблюдение в кибернетичното пространство. Системата включва сондиране на трафика на мобилните телефонни компании и Интернет доставчиците (ISP), като се контролира както вътрешния, така и международния трафик. Системата позволява и създаване на база данни от архивиране на съобщения, която да подпомага бъдещи търсения или картографиране на контактите на хората.

Всяка от специалните служби на Сирия има действащ денонощно оперативен център, в който работят млади студенти в областта на информационните технологии. Тези студенти или доброволно стават офицери в сигурността, или се разпределят там, за да отслужат задължителната си военна служба от осемнадесет месеца. Тъй като държавните структури за сигурност задържат при операциите нови опозиционери и конфискуват компютрите им, задачата на IT- студентите е да сканират техните хард дискове, за да се възстанови изтрита информация и данни за онлайн банкови сметки.

Сирийската служба за сигурност на комуникациите, с кодово име „Branch 225", е основната структура, която взима решения по отношение на комуникационна сигурност в Сирия. Тя не само има пряк контакт с мобилните телефонни компании, интернет доставчиците и другите комуникационни компании, но също така и с дружествата за доставка на ток и вода. „Branch 225" е свързана и с телекомуникационната компания на Сирия Telecommunications Establishment (STE), която е основната структура за комуникации в страната и контролира всички доставчици на интернет услуги и стационарни телефони. STE има Оперативен център в квартал Muhajireen на Дамаск, който е пряко свързан с „Branch 225". От началото на бунта в Сирия, „Branch 225" затъмнява всички райони, в които правителствените сили започват да провеждат операции срещу бунтовниците, за да се прекъсне всякакъв контакт с външния свят. Тази служба действа главно от климатизирана стая в сградата на държавния телеком в Muhajireen, където е инсталирана система за наблюдение на Area SpA . Въпреки, че сирийското правителство отрича всякакви връзки със Сирийската електронна армия (SEA), беседи, извършени под прикритие с членове на SEA разкриват, че сирийското правителство наема членове на тази организация и други хакери, за да провеждат различни операции срещу опозицията.



На 27.09.2011 г. е от SEA е хакнат официалният уебсайт на Харвардския университет. Интернет страницата на университета е възстановена, но администраторите я снемат в продължение на няколко часа. Началната страница показва снимка на сирийския президент Башар Асад и съобщението „Сирийската електронна армия беше тук". Асад е във военна униформа и застанал пред сирийския флаг. Според говорителя на Харвард „Атаката на уебстраницата на университета е дело на изключително опитен индивид или група".

В началото на 2012 година започва истинска кибер война. Хакнат е личният и-мейл на сирийския президент. Преди това в операция, наречена #OpSyria, хакерската общност Anonymous се прицелва в сирийското кибернетично пространство. Първо те хакват уебсайта на сирийското министерство на отбраната, след това уебсайта на телевизионната мрежа на сирийското правителство и накрая цел на хакерите става сирийският президент Башар Ассад.

На 07.02.2012 г. е компрометирана про-правителствената мрежа за телевизионни новини на Сирия. Сирийската държавна телевизия съобщава, че е хакната системата за текстовите съобщения в новините.

Anonymous успяват да получат достъп и до 78 различни акаунта за електронна поща в сирийското президентство, включително и тази на ръководителя на президентската администрация Мансур Фадллалах Азам, и на президентския медиен съветник Боудиайна Схаабан. При тези атаки става ясно, че базовата компютърна сигурност е под всякаква критика, защото някои от акаунтите са били защитени с пароли от типа „12345“. Британският вестник „Гардиън“ събира 3000 имейли, които са били предадени на сирийската опозиция, които съдържат богата лична информация - включително семейни снимки и видеоклипове, сканиране на лична карта на президента и акт за раждане на член на семейството му – все неща, които трудно могат да се придобият или фалшифицират, дори и от най-добрите ресурси за фалшиви документи или разузнавателни агенции.



Акаунтите sam@alshahba.com и ak@alshahba.com, които според опозиционни активисти са били използвани от Башар Ассад и съпругата му Асма, са комуникирали и са се намирали в тясна връзка с широк кръг от хора, свързани със семейството и съветници, чийто и-мейл адреси лесно могат да бъдат проверени. Събитията и речите, посочени в тези и-мейли съвпадат с времената на реални събития. Акаунтите „sam“ и „ak“, които са били контролирани от опозиционните активисти, твърдят, че техните притежатели са реагирали в реално време на събитията случващи се в Сирия.

От друга страна експерти по сигурността се съмняват разпокъсаната опозиция в Сирия да има способността за достъп до електронна поща, без външна помощ, но други твърдят, че тези, които са на власт в Дамаск може просто да са били невнимателни. Сирийската опозиция твърди, че са придобили подробности за паролите от вътрешен за правителството източник, като този метод е по-вероятен.

Според в. “Гардиън“ има няколко имейл разговори, в които „sam“ и Башар са ясно идентифицирани като едно и също лице. През ноември 2011 г. например, Хадеел Ал-Али, прес асистент, изпраща и-мейл на sam@alshahba.com за интервю, което Ассад е дал на студентски активист - Хюсам Ариан, шест месеца по-рано. Тя прилага и снимка на Ариан с Ассад и скрийншотове на страницата на студента във Facebook, които включват статията.

В друг и-мейл, изпратен от Асма пише: „Фарес затвори всичките акаунти в Туйтър!“. Фарес Калас е асистент на Асма ал-Асад и други и-мейли във веригата показват, че той е поискал Туитър да затвори няколко фалшиви акаунти, претендиращи, че принадлежат на Башар.

В акаунта, използван от Асма, има множество имейли, изпратени между ak@alshahba.com и семейството на Асма ал-Асад, които предлагат убедителни доказателства. Много писма, изпратени до „ак“ от семейството й, започват със „Здравей Асма“, а един от хедърите на и-мейл на някой от семейството листва ak@alshahba.com, като Асма Акхрас, което е моминското име Асма ал-Асад.

Все повече експерти вярват, че кибервойната през следващите години ще бъде използвана не толкова за защита или за разпространение на особено чувствителна информация, както за организирани кибер-атаки по отношение на основната национална инфраструктура. Според Джон Басет, бивш високопоставен служител в британската агенция за радио-разузнаване - GCHQ, а сега старши сътрудник в Royal United Services Institute: „Това е първият път, когато бунтовници са получили достъп до толкова високо ниво в комуникациите на даден режим, по време на въстание. Това би могло да бъде повратна точка в развитието на кибервойната“.

Използвани са материали от www.voiceofgreyhat.com, www.cyberwarnews.info и www.jadaliyya.com

Автор: д-р Асен Пейчев
Авторът е експерт в областта на антитероризма и сигурността.
Почетен професор-лектор на IBC Cambridge.

МЕРКИ СРЕЩУ ФИНАНСИРАНЕ НА ТЕРОРИЗМА И ПРАНЕ НА ПАРИ

Част 2

Всяка държава е нужно да осъществи мерки за незабавно замразяване на финансовите средства и други активи на терористи и лица, които финансират тероризма и терористичните организации. Необходимо е да се гарантира, че подобна дейност ще се третира като престъпление съгласно наказателното законодателство.

Всяка страна трябва да предприеме мерки, включително законодателни, които да позволяват на компетентните власти да налагат запор и да конфискуват имуществото, представляващо средства, които са използвани, предназначени или заделени за финансиране на тероризъм, терористични актове и терористични организации.

На 23 Септември 2001 г. Президентът на САЩ издава административна заповед 13 224, с която са оповестени имената на 164 организации и лица, определени като финансиращи тероризма. Само в САЩ са замразени 34.2 млн. долара. Съюзниците на САЩ от евроатлантическия пакт са блокирали още 33.9 млн. щатски долара. В последствие общо 196 държави са изразили подкрепата си по отношение на възпиране финансирането на тероризма.

В началото на 2002 г. 144 държави разполагат с вътрешноправни разпоредби, които им позволяват да блокират банкови сметки и да замразяват авоари, предназначени за терористични цели.

Докладване на съмнителни операции, свързани с терористична дейност



С тази препоръка FATF изрично подчертава, че ако финансови институции или други стопански организации, задължени по нормативни актове за мерки срещу изпирането на пари заподозрат или имат сериозни основания да подозират, че дадени средства са свързани или по някакъв начин ще бъдат използвани за тероризъм, терористични актове или от терористични организации, те трябва да са задължени веднага да съобщят за съмненията си на компетентните власти.

Тази препоръка е реализирана в голяма степен в сега действащия в Република България „Закон за мерките срещу изпирането на пари". Мерките срещу изпирането на пари са подробно регламентирани в четири групи и тяхното прилагане е задължително за всички адресати на тези мерки - юридически и физически лица, посочени в чл. 3, ал. 2 на ЗМИП. Четирите типа мерки са посочени в чл. 3, ал. 1 на ЗМИП и са: идентифициране на лица; събиране на информация относно операции и сделки; съхраняване на информация относно операции и сделки; разкриване на информация относно операции и сделки. Задълженията на адресатите по реализирането на конкретния тип мерки са развити и конкретизирани в раздели на Глава втора на закона - "Идентифициране на клиенти, събиране, съхраняване и разкриване на информация".

Задълженията за идентифициране на клиенти са регламентирани в чл. 4, 5, и 6 на ЗМИП и конкретизирани в Глава първа, Раздел първи от Правилника за прилагане на Закона за мерките срещу изпирането на пари (ППЗМИП), приет с ПМС No. 223 от 9 октомври 1998 г. (ДВ, бр. 119 от 14 октомври 1998 г., изм., ДВ, бр. 14 от 2000 г., бр. 16 и 111 от 2001г.), в сила от 20.02.2001 г.

Предмет на задължението за идентифициране са клиентите на адресатите по ЗМИП. Терминът клиент не е легално определен, но от разпоредбата на чл. 6, ал. 1 е видно, че под клиентите са разбират юридически и физически лица. За търговските банки, например, това са българските и чуждестранните юридически и физически лица, с които банката е в правни отношения при осъществяване на дейността си по Закона за банките.

Идентифицирането се състои в установяване на характерните за тези лица белези, с които те се индивидуализират като участници в гражданските и търговски отношения.

Съгласно разпоредбите на ЗМИП идентифицирането на клиентите е задължително при хипотезите на чл. 4:

- при установяване на трайни търговски отношения с клиентите;
- при извършване на операции и при сключване

на сделки на стойност над 30 000 лв.;

- при обмяна на валута в брой на стойност над 10 000 лв.;

- в случаите на извършване на повече от една операция или сделка, които поотделно не надвишават 30 000 лв. - съответно 10 000 лв., но са налице данни, че операциите или сделките са свързани;

- извън горепосочените случаи, когато възникне съмнение за изпиране на пари.

Съгласно чл. 5 задължително се идентифицират и:

- представителят и представляваният, когато операцията или сделката се извършват чрез представителя;

- извършителят на операцията или сделката или приносителят на документи, ако операцията или сделката се извършат в полза на трето лице без упълномощаване и трето лице, в полза на което е извършена операцията.

Тези хипотези имат различна практическа проява при различните адресати и мерките срещу изпиране на пари по чл. 3, ал. 2 от ЗМИП, между които има и лица, които не са търговци. Например, доколкото търговските банки осъществяват дейността си чрез изпълнение на банкови сделки, които се осъществяват чрез сключване на съответните договори, а при отделните банкови операции се попълват формуляри за съответните нареждания, идентификацията на контрагентите или клиентите е задължителен елемент от банковата дейност. В практически план въпросът за идентифицирането на клиентите за банките се свежда до съответствието на изискваните от клиентите данни, във връзка с нормалната търговска дейност и обемът от изисквани данни за идентифициране на юридически и физически лица, съгласно разпоредбите на ЗМИП.

Съгласно чл. 6 от ЗМИП и чл. 2 от ППЗМИП идентифицирането на юридическите лица се извършва чрез:

- представяне на официално извлечение за актуалното им състояние от съответния регистър, а ако лицето не подлежи на регистрация - на заверен препис от учредителния акт и регистриране на наименованието, седалището, адреса и представителя;

- копие от удостоверение за данъчна регистрация за лицата, които по закон са задължени да се регистрират данъчно;

- копие от митническата регистрация за лицата, които по закон са задължени да се регистрират митнически;

- копие от съответната лицензия, разрешение или удостоверение за регистрация в случаите, когато определена дейност подлежи на лицензиране, разрешение или регистриране и лицата извършват сделки и операции във връзка с тази дейност;

- копие от временното удостоверение или от картата за идентификация по регистър "БУЛСТАТ" за лицата, които притежават единен идентификационен код по Единния държавен регистър на стопанските субекти.

- Данни за представляващия юридическото лице от официален документ за самоличност

Съгласно чл. 6 от ЗМИП и чл. 3 от ППЗМИП идентифицирането на физическите лица се извършва чрез:

- предоставяне от страна на клиента на официален документ за самоличност и регистриране на вид, номер и издател на документа, както и на името, адреса на лицето и единният му граждански номер, ако има такъв;

- физическите лица - еднолични търговци представят и документите, които се изискват от юридическите лица.

Когато възникне съмнение за изпиране на пари, адресатите на мерките срещу тяхното изпиране по чл. 3, ал. 2 от ЗМИП са длъжни да съберат информация относно съществените елементи и размери на операцията или сделката, съответните документи и други идентифициращи данни (чл. 7, ал. 1 от ЗМИП). Става въпрос за допълнителна информация за извършената сделка или операция.



ЗАКОН
ЗА МЕРКИТЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ

(Обн., ДВ, бр. 85 от 24.07.1998 г.; изм. с § 4 от Закона за деноминация на лева - бр. 20 от 05.03.1999 г.; изм. и доп., бр. 1 от 2001 г.; изм., бр. 102 от 2001 г.; изм. и доп., бр. 31 от 2003 г.; изм., бр. 103 от 2005 г., бр. 105 от 2005 г., бр. 30 от 2006 г.; изм. и доп., бр. 54 от 2006 г.; изм., бр. 59 от 2006 г.; изм., бр. 82 от 2006 г., бр. 108 от 2006 г., бр. 52 от 2007 г.; изм. и доп., бр. 92 от 2007 г., бр. 109 от 2007 г.; изм., бр. 16 от 2008 г.; изм. и доп., бр. 36 от 2008 г.; изм., бр. 67 от 2008 г., бр. 69 от 2008 г., бр. 22 от 2009 г., бр. 23 от 2009 г.; изм. и доп., бр. 93 от 2009 г.; изм., бр. 88 от 2010 г., бр. 101 от 2010 г., бр. 16 от 2011 г., бр. 48 от 2011 г.; изм. и доп., бр. 57 от 26.07.2011 г.)

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (Изм., ДВ, бр. 54 от 2006 г.) С този закон се определят мерки за превенция на използването на финансовата система за целите на изпирането на пари, както и организацията и контролът по тяхното изпълнение.
Чл. 2. (Изм., ДВ, бр. 54 от 2006 г.)
(1) Изпиране на пари по смисъла на този закон е:
1. преобразуването или прехвърлянето на имущество, придобито от престъпна дейност или от акт на участие в такава дейност, за да бъде укрит или прикрит незаконният произход на

Министърът на финансите може да дава задължителни указания относно условията и реда за събирането на информация при съмнение за изпиране на пари (чл.7, ал. 3 от ППЗМИП).

Лицата по чл. 3, ал. 2 от ЗМИП са задължени да събират допълнителна информация за операция или сделка по искане на агенция "Бюро за финансово разузнаване" (АБФР) съобразно неговите указания (чл. 13 от ЗМИП и чл. 8 от ППЗМИП).

