PROFESSIONAL

Брой 6, година III, януари - март 2011

ЗАЩИТА ОТ ПОДСЛУШВАНЕ



ISSN 1314-0574
9 771314 057400

Разпространява се безплатно

„ПРОФИСЕК-НС” ООД



В СФЕРАТА НА СИГУРНОСТТА:

Издателска и рекламна дейност;
Организиране и провеждане на обучение;
Консултантска дейност;
Проектиране и изграждане на системи за сигурност.

АДРЕСИ:
гр. София, ул. Бигла 16А, вх. Б
гр. София, бул. Стамболийски № 108, ет. 1, ап. 6
e-mail: ns@profisec.bg
тел./факс: 02/962 05 23
www.profisec.bg

НС ПРОФИСЕК

Уважаеми читатели,

Приоритетно значение за списание **PROFESSIONAL** имат проблемите на сигурността, охраната и бизнеса. Правилното решаване на свързаните с това задачи изисква активното участие на различни държавни и частни организации. Необходимо е отчитане на успешния опит на всички субекти в България, и в други страни, и внимателното му приложение спрямо нашите условия. Особено важна задача на вашето и нашето списание е да съдейства за подготовката на висококвалифицирани специалисти.

Готови сме да предоставим място за публикации на статии, свързани с темите на списанието.

СИГУРНОСТ

Защита от нерегламентирано подслушване 2

Сигурността в нашето ежедневие 6

Контролирана доставка 12

ЗАЩИТА НА ИНФОРМАЦИЯТА

Политика за мрежова сигурност 14

Защита на GSM от подслушване 16

НАЦИОНАЛНА СИГУРНОСТ

Международната сигурност и националната сигурност 18

Специални обществени поръчки 20

ОХРАНА

Ефективна подготовка на охранители 23

Мобилни комплекси за периметрова охрана 26

СПЕЦИАЛНИ ЧАСТИ

Антитерористични операции 29

БИЗНЕС

Езикът на тялото 32

Седем стъпки за ефективен конкурентен бенчмаркинг 34

ХОБИ

Стрелба - форми на тренировъчна дейност 36

ОРЪЖИЯ



Израелската Tavor TAR 21 стр. 38

ЕКСТРЕМНО

Военни игри - еърсофт

Всяка неделя в Лозен!

Страйкболни оръжия под наем:

Камуфлажна униформа, очила/маска, каска и добро настроение - БЕЗПЛАТНО.

Игрите могат да се провеждат на място по ваше желание и да бъдат комбинирани и допълвани, в зависимост от индивидуалните нужди на вашата организация.

За повече информация посетете **www.strikeball.org** или се свържете на тел. 0888255468 с Георги Ангелов



PROFESSIONAL

Национална асоциация на фирми за търговска сигурност и охрана (НАФТСО)

Заедно ще постигнем повече!

Сдружение с идеална цел, което обединява търговски дружества, предоставящи услуги в сферата на сигурността. Уеб адрес: **www.naftso.org.**

Центърът за изучаване на рисковете и сигурността (ЦИРС) към Нов български университет (НБУ) е научно-изследователско звено, което работи в областта на сигурността от 2004 година, като освен изследователска дейност, обучава студенти и докторанти в бакалавърски, магистърски и докторски програми.

ЦИРС организира научни прояви и публикува доклади и научни съобщения от национални и международни конференции, както и участва със свои преподаватели и студенти в прояви от този характер, организирани у нас и в чужбина.

Водени от необходимостта да се даде поле за научни изяви на колегите от ЦИРС, както и на специалистите по сигурността в страната, преподавателите от Центъра предвиждат създаването на списание по проблемите на сигурността, с периодичност два пъти годишно.

Списанието ще предлага възможности за публикуване в редица раздели, посветени на различни аспекти на изследване на сигурността.

В първия брой на списанието, с работно заглавие "Сигурност 21 в." ще се предложат статии от авторите доц. д-р. Юлиана Каракънева, доц. д-р. Христо Георгиев, проф. д.и.н. Димитър Йончев, д-р. Николай Радулов, както и на други специалисти в областта.

Списанието ще публикува материали на външни автори, при условие, че предложените материали получат положителни научни рецензии.

За контакти с издателите на списанието се обръщайте към:

Доц. д-р. Христо Георгиев, Директор на ЦИРС

Тел./факс 00359 (2) 8110 272

ГЛАВЕН РЕДАКТОР - Николай Цапрев

ЗАМ. - ГЛАВЕН РЕДАКТОР - Слави Райков

Отговорен редактор - Марияна Николова

Оформление и дизайн - Христо Грънчаров

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 - FOTOLIA, iStockphoto и Dreamstime

тираж - 3000 бр.

PRINT - INARTVISION

инж. Николай Цапрев

ЗАЩИТА ОТ НЕРЕГЛАМЕНТИРАНО ПОДСЛУШВАНЕ

През първите месеци на 2011 год. една от основните теми в медиите и публичното пространство беше подслушването. Законно или незаконно, със санкция или без санкция. Покрай скандалите със СРС се появиха множество публикации и репортажи показващи всякакви способи и средства за подслушване. Стана ясно, че в България отдавна подслушването е лесно достъпно, широко разпространено и обичайна практика. Имам предвид всички видове подслушване извън разрешените от закона. Някой хора бяха развеселени от този факт, други притеснени, а на трети им беше любопитно. Странна е реакцията, която се наблюдаваше през това време. Вместо притеснение за личните, фирмените и други данни и чувствителни видове информация и предприемане на мерки за тяхната защита, се наблюдаваше засилен интерес към всякакви видове и начини за подслушване. Сайтовете, продаващи „шпионски" атрибути буквално бяха блокирани от посещения. Повечето от тях бързо изчерпаха наличните стоки. Наблюдението на трафика в интернет и анализа на ключовите думи, използвани в интернет търсачките показа засилен интерес към методите за подслушване.

Логично е този засилен интерес да доведе до увеличаване на броя и усъвършенстване способите на нерегламентираните подслушвания в страната.

В същото време се наблюдава увеличаване на предлагането на услугата, имаща за цел да разкрие и неутрализира подслушващи устройства в дома, офиса, автомобила, GSM–а и на други места. При предлагането на тази услуга често разни хора и фирми разнасят черни кутийки с антени, правят тайнствени физиономии и дават заключения и съвети на тези, които са ги наели. В сайтовете за шпионски атрибути се продават и вълшебни кутийки на цена около 200-300 лв., чието предназначение е да откриват подслушвателни устройства или да блокират тяхната работа. За незапознатите използването на подобни устройства изглежда лесно, интересно, разумно и работещо. На запознатите с тези технологии им е ясно, че това са пълни глупости и е само добър способ за прибиране на пари.

Нека видим какво в действителност представлява услугата, имаща за цел да защитава от подслушване. На жаргон този вид услуга е известна като чистене или прочистване. Военния термин използван в армията на САЩ и армиите на страните членки на НАТО, който придобива все по-голяма гражданственост е TSCM (Technical Surveillance Counter-Measures). На български език няма точен термин. Горният термин се определя като изследване, извършвано от квалифициран персонал, с цел да се установи наличие на технически средства за наблюдение и контрол, да се определят слабостите в системата за сигурност, които могат да доведат до техническо проникване и изтичане на информация от обследвания обект. TSCM изследването трябва да даде професионална оценка на техническата сигурност на обекта, като за целта се извършва задълбочена визуална, електронна и физическа проверка.

С навлизането на компютрите, мобилните телефони и множество средства за жичен и безжичен пренос на данни, както и наличието на различни протоколи за пренос на данни, при извършването на проверките за подслушване все по-голяма тежест имат елементите на информационната, комуникационна и физическа сигурност, както и изследването на електромагнитните излъчвания.

Голямо внимание трябва да се обърне на навиците и обучението на персонала, както и на конструктивните особености на обекта.

Проверката за наличие на подслушвателна апаратура и изтичане на информация по технически път е методичен, последователен и широко обхватен процес, извършван от добре подготвени хора, разполагащи и използващи голям набор от технически средства и похвати.

За да извърши някой защита от подслушване би следвало да знае способите за подслушване. Без познаване на способите за подслушване, техническите средства, хардуерни, софтуерни продукти и инженерни решения, използвани за тази цел, както и демаскиращите ги признаци не е възможно да се открие добре поставено подслушвателно устройство.

Без внимателно изследване на обкръжаващата среда, техническите средства, охраната и организацията на работа в даден обект, не може да се направи анализ на риска, да се определи степента на застрашеност, вероятните цели на подслушването, вероятните изпълнители, вероятното ниво на използваните техническите средства и способи, както и възможността да бъдат използвани спрямо обследвания обект.

От това какъв е проверявания обект и кой има ин-



терес да го подслушва могат да се направят изводи относно финансовия ресурс и техническата обезпеченост на вероятните извършители на подслушването, а от това могат да се направят изводи за вероятно използваните устройства. Ниската техническа обезпеченост и ниския финансов ресурс, водят до масово използване на предлаганите по интернет средства за подслушване, намиращи се в ценовия диапазон 100 – 500 лв. и работещи по не повече от четири-пет различни начина. Това ограничава сферата на тяхното използване и ги прави сравнително лесни за откриване. Хората, разполагащи с голям финансов ресурс могат да си позволят професионална техника и да използват професионалисти за нейното поставяне, а това означава, че за откриването на такава техника се изисква сериозна работа, добра техника и подготовка на екипа.

На базата на собствения си опит, бих направил следната класация на най-застрашените от подслушване хора. Не коментирам лицата, извършващи действия против националната сигурност и обществения ред.

– Застрашени от подслушване са: известни хора, кино звезди, знаменитости.

– Помещения за търгуване на стоки или ценни книжа, инвестиционни банкери, инвестиционни посредници, брокери, преговарящи по договори, подготвящи оферти.

– Бизнеси, които се местят в нови офиси или развиват нови съоръжения и проекти, бизнес, който е обект на враждебни поглъщания.

– Хора, които имат достъп до класифицирана информация.

– Хора или бизнеси въвлечени в граждански съдебни процеси.

– Офиси и лица, занимаващи се с политически кампании, политически ситуации.

– Жертви на вманиачени преследвачи.

– Доброволчески организации.

– Религиозни групи или деятели.

– Учени, разработващи нови технологии и устройства.

– Фирми и лица обекти на промишлен шпионаж.

По-долу са изброени тези, които най-често извършват подслушванията:

– Конкуренти или съдружници.

– Участници в търгове спрямо останалите участници или спрямо възложителите.

– Съпрузи и любовници.

– Началници спрямо подчинени, подчинени спрямо колеги и началници, човешки ресурси, вътрешна сигурност.

– Съседи, любопитни, маниаци, случайни.

Горната подредба е направена съгласно статистически данни за честотата на прилаганите и поръч-

вани подслушвания. Ако някой има съмнения може да отвори пресата за последните две години, да види изнесените случаи на нерегламентирани подслушвания и да направи собствен анализ. Ще припомня някой от тях. Общината в Бургас – залата за заседания на комисиите по търговете, МВР – Стара Загора – бивш началник подслушвал подчинените си и проверяващите от министерството, Военна полиция – бивш началник подслушвал подчинените си, Фитнес залата на хотел Шипка на Министерството на отбраната, таксита на софийска таксиметрова компания, хотелски стаи.