Условие за събирането на допълнителна информация съгласно чл. 7, ал. 1 от ЗМИП е възникнало съмнение за изпиране на пари. Кога и на какво основание може да се счита, че е налице това условие? За различните адресати на мерките за предотвратяване и разкриване на действията по изпиране на пари отговорът е

различен. Той се основава на определени факти, произтичащи от спецификата на дейност на различните лица, за които мерките са задължителни съгласно чл. 3, ал. 2 от ЗМИП. За банките, например, тези факти следва да се изведат от спецификата на конкретните банкови сделки и операции.

При съмнение за изпиране на пари адресатите на мерките срещу изпиране на пари по ЗМИП са длъжни да уведомят незабавно АБФР. Императивът на чл. 11, ал. 1 от ЗМИП изисква това уведомяване да става преди извършването на операцията или сделката. Хипотезата на алинея втора на същия член допуска това да става и незабавно след извършването на операцията или сделката, когато забавянето на операцията или сделката е обективно невъзможно. Посочените разпоредби не изключват възможността уведомяване на АБФР да се осъществи и по-късно, когато са възникнали съмнения за изпиране на пари, при съпоставка на няколко факта или в резулта на оценка на висшестоящи или други длъжностни лица, които не са участвали пряко и непосредствено при осъществяването на съмнителната операция или сделка.

Уведомяването на АБФР се извършва в писмена форма, по образец, утвърден от министъра на финансите или от определено от него длъжностно лице от АБФР. Към образеца се прилагат служебно заверени копия на всички събрани документи за операцията или сделката и за идентифицирането на клиентите.

В неотложни случаи уведомяването може да се извърши в устна форма, с последващо писмено потвърждение в срок на 24 ч.

Международно сътрудничество

Съгласно тази препоръка на FATF всяка държава трябва да осигурява помощ в борбата с тероризма на друга заинтересована държава на базата на двустранен договор, споразумение или друг механизъм за взаимно правно сътрудничество или обмен на информация. Всяка държава трябва възможно в най-голяма степен да сътрудничи във връзка с прилагането на наказателни и граждански нормативи, при разследвания и дела, свързани с финансирането на тероризма, терористични актове и терористични организации.

Държавите следва да предприемат всички възможни мерки, за да не допуснат предоставяне на сигурно убежище на лица, обвинени или подозирани във финансиране на тероризма, терористични актове и терористични организации. Те трябва да имат процедури за екстрадиране на такива лица.

Такава процедура е регламентирана в Закона за чужденците в Република България (ДВ, бр. 153 от 23 декември 1998 г., изм., бр. 70 от 1999 г., бр. 42 и 112 от 2001 г.). Съгласно чл. 42 от закона експулсиране на чужденец се налага, когато неговото присъствие в страната създава сериозна заплаха за националната сигурност или за обществения ред. Член 10, ал. 1. т. 3 регламентира, че чужденец не се допуска в страната, когато има данни, че е член на престъпна група или организация, или че извършва терористична дейност.

След терористичните актове от 11 септември 2001 г. се наблюдава активно международно антитерористично сътрудничество и тяхно взаимодействие между държавите по отношение на замразяване авоарите на терористите и на техните поддръжници. Засилва се сътрудничеството при разследванията и обмена на информация между правозащитни, полицейски и разузнавателни органи на различни държави.

На 6 октомври 2001 г. Финансовите министри на Г- 7 са приели мащабен план за възпрепятстване финансирането на тероризма. Отправен е призив за активизиране на международното сътрудничество и на усилията за противодействие срещу финансирането на тероризма.

На 15 октомври 2001 г. към между-американската комисия по проблемите на противодействието срещу тероризма (CICTE) е създадена специална подкомисия, натоварена с активизиране на сътрудничество по проследяване движението на финансовите активи на терористичните организации и на техните поддръжници.

На 31 октомври 2001 г. финансовите министри и управителите на централните банки на Г- 20 са приели план за многостранно сътрудничество за отказ на достъп на терористи и на техните съучастници до банковите и финансовите системи, както и за недопускане използването на банковите системи за изпиране на "мръсни пари" и транзакции на средства на терористи.

В официално комюнике от 17 ноември 2001 г. международната монетарна и финансова комисия на международния валутен фонд (МВФ) призовава всички страни-членки, в рамките на юрисдикциите си, да замразят авоарите на терористите. Заявява се, че МВФ ще активизира усилията си за преразглеждане и оптимизиране на финансовите и правни рамки на страните-членки, за да се гарантира, че са блокирани всички възможности за финансиране на тероризма.

На 15 декември 2001 г. между САЩ и Европа е подписано споразумение за улесняване обмена на разузнавателна и аналитична информация за тероризма.

Алтернативни преводи

В така озаглавения раздел от мерки FATF отправя препоръки, отнасящи се до банките и небанковите финансови институции. Съгласно тези препоръки всяка страна трябва да гарантира, че физически и юридически

лица, извършващи подобна дейност незаконно, са обект на административни, граждански и наказателни санкции. Всяка държава трябва да предприеме мерки и да осигури физическите или юридическите лица, които предоставят услугата превод на пари, включително чрез



неофициални системи или мрежи за преводи на пари, включително чрез неофициални системи или мрежи за преводи на пари, да бъдат лицензирани или регистрирани, и дейността им да бъде подчинена на режим, съответстващ на препоръките на FATF, отнасящи се до банките и небанковите финансови институции.

Електронни преводи

Съгласно тази препоръка на FATF държавите трябва да предприемат мерки и да задължат финансовите институции и всички, които извършват парични преводи да вписват точна и съдържателна информация за вносителя на средствата и наредителя на преводите (име, адрес, номер на сметка, бенефициент и др.) и да съхраняват събраната информация.

Държавите трябва да предприемат мерки и да гарантират, че финансовите институции, осъществяващи парични преводи, извършват засилена проверка и контрол върху съмнителни операции по превод на парични средства, особено когато няма пълна информация за вносителя.

Ключов за определяне кога възниква задължението по чл. 11 от ЗМИП за уведомяване на АБФР и по чл. 7, ал. 1 от ЗМИП за събиране на допълнителна информация за съществени елементи на паричния превод е въпросът, кога може да се счита, че има възникнало съмнение за изпиране на пари. За да има съмнение, то трябва да се основава на определени факти. За банките, например, тези факти се извеждат на базата на анализ на теорията и практиката на банковата дейност и на конкретните банкови сделки и операции. Фактите или признаците, които могат да породят основателно съмнение, че конкретния превод се използва като средство за изпиране на пари, са част от съдържанието на понятието "критерии за разпознаване на съмнителни операции или сделки на клиенти", което използва ЗМИП.

Тези критерии обобщават известния в публичното пространство опит на финансовите институции и не следва да се възприемат като единствените факти или признаци, които могат да бъдат определени като критерии за разпознаване на съмнителни парични преводи. От друга страна отделните действия или обстоятелства в много случай са елементи на напълно законосъобразна дейност и зависи в значителна степен от компетентността на банковите служители да бъдат разграничени тези, които пораждат съмнения за изпиране на пари.

По смисъла на ЗМИП и правилника за неговото прилагане, като критерии за разпознаване на съмнителни парични преводи могат да бъдат определени следните факти и признаци:

- чести парични преводи, които не са свързани с основната дейност на клиента;

- нареждания на особено големи авансови преводи за чужбина от клиента по договори за покупко-продажба на стоки или услуги, с включена клауза "скрито" облагодетелстваща продавача, в случай на последващо неизпълнение от страна на купувача;

- нареждания от клиенти на преводи в други финансови институции почти непосредствено след направен депозит, когато дейността е несъвместима с основателната дейност на клиента;

- трансфери на средства по електронен път от клиенти, откриващи сметки, внасящи и незабавно прехвърлящи средства по сметка в друга банка и закриващи първите сметки;

- преводи от чуждестранни инвеститори за участие в приватизацията с последващо връщане на превода в други банки, различни от първоначалните в случаите, когато инвестицията не е осъществена;

- използване на акредитиви и други методи на търговско разплащане, при които външнотърговските документи пораждат съмнение за автентичност или когато такава търговска дейност е несъвместима с основната дейност на клиента;

- използване на акредитиви за търговско разплащане с бенефициенти в чужди държави по сделки, които не са в съответствие с обичайната дейност на клиентите;

- получаване на редовни и/или големи плащания по сметки от държави, които се свързват с производство и незаконно разпространение на наркотици, терористични организации или се разглеждат като центрове на организирана престъпност;

- използване на неистински документи, преправени или документи с невярно съдържание, представени пред банката като основание за задгранични преводи и плащания;

- натрупване на големи суми по сметките на търговското предприятие, несъответстващи на оборота му и последващо прехвърляне по сметка (сметки) зад граница;

- чести операции на непознати на банката клиенти, които извършват множество плащания към чужбина и към различни бенефициенти по плащания на стоки и услуги с широка номенклатура;

- внасяне на суми по разплащателни сметки, съпроводени с незабавни нареждания за превод;

- нареждания на преводи за чужбина от банки, нечленуващи в системата S.W.I.F.T., при което съответната банка не придружава нареждането с всички документи за основание на превод;

- нареждания на преводи за чужбина от т. нар. Bucket Shop (банки "в сянка", регистрирани обикновено в офшорни зони, в областта с данъчни облекчения или в държави със слабо законодателство, разполагащи със съвсем малък капитал, действащи като посредник за създаване на документация с цел подпомагане дейността по изпиране на пари);



- извършване на плащания към финансови институции в чужди страни и чуждестранни бенефициенти, за които банката има сигнали от БНБ, АБФР или от друг компетентен държавен орган, че вероятно се използват за изпиране на пари или терористични организации;

- клиенти, които постоянно внасят или депозират пари в брой за изплащане на банкови ордери, парични преводи или други търговски и бързоликвидни инструменти на паричния пазар;

- клиенти, които превеждат големи суми пари за, или от чужбина, с инструкции за изплащане кеш;

- клиенти, които искат да имат няколко сметки на доверително управление и няколко клиентски сметки;

- физическо или юридическо лице, чиято сметка се използва за получаване или изплащане на големи суми, които нямат видимо отношение към притежателя на сметката или неговия бизнес;

- клиенти, представени от чуждестранен клон или филиал в държава, която е известна с производство и/или разпространение на наркотици;

- клиенти, чужди граждани, които представят подправени, фалшифицирани или пораждащи съмнение за автентичност документи за самоличност;

- чуждестранни търговци, за които банката има сигнали от компетентни държавни органи, че са регистрирани формално компании - фасада, вероятно с цел прикриване на незаконни операции по изпиране на пари или финансиране на терористична дейност;

- нежелание да се даде пълна информация при откриване на сметка и нареждане на паричен превод или представяне на документи, чиято автентичност поражда съмнение за банковия служител.

Организации с идеална цел

Съгласно тази препоръка на FATF държавите трябва да ревизират адекватността на законите и наредбите по отношение на организации, които могат да бъдат подозирани във финансиране на тероризма. Оценява се, че организациите с идеална цел са изключително уязвими и отделните страни трябва да предотвратят използването им от терористични организации. Трябва да не се допуска да се експлоатират законни организации с идеална цел, като средство за избягване на възможността да се замразяват активи на терористи. Трябва да се предприемат мерки, които да не допускат скриване или отклоняване на средства от организации с идеална цел към терористични организации.

Като пример в тази насока може да се посочат редици актове на Министерството на финансите на САЩ. На 9 януари 2002 г. то замразява авоарите на две благотворителни организации, за които се предполага, че са свързани с терористичната мрежа "Ал-Каида" на Осама бин Ладен. Мотивът е, че организациите "Афганистански комитет за подкрепа" и "Дружество за възраждане на ислямското наследство" се представят като благотворителни, но на практика отклоняват събираните от дарители средства, предназначени за вдовици и сираци, като ги прехвърлят на терористичната организация.

Съгласно Резолюция 1373 от 28. 09. 2001 г. на Съвета за сигурност на ООН държавите трябва незабавно да предприемат мерки във вътрешната си политика за предотвратяване и ограничаване финансирането на терористичните групировки и тяхната дейност.

В изпълнение на посочената резолюция, на 19 декември 2001 г. САЩ представят пред Комитета на Съвета за сигурност на ООН срещу тероризма (UNSC) доклад за предприетите мерки за ограничаване на финансирането на тероризма. Предприетите мерки включват:

- замразяване на авоарите на 153 физически лица, групировки и организации, ангажирани с терористични действия;

- създадена на междуведомствена Група за фи-

нансови разследвания с цел разкриване на начините на финансиране на терористичните организации.

Република България активно се включва в международния фронт срещу финансирането на тероризма.

С Постановление No. 50 от 2001 г. (ДВ, бр. 20 от 2001 г.) е изменено и допълнено Постановление No. 39 от 2000 г. за изпълнение от Република България на Резолюция 1267 от 15 октомври 1999 г. на Съвета за сигурност на ООН. С посочените актове на Министерски съвет се разпорежда да бъдат замразени всякакви авоари и други финансови ресурси на терориста Осама бин Ладен, на лица и организации, свързани с него, включително на тези, които принадлежат към организацията "Ал-Каида", както и фондове, създадени чрез собственост на Осама бин Ладен или контролирани директно или косвено от него и от лица и организации, свързани с него. Забранява се предоставяне на такива фондове или финансови ресурси на Осама бинн Ладен, на лица и организации свързани с него, включително на организацията "Ал Каида", от български физически или юридически лица или от други лица, пребиваващи на територията на България.

Във връзка с Резолюция 1373 от 28 септември 2001 г. на Съвета за сигурност на ООН и на основание актовете на Министерския съвет на Република България е осъществена повсеместна проверка в банките и другите финансови институции за установяване и замразяване на сметки и авоари на физически и юридически лица, свързани с терористични организации или терористични актове.

Нормативната уредба, касаеща във вътрешен план проблемът пране на пари, се съдържа в следните закони: Административно процесуален кодекс (АПК), Наказателно-процесуален кодекс (НПК), Закон за мерките срещу изпирането на пари (ЗМИП), Валутен закон (ВЗ), Закон за административните нарушения и наказания (ЗАНН), Правилник за прилагане на Закона за мерките срещу изпиране на пари (ППЗМИП), Правилник за прилагане на Закона на Държавна агенция "Национална сигурност" (ППЗДАНС).

Материята, свързана с определянето на мерки срещу изпирането на пари по организацията и контрола по тяхното прилагане е правно уредена във ЗМИП, ППЗМИП, ППЗДАНС. Целта, която законодателят преследва е установените от него мерки да постигнат предотвратяване на това явление и повишаване на степента на неговата разкриваемост.