Най-често използваните средства и способи за подслушване са:

- Мини диктофони и мини камери, камуфлирани в различни предмети от бита – часовници, ключодържатели, запалки и т.н.

- Радио микрофони, GSM-микрофони, различни BLUETOOTH, Wi-Fi ,IP и WIRELESS устройства.

- Софтуер за подслушване чрез GSM телефони, компютри, лаптопи и таблети.

Характерното за горе изброените средства е, че са широко достъпни и сравнително евтини. Много от тях не са специално конструирани за подслушване устройства, а представляват стандартно оборудване, намиращо се в домовете, офисите, джобовете, чантите и автомобилите на хората. Използването им не изисква сериозни технически умения. Характерна особеност е, че всички средства позволяващи достъп до кабелен или безжичен интернет и до мрежите на мобилните оператори, позволяват подслушването да бъде извършвано от всяка точка на земята.



Изброените до тук способи и средства са само илюстрация. Всъщност широко известните способи за подслушване са повече от осемнадесет, а средствата, използвани за това са трудно изброими. Ето разнообразието съпътстващо най-известния и до скоро най-използван способ – подслушване чрез радио микрофон.

Радио микрофоните се различават по честотите, които използват, по това дали могат дистанционно да бъдат изключвани или включвани, дали се активират от шум или не, каква модулация използват, с дистанционно регулируема или постоянна мощност, използват ли криптиране на сигнала, протокол за пренос на данни, под носеща или други методи за маскиране на излъчването, дали са цифрови или аналогови, ползват ли пакетно импулсно излъчване (burst transmission) и т.н. Според Wikipedia описанието на последния термин е следното: „Предаване, което съчетава много висока скорост за предаване на информацията с много кратко време на предаването - т.е., съобщението е компресирано. Това е популярен метод на военните и шпионите, чиято цел е да се предаде голямо количество информация като едновременно с това се сведе до минимум възможността предаването да бъде открито или прехванато." Гражданския аналог на този вид предаване е изпращането на MMS през GPRS канала на мобилен телефон. Чрез MMS за няколко секунди може да бъде изпратен записа на 20-30 минутен разговор.

Отриването на най-известния и стар способ за подслушване, радио микрофон, би трябвало да е най-разработено методически и технологично и да е най-лесно. Всъщност вълшебните кутийки с антени, кръстени бъг-детектори са предназначени за откриване само на радио микрофони. Хубавото е, че цените им са ниски. Лошото е, че не вършат работа. В повечето случаи тези устройства работят в ограничен диапазон, прихващат основно аналогови сигнали с честотна или амплитудна модулация, като пропускат всички останали, а освен това дават множество фалшиви сигнали, прихващайки излъчвания нямащи нищо общо с подслушването.

За откриването на един работещ радио микрофон на цена 100 – 350 лв. са необходими няколко различни устройства за прихващане, изследване и локализиране на радио излъчванията. Това са минимум четири различни типа устройства и минималната цена на такъв комплект е около 15 000 лева. Освен това е необходима база данни, добър екип и добра методика на работа. Например, един работещ радио микрофон се открива много по-лесно от изключен такъв или работещ с понижена мощност. За целта проверката трябва да е изненада за подслушващите и да се извърши при условия, предполагащи интерес от страна на подслушващите – тоест да поддържат микрофоните включени.

Проверките за наличие на подслушвателна апаратура и за изтичане на информация през технически средства са няколко типа, в зависимост от начина на провеждането и обхвата им. Това определя цената, продължителността им и срещу какъв тип подслушване са насочени. Една поговорка гласи, че се залагат минимум три микрофона. Един за да бъде намерен от лаици, един за да бъде намерен от професионалисти и един за слушане.

Минималния обхват на една проверка включва:

Анализ на спектъра на радио честотите.

Проверка на захранващата мрежа.

Анализ на кабелните линии.

Проверка за наличие на технически средства в

конструктивни елементи и оборудване, използвайки средства за неразрушаващ контрол.

Подробна физическа инспекция и визуален оглед на рисковите места и оборудване.

Анализ на вероятните места за изтичане на информация.

Изготвяне на препоръки за повишаване на сигурността.

Времетраенето на една проверка е строго индивидуално. Зависи от вида на проверката и от самия обект. В някой случаи може да продължи няколко дни. Във всеки случай 20 минути не стигат само за разполагането и включването на оборудването. Давам примера с 20 минути, защото много „специалисти", разнасящи разни кутийки с антени, фазомери, мултицети, осцилоскопи и прочее „антишпионско" оборудване се „справят" в рамките на това време.

Всъщност принципа на проверката е много прост. Търсят се демаскиращите признаци на средствата за подслушване.

Единият проблем е, че те са много. Това са вибрации, звук, електромагнитни излъчвания, микровълни, лазерни и инфрачервени излъчвания, топлина, изкривяване на полета, промяна на протоколи за пренос на данни, промяна в работата на стандартни устройства и други. За прихващането на всеки демаскиращ признак трябва отделен уред и подход. Околната среда в градовете е силно замърсена от други подобни излъчвания. Освен това са взети мерки излъчванията на подслушващата техника да не бъдат открити.

Вторият проблем е, че подслушването винаги върви преди защитата. Първо някой открива нов способ за подслушване, прилага го на практика, минава време преди някой друг да го открие, минава още време преди да се разработи техника и методика, способни да откриват този вид подслушване и 10-20 години след това, тези средства и методи за защита се появяват на пазара за граждански цели.

Написаното до тук означава, че 100% гаранция при проверките няма. За това усилията трябва да бъдат насочени към разработването и налагането на система, недопускаща възможността за залагане и използване на средства за подслушване в даден обект, блокиране работата на евентуално заложени такива и своевременното им откриване. Налагането на такава система е свързано с обучение, прилагане на организационни и технически мерки, извършване на конструктивни промени и най-вече системна работа в тази насока.

Повече за подслушването през и на GSM апаратите можете да научите от 2-ри, 3-ти и 4-ти брой на списанието, които могат да бъдат прочетени и изтеглени безплатно от **www.profisec.bg.**



Бакой Бакоев
експерт в "ТЕХНОТЕСТ" АД www.technotest.bg

СИГУРНОСТТА В НАШЕТО ЕЖЕДНЕВИЕ

Човек в своето битие в голяма степен жизнено се нуждае от сигурност, която играе съществена роля в живота му. Сигурността е доминираща категория за определяне на психическото здраве, без което е невъзможно осъществяването на жизнените дейности на индивида.

Живеем в един глобален, динамичен и преди всичко несигурен свят. Наличието на криза, безработица и обедняване на населението винаги водят до увеличаване на криминалните прояви, като особено място сред тях заемат кражбите. Около 3000 обира на жилища са регистрирани за 2010 г. в София и района. Необходимо е да се отчете и, че много от хората по различни причини не уведомяват полицията за случилото се. Това предполага, че цифрата на влизането с взлом определено е по-голяма.



Освен това не може да се пропуснат и значителните по брой престъпления извършвани в търговски обекти, офиси, складове, банкови институции.

Тази картина не е само в нашата страна. По един банков обир се извършва средно на всеки час и половина в държавите от Европейския съюз, показват официални данни на Европейската федерация на банките. Около 6 000 банки годишно стават обект на грабежи в ЕС. В Европа се притесняват, че при кражбите от банки все по-често се прибягва до екстремно насилие. Това като тенденция до скоро не съществуваше в България, но неофициалните данни за изминалата 2010 г. водят до извода, че рязко се е променило съотношението между взломните кражби и въоръжените обири.

Има ли някакъв начин да се ограничи тази тенденция и да се увеличи процента на неуспешни опити за кражби? Тези въпроси определено вълнуват почти всеки. Отговорът не е едностранен и не може да бъде дадена гаранция, че съществува средство или система, която ще възпре напълно криминалния контингент. Той се корени и в онази максима, в която се казва, че всяко нещо съградено от човека винаги намира свой антипод измислен от друг. Въпреки това, че абсолютна гаранция не съществува, на пазара се предлагат множество продукти и услуги за изграждане на системи за физическа защита за възпрепятстване на престъпленията.

В ежедневието си постоянно се сблъскваме с многобройните иновативационни новости в сферата на сигурността, които включват най-новите hi-tech технологии. Сигнално-охранителни системи, видео наблюдение, умни сгради и автомобили, мобилна видео връзка, GPS проследяване, интегрираните системи за контрол на достъпа, електронни средства срещу кражба – списъкът е дълъг. Иновациите в тази област продължават да се появяват лавинообразно и цените, срещу които може да се търси сигурност за дома, офиса, търговския обект, склада, финансовите институции, държавните и обществени сгради вече достигат суми от десетки хиляди левове.

Въпреки изместването на така наречените „средства за физическа сигурност" от нови технологии напоследък експертите все по-често изтъкват, че сигурността следва да бъде комплексна. Именно поради това при оценката на риска всички елементи, влияещи върху степента на защита имат определено място в общата система. Наличието на възможности за заглушаване на сигналите излъчвани от СОТ, изолиране на видео наблюдението или неутрализиране на охраната, доказано от регистрираните случаи на дръзки обири, дава основание за твърдението, че времето на „старите" средства все още не е отминало.

Предназначението на тези продукти, съчетано със съвременните системи за охрана е да не се допусне или максимално да се затрудни проникването с взлом в сградите, ограничаване на достъпа



до ценни предмети, пари, информация и защита на хората. Не бива да се отминава факта, че тези средства предпазват и от прояви на вандализъм, природни стихии, аварии, пожар и терористични актове и също осигуряват определена безопасност на хората.

Ще разгледаме част от средствата, осигуряващи физическа сигурност на обектите. В тази категория са включени входните врати, прозорците, щорите, капаците, защитното остъкляване и хранилищата за ценности.

Входните врати.

Наричат ги лицето на една сграда. Напоследък при тяхното производство се съчетават съвременните технологии с използването на традиционни материали. Темата обаче засяга само тези, които осигуряват устойчивост срещу взлом и куршуми или популярно наречените „блиндирани врати". Техните качества, осигуряващи защитата им срещу отваряне, разбиване и пробиване, се базират на използваните конструкция и материали. Крилата на тези врати представляват оребрена стоманена рамка. Особено място в нея заема и допълнително монтираната защита на затварящия механизъм и ключалките. Така образуваната скара се запълва с подходящи материали, осигуряващи допълнителна защита срещу оръжие, огън, звук и топлина. Крилото се закрепва стабилно към усилена метална каса чрез панти и затварящи щифтове (активни и пасивни).

Прозорци, защитни капаци и щори

Конструкцията, използваните материали и технологията за изработване на крилата и рамките на прозорците, капаците и щорите е сходна с тази на вратите. Тук тя следва да бъде оптимална, съчетаваща максимална здравина в ограничени размери и тегло. Комбинират се материали като стомана, алуминий и PVC. Използват се усилени части на обкова и заключване на затварящи механизми.

За всички продукти съществуват допълнителни изисквания към техните каси. Те следва да осигуряват степен на защита най-малко равна с тази на крилото и да бъдат стабилно закрепени към отворите на стените. Разбира се преди да се заявят и монтират тези продукти е нужно да се провери от какво са изградени стените. Защото колкото и парадоксално да звучи има случай за искане монтаж на врата, притежаваща една от най-високите степени за защита, на стена изградена от пенобетон.

Обковът (заключващи механизми, ключалки, панти и дръжки) към указаните продукти следва да отговарят на определени изисквания, които гарантират общата устойчивост на продукта.