Мерките се прилагат от съответно задължените лица по чл. 3, ал. 2 от ЗМИП. **Категорията задължени лица са следните:**

1. Българска народна банка, кредитни институции, които извършват дейност на територията на Република България, финансови къщи, обменни бюра, както и другите доставчици на платежни услуги;

2. застрахователи, презастрахователи и застрахователни посредници, със седалище в Република България; застрахователи, презастрахователи и застрахователни посредници от държава-членка на Европейския съюз, или държава-страна по Споразумението за Европейското икономическо пространство, които осъществяват дейност на територията на Република България; застрахователи и презастрахователи със седалище в държави, различни от посочените, получили лиценз от Комисията за финансов надзор да осъществяват дейност в Република България чрез клон; застрахователни посредници, със седалище в държави, различни от посочените, вписани в регистър на Комисията за финансов надзор;

3. колективни инвестиционни схеми, инвестиционни посредници и управляващи дружества;

4. пенсионно осигурителни дружества и здравноосигурителни дружества;

5. органи по приватизацията;

6. лица, организиращи възлагането на обществени поръчки;

7. лица, организиращи и провеждащи хазартни игри;

8. юридически лица, към които има взаимоспомагателни каси;

9. лица, които предоставят паричен заем срещу залагане на вещи;

10. пощенски служби, които приемат или получават пари или други ценности;

11. нотариуси;

12. пазарен оператор и/или регулиран пазар;

13. лизингови предприятия;

14. държавни и общински органи, сключващи договори за концесии;

15. политически партии;

16. професионални съюзи и съсловни организации;

17. юридически лица с нестопанска цел;

18. регистрирани одитори;

19. органи на националната агенция за приходи;

20. митнически органи;

21. спортни организации;

22. Централния депозитар;

23. търговци на оръжие, петрол и петролни продукти;

24. лица, които по занятие извършват консултации в областта на данъчното облагане;

25. търговци на едро;

26. лица, които по занятие извършват правни консултации, когато:

а) участват в планирането или изпълнението на операция или сделка на свой клиент относно:

б) покупко-продажба на недвижим имот или прехвърляне на предприятие на търговец;

в) управление на пари, ценни книжа или други финансови активи;

г) откриване или разпореждане с банкова сметка или със сметка за ценни книжа;

д) набавяне на средства за учредяване на търговец, увеличаване на капитала на търговско дружество, за предоставяне на заем или за всяка друга форма на набавяне на средства за осъществяване на дейността на търговеца;



е) учредяване, организиране или упражнение на дейността на търговец или друго юридическо лице, офшорна компания, компания, предоставена за доверително управление, или друга подобна структура;

ж) доверително управление на имущество;

з) действат за сметка на или от името на свой клиент в каквато и да е финансова операция или сделка с недвижим имот;

27.лица, които извършват по занятие посредничество при сделки с недвижими имоти;

28.лица, които по занятие предоставят:

а) адрес на управление, адрес за кореспонденция или офис за целите на регистрация на юридическо лице;

б) услуга по регистриране на юридическо лице, офшорна компания, компания на доверително управление или друга подобна структура;

в) услуги на доверително управление на имущество или на лице по буква "б".

Всяко от задължените лица приема вътрешни правила и прилага специфични критерии за разпознаване на съмнителни операции, сделки и клиенти.

29.лица, които по занятие извършват счетоводни услуги

30.частни съдебни изпълнители

Съгласно чл. 16 ал. 1 ЗМИП задължените лица трябва в 4-месечен срок от регистрацията им да приемат вътрешни правила за контрол и предотвратяване изпиране на пари, които се утвърждават от председателя на Държавна агенция "Национална сигурност" (ДАНС).

Вътрешните правила се изпращат на председателя на ДАНС за утвърждаване в 14- дневен срок от тяхното приемане (чл. 16 ал. 3 ЗМИП).

С вътрешните правила се установяват:

- ясни критерии за разпознаване на съмнителни операции или сделки и клиенти;
- условията и реда за събиране, анализиране, съхраняване и разкриване на информация за операции или сделки;
- правила за организиране и за работа на специализираните служби;
- разпределение на отговорността за прилагане на мерките срещу изпиране на пари по клоновете на лицето и мерки, включващи процедури за оценка на риска по отношение на клонове и дъщерни дружества при условията на чл. 3В, ал. 2 ЗМИП, ако имат такива;
- използване на технически средства по превенция на изпиране на пари;
- система за вътрешен контрол по изпълнение на задълженията, установени в ЗМИП и в актовете по прилагането му;
- правила за обучение на служителите от специализираните служби;
- правила за обучение на останалите служители;
- други изисквания, съобразно особеностите на дейността на лицата (чл. 17 ППЗМИП).

Вътрешен ход на процедурата

Вътрешните правила се утвърждават от председателя на ДАНС. Ако те не съответстват на ЗМИП или на ППЗМИП, не са приети от компетентен орган на лицето или предвидените в тях мерки не са достатъчни за постигане на целите на ЗМИП, председателят на ДАНС ги връща на лицето и дава задължителни указания за отстраняване на установените несъответствия. Лицата са длъжни в едномесечен срок от получаването им да отстранят несъответствията и да представят повторно вътрешните си правила на председателя на ДАНС за утвърждаване (чл. 19 ППЗМИП).

Лицата са длъжни в 7-дневен срок от получаване на лицензa, разрешението или удостоверението за регистрация или от започването на дейността, когато тя не попада под лицензионен или разрешителен режим или не подлежи на регистрация, да заявят в дирекция

"Финансово разузнаване" на ДАНС писмено адрес за контакти (чл. 20 ППЗМИП).

Създаване на специализирани служби

Изброените в чл. 6. ал. 5 ЗМИП лица са длъжни да създадат специализирани служби, които са натоварени със следните правомощия:

- събиране, обработване, съхраняване и разкриване на информация за конкретните операции или сделки;
- събиране на доказателства относно собствеността на имуществото, подлежащо на трансфер;
- изискване на сведения за произхода на паричните средства или ценности, предмет на операциите или сделките; произходът на тези средства се удостоверява с декларация;
- събиране на информация за клиентите и поддържане на точна и подробна документация за операциите им с парични средства или ценности;
- при съмнение за изпиране на пари предоставят събраната информация на ДАНС (чл. 6, ал. 5 ЗМИП).

Сътрудничество

Съгласно чл. 22 ППЗМИП органи, на които със специален закон им е възложено да упражняват контрол върху задължените лица, могат да си сътрудничат с ДАНС при изработване на ясни критерии за разпознаване на съмнителни операции или сделки и клиенти, както и на мерки за предотвратяване и разкриване изпирането на пари в съответните области.

Разкриване на информация

При съмнение за изпиране на пари, лицата са длъжни да уведомят незабавно ДАНС преди извършването на операцията или сделката, като забавят нейното осъществяване в рамките на допустимия срок, съгласно нормативните актове, уреждащи съответния вид дейност.

Ако забавянето на операцията или сделката е обективно невъзможно, те уведомяват незабавно след извършването й. То може да се извърши и от техни служители, които не отговарят за прилагането на мерките срещу изпирането на пари. В тези случаи ДАНС запазва анонимността им (чл. 11, ал. 1-3 ЗМИП).

Съгласно чл. 18, ал. 1 ЗМИП, ДАНС може да получи информация за съмнение за изпиране на пари, както от задължените лица и от държавни органи, така и чрез международен обмен.

Съгласно чл. 13, ал.1, във връзка с чл. 11 и 18 ЗМИП, при уведомяване на ДАНС от посочените по-горе лица или от техни служители, както и от държавни органи или чрез международен обмен, тя може да поиска от субектите, които извършват дейност на територията на Република България информация относно съмнителни операции, сделки или клиенти. Поискана информация се предоставя в определения от нея срок. При писмено уведомяване от тях, тя може да поиска информация при същите условия и от Българска народна банка (БНБ) и кредитни институции, извършващи дейност на територията на страната (чл. 13, ал. 2 ЗМИП).

ДАНС може да поиска от държавните и общински органи информация, при посочените по-горе условия, която не може да й бъде отказана. Тя се предоставя в предвидения от нея срок. За нуждите на анализа й ДАНС получава информация от БНБ, която е събирана по В3 (чл. 13, ал. 3 и 5 ЗМИП).

Исканата от ДАНС информация не може да бъде отказана или ограничена от съображения за служебна, банкова или търговска тайна **(чл. 13, ал. 7 ЗМИП)**.

Регистри, водени от дирекция "Финансово разузнаване" на ДАНС

На основание чл. 11А, ал. 1 и 2 ЗМИП задължените лица уведомяват дирекцията за всяко плащане в брой на стойност над 30 000 лв. или тяхната равностойност в чужда валута, извършено от тях или техен клиент. Дирекцията води регистър за тези плащания, като той може да се използва само за целите на противодействието за изпирането на пари. Тя води регистри освен за плащанията в брой на стойност над 30 000 лв., а и за информация за изпиране на пари и за финансиране на тероризма (чл. 32д, ал. 7, т. 1 ППЗДАНС).

Дневник за съобщения от служители за възникнало съмнение за изпиране на пари

Лицата, за които са задължителни мерките за превенция срещу изпирането на пари, са длъжни да завеждат в специален дневник всяко съобщение на свой служител за възникнало съмнение за изпиране на пари, което е направено пред представител на специализираната служба или пред член на управителните органи, независимо от начина, по който то е извършено. Дневникът трябва да е прошнурован, прономерован и заверен с подписа на ръководителя на специализираната служба и с печата на съответното лице. При завеждане на съобщението ръководителят на специализираната служба или оправомощен от него служител открива преписка, в която се събират и подреждат по реда на тяхното постъпване всички документи, имащи отношение към извършените от служителите на задълженото лице действия, които са свързани с него. В тези случаи ръководителят на специализираната служба отговаря за правилното съхраняване и водене на дневника и на преписките в него. Ако не е възможно създаването на специализирана служба задължените лица изпълняват лично задълженията си по воденето и съхраняването на дневника. Също така председателят на ДАНС може да дава задължителни указа-

ния на лицата относно условията и реда за събиране и съхраняване на информация (чл. 12, ал. 1-7 ППЗМИП).

Извършване на проверки

Целта на проверките е да се упражни контрол върху прилагането на мерките, както и да се преодолее съмнението за извършване на изпиране на пари.

Органите за надзор върху дейността на лицата по чл. 3, ал. 2 и 3 ЗМИП са длъжни да предоставят информация на ДАНС, ако при осъществяване на надзорната си дейност установяват извършване на операции и сделки, свързани със съмнение за изпиране на пари или неизпълнение на задълженията по чл. 11А ЗМИП. При извършване на проверки те проверяват изпълнението на изискванията на ЗМИП от проверяваните лица. При констатиране на нарушение уведомяват ДАНС, като изпращат извлечение от констативния акт в съответната му част (чл. 3А ЗМИП).

Съгласно чл. 32 д, ал. 7, т. 14 ППЗДАНС, във връзка с чл. 23, ал. 1 ППЗМИП, ДАНС е компетентният орган, който може да извършва проверки на място на посочените лица, по прилагането на мерките по превенция срещу изпирането на пари и финансирането на тероризъм, както и при съмнение за изпиране на пари и финансирането на тероризма.

Съгласно чл. 23, ал. 2 ППЗМИП, контролните органи на ДАНС са определени от председателят й длъжностни лица от състава на ДАНС.

На основание чл. 23, ал. 3 ППЗМИП, проверките се извършват въз основа на писмена заповед на председателя на ДАНС или упълномощено от него длъжностно лице. В нея се посочват целите, срокът и мястото на проверката, проверяваното лице, както и името и длъжността на проверяващите лица. При извършването на проверка на място, контролните органи имат право:

- на свободен достъп до служебните помещения на лица, при които се извършва проверката;

- да изискват документи, сведения и писмени обяснения за обстоятелства, свързани с предмета на проверката (чл. 23, ал. 4 във връзка с чл. 15, ал. 2, т. 1 и 2 ППЗМИП).

Административно наказателна отговорност

1. Административни нарушения и наказания

При нарушение на изискванията за уведомяване на ДАНС, както и ако лицата по чл. 3, ал. 2 и 3 ЗМИП или тези, които ги управляват и представляват, както и техните служители, уведомят свой клиент или трети лица за представени от тях документи на ДАНС или разкрият информация относно нейното уведомяване, се наказват с глоба от 5000 до 20 000 лв., ако деянието не представлява престъпление (чл. 23, ал. 2 във връзка с чл. 11А и 14 ЗМИП).

Административно наказателна отговорност носят и лицата, които са нарушили изискванията за приемане на вътрешни правила за контрол и предотвратяване изпирането на пари. Санкцията за тях е глоба в размер от 200 до 2000 лв., освен ако деянието осъществява състав на престъпление (чл. 23, ал.2 ЗМИП).

Когато извършителят на посочените по-горе нарушения е едноличен търговец или юридическо лице се наказва с имуществена санкция в размер от 2000 до 50 000 лв.

2. Реализиране на административно наказателната отговорност

Актовете за установяване на административни нарушения се съставят от длъжностни лица на Министерство на финансите или ДАНС, а наказателни постановления се издават от министъра на финансите или председателя на ДАНС, или от оправомощени от тях длъжностни лица (чл. 24, ал. 1 ЗМИП).

3. Обжалване на наказателните постановления

Чл. 24, ал. 2 ЗМИП предвижда обжалването на издадените наказателни постановления да се развива по реда на ЗАНН. Жалбата следва да се подаде в 7 - дневен срок от връчването на наказателното постановление, чрез наказващия орган до районния съд, в чийто район е извършено или довършено нарушението, а ако е извършено в чужбина - пред Софийски градски съд (чл. 59, ал. 1 и 2 във връзка с чл. 1, изр. 1 ЗАНН). Решението на съда подлежи на касационно обжалване пред административният съд на основанията, предвидени в чл. 348 НПК и по реда на глава дванадесета АПК (арг. чл. 63, ал. 1 ЗАНН).

Специализираната административна дирекция "Финансово разузнаване-ДАНС" организира безплатни обучения за счетоводители и за лица, които осъществяват счетоводни услуги. Лекциите се четат от висококвалифицирани експерти от САД "Финансово разузнаване", което е гаранция за висококачествено обучение на този вид кадри, при прилагането на закона.

Автор: инж. Емил Димитров

СЕКЮРИТИ ОБКОВ

За хора, които живеят активно и използват всяка възможност за излизане, разходките или почивките завършват понякога с неприятна изненада. Домът е разбит, всичко е обърнато нагоре с краката, шкафчетата и гардеробите претършувани, а всички по-ценни вещи изчезнали.

Според сведение на криминалистите, незащитените прозорци или такива, в които е вложен обикновен обков, държат водеща позиция при обирите с взлом - 80%, като преодоляването на този тип прозорци е изключително бързо, лесно и безшумно и при това не са необходими специални инструменти. Почти 70% от взломните кражби се извършват със стандартна права отвертка, чийто накрайник не е повече от 10 мм. Много хора, които са си сложили вече от новите видове дограми смятат, че по презумпция вече са защитени. Точно те обаче са първите, набелязани от крадците или друг вид престъпващи закона хора. При нерегламентирано проникване в жилище или офис не винаги става въпрос за обир, не са редки случаите на кражба на интелектуална собственост чрез „хакване" на компютри или пък монтиране на подслушватели или друг тип апаратура.



По какъв начин това може да се избегне и необходимо ли е да се правят подобрения?

За да се отговори правилно на този въпрос, трябва да се знаят най-честите места, през които „посрещаме" неканени гости:

При еднофамилни къщи 52% от проникванията стават през терасите и 32% през прозорците.

Блокове и офиси - 32% през терасите, 21% през прозорците и 47% през вратите.

Как да се подсигурим?

Първото, което трябва да направим е консултация със специалист, който да посочи къде са ни слабите места и съответно да препоръча най-подходящата за случая защита.

Като най-практично решение се налага използването на противовзломен обков, който дава възможност за доработка съобразно нуждата за повишаване нивото на сигурност. Този тип обков се произвежда от високо устойчиви материали, гарантиращи според класа сигурност „задържане на проникването" до 40 минути. Предлагането на пазара е различно и варира от най-простите решения, през използването на обков с повишена сигурност – клас WK-1 или WK-2, до използване на автоматизирани системи, проверяващи дали обекта е защитен в случай на забравен прозорец например. Така, че и тук отново е наложителна консултация със специалист за всеки конкретен случай.

При някои обкови е възможно да бъдат интегрирани детайли, които да са свързани пряко към алармената система, която контролира заключването и „достъпа".

Поради недостатъчната сигурност на използваните брави, патрони и механизми, друг често използван начин за взлом е през вратата. Тук възможните решения са още повече – ролки, куки, куки с шипове, чиято специална форма прави лесно и удобно заключването при







максимална за модела сигурност. Освен надеждността, този тип брави дават и равномерно разпределение на притискането по цялата височина на вратата. Много често всички ние инвестираме значителни средства и монтираме врати комбинирани с брави, използващи перчат ключ тип „касов" и сме сигурни в надеждността им. Бързо обаче се убеждаваме в противното, след като неизбежното стане реалност и тогава сме готови да инвестираме в сигурност значително повече средства от първоначално предвидените. Затова преди да предприемем стъпка за промяна е добре да се посъветваме със специалистите, които потвърждават, че често допълнителното подсигуряване отказва крадците. Използването на допълнителни подсигурявания се изисква при врати, отговарящи са стандарт DIN 18103, DIN 18251-3, DIN EN-V 1627-30, както и клас сигурност от WK-1 до WK-3. Вариантите за допълнително подсигуряване могат да бъдат от допълнително пасивни щифтове до „интелигентни" брави, използващи кодиращи чипове, дактологичен отпечатък и патрони, създадени по най-високите изисквания за сигурност в света, използващи 1 000 000 (един милион) възможни комбинации (обикновените месингови патрони използват до 33 000 възможни комбинации).

Най-високите изисквания за сигурност, отговарящи на съвременните нужди се използват от всички големи фирми. Нарастващите изисквания към сигурността, професионалните анализи и документация са неразделна част от иновациите. Поговорката „Възможността привлича крадците" се отнася имено за тези от тях, които си търсят обекти в часовата зона от 12 до 18 часа и които не представляват пречка за преодоляването им.



Автор: инж. Николай Цапрев

СМАРТФОНИТЕ – ПРОБИВИ И ЗАЩИТА

С тази статия екипът на Профисек продължава поредицата, разглеждаща мобилните телефони като елемент от системата за защита на информацията.

В днешно време всеки човек носи със себе си и използва един или повече мобилни телефони. Клетъчният мобилен телефон или GSM, както сме свикнали да го наричаме, е устройство, без което съвременния човек не може да комуникира и същевременно го използва ежедневно за най-различни други цели. Тенденцията към усложняване на телефоните и добавянето на нови функции към тях е ясно очертана. Почти всеки нов модел има добавено още някакво устройство и някаква допълнителна функция. И понеже мобилния телефон отдавна не е само телефон, бе въведен терминът „Смартфон“. Според Wikipedia “смартфонът” е мобилен телефон, конструиран на мобилна компютърна платформа, с по-усъвършенствани компютърни възможности и интегрираност на функциите от нормален телефон. Именно наличието на много функции, събрани в едно устройство е основата на успеха на смартфоните. Според статистиката пазарният дял на смартфоните след октомври 2011 година е надхвърлил 52% от общите продажби на мобилни телефони и продължава да се увеличава.



Характерното при смартфоните е, че за да работят всички функции и приложения е необходим мощен процесор, различни сензори, комуникационни модули и операционна система. На практика в джоба си ние носим един мини компютър, по-мощен и с по-големи възможности от лаптопите среден клас, продавани преди 4-5 години. Както при всеки компютър, една от основните роли за производителността и функционалността се пада на операционната система. На пазара са утвърдени устройства, работещи основно със следните операционни системи: Android, OS X iPhone, Blackberry OS, Symbian, Windows mobile и други. Пазарният дял при операционните системи е в същия ред. Най-голям пазарен дял след октомври 2011 година има операционната система Android, следвана от iPhone и Blackberry. Тоест, най-разпространените в момента смартфони работят с тези системи. Няма да разглеждаме функционалността, предимствата или недостатъците на тези операционни системи. Ще се концентрираме върху най-разпространената OS Android и нейните предимства и недостатъци от гледна точка на защитата на информацията.

Нека започнем с едни от основните проблеми.

Един от основните проблеми е, че Android непрекъснато докладва на някого къде сме и какво правим в момента. Има много статии в интернет и въпросът е разглеждан подробно. Ако не ви се търси в мрежата, просто се опитайте през основното меню за настройки да разрешите използването на безжичните мрежи в помощ на GPS, при включен достъп на телефона до мобилен интернет и прочетете съобщението, излизащо на екрана. Съобщението е „Allow Google’s location service to collect anonymous location data. Collection will occur even when no applications are running“. Което в свободен превод означава, че разрешавате на Гугъл да събира данни за вас, и че това ще се случи дори и дадените приложения да не са активни. Ако откажете, няма да можете да използвате AGPS функцията и Google Maps. Според публикациите в медиите, събирането на данни се прави основно с търговски цели или с други благородни такива, но това не

променя същността на въпроса. Операционната система Android и системните приложения непрекъснато предават данни за вас и вашите действия към нечии сървъри.

Вторият проблем е свързаността на смартфона с интернет. Всъщност той и за това е създаден - да е свързан



в интернет и да дава възможност за пълноценна работа и забавление на собственика си в мрежата. Проблемът е, че Android пристига с много приложения, всяко от които иска достъп до интернет и всяко от тях приема и изпраща данни към различни сървъри. Всичко това става често без знанието и разрешението на потребителя. Предават се различни по вид данни, като предпочитани сайтове, търсени продукти, теми, ключови думи, история на браузването, местоположението на телефона, състояние на телефона, използвани програми, активни версии на софтуера в момента и много други, за които дори не подозирате. Тези приложения никой специално не ги е поискал, но те пристигат инсталирани на телефона и за съжаление много от тях са на практика неунищожими. Деинсталирането им не дава резултат, защото след известно време се самоинсталират на ново и то без разрешение.

Следващият проблем е начина на работа на споменатите по-горе приложения. Освен тези, стартирани от използващия телефона, има и много, които се стартират самостоятелно. Прекратяването на използването на дадено приложение всъщност не води до неговото спиране. Просто от екрана изчезва иконката и не се изобразява дадено съобщение, но приложението продължава да работи, освен ако изрично не бъде спряно. Спирането става през менюто за настройки на телефона или чрез използването на допълнително инсталирано приложение. Тоест, периодично трябва да се проверяват работещите в определен момент приложения и да се спират ръчно. Тук не става въпрос само до сигурност на информацията, но и до разход на батерия и трафик в интернет, което за някой хора може би е по-важно.

Едно от основните предимства на Android, е отвореността на системата и възможността за свободна разработка на приложения. Това, обаче е и основният й недостатък от гледна точка на сигурността. За тази операционна система има най-много безплатни и платени приложения. Това позволява смартфонът да придобие невероятни функции. Има на практика всичко, което може да пожелае човек. Проблемът е, че никой не проверява какви са пълните функции на тези приложения и какво всъщност правят. Дали са програми, които работят съгласно описанието им в Android market или имат и други скрити изненади. Сигурността е делегирана на потребителя. Android market не носи отговорност за наличието на зловреден софтуер в приложенията, които можем да изтеглим и инсталираме от там. Тоест, инсталирайки на телефона едно прекрасно и полезно приложение, е много вероятно да си инсталираме и един или повече качествени вируси или друг вид шпионски и зловредни програми.



Като стана дума за шпионските програми, нека споменем и шпионския софтуер за GSM. Android е най-благодатната платформа за инсталиране на такъв софтуер. Благодатна в смисъл, че на пазара има много и различни софтуери, инсталират се лесно и бързо, работят добре и незабелязано.

Android има и добри страни. Ако вече притежаваме смартфон с операционна система Android, можем да използваме наличието на многото функции и безплатни приложения в интерес на личната ни сигурност. Можем да се опитаме да контролираме слабите страни и чрез добавяне на допълнителна функционалност да превърнем смартфона в активно средство за защита.

Ето и някой идеи:

1. Контрол на трафика и работата на приложенията. За целта може да се направи следното:

Деинсталиране на излишните приложения.

Контролиране на работата на приложенията, чрез вградената програма или инсталиране на допълнителна програма от рода на Task killer, посредством която да се управлява работата на останалите приложения.

Спиране на достъпа до интернет през мобилните мрежи или Wi-Fi. Включването и изключването на тази функция е изключително лесно и бързо.

Инсталиране на приложение за контрол на трафика в интернет. Съществуват приложения от рода на Mobile counter, които позволяват тотален контрол на

количеството данни предавано през интернет, каналите за предаване и приложенията, чрез които е осъществен трафика.

Горните мерки позволяват сериозен контрол върху предаваната и получаваната от интернет информация, както и регистриране и предотвратяване на допълнителен нежелан трафик. Освен това помагат за откриване наличието на инсталиран шпионски софтуер и блокиране на работата му.

2. Криптиране съдържанието на паметта и на комуникацията.

Android поддържа множество приложения, служещи за криптиране съдържанието на паметта. Тези приложения криптират всички видове файлове, като ги правят недостъпни за разчитане от други лица. Това е частично решение, понеже съдържанието на телефонния указател, SMS и MMS остават некриптирани и следователно достъпни. Съществуват и програми, позволяващи тяхното криптиране, но те се позиционират в сериозен ценови диапазон.

Подслушването на телефонните разговори, интернет трафика и SMS, може да бъде избягнато чрез използване на програми от рода на Viber и WhatsApp. Въпросните програми позволяват разговор и SMS-чат през GPRS и VoIP канали. Това води до допълнително криптиране на връзката, преминаване през сървъри, различни от тези на мобилните оператори и в крайна сметка елиминират стандартните методи за подслушване. Освен това са удобни и безплатни. Автоматично проверяват в телефонния указател на телефона на кой от отбелязаните там телефони са инсталирали тези приложения и позволяват директна и защитена връзка с познатите хора.

3. Защита на телефона от неоторизиран достъп.

Приложения от рода на PhoneLocator Pro позволяват телефона да се защити от неоторизиран достъп, като се блокира работата му и при опит същия да бъде разблокиран, телефонът прави снимка и я изпраща на определен имейл адрес. При загубване или кражба на телефона, същият може дистанционно да бъде блокиран, да бъдат изтрити файловете, да се установи местоположението на телефона, а в някой случаи да се видят и чуят лицата и гласовете на хората, които го използват в момента. Тези приложения позволяват контрол върху апарата в отсъствие на собственика, предотвратяват нежелано използване, и защитават наличните в паметта данни.



4. Инсталиране на антивирусна програма. Съществуват платени и безплатни антивирусни програми за смартфони. Използването на такива програми не е тотално решение на въпроса със сигурността, но помага да се избегнат нежелани инциденти. Освен това някой от антивирусните програми съдържат комплект от функции, които позволяват контрол върху телефона и покриват описаните мерки в т. 1 и 3.

5. Превръщане на смартфона в охранителна система. Смартфонът може да бъде превърнат в дигитален видео рекордер за охрана и може да бъде оставен да охранява помещение. Използвайки камерата, като детектор на движение, телефонът може да регистрира движение в помещението, да направи автоматично запис на видео клип и в зависимост от настройките да изпрати SMS, MMS, и-мейл или директно да транслира звук и образ на друг телефон или компютър. Могат да се регистрират вибрации, преместване в пространството, шум, промяна на осветеността и други параметри, които да задействат аларма и да изпратят алармен сигнал.

6. Използване на смартфона като бъг-детектор

С инсталирането на подходящи приложения телефонът може да се използва като детектор на безжични устройства за пренос на данни, за откриване на скрити видео камери, за откриване на скрити електронни устройства и наличие на електромагнитни полета.

Чрез приложения, позволяващи сканиране характеристиките на мобилната мрежа могат да бъдат регистрирани данни, даващи основание да се предположи наличие или не на подслушвател на GSM в близкото физическо обкръжение.

Тези приложения и дейности вече са игри за напреднали или параноици или и двете…

Важното е да се знаят възможните рискове при използването на дадена технология или устройство и начините за тяхното контролиране или отстраняване, с цел намаляване на вредните последици, а защо не и извличане на полза. Android е прекрасна платформа, лесна за работа, интуитивна и не случайно е най-разпространената операционна система. Положението с другите операционни системи е подобно. В крайна сметка е въпрос на избор на всеки ползвател, кое е по-важно за него удобството за работа и множеството функции или защитата на личните данни. Всеки избира сам. Например, дали да използва рекламираните в последно време системи за разплащане през мобилните телефони.



ПРОФИСЕК

ПРОФЕСИОНАЛНА СИГУРНОСТ

РИСК МЕНИДЖМЪНТ

ФИРМЕНА СИГУРНОСТ

ЗАЩИТА НА ИНФОРМАЦИЯТА

СИСТЕМИ ЗА СИГУРНОСТ

website: www.profisec.bg
адрес: гр. София, ул. Бигла 16А, вх. Б
тел./факс: 02/962 05 23

Автор: Борислав Михайлов

ЗАЩИТА НА ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ

В съзнанието на средностатистическия български потребител понятието "интелектуална собственост" не буди богат набор от асоциации, особено ако се абстрахираме от актуалната към момента кампания, предлагаща откровено странен паралел между интелектуалния труд и съдържанието на домашния хладилник. Подобна липса на информираност е разбираема в рамките на незаинтересованите среди, но пренасянето на същото статукво в частния сектор и наличието на дезинформация сред управленските кадри по въпросите на интелектуалната собственост и нейната значимост за предприятията може да доведе до подчертано негативен резултат.

Понятието "интелектуална собственост", което априори бива асоциирано по-скоро с научната сфера на дейност, всъщност е неразривно свързано с термини като патенти, промишлени дизайни, търговски марки, полезни модели, лицензи, които имат лесно измерима икономическа значимост в бизнес средите. Обвързването на тези обекти на интелектуалната собственост с практическото им приложение и защита обаче се явява все още труден и слабо развит процес.



Нагледен пример за значимостта на интелектуалната собственост на предприятието можем да намерим още в първия асоциативен елемент, чрез който то бива възприето от потребителя и служителите си, а именно търговската марка. Субективността при възприемането на търговската марка от страна на широката общественост я превръща в уникална, не само като обект на индустриалната собственост (с оглед психологическата ѝ значимост), но и като елемент на фирмения маркетинг. Този двойствен характер намира и чисто вербално изражение в английските термини brand и trademark, отразяващи съответно пазарния и правния термин за търговска марка - а това на свой ред е пряк атестат за нивото на взаимно проникване между правните и бизнес тълкуванията при анализа на обектите на интелектуална собственост.