Защитни стъкла

Защитното стъкло има висока степен на устойчивост на взлом и куршуми и осигурява максимална защита на сградите и хората в тях. Разработването на защитно остъкляване премахна дискомфорта от липсата на естествена светлина в помещенията при спуснати плътни капаци и щори, както и не винаги лице приятната гледка на монтираната решетка. Най-новата технологията за остъкляване се базира на използване многопластовото стъкло съчетано с ламинатно фолио. Тези стъкла се използват и при опазването от кражба на ценни предмети в музеите, защитата на касовите гишета във финансовите институции и човека зад тях от простреляване със стрелково оръжие.

Пластовото стъкло се произвежда чрез свързване на два или повече слоя обикновено прозрачно стъкло и защитно фолио, най-често поливинил бутарил (PVB). Няколко от основните предимства на продукта е, че слоя фолио задържа пластовете стъкло, свързани дори след счупването им, и високата му якост предотвратява начупването на стъклото на големи остри парчета, което е гаранция освен за взломо устойчивост и куршумо устойчивост, така и за безопасност.

Защитните стъкла имат още една положителна страна. Те предлагат степен на защита на обитателите при инциденти. При случайно падане на човек върху остъкляването, фолиото осигурява равномерно поемане на удара и не допуска пробив на

стъклото, а при неговото напукване не се отделят остри и опасни фрагменти.

На пазара се предлага и защитно фолио, което се залепва върху вътрешната плоскост на вече съществуващото остъкляване. Този начин на укрепване определено стабилизира стъклото, води до значително по-трудното му разбиване и преди всичко осигурява безопасност поради липса на стъклени отсколки в помещението при неговото разрушаване. Слабост, която се допуска в този случай е, че слоя фолио не покрива краищата на стъклопакета и не се укрепва в рамката на крилото. Така при силен удар може по-лесно да се отдели цялото стъкло от рамката. Като цяло прозорецът със стъклото не отговарят на завишените изисквания поради факта, че рамката и касата на прозореца не са с необходимите качества и не ограничават опитите за проникване с взлом.

Хранилища за ценности

Почти няма офис или търговски обект, в който да липсва металния сейф (свободно стоящ или вграден) . Той е най-разпространеният представител на групата средства за защита наричана – хранилища за ценности. Тук, освен него, влизат АТМ сейфовете, съхраняващи парите в банкоматите, трезорните помещения (масивни и модулни), трезорните врати и депозитните системи.

Тези продукти се монтират в сградите, а някои от тях като АТМ сейфовете и депозитните системи и на техните фасади. Предназначението им е да осигурят съответната степен на защита на ценности, пари в брой или информационни носители, както от взлом, така и от въздействието на пожар или друго стихийно бедствие.

При тях съществуват допълнителни изисквания към вгражданите ключалки, а при свободно стоящите сейфове и депозитни системи и за стабилното им закрепване (анкериране) към стените или пода на помещенията/сградите.

Изисквания към продуктите за физическа защита

Специфични изисквания, на които следва да отговарят изброените продукти и степените осигуряващи определени нива на защита са регламентирани в европейски норми, приети като български държавни стандарти.

За врати, прозорци, капаци и щори това е стандарт БДС ENV 1627. Той посочва шест класа на съпротивление (от 1-ви до 6-ти) срещу взлом, като първият клас е с най-малка степен на защита, а шестият с най-високата. Тези класове се определят на основание показаните резултати при три вида изпитвания, регламентирани в съответните стандарти БДС ENV 1628 - статично (натиск), БДС ENV 1629 - динамично (удар) и БДС ENV 1630 - ръчно (с използване на инструменти). Освен това в тези продукти следва да бъде вграден обков с доказани качества, осигуряващи дадения клас посочени в стандарти като БДС EN 1303 - за секретните патрони на ключалки, БДС EN 12209 за механични ключалки и БДС EN 1906 за дръжки.

Друг стандарт за тези изделия е БДС EN 1522, който определя седем класа (от FB1 до FB7) за устойчивост срещу куршуми на стрелково оръжие. Класовете се определят в зависимост от калибъра и вида на използваното оръжие, като се започне с най-лекото оръжие- малокалибрена пушка, пистолет и се достигне до големокалибрена пушка.

Изискванията за защитните стъкла се регламентират в БДС EN 356. Посочени са осем класа (от P1A до P8A) за устойчивост срещу ръчна атака. Изпитванията се извършват с нанасяне удари върху стъклото със стоманена сфера или брадва. Вторият стандарт за стъклата е БДС EN 1063 с, който се регламентират седем класа на защита от куршум (от BR1 до BR7). При изпитването на стъклата се използват същото оръжие и боеприпаси, както при вратите. Тук в обозначението се използват символите S и NS, означаващи съответното наличие или липса на отсколки зад стъклото. Когато се оценява комплексно остъклена врата или прозорец се изисква вложеното стъкло да покрива напълно степента на защита на цялото изделие.



За хранилищата за ценности стандартите са няколко и посочват тяхната степен на съпротивление на взлом. Стандартът БДС EN 14450 за сейфове покрива най-ниските класове за защита, обозначени с S1 и S2. Основният стандарт за хранилищата за ценности е БДС EN 1143-1. В него се регламентират съответните степени на защита за сейфове, АТМ сейфове, трезорни помещения и трезорни врати. Втората част на този стандарт БДС EN 1143-2 определя нивата на защита на депозитните системи. Освен класификацията на тези продукти стандартите регламентират и начина за изпитване. Методът е с използването на набор от инструменти да се достигне частичен и/или пълен достъп до съдържанието на хранилището. В зависимост от времето, за което е направен отвора и категорията на използваните инструменти се изчислява неговата степен на съпротивление. Тя се обозначавана с 0 (минималната) или римска цифра от I до XIII (максималната). За депозитните системи допълнително към това обозначение се изписват буквите D (дневен) и N (нощен).



Стандартите регламентират и начина за изпитване и класификацията на продуктите на устойчивост на взлом след използване на взрив (обозначава се с индекс EX) и използване на инструменти с диамантени остриета (обозначават се с индекс CD).

Отделно бравите, вграждани във вратите на хранилищата, следва да притежават степен на защита съгласно стандарт БДС EN 1300, а анкерното закрепване на сейфове и депозитни системи се изпитва за устойчивост чрез прилагане сила на опън/натиск.

Необходимо е да се знае, че върху всеки продукт (хранилище за ценности), който отговаря на посочените стандарти следва да бъде монтирана маркировъчна табелка, върху която е нанесен номера на стандарта и степента на съпротивление на взлом.

За въвеждане на изискванията на тези стандарти в страната ни съществуват редица подзаконови документи, като Наредба № I-171 от 2 юли 2001 г. за организацията и контрола по обезпечаването на сигурността на банките и небанковите финансови институции издадена от МВР и БНБ и Методика за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация, приета от ДКСИ с Протокол № 165-I/30.06.2004г

Прави впечатление, че изискванията към продуктите за физическа защита, посочени в стандартите се прилагат само в някои по-специфични сфери на дейност – като банковата и тази касаеща класифицираната информация, а в останалите области те не са застъпени и не са отразени. В съществуващите европейски документи, регламентиращи изискванията към планирането и построяването на сградите, указващи различни методи и мерки за превантивна дейност срещу престъпленията за зависимост от резултатите на анализа на риска, се определят класове за тяхната сигурност. За всеки клас се препоръчва използването на дадено средство за физическа защита, отговарящо на ниво на сигурност, посочено в коментираните стандарти. Такива документи са: CEN/TS 14383-3, който посочва изискванията за предотвратяване на престъпления при проектиране и планиране на жилищни сгради; CEN/TS 14383-4 за магазини и обществени сгради (офиси), CEN/TS 14383- 5 за горивозарядни станции и др. Въпреки, че като член на Европейския съюз България е приела тези документи (същите са включени в каталога на БИС) в българските подзаконови документи, които касаят строежите, конкретно Наредба № 7/08.07.1998 г на МРРБ за системите за физическа защита на строежите се указват категории на обектите, но никъде няма отразени конкретни изисквания към техните елементи, отговарящи на дадената категория.

Оценяване на продуктите

Как да бъдем сигурни, че предлаганият ни продукт притежава необходимата степен на защита и кой може да ни даде гаранция за неговото ка-

чество? Доказателство може да бъде единствено оценяване на съответствието, т.е. доказване чрез изпитване, контрол и оценка, че определените изисквания, заложени в нормативно-технически документ (стандарт), за даден продукт, са изпълнени.

Съществуват три нива за оценяване на съответствието в зависимост от това кой го извършва:

- Оценката се извършва от „Първа страна“ - лицето, което представя продукта. Това е производителят, който чрез писмен документ - декларация гарантира качеството на продукцията си;

- Оценката се извършва от „Втора страна“ - лицето, което ще използва продукта. Оценката на съответствието тук е насочена към проверката до каква степен декларацията, дадена от производителя, отговаря на истината;

- Третата степен и определено най-сигурна е оценката извършена от „трета страна“, независима от производител и потребител - така наречения орган по оценяване на съответствието. Той на базата на извършената оценка издава сертификат за конкретния продукт. Тази дейност се нарича сертификация и в преобладаващите случаи не представлява едноактно действие. След издаване на сертификат за продукта продължава дейността с извършване на по следващи оценки (надзор). Те имат за цел непрекъснат контрол над продукта и неговият производител и недопускане несъответствие с доказаните показатели. Организацията, която извършва тази дейност се нарича орган по сертификация на продукти. Изискванията на, които следва да отговаря подобна структура са регламентирани в БДС EN 45011 (ISO/IEC Guide 65).

Какво гарантира, че съответния орган е достатъчно компетентен и независим за извършване на съответната дейност и отговаря на изискванията на посочения по горе документ? Доказателство за това е наличието на акредитация, дадена му от съответния национален акредитиращ орган. За България този орган е определен от Закона за акредитация и е ИА „Българска служба за акредитации” (БСА).

В България единственият акредитиран орган за сертификация на продукти за физическа защита е направление „Оценяване” към ТЕХНОТЕСТ. Той притежава издаден сертификат от ИА „БСА” Рег. No 4 ОСП. В декларирания му обхват са включени продуктите сейфове, трезорни помещения, трезорни врати, депозитни системи, пешеходни врати, прозорци, капаци, щори и защитни стъкла.

Подизпълнители на органа за сертификацията на средствата за физическа защита са изпитателните лаборатории на направление „Изпитвания” – ТЕХНОТЕСТ, Института по отбрана – МО и „Минпроект” ЕАД.

Тези лаборатории са уникални поради факта, че единствени в страната ни притежават стендово оборудване и извършват изпитвания по изискванията на цитираните стандарти.

На какви изисквания следва да отговарят продуктите и каква е процедурата, по която дадени производители могат да получат сертификат за техните изделия?

Основните изисквания са две:

- резултатите от извършените изпитвания на образци от продукта да показват, че той отговаря на един от посочените по-горе стандарти;

- условията на производство на съответния производител да отговарят на необходимите критерии заложени в процедурата на органа.

Достъп до услугата за сертификация имат всички производители на продукти за физическа защита, които изпълняват изискванията, независимо от притежаваните производствени мощности и брой на персонала.

Редът за издаване на сертификат е посочен в утвърдена схема по сертификация и процеса на оценка се извършва съгласно приетите процедури. В схемата е отразен и по следващия надзор, извършван от органа по сертификация с цел потвърждаване на дадената оценка на съответния продукт.