Изграждането на ценност на търговската марка се явява основна цел в рамките на всяка една маркетингова стратегия, но подкопаването на устоите, върху които се крепи изграждана с десетилетия марка, е лесно осъществимо при липсата на контрол на пазара. Вероятността потребителят да бъде заблуден по отношение на продукта, който придобива, и съответно да прехвърли тази заблуда върху опита си от съответната марка, се явява все по-значим проблем за глобалния

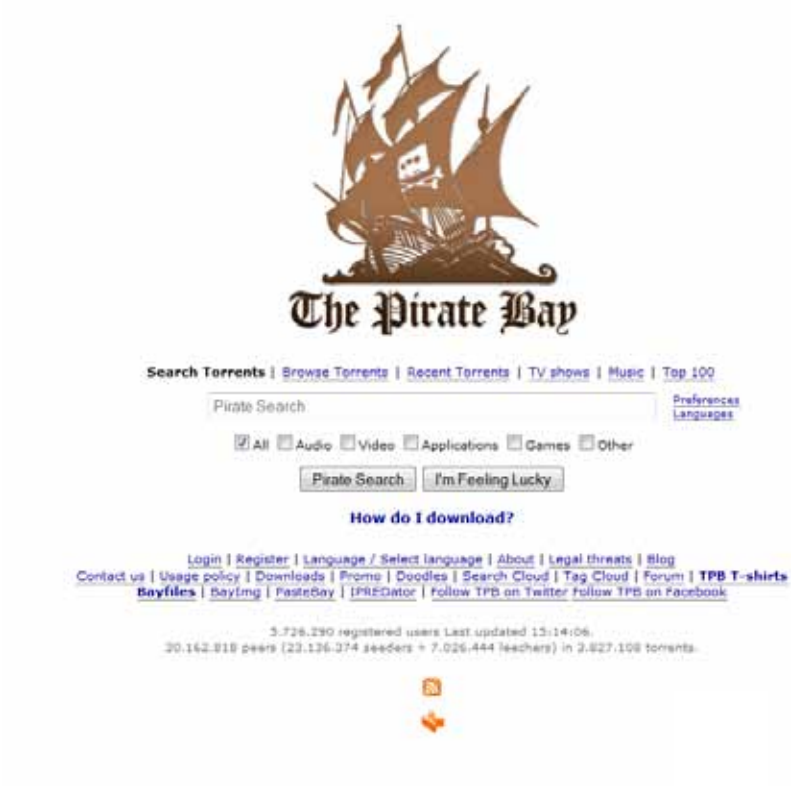
бизнес. Случаите на фалшифициране на търговски марки чрез използване на трудно различими детайли в образните елементи или чрез разместване на букви са добре документирани на българския пазар, но е важно да се отбележи, че подобни казуси далеч не се ограничават със световноизвестни брандове, а напротив - злоупотребите, целящи заблуда у потребителя, могат да отворят път за навлизане дори и на тясно специализирани пазарни сегменти.



Авторското право, неговото възникване, отстъпване и особено опазване също попада в графата обекти на интелектуалната собственост, чиято значимост нараства. Все по-актуална става, от една страна, нуждата на потребителите от ясни правила за баланс на интересите при икономическа реализация на интелектуалната собственост, а от друга - потребността за самите автори да са налице конкретни постановки относно собствеността им върху резултатите от тяхната дейност. Авторско-правните въпроси, свързани с отстъпване на правата за използване или с чисто икономическата изгода при пазарната реализация на труда, и към момента не са разгледани в нужните детайли от законодателя - а това позволява търсенето на дупки в законовите норми, които да бъдат експлоатирани за сметка на първоизточниците на научните или художествени произведения.

Тук намира място и бегло споменатия в началото на настоящия материал въпрос, свързан със свободното използване на произведения, което според законовите норми е допустимо да се извършва, в случай че то "няма самостоятелно икономическо значение" и отговаря на т.нар. "тройно правило", възприето в българското законодателство на базата на редица международни договори. Според същото, свободното използване следва да бъде сведено до специални случаи, посочени в закона; да не пречи на нормалното използване на научните произведения; както и да не уврежда законните интереси на авторите и други притежатели на авторско право. Така законово предписаният режим на свободно ползване от една страна защитава правото на крайния потребител на достъп до информация, но от друга страна чрез понятия като "нормално използване" и "неоснователно увреждане", които са критерии за допустимост на съответното свободно ползване, създава възможност за прекалено широко тълкуване - а липсата на конкретно регламентиране по отношение на свободното използване става причина за редица проблеми и недоразумения.

С оглед горното и в контекста на предписаното от законодателя зачестилите напоследък кампании, визиращи крайния потребител, който всъщност рядко търси икономически ползи от използването на съответния обект на интелектуална собственост, изглеждат погрешно насочени на фона на все така актуалния проблем с незаконния презапис и възпроизвеждане с цел пласиране на т.нар. "черен" пазар. Що се отнася до софтуерните продукти, водещите разпространители търсят решението на този въпрос във все по-силното застъпване и използване на Интернет, като средство за проверка и контрол на собствеността върху продуктите, както и ограничаване на функционалността на продукта при липса на надлежна регистрация. Спорно е обаче доколко този подход е приложим по отношение на редица други интелектуални продукти - което на свой ред налага ясната нужда от по-адекватен режим за използването им. Налице са организирани системи на свободни лицензии (пример за това е организацията Creative Commons), които на практика се оказват по-добрият вариант на закрила на авторски произведения, тъй като дават възможност на създателя сам да определи режима на тяхното използване, а не да се задължава по универсални правила. Именно използването на подобни лицензии носи най-голям потенциал за противодействие на интелектуалното пиратство, тъй като тяхната цел е да обезсмисли самото съществуване на последното. Тук обаче отново следва да се отбележи нуждата от задълбочено познаване на разглежданата материя, с цел ясно и конкретно дефиниране на интелектуалния продукт и евентуалната свобода на достъп до него от страна на авторите или съответно управленските кадри на създалото го предприятие.



Друг, не по-малко значим обект на интелектуалната собственост се явява един от основните активи на всяко едно предприятие - а именно, ноу-хауто (от англ. know-how) на фирмата, или иначе казано, специализираните практически познания в дадена област (Търговският закон борави с понятието "производствен опит"). С оглед специфичния характер на ноу-хауто е нормално да приемем, че то е обект на фирмена тайна. Липсата на достатъчно добре развити мерки за контрол и ограничаване на достъпа до този вид фирмена тайна се оказва обаче само един от проблемите, които можем да свържем с опазването на фирменото ноу-хау. Не по-маловажен е въпросът, свързан с отстъпване и лицензиране на "производствен опит", което носи огромен потенциал като форма на двустранно изгодно договаряне, но и редица опасности за изтичане на чувствителна информация. Нивото на развитие на т.нар. "Икономика на знание" в Западна Европа и САЩ позволява на тези пазари да се говори все повече за "отворени иновации" и чрез публичното оповестяване на подобна информация и знания (натрупани предимно в академичните среди) да се търси допълнителен стимул за развитието на стопанството. На българския пазар обаче, преобладаващата форма на споделяне на ноу-хау е чрез договорни взаимоотношения, в които страните поемат ангажимент да не разкриват съответната информация, свързана с ноу-хау, но рядко пъти обръщат достатъчно внимание на точното определяне на съдържанието й и достъпа до нея. Така, на практика преотстъпеното ноу-хау често пъти се оказва загубено конкурентно предимство - особено когато липсата на достатъчна яснота относно нуждата за прецизиране и контрол се комбинира с актуалния проблем, свързан с текучеството на кадрите.

Очевидно е, че така представените обекти на интелектуалната собственост всъщност нямат характер на абстрактни понятия, с които се борави единствено теоретично. Реалното им измерение и проникване всъщност е далеч по-осезаемо, отколкото може да се очаква на пръв поглед. От гледна точка на предприятието, тази констатация води до заключението, че интелектуалната собственост следва да бъде разглеждана като сериозен актив - и като такъв, да подлежи на същото ниво на опазване, каквото се предвижда за останалите материални и нематериални фирмени активи. Успешното опазване на интелектуалната собственост трябва да бъде една от основите, на които да се гради цялостното гарантиране на фирмената сигурност, а не второстепенен детайл от нея - особено като се има предвид, че мерките, нужни за опазване на интелектуалната собственост, до голяма степен допринасят и за изграждането на общо приложими добри практики за съхраняване на информацията.

Разгледаното по-горе представя само част от проблемите, които обхваща интелектуалната собственост и които подлежат на ограничаване или предотвратяване при условие, че за защитата й бъдат отделени нужните ресурси. В случая е особено важно да се подчертае непрекъснатото развитие на проблематиката в тази сфера - поради което нуждата от информираност и експертен анализ, извършван от и с помощта на специалисти в сферата, може да се разглежда като постоянна. Въз основа на нуждата от задълбоченост и интердисциплинарен подход при анализа на тези предизвикателства пред предприятието, заплахата от злоупотреба или неправомерно използване на интелектуалната собственост може в контекста на военната терминология лесно да бъде окачествена като асиметрична. Поради това е наложително да е сигурно, че средствата за защита адекватно отговарят на подобен вид опасност, а не целят само осигуряване на съответствие с правните норми.

Автор: д-р Славейко Данчев

ЕТАПИ НА ПРОТИЧАНЕ НА ТЕРОРИСТИЧНАТА ОПЕРАЦИЯ

Изследванията, направени от различни служби занимаващи се с анализ на заплахите за нападения над политически личности, показват общи закономерности. Въпреки, че терористът има определено предимство с акта на изненадата, той има също и слабости, които могат да се използват от правоохранителните органи или частните структури за охрана. Противодействието на един терористичен акт ще бъде ефективно тогава, когато специализираните служби познават добре етапите на терористичната операция. Изследователи по проблемите на противодействието на тероризма дефинират етапите на терористичната операция от 3 до 5.

В изложението по-долу ще разгледаме организацията на изпълнение на терористична операция, съдържаща пет етапа. Считаме, че петте етапа дават по-добра диференциация на отделните дейности, които са включени в изпълнението. Тези етапи са: избиране на обект, проучване на обекта, планиране на операцията, нападение и бягство от мястото на извършване на операцията.

1. ИЗБОР НА ОБЕКТ НА ТЕРОРИСТИЧНА ОПЕРАЦИЯ

В тази фаза групата, организирана или не, избира целта. Изборът на обект съдържа два компонента – мотивационни и целеви.

- Мотивите за избор на обект на терористична операция могат да бъдат от политически характер, идеологически, икономически, етно – религиозен, личностни, психологически и пр.

а) Политическите мотиви на терористичната група обикновено имат за цел смяна на съществуващия обществен строй, смяна на управляващото правителство, елиминиране от политическия живот на политическа личност, която е причина за репресии, политически хаос и пр. При този мотив за избор на обект, могат да се преследват цели във вътрешно-политически или международен план.

б) Икономически мотиви за избор на обект на терористична операция възниква когато субектите на операцията са мотивирани от убеждението, че обектът на операцията е отговорен за лошото икономическо състояние на страната.

в) Етно-религиозни мотиви за избор на обект на терористична операция възниква когато субектите на операцията са мотивирани от убеждението, че обектът е виновен за репресии спрямо религиозната общност или етническата общност, която представляват. Този мотив може да възникне в райони, в които има компактни религиозни или етнически общности.



г) Лични причини за мотиви за избор на обект на терористична операция. Субектът или субектите, имащи намерение, планиращи и подготвящи извършването на терористичната атака са разочаровани от нерешаването на социални проблеми, жилищни, парични и пр. и считат, че виновник за това е определено високопоставено лице. Възможно е субектът/субектите да са водени от силна лична омраза, желание за мъст и пр.

д) Психологически причини, като мотиви за избор на обект на терористична операция. В този случай говорим за умствени разстройства, наличие на психически проблеми, емоционална нестабилност.

- Целевият компонент за избор на обект на терористична операция може да бъде на прагматичен или символичен признак.

а) Символичният обект е лице или обект, който

олицетворява противника, като виновник за всичко негативно случващо се в държавата. Символична цел на терористичната операция може да бъде характерна сграда, посегателството, над която идва да покаже безсилието на държавната власт да се справи със ситуацията.

б) Прагматичен обект се определя, когато субектите на терористичната операция преследват облагодетелстване от действията. Това може да бъде отвличане на определен обект, за който да се иска откуп.

Обект на терористична операция от страна на терористични организации или отделни лица може да бъде президент, министър председател, председател на парламент, министър, началник на Генерален щаб, представител на международна организация, посланик на държава от водещите в световната политика и пр.

Материалните обекти, които могат да бъдат атакувани от терористичните организации или отделни лица са сградите на министерски съвет, президентство, военни учреждения, посолства, полицейско управление или сграда и ведомство, в което има голямо струпване на хора.

Целта е да се избере жертвата, която ще произведе най-голям ефект при минимален риск. Терористите се стремят да изберат високопоставено лице или местоположение, където охранителните мерки са най-слаби.

2. ПРОУЧВАНЕ НА ОБЕКТА

В този етап се събира максимално необходимата разузнавателна информация за обекта на терористичната операция. Един от основните методи, които използват терористите на този етап е наблюдението. Наблюдаващата група събира информация в няколко направления.



На първо място е информация за самия обект. Събира се информация за навиците на обекта, часове на излизане от къщи, маршрути на придвижване до работното място, близки връзки, които го посещават, места, които най-често посещава, семейна среда – деца, съпруга, други роднински връзки. Чрез наблюдение и разузнавателни беседи се добива информация за деловата му активност, отношението и поведението му при провеждане на масови мероприятия, отношение и начин на контактуване със средствата за масово осведомяване.

На второ място е режима на охрана на обекта. Обръща се внимание, на работата на персоналната и обектова охрана. Уточнява се какъв е броя на лицата, изпълняващи задачи като лична охрана, разположение на постовете около дома, начин на носене на службата, има ли пропуски в пропускателния режим. Обръща се особено внимание на режима на посещение на външни лица по местоживеене и месторабота. Наблюдава се по какъв начин се проверяват пощенските пратки, как се пропускат и по какъв ред се заявяват поръчки за ремонти, кабелни и интернет оператори и пр.

На трето място е проучването на маршрута за движение на обекта на терористичната операция. Обръща се внимание на местата, при които кортежа забавя движението си. Това са най – удобните точки, при които може да се извърши терористичната операция. При положение, че обектът на терористичната атака има няколко маршрута за придвижване от дома до работното си място или до други често посещавани места, терористите се стремят да добият информация за цикличността на смяната на маршрутите. Ще подчертаем, че в извънградски условия потенциално опасни са места с остри завои, където кортежа задължително намалява скоростта си. Атаката може да се извърши и на места, където има големи пътни неравности. Това дава възможност за внезапност на нападението. Удобството на извънградските условия, е че нападателите до последния момент не се виждат от екипа за охрана. В извънградски условия екипа за атака винаги може да си осигури числено и огнево преимущество. Най-често обаче терористичните атаки се провеждат при пристигане и тръгване на кортежа по местоживеене или месторабота. Характерен пример за това е опита за покушение над президента на Грузия Едуард Шевернадзе. При потегляне на кортежа от сградата на президентството е взривен лек автомобил на КГБ и произведен изстрел от гранатомет. Благодарение на заслона направен от страна на оперативния автомобил е спасен живота на Шевернадзе, но загива човек от охраната му.

Периодът за изучаване на обекта на терористична-

та атака може да продължи три - четири месеца. Световната практика в това отношение показва, че либийските и германските терористични организации провеждат най-щателно предварително изучаване на обектите. Проучването може да продължи и повече от посоченото време, но терористите винаги се опасяват, че по-продължителното събиране на разузнавателна информация може да ги разкрие. Самото проучване на обекта и събирането на информация за него може да продължи и до деня на извършване на терористичната атака.



Най-често използвани методи за събиране на информация са фотографиране, заснемане с видеокамера, писмени бележки. Наблюдението се води като се търсят подходящи места около дома, по месторабота или по трасетата за придвижване. В много случай се използват автомобили, за да се води наблюдение и да се проследява обекта по маршрутите му за придвижване, с цел натрупване на всякаква необходима информация за операцията. В арсенала на терористите са и използването на незаконни методи за подслушване, набиране на платени информатори и пр.