Дейността по сертификацията на продукти не е насочена само, за да се установи възможностите на производителя за произвеждане на съответното изделие и му се издаде сертификат. Резултатите от нея могат да бъдат използвани от потребителите за защита на техните интереси, от специалистите по сигурността при изграждане на съответните системи за охрана, от застрахователите за оценка на риска при сключване на застрахователни полици за имущество, от регулаторните органи при въвеждане в практиката съответните изисквания на нормативните документи.

Сертификацията на продуктите за физическа сигурност е особено важна за гарантиране на нивото на защита, защото за разлика от други продукти, чиито качества могат да бъдат оценени в процеса на тяхната експлоатация, единственият начин за доказване устойчивост на взлом и куршуми е провеждане на разрушителни изпитвания. Така при покупка или монтиране на едно изделие без сертификат няма процедура, която да определи неговото ниво на защита, без да го унищожи или при най-лошия сценарий да изпита качествата му при една взломна кражба. На това основание Ви съветваме - осигурете си сигурност и спокойствие с продукти за физическа защита, притежаващи легитимни сертификати.

Коментари, мнения и въпроси на e-mail:
techno-cert@medicom.bg



КОНСУЛТАЦИИ И НАДЗОР
В ПРОЕКТИРАНЕТО
И СТРОИТЕЛСТВОТО

гр.София, р-н Триадица, м."Жил. група Южен парк", бл. 28,
evronorm_bg@abv.bg, тел./факс: 963 00 65

"ТРИСТАН 02" ООД

www.tristan02.com

Акумулатори за:
- Леки и тежкотоварни автомобили
- Мотори, ATV, моторни шейни
- UPS системи, СОТ системи
- Пожароизвестителна техника



гл.ас. д-р Симо Михов
Преподавател в Академия на МВР

КОНТРОЛИРАНА ДОСТАВКА В РАМКИТЕ НА ПОЛИЦЕЙСКОТО СЪТРУДНИЧЕСТВО В ЮГОИЗТОЧНА ЕВРОПА

Контролираната доставка, визирана в Конвенцията за полицейско сътрудничество в Югоизточна Европа е един от основните инструменти на международното полицейско сътрудничество за противодействие на трансграничната престъпност в Балканския регион. В изпълнение на тази конвенция, Република България е сключила с други страничленки по нея редица двустранни и тристранни протоколи и споразумения.

Контролираната доставка е оперативен способ, който се прилага при използването на технически средства - електронни и механични съоръжения, както и вещества, които служат за документиране на дейността на контролирани лица и обекти, с цел изготвяне на веществени доказателствени средства по дадено наказателно производство. Тя се прилага от разузнавателния орган и се използва от разследващия орган в кръга на компетентността му при непрекъснат контрол на територията на Република България или друга държава в рамките на международното сътрудничество и се изразява във внасяне, изнасяне, пренасяне или транзитно превозване през територията на Република България от контролираното лице на вещ - предмет на престъпление, за да се разкрият участниците в трансгранично престъпление.



Във връзка с последното, от гледна точка на териториалния обхват на една контролирана доставка могат да бъдат разграничени следните два вида:

1. Вътрешна – разрешение за нея се дава от Председателя или упълномощен от него Зам. председател на съответния териториално компетентен окръжен (или Софийски градски) съд;

2. Международна (или трансгранична) контролирана доставка – компетентен орган да се произнася по отправена от друга държава молба за котролирана доставка през територията на България е Върховна касационна прокуратура. Когато международната котролирана доставка е по инициатива на български разследващ орган, освен разрешение от председателя или упълномощен от него зам. председател на съответния териториално компетентен окръжен (или Софийски градски) съд, Върховна касационна прокуратура, в качеството си на контролен орган, трябва да се произнесе с постановление във връзка с нейното осъществяване.

Обект на контролирана доставка може да бъде единствено вещ, която е предмет на престъпление, а не контролираното лице (лица), което я пренася. Като най-чести обекти на контролираната доставка могат да бъдат посочени следните категории: наркотични вещества и прекурсори, огнестрелни оръжия и взривни вещества, културно-исторически ценности, фалшива валута и предмети, които са обект на престъпление или за които има намерение да се използват в престъпление.

Освен изведените по-горе, обект на контролирана доставка могат да бъдат и други недвижими вещи, които са предмет на престъпление. Физически лица не могат да бъдат обекти на контролирана доставка (напр. при трафик на хора с цел сексуална или трудова експлоатация, при каналджийство и др.).

Осъществяване на международна контролирана доставка на територията на страните-членки на Конвенцията за полицейско сътрудничество в Югоизточна Европа

Осъществяване на международна контролирана доставка, съгласно Конвенцията за полицейско сътрудничество в Югоизточна Европа (КПСЮЕ) може да се иска между две или повече държави, подписали Конвенцията, в рамките на национални разследвания на престъпления, за които се предвижда екстрадиция. Тогава при писмено запитване от едната договаряща страна другата договаряща страна може, ако е целесъобразно, да разреши контролирана доставка на своя територия. За иницииране на една контролирана доставка в рамките на полицейското сътрудничество в Югоизточна Европа е необходимо молещата договаряща страна да обясни, че без такава мярка установяването на извършителите или на каналите за разпространение би било крайно затруднено. Ако съдържанието на контролираната доставка представлява определен риск за участващите лица или заплаха за обществото, замолената договаряща страна има право да изиска спазването на определени условия, преди да разреши или да откаже искането.

Замолената договаряща страна поема контрол върху доставката при пресичане на границата или на място на поемане, което е договорено от правоприлагащите органи, за да се избегне нарушение на контрола, и гарантира постоянно наблюдение на пратката по начин, който позволява намеса на полицията по всяко време.

Обектът на контролираната доставка (или лицето/лицата, или превозното средство, в което е установено че се намира обекта на контролираната доставка) трябва да бъде под постоянен и непрекъснат визуален контрол от страна на служителите, изпълняващи наблюдението над него. Между екипа, изпълняващ наблюдението, групата за реализация и задържане и Центъра, ръководещ операцията по провеждането на контролираната доставка, задължително трябва да има сигурна и постоянна връзка.

След поемането от страна на замолената договаряща страна служителите на молещата договаряща страна могат да продължат да следват контролираната доставка заедно със служител на замолената договаряща страна при договореност със замолената договаряща страна. Служителите на молещата договаряща страна са длъжни да съблюдават законите на замолената договаряща страна. Ако компетентните правоприлагащи органи на замолената договаряща страна не могат да се намесят

навреме и ако продължаването на контролираната доставка представлява сериозен риск за живота и здравето на лицата или причинява сериозна щета върху собствеността, или ако доставката не може повече да се държи под контрол, служителят на молещата договаряща страна може да изземе контролираната доставка. Ако е необходимо, служителите на молещата договаряща страна могат да спрат и арестуват лицата, които придружават пратката, до намесата на правоприлагащите органи на замолената договаряща страна. При всички случаи молещата договаряща страна информира незабавно правоприлагащите органи на замолената договаряща страна. Когато една контролирана доставка е иззета на територията на замолената договаряща страна, тя може да бъде предадена на молещата договаряща страна въз основа на писмено запитване. Лице, което е било арестувано от компетентните местни органи може да бъде задържано за разпит независимо от своето гражданство. Съответните разпоредби на националното право се прилагат mutatis mutandis. Ако лицето не е гражданин на договаряща страна, на чиято територия лицето е арестувано, това лице се освобождава не по-късно от 6 часа след задържането, като не се включват часовете между полунощ и 9.00 ч. сутринта, освен ако компетентните местни органи не са получили предварително молба за предварителен арест на това лице за целите на екстрадицията под каквато и да било форма.

Общи условия във връзка с осъществяването на контролирана доставка:

- служителите, извършващи наблюдението, трябва да спазват правото на договарящата страна, на чиято територия действат; те трябва да се подчиняват на инструкциите, издадени от компетентните местни органи;
- по време на наблюдението служителите трябва да носят документ, удостоверяващ даденото разрешение;
- служителите, извършващи наблюдението, трябва във всеки един момент да могат да докажат, че действат в качеството си на длъжностни лица;
- забранява се влизането в частни домове и места, до които няма публичен достъп;
- служителите, извършващи наблюдението, не могат да призовават или арестуват лицето, което наблюдават;
- за всички операции се изготвя доклад до органите на договарящата страна, на чиято територия е извършено наблюдението; служителите, извършващи наблюдението, могат да бъдат помолени да се явят в съда;



- органите на договарящата страна, от която идват наблюдаващите служители, когато са замолени от органите на договарящата страна, на чиято територия се извършва наблюдението, подпомагат разследването, което следва операцията, в която са участвали, включително съдебното производство, при условие че самоличността на участващите служители е защитена.

Официално писмено запитване, с което се изисква контролирана доставка, чийто контрол започва или продължава в трета държава, се удовлетворява само когато в запитването е посочено, че определените в Конвенцията условия са изпълнени и от третата държава.

Компетентни органи в Р България

във връзка с осъществяването на международна контролирана доставка са ГДБОП, ГД "Гранична полиция", СДОТО-МВР, Териториално компетентен Окръжен съд или СГС (при контролирана доставка по инициатива на България), Върховна Касационна Прокуратура, П Агениция "Митници".

Процедура за осъществяване на международна контролирана доставка в рамките на полицейското сътрудничество в Югоизточна Европа по инициатива на Р България

Процедурата най-лесно може да бъде представена в следните последователни стъпки :

1. а) Получаване на сигнал за подготвян незаконен експорт на недвижима вещ – предмет на престъпление - откриване на наказателно производство във връзка с това; или

б) Получаване на информация в хода на вече открито наказателно производство за подготвян трафик на вещ – предмет на престъпление;

2. Максимално запълване на информационните празноти по т. 1, докато количеството информация относно подготвящия се трафик се прецени като достатъчно за иницииране на международна контролирана доставка;

3. Използвайки каналите за връзка на международното полицейско сътрудничество, вземане на принципно съгласие от всички страни по пътя на трафика (в това число и от страната, установена като крайна дестинация на трафика);

4. Вземане на официално съгласие от всички страни, по пътя на трафика (в това число и от страната, установена като крайна дестинация на трафика);

5. Оформяне на "Искане" до Върховна касационна прокуратура, с копие до Агенция "Митници" за получаване на разрешение установеното превозно средство (или човек), с което се пренася обекта на трафика, безпрепятствено да премине границата на Република България;

6. Издаване на Постановление от Върховна касационна прокуратура, с копие до Агенция "Митници", с което на практика се разрешава да се извърши контролирана доставка през територията на страната;

7. Подготовка на необходимите документи за въвеждане в експлоатация на СРС и получаване на разрешение за последното от териториално компетентния окръжен съд (или от Софийски градски съд).

8. Осъществяване на непрекъснат контрол над обекта на контролираната доставка до напускане пределите на страната и предаването му на компетентния орган от съседната страна-членка на Конвенцията, който да продължи контролирането на обекта;

9. Уведомяване Върховна касационна прокуратура за постигнатия резултат.

Източници :

1. Закон за специалните разузнавателни средства, обн. ДВ. бр.95 от 21.10.1997г., последни изм. ДВ. бр.1 от 4.01.2011г.