На съвременния етап на комуникации и развитие на информационните технологии терористите нямат проблеми със събирането на необходимата им информация за обекта на терористичната атака. Улеснени са от средствата за масово осведомяване: Интернет, телефонни указатели, библиотеки, официални правителствени сайтове, справочници и др.

Възможностите на медиите се увеличиха неимоверно през последните години и предлагат голямо количество данни и информация за маршрута на охранявани правителствени служители, за колите, с които се движат, за навици и пр. В манията си да се конкурират в отразяване живота на едно или други високопоставено лице, в позитивна или негативна светлина, медиите неволно се явяват един отличен източник на информация за разузнавателната група на терористите.

Такова проучване винаги е необходимо, дори и непосредствено преди нападението, защото то не може да се осъществи без него.

При проучване на обекта повечето терористични групи действат в малки екипи с проста организация.

Ако направим една ретроспекция на някои от извършените големи терористични атаки над високопоставени персони ще констатираме, че използваната технология се покрива с вече разгледаната по-горе.

При отвличането на Алдо Моро, терористите от "Червените бригади" са познавали деловата му активност и ежедневните му навици и са планирали отвличането му, използвайки тази информация. Известно им е било, че той всеки ден тръгва около 09:00 часа от дома си и се движи по един и същи маршрут. Факт е, че на 16 март 1978 г., малко преди девет часа, председателят на Националния съвет на италианската Християндемократическа партия Алдо Моро излиза от дома си. Качва се в син служебен „Фиат 130", личната му охрана тръгва след него с бяла алфа. Моро не изменя на навиците си. Първото, което прави политикът всяка сутрин преди работа е да посети църквата на площад „Деи Джоки Делфичи", където започва работния си ден с молитва. След църквата маршрутът му е към седалището на Камарата на депутатите. Тази информация е използвана от терористите и на нейна база е направена организацията по отвличането му.

3. ПЛАНИРАНЕ НА ОПЕРАЦИЯТА

Този етап е сравнително пасивен от страна на терористите. Веднъж избрала обекта и събрала достатъчно информация за него, групата преминава към фаза на планиране на операцията. През него се извършват редица дейности като:

а. Пълен анализ на получената от предишния етап информация.

б. Разчет на необходимите средства за оръжие, боеприпаси, автомобили, радио свързочни средства, пари, включително и фалшиви, оборудване и брои на участниците в операцията. Прецизират се допълнителни средства за евентуално бягство и напускане на страната със самолет или други транспортни средства.

в. Във фазата на планиране на операцията, най-важната задача на групата е да прецени тактическите

си преимущества и да разработи детайлно на всички елементи на терористичната операция. Терористите планират внимателно операцията си и осигуряват предимство пред охранителните екипи, като използват следните елементи:

- Изненада – много важен елемент за успешно протичане на терористичната операция;

- Разполагане на подходящо място – високо или такова, което осигурява продължително време видимост и дава възможност да се контролира цялата обстановка по време на протичане на операцията;

- Разполагане на групите за наблюдение и атака по такъв начин, че да не бъдат открити или фиксирани от охраната на обекта на атака. Терористите предпочитат да се сливат с тълпата, с което се избягва евентуалното подозрение или идентифициране от страна на обекта или охраната му;

- Разполагане в такъв обсег на района за извършване на терористичната атака, който да дава възможност на извършителя на атаката да използва планираното за целта оръжие. Групата трябва да има възможност да достигне обекта успешно с оръжието, което използва. В зависимост от обема от охранителни мерки, спрямо охраняваното лице се избира вида на оръжието и начин на действие на групата.

При използването на нож или късоцевно оръжие, изпълнителя трябва да има възможност да е в най-близкото обкръжение на обекта. При засилени мерки за охрана на обекта на терористична атака, трябва да се осигури подходящ обсег за използване на късо или дълго огнестрелно оръжие. За късото не повече от 20 метра. В много случая се действа чрез залагане на взривно устройство по пътя за движение на кортежа или на други подходящи места, свързани с движението и пребиваването на високопоставеното лице.

При слаби охранителни мерки се избира метода на атака с нож или късоцевно оръжие (пистолети с различен калибър). В историята са известни и случай, в които при такъв обем от мерки се действа със самоубийци-камикадзе. Типичен пример за действие от малка дистанция, чрез използване на късоцевно оръжие е опита за покушение над Папа Йоан Павел II и Индира Ганди, министър председател на Индия. Индира Ганди е убита от собствените си телохранители.

Пример за използване на самоубиец-камикадзе е покушението над Раджив Ганди по време на предизборната му обиколка през месец май 1991 г. При убийството на Беназир Бхуто е използван комбиниран метод. Първо са произведени три изстрела с пистолет от преминаващ мотоциклетист и веднага след това се взривява атентатор самоубиец.

Пример за действие при засилени мерки за сигурност е убийството на тридесет и петият президент на САЩ Джон Кенеди през 1963 г. Кенеди е убит със стрелба от разстояние от дълго стрелково оръжие.

- Числено и огнево превъзходство. Едно от важните условия за успех на терористичната операция, с елемент на изненада е осигуряването на числено и огнево превъзходство. В следващия момент органите за опазване на обществения ред и сигурност ще се организират и призоват допълнителни сили и средства за отбиване на атаката и обезвреждане на нападателите;

Тук за пример отново бихме могли да дадем отвличането и убийството на Алдо Моро. Групата от терористичната фракция "Червена армия" е била от 11 човека, срещу 5 души лична охрана. Изстреляни са 91 куршума, от които 45 срещу личната охрана на Моро.

- Избор на време, място и условия на атаката. В резултат на извършено разузнаване на обекта на терористична операция и направения анализ, групата избира място, време и условия, които благоприятстват изпълнението на операцията.

Удобно място е ежедневния маршрут на охраняваното лице от дома до работното място и обратно или до най-често посещавани други любими места.

Практиката е показала, че повечето удобни за действие места са близо до дома или местоработата на лицето, обект на терористична операция, защото високопоставеното лице пътува по тези маршрути всеки ден. Практически може да бъде и всяко друго място, което охраняваното лице посещава в продължение на голям период от време. Високопоставеното лице може да посещава църква, училище, седмични срещи в други правителствени учреждения и пр. Местата около дома и местоработата на високопоставеното лице са удобни са извършване на терористичната атака, тъй като там той се качва и слиза от колата и се създава идеална възможност за провеждане на операцията. При пристигане и тръгване на кортежа от дома или местоработата на охраняваното лице, скоростта на кортежа или автомобила е най-ниска и това също е благоприятно предимство за извършване на операцията.

Терористичната група може да избере и други места от маршрута за движение на кортежа на високопоставеното лице, където той забавя движението си и това дава възможност на стрелящия да порази по-лесно обекта. Практиката е показала, че терористите могат да създадат и възможност за забавяне или спиране на кортежа, чрез друг автомобил или да се възползват от задръстванията по трасето и да осъществят терористичната атака.

- Отвличане на вниманието, вторично или допъл-

нително нападение. В използваните тактически прийоми на терористите влизат и действия, които имат за цел да отвлекат вниманието на органите за сигурност от действителния обект на атака или планираното място. По този начин службите за сигурност и обществен ред концентрират силите си на „фалшивото място" и се създават по – благоприятни условия за успешното извършване на действителната терористична операция;

- Извършване на обучение и усъвършенстване или придобиване на практически способности за извършване на планираното нападение. При този елемент групата за извършване на операцията се упражнява в стрелба със съответно избраните оръжия за реализация на терористичната атака. Обучават се за използването и на по-сложни експлозивни устройства.

- При планиране на отвличане на високопоставено лице се планира детайлно времето, мястото и начина на извършване, както и осигуряването на скривалище за отвлечения, храна и вода, 24-часова охрана на отвлеченото лице, маршрут за бягство, тактика за преговори, начини за връзка между членовете на отделните включени в операцията групи и начина на контакт със силите



за сигурност.

- Планира се времето и начина за заемане позиция на мястото за нападение преди самото нападение, без да се предизвика подозрение и привлече вниманието на органите за сигурност (изискването е да се заеме позиция минимум 20 минути преди нападението).

- Маршрут и план за бягство. На планиращия етап с обсъждане на всички детайли по операцията, особено внимание се отделя на маршрута и начина на оттегляне от мястото на нападението. Предвиждат се съответните транспортни средства, евентуални квартири, в които ще се наложи да се скрият за известно време участниците в операцията. Планира се изработването или снабдяването с фалшиви документи за самоличност, самолетни или други билети за пътуване и пр.

- При терористични организации с голям паричен и човешки ресурс се извършва и проиграване на цялата терористична операция или отделни нейни елементи. Това действие е известно като „репетиция" или „суха тренировка". При нея се отчитат времената за придвижване на групата от едно място на друго, времето за изтегляне и пр.

4. НАПАДЕНИЕ

В този етап се осъществява разработения план на терористичната операция. В планирания ден и час групата за извършване на операцията, като в определени случай това може да бъде само едно лице, извършва терористичната атака. За провеждане на предварителна отвличаща атака се отделят групи и лица в порядъка от 3 до 5 човека. При терористични организации с възможности и достатъчна финансова подкрепа има поддържаща група и група за осигуряване на оттеглянето. При нападението има няколко характерни момента.

а. Разстановка на всички терористични сили на определените съгласно плана места.

б. Началото на фазата нападение може да включва и „идентифициране" на обекта. Непосредствено преди терористичната атака изпълнителя/изпълнителите искат да се сигурни, че това е обектът на нападение. Преди започване на самата операция изпълнителя/изпълнителите искат потвърждение на факта, че обектът е на определеното място във времето, за което е планирано нападението.

в. Лицето, което отговаря за идентифициране на обекта се разполага близо до зоната на атентата и я напуска преди неговото започване. Възможно е след като идентифицира обекта на атаката същото лице да се включи и в екипа за атака. Възможно е обаче и да не бъде част от нападателния екип при групово планираното нападение.

Използвайки радио свързочна връзка, мобилен те-

лефон, радиостанция, сигнални светлини, махане с ръка или сигнал, подаден по друг предварително уточнен начин групата пристъпва към изпълнение на терористичната операция. Практиката е показала, че от подаване на сигнала до започване на терористична операция минават от 20 секунди до минута.

г. Ако групата няма успех с първия план за извършване на терористична операция, изпълнението на втори опит ще бъде по-труден, по-опасен и скъпо струващ. Органите за сигурност ще са започнали дейност по разкриване, предотвратяване и пресичане на следващи опити за терористична операция над високопоставеното лице.

При предварително набелязване на обекта на терористична операция, групата може да работи по дава подхода по отношение на високопоставеното лице – физическо ликвидиране или отвличане.

Направените разсъждения по-горе разглеждаха случаите на физическо ликвидиране на високопоставеното лице, при провеждане на терористична операция.

При планиране, подготовка и извършване на отвличане, по време на терористична операция, терористичната група е подготвила място, на което то ще бъде държано. В случая терористите разчитат на изненадата и внезапността. Действат три групи – едната атакува, втората група елиминира съпротивата на охраната, а третата осигурява оттегляне от мястото на нападение. Следващата фаза е поставяне на искания от страна на терористите към официалните държавни власти или близките на отвлечения. Исканията могат да имат политически характер, икономически и пр. С това действие терористите биха искали и да се легитимират, че съществуват, да печелят симпатизанти. В немалко случаи заложника бива убиван, независимо дали са изпълнени исканията или не.

Тук отново за пример можем да дадем нападението и отвличането на Алдо Моро. Похитителите, които държат високопоставения политик в плен в продължение на 54 дни, издигат редица политически искания за освобождаването му, поставят и искане за освобождаване на група терористи, но преговорите остават без резултат.

5. БЯГСТВО

При планиране на терористична операция се отделя внимание и на бягството или оттеглянето от зоната на нападението. Групата се нуждае от място за нападение, даващо възможност за оттегляне.

Изследователи на тероризма са стигнали до извода, че независимо от мотивите и изповядваните каузи, терористите не са готови да умрат на всяка цена за идеалите, за които се борят и изповядват. С изключение на самоубийствените атентати, малко терористични групи планират операции, при които предварително залагат на самоунищожение. Според изследователи на тероризма самоубийствените мисии не са толкова чести, за колкото се смятат.

Групата за атака, групата за поддръжка, подпомагана от групата по осигуряване на изтеглянето, използвайки предварително разработения план, се опитват да напуснат по най-бързия начин мястото на терористичната операция. В случая могат да се използват предварително подготвени и поставени на определени места леки автомобили. След това се прехвърлят на други,



като първия се изоставя и унищожава чрез запалване или взривяване. Целта на групите е да заличи следите. След това по предварително разработеният план, групата се разквартирува по различни адреси или напуска страната.

В зависимост от ситуацията терористичната организация може да използва резултатите от терористичната операция, за да се популяризира, да заяви съществуването си или да спечели обществена поддръжка за политическа или лична изгода и пр.

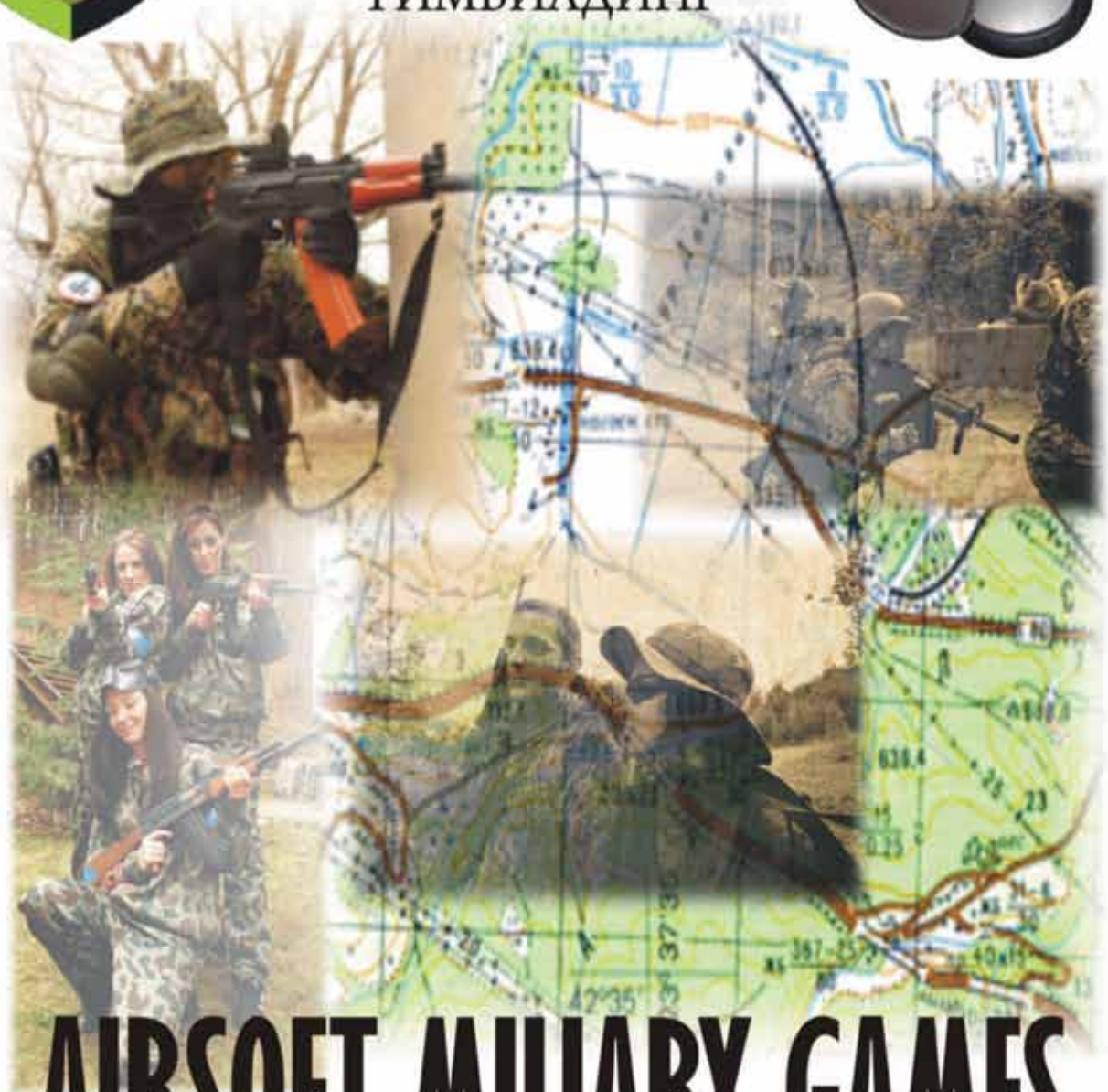
Познаването и изучаването на етапите на терористичната операция и организации, групи или отделни лица, е важно условие за създаване на теоретико-практически модел за действие и взаимодействие между службите за охрана и специализираните звена, службите на МВР и ДАНС. Това създава условия за ефективно противодействие на заплахите към охранявани високопоставени лица и опитите за извършване на терористични атаки към тях и материални обекти от особено важно, стратегическо, национално или гражданско значение.

БЪЛГАРСКИ СТРАЙКБОЛ

VITOSHA

ВОЕННИ ИГРИ
ПРИКЛЮЧЕНИЯ
ЗАБАВЛЕНИЯ
ТИМБИЛДИНГ





AIRSOFT MILIARY GAMES



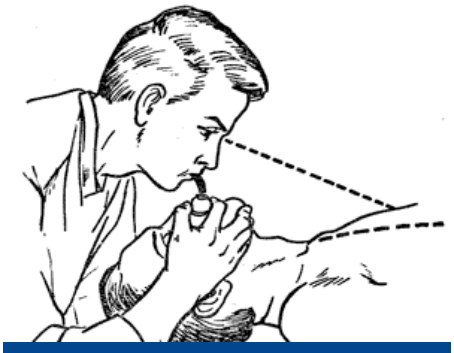
СТРАЙКБОЛ КЛУБ "ВИТОША" **http://teambuilding-vitosha.com/** 0888255468 airsoft@abv.bg Skype: brutalentir

Автор: д-р инж. Милен Иванов

СРЕДСТВА И УСТРОЙСТВА ЗА ОКАЗВАНЕ НА ПЪРВА ПОМОЩ ЗА ТЕЛОХРАНИТЕЛИ И ОХРАНИТЕЛИ

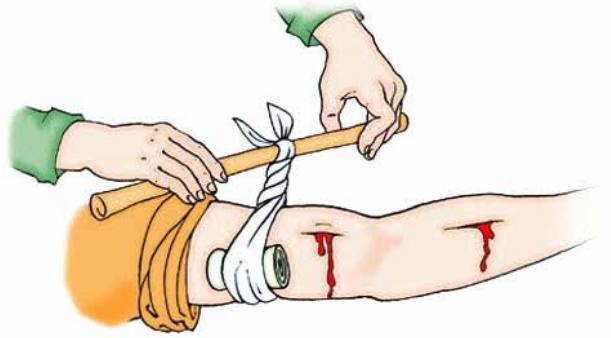
Охранителите и служителите от службите за корпоративна сигурност, постоянно се намират в зони с повишен риск. В екстремални ситуации (техногенни катастрофи в охранявания обект, нападение над него) охранителите, хората работещи в обекта и случайно преминаващи могат да получат тежки травми и да бъде застрашен животът им. Като се има предвид, че сериозните травми могат да предизвикат смърт само за няколко минути и даже секунди, а времето за пристигане на „Бърза помощ“ даже в рамките на населените места е над 10-15 минути, е очевидна необходимостта от взимане на мерки за продължаване на живота на пострадалите до пристигането на специалисти, които да окажат квалифицирана медицинска помощ. Това налага охранителите да знаят и да могат самостоятелно да оказват първа медицинска и екстрена реанимационна помощ. Качеството на тази помощ, зависи от материалното осигуряване със средства за нейното оказване, т. е. от съдържанието на аптечката за първа помощ.

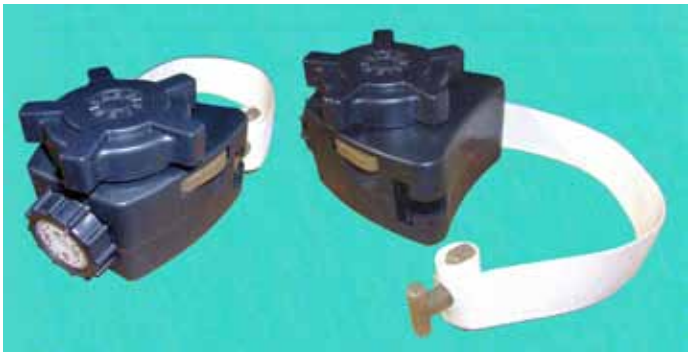
За да има шанс пострадалия да оживее, е необходимо да се изпълнят определени действия. Едно от тях е извършването на изкуствено дишане „уста в уста“ или „уста в нос“. Често обаче лице, което не е медик трудно преодолява погнусата, свързана с наличието на кръв и секрет по лицето на пострадалия. Освен това, широко разпространените епидемии от вирусни хепатит, туберкулоза и СПИН, прави това действие опасно. Затова в аптечката на охранителя е необходимо наличието на устройство за извършване на изкуствено дишане, което позволява да се отстрани непосредственият контакт на пострадалия и реаниматора и да се разделят въздушните потоци. Въпреки, че наличието на такова устройство е задължително по закон във всеки автомобил, доста често то е старо и негодно за употреба. Освен това инцидентът може да се случи далеч от превозно средство.





При нападение на охраняван обект, охранителите могат да получат наранявания от хладно и огнестрелно оръжие, които са съпроводени с обилно кръвотечение и ако са засегнати големи артерии, са способни да доведат до смърт на ранения в рамките на броени минути. Затова е необходимо максимално бързо да се направи кръвоспираща превръзка и да се постави турникет. Съществуват няколко модела турникети - турникет на Петит, Есмархов турникет, турникет „Алфа“, или просто гумен еластичен маркуч. Проблемът, обаче при всички тях е, че имат един съществен недостатък: нито един от тях не може за бъде поставен от ранения сам на себе си. В условията на продължаващо нападение охранителят





може да остане сам. Затова за него е жизнено важно в аптечката си да има съвременен турникет, който може да бъде използван за оказване на самопомощ. Освен, че

може да се използва от ранения, той позволява и да се дозира усилието на притискане, за да не се повредят, намиращите се под него кожа, мускули и нерви.

Бронежилетката отдавна е неотменен атрибут на охранителя. При много видове стрелково оръжие обаче, кинетичната енергия на куршума е толкова голяма, че даже попадение в бронежилетката предизвиква сериозни наранявания с образуване на кръвонасядания и счупване на ребра. Това е съпроводено със рязка болка и ограничаване на подвижността на човека, което в бойни условия силно намалява ефективността на действията на охранителя и в крайна сметка може да му струва и живота. Най-ефективното средство в тези ситуации е охлаждането на мястото на поразяване. Тъй като никой охранител не носи със себе си торбичка с лед, а вероятността да бъде ранен в близост до фризер (за да използва лед или замразено месо) е малка, затова наличието в аптечката на хипотермичен (охлаждащ) пакет е задължително. Той е компактен и с него може да се борави лесно - добавя се вода и се притиска към поразеното място. Ниската температура намалява чувството за болка и кръвонасядането. А ако хипотермичния пакет се използва за охлаждане на рани (след превръзването й със стерилна превръзка), то това просто действие „консервира“ раната (намалява кръвотечението, отока и размножаването на болестотворни микроорганизми), което позволява да се отложи първичната хирургическа обработка на раната и намалява риска от загнояване.



Задължително в аптечката трябва да има и превързочни средства - бинтове, марли, стерилни салфетки (напоени с кръвоспиращи и дезинфициращи вещества) и лейкопласт. За обработка на краищата на раните е необходимо да има йодов разтвор или кислородна вода.

Освен тези средства, аптечката за първа помощ за охранителя трябва да бъде окомплектована със обезболяващи препарати, а също така и със медикаменти използвани при сърдечни болести (валидол или нитроглицерин), и незаменимия при колабиране - амонячен разтвор. Като се има предвид и опасността от заразяване е задължително да има и гумени хирургични ръкавици.

Тези медикаменти и устройства трябва да са поставени в калъф или кутия, от която те да могат да се изваждат във всеки един момент. Достъпът до тях трябва да е толкова лесен, колкото е лесен достъпа до пистолета в кобура. Понякога това може да се окаже по-важно, от възможността за изстрел.

По отношение на екипировката на телохранителите, тя трябва да се различава от тази на обикновения охранител. Тъй като задачата на телохранителя не е да си оказва помощ сам на себе си или на ранен колега, а да спаси живота на охраняваното лице,. Затова е необходим допълнителен набор от медикаменти и устройства, позволяващи да се продължи живота, включително и устройства за компресионно-декомпресионна реанимация, която значително повишава ефективността на сърдечната реанимация. Сред най-необходимите медикаменти са препаратите, защитаващи главния мозък от кислороден недостатъчност (антихипоксанти), органопротектори; средства, повишаващи съпротивителните способности на организма (адаптогени); глюкокортикостероиди, сърдечно-съдови средства и т.н. Допълнителните средства и устройства може да се поставят в багажника на автомобила, а основните в чанта за скрито носене на кръста. В автомобилите на екипа на достъпно място трябва да има комплект противогази, които в необходимия момент, ако атаката е придружена и с обгазяване, да бъдат използвани от охранителния екип и от охраняваните лица.

В заключение трябва да се отбележи, че наличието на всичко необходимо в аптечката не гарантира, че помощта на пострадалия ще бъде оказана от телохранителя или охранителя в необходимия обем. За да може в критична ситуация да се използва този набор, са необходими знания и умения, които се придобиват в процеса на обучението, за оказване на първа медицинска помощ. Само доведените до автоматизъм изпълнения на определен алгоритъм от практически навици може да позволи да не се изгуби ценно време в сложна ситуация и да се спаси човек. Такива начални знания и навици в България могат да се придобият на курсовете, организирани на Български червен кръст. Но, за да може един телохранител наистина да е способен да спаси живот при всяка една ситуация, е необходимо той да премине специализиран курс по екстремална медицина.

Автор: д-р, инж. Милен Иванов

СНАЙПЕРСКИТЕ ПУШКИ - НАЧИН НА УПОТРЕБА



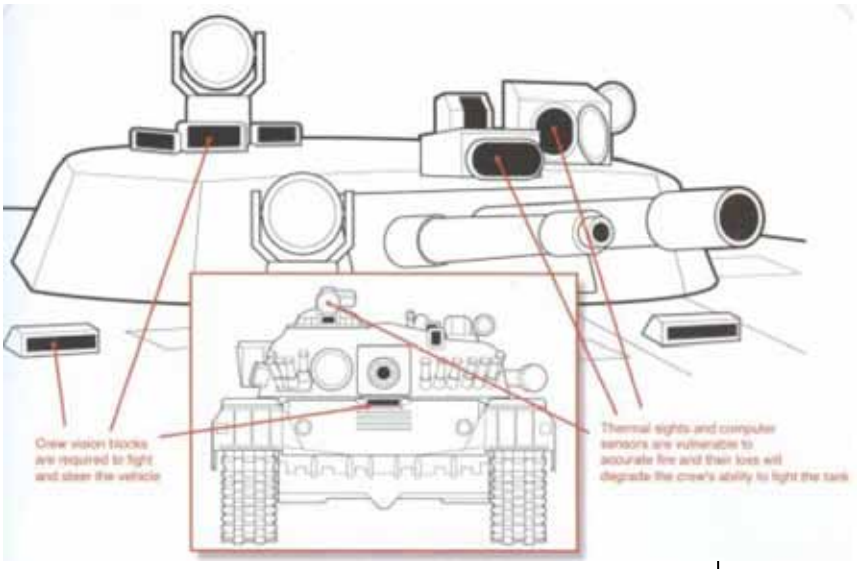
Един от съвременните аспекти на снайперската тактика, безспорно е използването на тези добре обучени стрелци за поразяване на материална част, оборудване, машини и превозни средства, които могат да включват всичко - от самолетни радари, генератори, танкове, екипажите обслужващи различни оръжейни системи, военни и граждански самолети и дори военни кораби, комуникационни системи, и ракетни системи. Конфликтите през последните години генерираха изобилие от примери за ефектите от такова използване на снайперистите и за влиянието, което оказват техните умения на воденето на бойните действия.

Има изобилие на информация за това къде да бъде прострелян човек, за да се постигне максимален ефект - графични диаграми на човешкия мозък и други части от анатомията и какво въздействие им оказват високоскоростните боеприпаси. За разлика от това почти липсва литература, с акцент върху това, какво се случва с машините и оръжия, когато биват поразени от куршум, изстрелян от снайперска пушка. Например, традиционно, бронираните машини и танковете се описват като цели, които не се атакуват с леко стрелково оръжие. Много наставления описват танковете като чудовища, притежаващи добра защита от поражения, нанесени от леко стрелково оръжие и мини. Това може да е вярно от гледна точка на екипажа под бронята, но не е вярно за танка като цяло. Танковете, и всъщност всички бронирани автомобили са клаустрофобично място, и поради това, екипажите им прекарват по-голямата част от времето си извън тях, като главата и горната част на тялото им е показана през люковете извън защитата на дебелата броня. Те са подходяща цел за снайперска атака, и тъй като танкът е толкова ефективен, колкото е ефективен неговия екипаж, премахването на екипажа прави и самия танк безполезен. Нивото на шума в работещия танк е толкова високо, че членовете на екипажа трябва да носят шлемофони и да са свързани с вътрешна разговорна система, за да общуват, а това силно ограничава слуха им. В гореща и задушлива среда, и с



ограничен слух, членовете на екипажа, намиращи са на купола на танка предоставят на снайпериста възможност да ги елиминира бързо, дори с пушка с болтов затвор. Преди втората цел да осъзнае защо партньорът му се е отпуснал напред той също ще бъде поразен. Но дори и вторият член на екипажа да осъзнае, че се намират под обстрел, купола, т.е. бойната система на танка остава обслужвана само от един член на екипажа, който в момента е зашеметен и има силно ограничени възможности за наблюдение и за управление на огъня.

Съвременните танкове имат набор от оптични и термовизионни системи и камери, които могат да направят начинаещ снайперист много лесна мишена, но за опитен и добре обучен снайперист тези системи не представляват голяма заплаха. По-голямата част от тези системи разчитат на оптични лещи, които трябва да бъдат насочени към целта, за да може тя да бъде разкрита, а това предоставя на снайпериста чиста линия за огън срещу окулярите и шанс да унищожи оптиката и ефективността на самата система. Някои армии вече са признали този проблем, главно вследствие на попадения на шрапнели или камъни, хвърлени от недоволно население при миро-опазващи операции и затова на танковете се монтират екрани от ограничителна мрежа, с цел защита на лещите. Това обаче не е от голяма полза срещу снайперист, стрелящ от сравнително близко разстояние и използващ оръжие калибър .338 или .50.