2. "Конвенция за полицейско сътрудничество в Югоизточна Европа"

3. "Конвенция за прилагане на споразумението от Шенген от 14 юни 1985г."

4. "Наръчник за международно оперативно полицейско сътрудничество" – Министерство на вътрешните работи на Република България

5. Наказателно-процесуален кодекс, Обн. ДВ. бр.86 от 28.10.2005г., последни изм. ДВ. бр.101 от 28.12.2010г.;

6. "Протокол за засилено тристранно сътрудничество в борбата с престъпността и особено трансграничната престъпност, между Правителството на Република България, Правителството на Румъния и Правителството на Република Сърбия", подписан на 29.09.2008г., в сила от 01.10.2009г.

7. "Споразумение между правителството на Р България и правителството на Румъния за трансгранично полицейско сътрудничество по наказателно-правни въпрос", 19.05.2009г., в сила от 16.06.2010г.;

8. «Споразумение между Правителството на Република България и Правителството на Република Сърбия за полицейско сътрудничество» - подписано на 20.05.2010г.;

инж. Румен Дончев

ПОЛИТИКА ЗА МРЕЖОВА СИГУРНОСТ ЧАСТ № 3

продължение от предишния брой..

След като в предишните две статии разгледахме нормативната база, общите изисквания и правила при налагане на политиката за мрежова сигурност, предстои да разгледаме конкретни мероприятия за защита.

Организационните мероприятия за защита на автоматизираните информационни системи / АИС/ включват:

- създаване на документи с правила за инсталиране на компютърните системи, правила за полагане на кабелните системи на локалната мрежа;
- създаване условия за спазване изискванията на Физическа сигурност
- при планиране на политиката за мрежова сигурност трябва да се има предвид и ограничаване на физическия достъп на външни лица до данните в мрежата.



Мероприятията могат да бъдат насочени в следните направления:

Използване на технически средства за защита за физически достъп до съответните помещения, компютърни устройства и активно оборудване

- система за видеонаблюдение;
- алармена система (СОТ);
- кодови брави;
- система с персонални магнитни карти;
- всяко устройство да се маркира с инвентарен номер;
- да се изисква легитимиране на външните посетители, преди да бъдат допуснати до оборудването;
- работните станции и сървърите да се държат в заключващи се помещения с организиран физически контрол на достъпа до тях;
- там където това не е възможно, да се въведе софтуерна защита.

Защита на структурно кабелните системи / СКС/ и кабелите срещу директен физически достъп

Мрежовите кабели, както и структурно кабелните системи /СКС/ трябва да бъдат положени така, че да няма възможност за физически достъп до тях. При изграждане на локална компютърна мрежа е необходимо да бъде направено т.н. структурно окабеляване.

Мрежовите кабели трябва да бъдат положени в специални канали или да бъдат скрити в окачени тавани или подови настилки. Кабелите с усукани двойки проводници са особено лесни за подслушване. При оптичните кабели това е възможно, но е значително по-трудно, поради което в последно време фирмите, който имат необходимост от по-висока степен на защита на данните използват оптични кабелни трасета.

Техническите мероприятия в защита на компютърните системи включват:

- въвеждане на нива на сигурност на операционната система;
- политика за използване на паролите;
- криптиране на файловете;
- използване на цифрови подписи;
- използване на протоколи за сигурност при предаване на данните по мрежата;
- използване на защитни стени и прокси сървъри;
- спазване на правилата за антивирусна защита;
- физическа сигурност на данните.

Политиката за мрежова сигурност изисква използване на комбинирани методи за сигурност.

Нива на сигурност на операционната система

Съвременните операционни системи с файлова система NTFS позволяват въвеждане на нива на

сигурност. Всеки потребител притежава собствен акаунт с парола за достъп. Акаунтът се състои от потребителско име и параметри за влизане в мрежата, зададени за конкретния потребител. Тази информация се въвежда от администратора и се съхранява в мрежата от операционната система. За всеки потребител се задават:

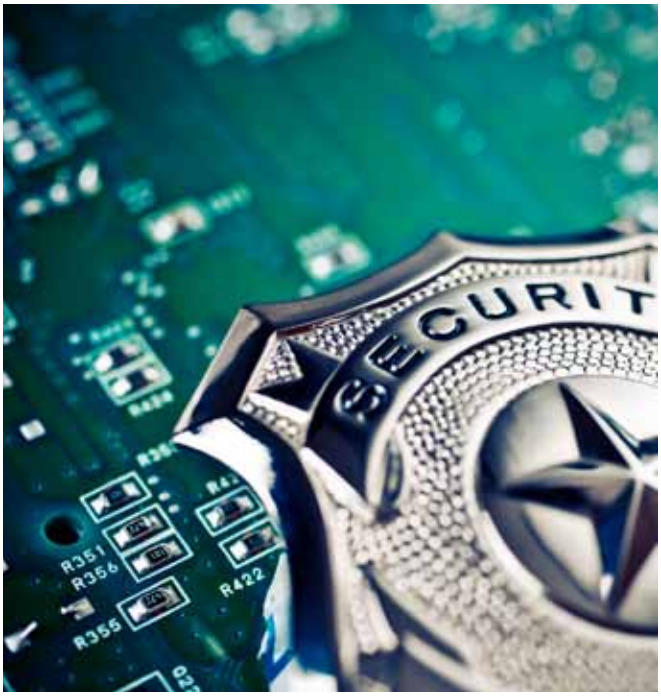
- права за достъп до системата и нейните ресурси;
- време за влизане;
- потребителска директория;
- дата на изтичане.

Важен момент при задаването на тези настройки е дефинирането за всеки акаунт на достъпа до ресурсите на системата!

Операционната система предлага ключови потребителски акаунти, които автоматично се активират по време на инсталацията.

Administrator – първоначален акаунт. Той е с пълни права в мрежата и може да:

- стартира мрежата;
- инсталира файлове и програми на операционната система;
- настройва първоначалните параметри на системата за сигурност;
- създава други потребителски акаунти;
- поделя директории и принтери.



Guest – посетителски акаунт. Дава временен достъп до мрежата на някой, който няма акаунт.

Мрежовите операционни системи могат да поддържат хиляди акаунти. Мрежовият администратор ще бъде затруднен, ако реши да извърши някакви настройки върху всички акаунти или дори само върху част от тях. Почти във всяка мрежова операционна система различни потребителски акаунти се обединяват в един общ акаунт, наречен група.

Групата е акаунт, съдържащ други акаунти. Основната причина за въвеждането на групите е улесняване на администрирането. Групата дава възможност на администратора да третира голям брой потребители като един-единствен акаунт.

Правата за достъп се настройват за групата и всичките й членове автоматично ще по¬лучат и наследяват тези права. Правата за достъп за различните групи могат да бъдат различни. Така например за потребителите в Group_1 може да бъде разрешен пълен достъп до file1.doc - да могат да четат, променят и съхраняват файла, но за потребителите от Group_2 – само да четат този файл.

Освен на NTFS ниво, правата за достъп до папка или файл могат да се задават и чрез ключовете в Windows Registry. Това ограничава потребителите във възможността им да инсталират програми и да ги конфигурират.

Home Edition версиите на Windows XP и Windows Vista предлагат ограничено поддържане на сигурност – дефинирани са само три вида потребители: администратори, обикновени потребители и гости. Задаване на NTFS права е възможно само в режима Safe Mode.

Всяка фирма или организация трябва да изгради своя политика за контрол на достъпа до ресурсите на системата.

Сигурност на паролите

Важен момент от политиката за мрежова сигурност е използването на възможно по-трудни за разгадаване пароли. Политиката за сигурност на паролите трябва да включва следното:

- Паролата не трябва да съдържа имена на роднини, рождени дати, адреси, телефони;
- Да не се използват смислени думи, които се съдържат в речниците. Комбинацията между букви и цифри е добър вариант;
- В паролата да има включени главни и малки букви, цифри и специални символи на случайни позиции (например DoY%s86$);
- Паролата трябва да бъде лесна за запомняне от потребителя. В противен случай тя ще бъде записана на хартия, което не е желателно;
- Да се използват дълги пароли (поне 8 символа);
- Периодично потребителите трябва да сменят паролите си;
- Съвременни операционните системи притежават възможности за задаване на правила при въвеждане на потребителските пароли – минимална дължина, история, срокове за изтичане на паролата, както и изисквания към символите, които са включени в паролата.

В следващата статия ще покажем мероприятията, свързани с защитата преноса на данни в локални и глобални мрежи, изискванията към хардуера и организацията на работа.

инж. Николай Цапрев

ЗАЩИТА НА GSM ОТ ПОДСЛУШВАНЕ

В последните няколко месеца започнаха да се изнасят все повече данни за нерегламентирано подслушване на GSM апаратите. В някой медии бяха излъчени репортажи, показващи как става това. Най-достъпният метод за подслушване е чрез инсталиране на шпионски софтуер в GSM апарата.

В момента на пазара се предлагат масово подобни софтуери на цени между 200 и 1000 лв. Няколко фирми предлагат инсталиране на софтуера и поемат гаранция върху работата на продукта. Какви са възможностите на подобни софтуери всеки може да види от множеството репортажи или от статиите „Врагът във вашия джоб публикувани" в броеве 2, 3 и 4 на списание **PROFESSIONAL**, които можете да изтеглите безплатно от www.profisec.bg.

При наличие на евтини и лесно достъпни начини за подслушване, резонен става въпроса за защитата на информацията и данните обработвани, предавани и съхранявани в GSM апаратите. В продължение на политиката си да предлага на клиентите информация и решения на различни проблеми, екипът на Профисек ЕООД реши да сподели няколко идеи за намаляване на риска от подслушване на GSM телефон.

Шпионските софтуери работят по три основни начина.

Събират информацията от разговорите, SMS, паметта, GPS, камерата и т.н. от заразения телефон и в даден момент през GPRS изпращат информацията до друг телефон или сървър. В този случай информацията се предава след приключване на разговорите, в паузите, когато телефона не се използва.





Вторият начин е чрез откриване на паралелна конферентна връзка. В този случай при провеждане на разговори, шпионския софтуер принуждава телефона да открие втора линия и така телефонът предава едновременно информация и на трети абонат. Тогава разговорите се подслушват в реално време.

Третият начин е чрез дистанционно активиране на стандартния звуков канал на телефона, когато апарата е в покой и не се използва. Този начин се използва за подслушване разговорите около телефона и за извличане на информация от паметта.

Има софтуери, които използват комбинация от трите начина.

Защитата от подслушване би следвало да се основава на откриване на демаскиращите признаци за присъствие и работа на шпионски софтуер и на пресичане пътищата за достъп до информация.

Основен демаскиращ признак е включването и работата на телефона без знание на използващия го. Понеже шпионските софтуери извършват това незабелязано, за регистрирането на подобен факт е необходима апаратура или определени действия.

Едно от възможните устройства е индикатор на излъчването. Подобни индикатори се продават сво-

бодно, проблемът е с фалшивите сигнали, на които реагират опростените и евтини модели. Необходимо е индикатора да е специализиран за индикиране на видовете протоколи за пренос на данни и честоти, използвани от телефона. Някой индикатори включват автоматично и звуков сигнал с бял шум, като по този начин блокират микрофона на телефона.

Втори способ за откриване, а понякога и блокиране работата на шпионски софтуер е чрез поставянето на предплатена SIM карта. Някой от шпионските софтуери се настройват към определен номер и спират да работят след промяна на номера или няколкократно рестартиране на телефона чрез изваждане на батериите. С промяната на номера и рестартирането на телефона има голяма вероятност да се блокира работата на софтуера. При използване на предплатена SIM карта в зависимост от мобилния оператор получавате SMS с остатъка по сметката, след всяко действие с телефона, изискващо достъп до мрежата и взимащо пари от сметката. Ако при телефон, оставен дълго време в покой се получат едно или няколко последователни съобщения за намаляване на сметката, това означава, че телефона работи без знание на собственика и вероятно е заразен със шпионски софтуер.

Третият способ е чрез изследване на сметките. Изследването на изходящите разговори, както и трафика в интернет, може да покаже обем на трафика, не съответстващ на проведените разговори, както и връзки с непознати номера или по-чести от реалното свързвания с познати номера. Този способ е подходящ за лица или телефони с малко провеждани разговори и нисък или почти никакъв трафик в интернет.

Четвърти способ – проверка, включена ли е възможността за водене на конферентни разговори и изключване на същата. По този начин ще се блокира работа на софтуер, основаващ се на подслушване чрез създаване на конферентна връзка.





Пети способ е инсталирането и използването на антивирусен софтуер. В интернет се предлагат антивирусни софтуери за почти всички операционни системи използвани в мобилните телефони. Ефективността на такъв софтуер е както на всяка антивирусна програма. Ефективен за познатите и не ефективен за непознатите шпионски софтуери. Освен това не всяка програма се разпознава като вирус.

Шести способ за защита е посещение при специалист. В този случай се извършва преглед на работата на телефона, използват се методи за откриване, блокиране или премахване на шпионски програми. След приключването работата по телефона, специалистът трябва да даде и препоръки относно начина на работа с GSM апарата за недопускане на ново заразяване.

Характерно за шпионския софтуер е, че се инсталира по-лесно на телефони с операционна система и естествено на смартфони. Принципа е следния - колкото по-добър и с повече екстри е телефона, толкова по-лесно се заразява с шпионски софтуер.

На телефон без достъп до интернет, без операционна система, без BLUETOOTH и други безжични модеми е почти невъзможно да се инсталира и пусне да работи шпионски софтуер.

На всяко действие рано или късно се появява противодействие. Защитата от подслушването е възможна, но зависи от подготовката и възможностите за противодействие на подслушваните лица. Наличието на знания и формирането на навици помага за справяне с проблема. Дадените по-горе способи са сравнително лесни и с ниска себестойност, което ги прави приложими за широк кръг от лица.

Ако желаете да научите повече за устройствата и методите, предотвратяващи нерегламентирано подслушване на GSM, посетете уебсайта на Профисек ЕООД - **www.profisec.bg**

Тодор Кобуров
доцент, доктор по политология

МЕЖДУНАРОДНАТА СИГУРНОСТ И НАЦИОНАЛНАТА СИГУРНОСТ



През периода на Студената война сигурността на национално равнище се свързваше със защитата на националните граници и ненамесата във вътрешните работи. Смяташе се за общоприето, че държавата може да гарантира своята сигурност, като поддържа определено равнище на военна готовност и като участва пълноправно в един от двата военнополитически блока - НАТО или Варшавския договор. Съображенията за гарантиране на националната сигурност обикновено доминираха над интересите на международната сигурност. Господстващото разбиране на националната сигурност като военна даде своето отражение и върху понятията - международна и световна сигурност. Същевременно националната и международната сигурност биваха противопоставяни. Проблемът за сигурността в глобален мащаб през този период се определяше от взаимоотношенията между двете световни суперсили САЩ и СССР.

Днес обаче проблемът сигурност получи съвсем нови измерения. Светът излезе от периода на биполярно противопоставяне и навлезе в етап, който политолозите наричат с различни имена - глобализация, нова ера, нов световен ред, нова цивилизация, край на историята, полицентричен свят и т.н. В променените условия е необходим и нов, много по-широк подход към проблема за сигурността.

Според един известен френски изследовател, днес "сигурността е проблем, чиито многобройни страни се простират от международното положение до самолетните катастрофи, от тероризма до атомната енергия, от страха пред "нашествието" на имигрантите до тревогите на останалите без помощи безработни". За да бъдем в състояние да решим проблемите на нашето време, несъмнено трябва да открием преди всичко рецепти в икономическата, политическата и военната област, съобразени с новите условия в света, но същевременно без да изпадаме в плен на отживели времето си схеми.

Днес държавите станаха твърде взаимозависими и една криза или регионален конфликт незабавно предизвикват реакции в целия свят. В съвременните условия все повече се говори за обща сигурност, за глобални и регионални договорености, които да гарантират националната сигурност на държавите. Въпреки, че военните и политическите аспекти продължават да играят ключова роля, сигурността днес не се свежда само до тях. В резултат на продължителни дебати още през 1989 г. ООН единодушно прие новата концепция за сигурност - "Сигурност във всички аспекти".

Според едно популярно определение сигурността е мирен начин за уреждане на международни спорове, за регулиране на въоръжаването и разоръжаването. Според друго определение, сигурността е състояние, при което се гарантират жизнените интереси на гражданите, обществото и държавата от вътрешни и външни заплахи.

Определенията, разбира се, винаги са нещо относително, а много често не отразяват богатството на житейските прецеденти. Ние живеем в регион, който от столетия се характеризира с циклична нестабилност и несигурност и не случайно е наричан "барутен погреб на Европа". Водени от това, трябва да се освободим от илюзиите, когато се опитваме да анализираме сигурността от чисто абстрактни позиции.

Опитът за дефиниране на понятия като международна сигурност и национална сигурност, като подвид на по-общото понятие сигурност не трябва да пренебрегва главния въпрос:

Дали днес живеем в свят, регион и страна, които можем да определим като по-сигурни?

Самото поставяне на този въпрос носи със себе си известна доза скептицизъм, което още повече стимулира опитите не само за теоретично осмисляне на проблема, но и за търсене на практически алтернативи на решения.

Също като демокрацията, сигурността никога не е окончателна. Има едно сполучливо определение за сигурността като "школа по прагматизъм и скромност". Тя се влияе от процеси с цикличен характер и зависи от динамични равновесия, съставени от действия и противодействия, от провали и успехи. Сигурността напредва само чрез провали, чрез връщане към опита и трупане на знания. Основна роля в цикличния характер на сигурността играе инцидентът.

"…Всеки от нас придобива знания за сигурността само чрез произшествия, които лично е преживял, или инциденти, на които е станал съпричастен. При всяка професия, при всяка дейност… е очевидно, че грешките и провалите са по-поучителни от успехите. Само чрез изпитанията човек получава представа за границите и праговете, които не бива да бъдат прекрачвани." Този цитат, взет от книгата на Пиер Лакост „Мафиите срещу демокрацията" сполучливо набляга на практическата страна на проблемите със сигурността.

Известният френски специалист обръща внимание и на един проблем, който е актуален и за нашето общество в момента, а именно - смесването на икономическата и политическата власт, което има пагубни последствия както за обществения морал, така и за сигурността на демократичните институции. Успоредно с това, прекалената политизация също има негативни проекции: "политическите страсти пречат на трезвата преценка дори на най-даровитите и най-информираните мъже и жени…."



В стремежа на новите демокрации за интегриране към ЕС и НАТО прави впечатление използването на още няколко категории, които неизменно присъстват в публичните дискусии и на които трябва да се спрем по-обстойно. Това са категориите: интеграция, преход към демокрация, консолидиране на демокрацията и др.

Основният въпрос, отнасящ се до интеграцията в сферата на политиката за сигурност, е въпросът:

Могат ли всички държави от Югоизточна Европа да се интегрират в структурите на НАТО (преди всичко) и ЕС в обозримо бъдеще, или не?

Под "интеграция" се разбира дългосрочно международно политико-военно сътрудничество. В сферата на сигурността това означава, че политиката за национална сигурност трябва да бъде в съответствие с политиката за сигурност на международната организация, към която държавата желае да се присъедини. Във военно отношение това означава, че военен персонал и национални бойни единици, трябва да бъдат поставени на разположение на организацията, като суверенитетът на националното управление над тях в известна степен е ограничен.

За държави като Словакия, Словения, Румъния и България, които имат сравнително малко население и ограничена социално-икономическа база, беше очевидна невъзможността те сами да поддържат потенциала, необходим за защита на тяхната територия при всякакви обстоятелства. Тези страни, както и други източноевропейски страни, навлязоха след 1989 г. в един мъчителен трансформационен период на реформи. Според някои изследователи, преходът към демокрация трябваше да бъде един сравнително краткосрочен период, който да включва:

- установяване и конституционно легитимиране на институции, осигуряващи разделението на властите;
- развитие и функциониране на две или повече политически партии;
- периодично провеждане на избори (поне веднъж на 4-5 години);
- установяване на представителни парламентарни органи;
- защита на индивидуалните права и свободи;
- функциониране на действително плуралистична преса и други средства за масова информация.

Оказа се обаче, че въпросът за краткосрочността е съвсем относителен и поне в българския случай е нещо по-специално. От тази гледна точка трябва да обърнем внимание и на понятието "консолидиране на демокрацията". Има три условия за консолидиране на демократичните институции:

1. Постигане на консенсус между политическите партии относно структурите и основните черти на демократичната държава.
2. Съгласие относно външнополитическата ориентация (стратегия) на страната.
3. Успешна смяна на "дясно" и "ляво" управление, без военна интервенция и/или граждански конфликт.

Тези условия по същество бяха изпълнени от тези посткомунистически страни, които успешно се интегрираха в НАТО и ЕС. Същевременно още в началото на преходния период далновидно беше отбелязано, че най-голямите опасности за страните от Югоизточна Европа са национализмът и неговият сиамски близнак – популизмът - опасности, които според мен продължават да съществуват и днес.

В следващият брой, ще ви представим гледната точка на автора за кризата на политическите режими от края на XX и началото на XXI век и пътищата за изход от нея.

Главен комисар ОР инж. Слави Райков

СПЕЦИАЛНИ ОБЩЕСТВЕНИ ПОРЪЧКИ

Уважаеми читатели в бр. 4 и бр. 5 на списание **„PROFESSIONAL"**, Ви предоставихме полезна информация и практически съвети по прилагане на Закона за защита на класифицираната информация (ЗЗКИ), при сключване и изпълнение на договори, свързани с достъп до класифицирана информация.

Темата ще бъде продължена и в следващите броеве на списанието, но в сегашния брой ще ви запознаем с една също така много интересна тема, свързана с възлагане и изпълнение на договори по Наредбата за възлагане на специални обществени поръчки (НВСОП).

В чл. 1, ал. 1, т. 1 от НВСОП са разписани възможните варианти за възлагане на специални обществени поръчки (СОП). Те се възлагат по Закона за обществените поръчки (ЗОП), като за това е необходимо да са налице следните условия:

а) да са свързани с отбраната и сигурността на страната, които са предмет на класифицирана информация, представляваща държавна тайна;

б) изпълнението на обществената поръчка да е придружено със специални мерки за сигурност, в съответствие с действащото в страната законодателство;

в) да касаят доставки и услуги, свързани с производството и търговията с оръжия, боеприпаси и военна техника;

В конкретния случай по-обстойно ще разгледаме възлагането на специални обществени поръчки по чл. 1, ал. 1, т. 1, б., „б" от НВСОП, „изпълнението, на които трябва да бъде придружено със специални мерки за сигурност, в съответствие с действащото в страната законодателство".