В допълнение на оптиката за наблюдение, модерните танкове са оборудвани с набор антени и сензори, необходими за система за контрол на огъня на танка. Те позволяват да се прихващат и унищожават цели докато танка се движи и то дори в екстремни граници. Ако тези системи бъдат повредени или унищожени, екипажът трябва да се върне към старите методи за изчисляване на данните за стрелба и произвеждане на изстрел, което води до значително намаляване на възможностите на брониранта машина. С използването на снайпери .50-калибър за поразяване на области като водещите ролки, двигател, горивни резервоари, външни силови агрегати, също може да се намалят бойните способности на танка.



Използването на снайперисти за стрелба по бронетранспортьори (БТР) е друга област, в която може да се разгърне максимално потенциала на снайперската атака. БТР-ите имат много по-лека защитна броня от тази на танковете и тя лесно може да бъде поразена от леко стрелково оръжие и ракетни системи. Екипажите им страдат от същата тенденция да се возят над броневата защита и следователно да са лесна цел за снайперски огън. Веднъж принуден да се скрие в корпуса на машината екипажът има ограничена възможност да наблюдава бойното поле. Това намалява ефективността на бойната машина и увеличава потенциала за успешна атаката на противника, което показва отново колко много снайперистите могат да повлияят на баланса на силите в боя. С появата на преносими оръжия .50 калибър и бронебойните, силно експлозивни или запалителни боеприпаси, леките бронетранспортьори вече са силно уязвими.



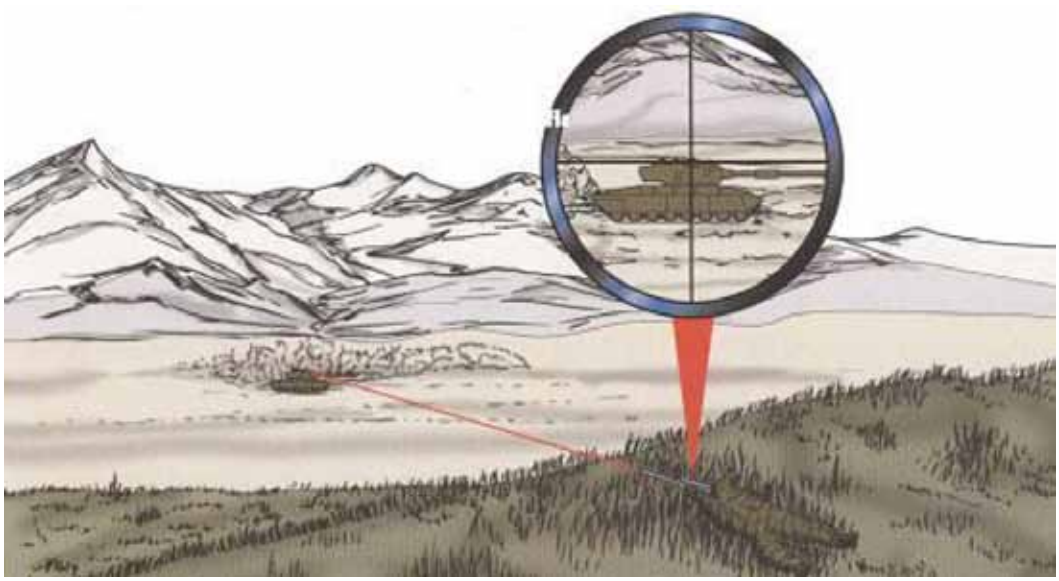
резервоари с гориво, контролни устройства и т.н. Да не споменаваме, че и екипажа, който обслужва тези ракети, най-често е съставен от високо класни и ценни специалисти, и също представлява важна цел.

Други важни цели за поразяване от снайперисти могат да са: разчетите и системите за управление на огъня на зенитната артилерия, тежката полева артилерия и минохвъргачките, радари и системи за сигурност, радио и комуникационни системи, командири и политически лидери, самолети (бойни и транспортни), кораби и др.

Друга, често поразявана цел от снайперисти са небронираните военни транспортни средства. Те са уязвими по отношение на всички снайперски боеприпаси, и могат да бъдат унищожавани, както екипажите, така и превозните средства, в зависимост от тактическата им стойност.

Силно уязвими са и всички видове ракетни системи, което ги прави мишена за снайперските оръжия от различни калибри. Всяка ракетна система се състои от няколко задължителни елемента, като машина за изстрелване, радар за насочване, и различно оборудване за определяне на местоположението на целта, и всички тези елементи са от съществено значение за цялостната оперативна ефективност на ракетната система. Ако е обучен да разпознава тези елементи и различни системи, снайперистът е в състояние да локализира и идентифицира основните компоненти на ракетната система и да използва по най-ефективен начин оръжието си, за да намали или да унищожи способността им да функционират. Например радара за позициониране на целта има механични системи, приемник и чиния, както и блок за управление с електроника, и всички те се повреждат лесно от точен огън. Самата ракета има механични системи за насочване и

Тези възможности да повлияят на баланса на силите и изхода на военните операции със сравнително прости и евтини за използване средства в последните години дават силен тласък на развитието на конструкторската мисъл в насока към разработване на нови поколения снайпери и боеприпаси за тях. Подобрява се подготовката на снайперистите. Увеличава се техния брой и включването им както в армейските и полицейски сили със специално предназначение, така и в стандартните войскови подразделения. От друга страна това води до появата на множество системи за успешно откриване и локализиране на снайперисти, за които ще разкажем в следващия брой на списанието.



Автор: Марияна Николова

БЕНЧРЕСТ



Какво е „Бенчрест", как и къде се практикува това интересно хоби ни разказа Роберт Атанасов - главен редактор и издател на списание „Български ловецъ" и професионален ловец, познат на ловното общество от телевизионната поредица „Време за лов", излъчвана по телевизия „ТВ7", по „Хоби ТВ" и редица ловни филми.

Бенчрест е високо прецизна снайперова стрелба с оръжие с централно възпламеняване. В България първият бенчрест клуб е основан преди около 10 години от Светослав Стефанов, по прякор Томпсъна, той е един от най-компетентните хора в тази област. В последствие се формира и федерация на прецизните стрелци - Българска бенчрест федерация. Периодично всяка година се провеждат национални състезания. Тазгодишното състезание се състоя на 15, 16, и 17 юни. На 14 юни беше тренировъчен ден, на 15 юни - стрелба на 100 м., на 16 юни - стрелбата на 300 м., а на 17 юни на 500 м., или половин километровата дистанция за най-добрите стрелци. Събитието се проведе във Враца на ведомствено стрелбище, високо в планината, красива местност и страхотна емоция за всички почитатели на прецизната стрелба. За състезанието всеки сам се подготвя както намери за добре, неангажиращо.

Който реши да участва като състезател е важно е да знае за регламента и оръжията, които се допускат. Оръжията са в три класа: първи клас – ловен, това е класическата ловна карабина, в произволен калибър с централно възпламеняване - разрешени са оръжия от .22 до .40 калибър. Във втория клас калибрите са пак същите, но той се води тактически, в който може да използват оръжия с подвижни бузи, с облекчено усилие върху спусъка, с плоска полуложа, т.н. тактически оръжия, които се използват при военни, полиция и специални части. Третият клас, най-високия е „бенчрест", в който се използват специално подготвени карабини, не серийно производство, с различни калибри, отново до .40. Състезанието винаги е много оспорвано и става все по-оспорвано, защото нивото на състезателите като подготовка и оборудването, с което разполагат непрекъснато търпи прогрес. Разликите между спечелилите първите места стават все по-малки. Турнирите в трите класа винаги са оспорвани, а състезателите са около 40-50 човека максимум.

Всички, които желаят да участват са поканени. Необходимо е желаещият да притежава едно от тези оръжия, няма право да наема оръжие или да използва оръжието на друг човек. Като цяло за трите дни на състезанието са нужни около 90-100 патрона на състезател в съответния клас. Стреля се по мишени – два броя, първата е проверовъчна – попаденията в нея не са зачетни, а втората мишена е зачетната. Трябва да се направят пет изстрела на минимално разстояние един от друг. За разлика от други видове стрелба, където целта е да се уцели десетката, тук целта е групата от пет изстрела да е максимално събрана, да има най-малък диаметър. Този участник, който има в три поредни мача най-малък сбор от диаметъра на групите изстрели е победител. Стрелбата се изпълнява от специална маса, върху която се поставя оръжието. То е в статично положение и дава възможност да се извлече максимума. Практикуващите бенчрест са наясно колко трудно е да се направят 5 изстрела в една и съща дупка на 100 м разстояние. Когато то е 200, 500 или 1000 м, подобна възможност става илюзорна. Важно е да се покаже, че оръжието, подборът на боеприпаси и всичко останало е направено по максимално добър начин, а стрелецът от своя страна притежава необходимите качества, за постигане на целта.

Голям плюс и победа за българските състезатели, е правото да могат да самоснарядяват боеприпаси, т.е. подготовката на боеприпаса се прави изцяло от състезателя, а не както в миналото - с готови, закупени амуниции. Това е възможно благодарение на усилията на членовете на федерацията по бенчрест, с чиято помощ е приет закон, позволяващ самоснарядяването.

Бенчрест федерацията планира в бъдеще да прави това събитие поне три пъти на година. Макар, че състезанието, дори веднъж годишно, дава преценка за подготовката на хората и мотивира заниманието им с тази спортна дейност. Като хоби то е скъпо - оборудването на средно ниво, например в ловен клас, излиза над 10-15 000 лв. Отделно се заплащат боеприпасите, които не са евтини, има и допълнителни разходи, като престоя по време на състезанието, тренировките и т.н. Приходи няма, цялата необходима база се поддържа с волни пожертвувания на членовете на федерацията. На практика състезателите не търсят признание, а подобряване на собствените си качества като стрелци. Това е благороден мотив, макар и да не е вечен, е страхотна движеща сила за търсене на съвършенството в себе си. Може да се сравни с изпадане в нирвана и пълна хармония с оръжието, стрелеца и обстановката.

Повече информация за бенчрест може да се намери на http://www.bglovec.com и на страниците на списание Български Ловецъ.

СНАЙПЕРСКАТА ВИНТОВКА ВССК „ВЫХЛОП“: ЛИКВИДАТОРЪТ

Когато един изстрел решава всичко...

В началото на 21-и век с бурното нарастване на актовете на тероризъм в световен мащаб, без съмнение възниква и необходимостта от създаване на нови, специфични оръжия за борбата с новите специфични задачи, с които все по-често се сблъскват армейските и антитеристичните подразделения на засегнатите от тях държави. Спирането на коли-бомби, обезвреждането на импровизирани взривни устройства от разстояние, ликвидирането на терористи, намиращи се в обкръжението на цивилни лица или заложници, са все неща, с които конвенционалното армейско и полицейско въоръжение, стоящо в различните армии, в много случаи не успява да се справи достатъчно ефективно. Именно за подобен тип задачи в днешно време до голяма степен се разчита на снайперската стрелба, но не със стандартните снайперови карабини, а с такива изпълнени в 50-ти калибър (12,7 мм) – или иначе казано, крупнокалибрени, специални снайпери.

Точно поради тези причини през 2002 г. Центърът за специални задачи на федералната служба за сигурност на Руската Федерация (ФСБ) възлага специална поръчка на централното конструкторско бюро на именитите оръжейни заводи в град Тула: да се разработи специална, крупнокалибрена безшумна и безпламенна карабина, която да обезпечава изключително ефективно поразяване на защитени цели, като например автомобили, лека бронетехника, жива сила на противника, намираща се в укрития или защитена с бронежилетки и други подобни задачи.

Резултатът от работата на тулските оръжейници е крупнокалибрената снайперска карабина "Выхлоп", представена за първи път през есента на 2005 г. на московското оръжейно изложение „Интерполитех”.



Снайперската винтовка ВССК "Выхлоп"

След представянето й започват изпитания на новата карабина и доколкото е известно, скоро след това неголеми серии от нея са приети на въоръжение в някои спецотряди на Федералната служба за сигурност на Русия.

Новото оръжие е изпълнено по схемата „булпап” (пълнителят и затворът се намират в задната част на оръжието, зад ръкохватката), което е малко нетрадиционно за руската оръжейна школа, но пък е напълно в синхрон със съвременните оръжейни концепции. В оръжието стандартно е интегриран заглушител, който освен почти безшумна (звукът от изстрела е само 123 децибела, което за този калибър е отлично) обезпечава и напълно безпламенна стрелба. Заглушителят, разбира се, може да се снема от цевта на карабината, което се прави при почистването и пренасянето й. Точно зад заглушителя на винтовката е интегрирана и сгъваема двунога, която осигурява стабилното й позициониране при заемане на стрелкова позиция. На оръжието могат на бъдат монтирани оптически и нощен прицел, а освен това то разполага и с резервни, механични мерни прибори, които са сгъваеми. Затворът на карабината е болтов, като заключването му става чрез ротация на ръкохватката за зареждане, която се намира от дясната страна на оръжието. Както вече споменахме, пълнителят се намира зад пистолетната ръкохватка и събира пет патрона.

Тук е моментът да кажем нещо и за боеприпасите: за тази карабина е разработен специален патрон, в калибър 12,7 х 54 мм. Новият боеприпас получава сигнатура СЦ-130 и използва силно утежнен куршум, който е дозвуков още при напускане на цевта (началната скорост е 290-295 м/с). Ползват се три разновидности на този патрон: СЦ-130ПТ, СЦ-130ПТ2, СЦ-130ВПС, като според производителите и трите вида боеприпаси обезпечават ефективна стрелба на разстояние до 600 метра.



12,7х54 мм специален патрон за комплекса ВКС / ВССК "Выхлоп", отляво-надясно: СЦ-130ПТ, СЦ-130ПТ2, СЦ-130ВПС

Теглото на куршума при първите два модела е 59 грама, като на 100 метра постижимата група с тях е 25 мм., а дулната им енергия на такова разстояние е от порядъка на 2500 джаула. Третият модел (СЦ-130ВПС) е с повишено пробивно действие, като на 200 метра производителите гарантират пробиването на 16-милиметрова стоманена плоча, а на 100 метра - тежка бронежилетка клас V (по руския стандарт). Дулната енергия на този патрон също е по-висока от тази на другите два – 3650 джаула на разстояние 100 метра.

В заключение можем да кажем, че налице е едно интересно оръжие. Прави впечатление, че оръжието не е полуавтоматично, което снижава темпа на стрелба, но затова пък болтовият затвор обезпечава по-висока точност и надеждност. Комбинирани с тежкия, мощен боеприпас, тези две качества несъмнено гарантират висока ефективност, когато нещата трябва да бъдат решени само за миг, само с един изстрел...

Parabellum,
по материали от Интернет

RENT AND SALE - 02 / 480 40 00, 0888 955 544



PROJECT:

AMFION LTD.
BUILDING WORKSHOP
02/964 12 80
0886 885 788
FAX: 02/963 35 57
WWW.AMFION-BG.COM

OFFICES

SHOPPING AREAS

PARKING PLACES


ДЗИ
PROSPERITAS SECURITAS
Част от KBC group
KBC
ТРАДИЦИИ
и иновативност