В приложимото законодателство няма точно и еднозначно определение на термина "специални обществени поръчки" (СОП). В нормативните документи на различни ведомства са записани няколко варианти на СОП. Като цяло може да се направи обобщение и заключение, че: "специалните мерки за сигурност" представляват съвкупност от дейности, мерки и изисквания, които се прилагат от възложителя на СОП, с цел обезпечаването на сигурността и защитата на дейността му и които не са мерките за сигурност и изискванията за защита на класифицирана информация, представляваща държавна тайна.

По същество възложители на СОП са субектите по чл. 7 от ЗОП, които също така са и „организационни единици" по смисъла на ЗЗКИ.

Поради тази причина, възложителят на СОП и ръководителят на организационната единица (РОЕ) са едно и също лице.

Това са Администрацията на Президента на Република България, Народното събрание, органите на държавна власт и местно самоуправление, дипломатическите представителства, юридически и други държавни органи създадени със закон, търговски дружества и организации с над 30% финансиране от бюджета, както и такива, които извършват дейност, чрез предоставена лицензия или концесия.

Кандидат за изпълнител на СОП може да бъде всяко българско или чуждестранно физическо или юридическо лице, което отговаря на изискванията за прилагане на специални мерки за сигурност.

По надолу ще разгледаме някой особености при планирането, подготовката и провеждането на СОП. Те касаят както възложителите, така и кандидатите за изпълнители на СОП.

Всяко едно от изброените по-горе ведомства, организации и дружества в края на предходната година съставя проекто-бюджет за следващата календарна година. В него се залагат средства за капиталови разходи и издръжка, в които се включват и средствата, необходими за възлагане и изпълнение на договори по ЗОП и НВСОП. Тези средства обикновено се планират по тримесечия, като изхождайки от практиката през първото тримесечие на годината процедури по ЗОП и НВСОП не се планират. Това се налага от факта, че средствата, планирани в бюджета се забавят и отпускат в края на месец януари и ако възложителят е второстепенен или третостепенен разпоредител при него бюджетът се захранва по банкова сметка в средата и дори в края на месец февруари. Ако пък бюджетът не е приет във варианта предложен от тях, то възможност за неговото актуализиране,

чрез прехвърляне на средства в рамките на одобрения бюджет по параграфи и под параграфи, в зависимост от приоритетите на бюджетния разпоредител, е възможно да се случи едва през третото тримесечие на годината.

Поради тази причина от съществено значение е правилното планиране и провеждане на процедурите по ЗОП и НВСОП, които при добър разчет на времето отнемат около 2-3 месеца.

Друг важен момент за правилно планиране и провеждане на процедурите по ЗОП и НВСОП е разпределението на задълженията на служителите от организационната единица – възложител на специалната обществена поръчка. За да не се допуска неразбирателство и конфликт на интереси в хода на провеждането на процедури по ЗОП и НВСОП е необходимо задълбочено и компетентно, в зависимост от длъжностните характеристики на служителите, да бъдат подробно разписани техните задължения и отговорности в утвърдените вътрешни правила за възлагане и провеждане на процедури по ЗОП, като част от утвърдената от ръководителя Система за финансово управление и контрол /СФУК/ на организационната единица-възложител на СОП.

При наличие на ясни задължения и отговорности на длъжностните лица, ясен и наличен бюджет и достатъчно време за провеждане, може да се стартира процедура за определяне на изпълнител на СОП:

1. За провеждането на процедура за възлагане на специална обществена поръчка, възложителят на СОП взема решение по своя преценка, въз основа на докладна записка от структурното звено – заявител. От съществено значение при описването на предмета на обществената поръчка в инициращия документ е да се упомене, че изпълнението на същата е възможно, чрез прилагане на специални мерки за сигурност и че компетентен да даде становище е служителят по сигурността на информацията /ССИ/ на организационната единица. На това основание би следвало възложителят на СОП да разпише резолюция на инициращия документ до ССИ за мотивирано становище.



СОП с предмет - допълнително оборудване на специални автомобили

2. В случаите на чл. 1, ал. 1, т. 1, б. „а" и б. „б" от НВСОП, ръководителят на организационната единица /РОЕ/, в конкретния случай възложителят на СОП взема решение за откриване на процедура за възлагане на специална обществена поръчка, след мотивирано писмено становище от служителя по сигурността на информацията. В него ССИ обосновава необходимостта от провеждане на процедурата и посочва кой е компетентния орган, който следва да даде становище, относно необходимостта от прилагането на специални мерки за сигурност.

3. Въз основа на мотивираното становище на ССИ, РОЕ изпраща писмо до компетентния орган за получаване на становище, относно необходимостта от прилагане на специални мерки за сигурност.

В зависимост от предмета на СОП, компетентният орган за получаване на становище, относно необходимостта от прилагане на специални мерки за сигурност е различен. Компетентността на тези органи се вменява със закон или друг нормативен документ, като в някои случай компетентен орган е и самият служител по сигурността на информацията /ССИ/ на организационната единица – възложител на СОП.

4. След като получи положително становище от компетентен орган, относно необходимостта от прилагане на специални мерки за сигурност, възложителят със заповед обявява решение за откриване на процедура за възлагане на СОП, която включва изискванията на чл. 6, ал. 1 от НВСОП и назначава комисия, която да извърши проучване, с цел установяване на възможни изпълнители на поръчката, като определя срок за извършване на проучването.

5. В срока на провеждане на проучването, комисията, назначена със заповед на възложителя на СОП изготвя доклад, който съдържа списък на установените възможни изпълнители на СОП.

6. Въз основа на доклада от комисията, възложителят на СОП изпраща писма със запитване за желание за участие до установените възможни изпълнители на СОП, като описва предмета на поръчката, който включва и специалните мерки за сигурност, които следва да

бъдат изпълнени от тях, необходимите документи, които трябва да предоставят при желание за участие и срок за писмен отговор.

7. След изтичане на указания срок и получаване на заявленията по чл. 7, ал. 2 от НВСОП от кандидатите за изпълнители на СОП, възложителят отправя писмено искане до компетентен орган за становище, относно изпълнението на специалните мерки за сигурност.

И в този случай, в зависимост от предмета на СОП компетентния орган за получаване на становище, относно изпълнението на специалните мерки за сигурност може да бъде различен. Този орган, в зависимост от неговата компетентност, може да бъде различен и от компетентния орган дал становище относно необходимостта от прилагане на специални мерки за сигурност, като в някои случаи също може да бъде и служителя по сигурността на информацията /ССИ/ на организационната единица - възложител на СОП.

8. При необходимост възложителят на СОП със заповед назначава работна група, която да разработи и предостави за утвърждаване конкурсна документация на основание чл. 28 от ЗОП и определя срок за нейното утвърждаване.

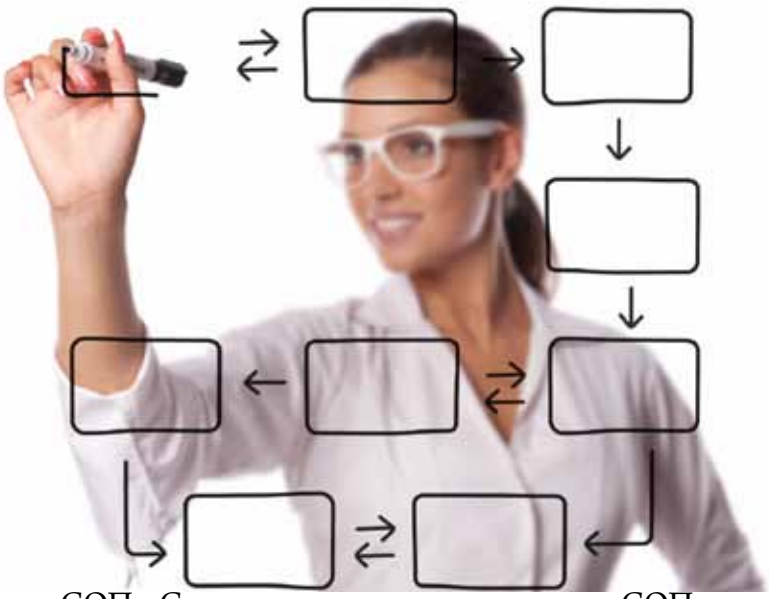
9. В указания от възложителя на СОП срок работната група предоставя за утвърждаване протокол, заедно с изготвената конкурсна документация.

10. След получаване на положително становище от компетентния орган, относно изпълнението на специалните мерки за сигурност, възложителят на СОП писмено уведомява потенциалните изпълнители за условията за получаване на решението за откриване на процедурата и/или на документацията за участие /ако има такава/, както и за мястото и срока за подаване на офертите.

11. Офертите се изготвят съгласно изискванията на чл. 9 от НВСОП и глава 4, раздел II от ЗОП, като срокът за подаване се определя съобразно сложността на поръчката и не може да бъде по-кратък от 7 работни дни от получаване на уведомлението. Процедурата за възлагане на СОП се провежда и когато е подадена само една оферта за участие.

12. След изтичане на срока за подаване на офертите възложителят на СОП с решение (заповед) назначава комисия за разглеждането им и определя срок за нейната работа. Съставът на комисията се обявява в деня, определен за отваряне на офертите.

13. След приключване на работата, комисията съставя окончателен протокол за дейността си, който се подписва от всичките членове на комисията и се утвърждава от възложителя



на СОП. Със заповед възложителят на СОП обявява класирането на кандидатите и определя изпълнителя на СОП.

14. След обявяване на класирането и определяне на изпълнителя на СОП, възложителят писмено уведомява кандидатите за резултатите от проведената процедура и определя срок за подписване на договор за възлагане на СОП с определения за изпълнител кандидат.

15. Възложителят сключва договор с кандидата, класиран на първо място, в срока определен в уведомлението, а при отказ от негова страна, с класирания на следващо място кандидат.

В договора възложителят може да определи към изпълнителя на СОП, специфични изисквания за изпълнение на специалните мерки за сигурност, като:

- допълнително проучване за надеждност от гледна точка на сигурността на кандидатите;
- изисквания за пропускателен режим в обектите, където ще се изпълнява договора;
- други специфични изисквания.

Възложителят на СОП има право едностранно да развали договор за възлагане на СОП в случай, че след сключването му възникнат или станат известни обстоятелства, в резултат на които изпълнителят не отговаря на изискванията за изпълнение на определените специални мерки за сигурност.

Познаването на процедурата за възлагане на специални обществени поръчки помага на възложителите и кандидатите за изпълнители.

На първите за по-добра организация, не допускане на грешки и правилно усвояване на бюджетни средства. На вторите за предварителна подготовка при кандидатстване и за безпроблемно изпълнение на договор, свързан с прилагане на специални мерки за сигурност.

Екип на "Профисек"

ЕФЕКТИВНА ПОДГОТОВКА НА ТЕЛОХРАНИТЕЛИ

Въпросът за изграждане на кадри в областта на личната охрана се решава от различните фирми по различен начин. Ключов момент в този бизнес е обучението на охранителните екипи и индивидуалната подготовка на отделния охранител. В днешно време, в световен мащаб, са се наложили три основни школи за подготовка на телохранители и модели на организация на охранителната дейност. Това са американската (САЩ), европейската (Великобритания) и израелската школа. Тук съвсем умишлено не включвам такива школи, като японската и китайската, поради факта, че влиянието им спрямо българския охранителен бизнес е нулев.

В зората на формирането на охранителния бизнес, веднага след регламентирането на този вид дейност в България, сериозните български бизнесмени, поддържащи собствени охранителни екипи и охранителните фирми, които се стремяха да поддържат високо ниво на услугата „лична охрана", бързо се ориентираха и започнаха да решават въпроса с подготовката кардинално. Цели групи от нечия охрана преминаваха в Израел подготовка по тази специалност. Явно личните контакти и достатъчно агресивната рекламна и маркетингова политика на многобройните израелски академии се оказаха печеливш ход от тяхна страна. Други изпращаха хора до САЩ или в Европа. В края на века някои големи охранителни фирми в България започнаха да канят в страната представители на утвърдени играчи на пазара на охранителните услуги, занимаващи се предимно с обучение, и най-вече с издаването на заветния сертификат за преминат курс.

През това време всеки чуждестранен инструктор и съветник правеше впечатление с дебелата си папка от подобни сертификати, дипломи, свидетелства и, което е много важно – препоръчителни писма. Ев-



ропейският пазар бе устроен по такъв начин, че работа първи си намираха бивши полицейски служители или хора, имащи стаж в различни специални подразделения.

За съжаление, самото обучение от тези чуждестранни експерти не осигуряваше работа. Най-ценното нещо бе дипломата, която те даваха, която може да се сложи в папка и да се показва при необходимост. Школата (академията, асоциацията, центъра, института и т.н.) работеха въз основа на своя собствен имидж, като защитаваха търговския си бранд. С натрупването на достатъчно опит стана ясно, че всъщност всички известни школи се занимават с препродаването на едно и също – един и същ материал под различни названия, термини и дипломи. И когато стана въпрос да се изясни дълбочината на преподавания материал и практическите аспекти на използването му в нашите условия, излезе наяве простата истина, че нито една международна школа не отчита местното законодателство, особеностите на културите и условията за работа, начина на живот и поведение на потенциалните охранявани лица…



Преподаваните знания в такива курсове са свързани главно с техника (техничност) на изпълнението на дадена тактика, които са правилни и стандартни, но практически неприложими в нашата действителност и поради националните ни особености. Голяма част от знанията са повърхностни и не отговарят на изискванията на българското законодателство, да не говорим за пълната липса на теми свързани с документите, които детайлно да регламентират дейността на телохранителя. Голяма част от материалите, преподавани и раздавани на курсовете могат да се намерят и в Интернет, и носят най-вече препоръчителен или информативен характер, но не съдържат изискванията към дейността на конкретния човек. И ако това е приемливо за чуждестранния пазар, то за нашите условия така е невъзможно да се работи професионално. От разговори с хора, преминали курсове в Израел, например, става ясно, че на тези обучения се набляга на заучаването на няколко прости тактики при стандартни ситуации, на стрелбата с огнестрелно оръжие и на физическата подготовка. На въпроса „Какво научихте там?“, почти винаги следваше стандартния отговор „Много стреляхме и тичахме…“. В интерес на истината стрелбата и тичането в България излизат доста по-евтино.

Друг пример. Наблюдавах курс за охранители провеждан от инструктор с европейска популярност. Инструкторът обучаваше курсисти, които се бяха записали индивидуално на групова тактика, като използваше методи за сформиране на екип. За обучаеми, които никога няма да работят заедно това е само загуба на време. Второ, тренировките по стрелба с огнестрелно оръжие бяха колективни, като обучаемите бяха в една редица – 20 човека и стреляха едновременно. По този начин един инструктор никога не може да оказва необходимата методическа помощ на отделния стрелец, да не говорим, че групата е сформирана от хора с различен стаж в стрелбата. Резултатът от подобен род обучение е само барутна пушилка. И трето няма тактическо сглобяване на отделните заучавани действия, а има общ стремеж да се натоварят максимално физически и психически обучаемите, което откъснато от конкретна ситуация се превръща в самоцел.

Голям пропуск в съвременното обучение на агенти за лична охрана е лошата правна подготовка, която се дава на обучаемите. Познаването на законодателството и особено тази му част, която е свързана с употребата на сила, помощни средства и оръжие трябва да е основна цел на подобни обучения. Телохранителят трябва да е вещ в познаването и тълкуването на чл. 12 и чл. 13 от НК, защото независимо от неговия правен статус спрямо охраняваното лице, той употребява оръжие само в условията на неизбежна отбрана и крайна необходимост. Не бива обаче тяхното заучаване да става механично и да се разчита, че като се знаят наизуст членовете и съдебната практика, то те се разбират и прилагат правилно. Обучаващият трябва да включва в тематиката задължително различни ситуационни игри, в които охранителя да може реално да реагира и след това да се разтълкуват правните последици от всяка реакция.

Голяма част от бизнесмените предпочитат да използват ограничената и пълната с песимизъм фраза: „Поръчат ли ме – ще ме убият!“. Това е дълбоко погрешна сентенция и най-лошото е, че тези настроения се предават и на охраната. За да не си самовнушават тази обреченост, агентите лична охрана трябва да са твърдо убедени в своята готовност, да имат всестранна подготовка и екипът да е сработен на високо ниво. Не всички бизнесмени, обаче имат нужда от телохранители. Не на всички е нужен човек с пистолет, за да ги пази. На някои е необходим просто грамотен шофьор и по съвместителство телохранител. Други наемат група за охрана от служители на правоохранителните структури, или група охрана за кратко време. И всеки иска за своите пари да има най-добрите! Но как да се определят най-добрите? Казано е, че „по делата ще ги познаете“ и аз бих го перифразирал – „по обучението им ще ги познаете“, защото човек реагира

така, както е обучаван, а не така, както пише в дипломата му! Днес например, по утвърдения стереотип, кандидатите да се нарекат добра лична охрана, трябва да имат неопетнен (от професионална и права гледно точка) стаж, минимум 10 години работа в НСО или СОБТ, да са членове на дадена професионална организация, а най-важното да имат достойни лични препоръки. Но това е само професионален портрет. Зад всичко това стои конкретен човек. Отделна характеристика за професионализъм е дипломата, удостоверяваща подготовката на телохранителя. Къде, кога и от кого е издадена тя? Кой го е обучавал и с какво той гарантира качеството на подготовката? Пазарът съществува вече 15 години и може смело да се каже, че бели петна в професионалната среда практически няма. За сметка на това няма утвърден на пазара бранд в тези услуги, въпреки, че персонално в пространството се подвизават различни гуру-та, и съществуват различни учебни центрове за подготовка на охранители. Всички те са далеч от необходимото ниво за тази услуга или ако те са атрактивни и актуални, инструкторите са чужденци, което ги прави абсолютно неприложими в България. Светъл лъч в тази сфера е единственото специализирано учебно заведение Колежът по охрана и сигурност „Св. Георги Победоносец".



Да се намери на пазара качествена стока е трудно и това го знае всеки бизнесмен. Но телохранителят е специфично явление. И когато възникне потребност от него, то професионалното ниво трябва да съответства на представите на потребителя, да бъде на неговите услуги. За да се разбере дали ще ни е полезна някоя вещ е достатъчно да я видим, премерим, пробваме и т.н. Телохранителят обаче е нужно да се „почувства". Как може да стане това? Най-лесно е да се познават стандартите в обучението и тези стандарти да са приложимите в България. В сигурността няма оттенъци. Телохранителят или е надежден, или не е.

Какви са основните грешки, допускани при подбора и обучение, какво издава недостатъци в нивото на професионализма в работата на телохранителя? Най-очевидни са дефектите в комуникацията (простото общуване) и набиващото се в очите суетене в стандартни ситуации. Непознаване на текущата ситуация и неразбиране на същността на ставащото. Глупави въпроси по форма и съдържание (т. е. въпроси, отговорът, на които е предварително известен, или трябва да бъде известен на телохранителя). Дискомфорт при съпровождане пеш, като със своите действия телохранителят пречи на охраняването лице да се предвижва. Проблеми и суетене при слизане и качване в автомобил, при преминаване през „тесни" места (коридори, асансьори, портални врати и т.н.). Да не говорим за небрежен външен вид и други демонстрирани вредни навици …

Всички тези недостатъци в голяма степен се отнасят към „деловите качества" на телохранителя, т. е. са общоприети изисквания. Те са и основата за взимане на решение за пригодността на кандидата за лична охрана. Ако охранителят е преминал курс на обучение и тези недостатъци не са отстранени, това означава, че школата, която го е обучавала не е от надеждните и професионалните в бранша. Когато се подбира охранител, освен изброените качества, е необходимо да се провери дали обучението му до момента е изградило професионални навици и умения. Основните от тях са:

- наблюдение и контрнаблюдение;
- съпровождане на охраняваното лице пеш;
- съпровождане на охраняваното лице с авто мобил;
- оперативно-технически оглед;
- екстремална медицина;
- владеене на специални умения за управление на автомобил;
- логическо мислене;
- правно осигуряване на собствената професионална дейност;
- управление на група от лична охрана;
- взаимодействие с право-охранителните органи;
- контрол на собственото психо-физическо състояние;
- професионална етика и етикет;
- действия под тревога;
- комуникации;
- близък бой (въоръжено и невъоръжено противодействие на нападение);
- спазване на постовата дисциплина.

Тези способности на телохранителите трябва да изучават и придобият на основните курсове в различните центрове, а на специализираните те да се усъвършенстват.

Има правила и принципи, форми и методи, и накрая стратегия, технология, тактика и техника за постигане на оптимален резултат. Параметрите и съдържанието на всеки от тези елементи са добре известни на професионалистите. И ако ви казват, че не може да се постигне 100% надеждност в тази сфера, то помислете над въпроса: „Може би, те просто не знаят, как да го постигнат?"

Учебният център на „Профисек" организира целия спектър от курсове за обучение в сферата на сигурността.

Посетете ни на адрес **www.profisec.bg.**

инж. Николай Цапрев

МОБИЛНИ КОМПЛЕКСИ ЗА ПЕРИМЕТРОВА ОХРАНА

В репликите на филмовите екшън герои често става дума за „осигуряване на периметъра". В разговорите на специалистите по охрана често присъства термина „периметрова охрана". В интернет има множество фирми предлагащи проектиране и изграждане на периметрова охрана. В действителност много малко хора знаят какво точно представлява периметровата охрана, а още по-малко са тези, които са изграждали такава система. Периметровата охрана е широка и сложна тема, чието разглеждане би изисквало повече от една статия. В настоящата ще разгледаме частен случай на периметровата охрана, а именно мобилни комплекси за периметрова охрана.

Периметровата охрана е комплекс от мерки, имащи за цел да детектират проникване или опит за такова през външните граници на охраняван обект, да възпрепятстват или забавят евентуалния нарушител, както и да го неутрализират. Външните граници на охранявания обект са всъщност охраняваният периметър. В миналото за охраната на периметъра се разчиташе основно на физически огради и препятствия и жива охрана. В днешно време все повече навлизат електронни системи за охрана на периметъра, работещи на различни физически принципи. Най-добрата защита на периметър се постига при съвместна работа на физически бариери и препятствия, електронни системи за охрана и жива охрана.



Външният периметър за охрана може да представлява ограда или система от физически препятствия с изградени входове и изходи, заобикалящи дадена площ, двор, прегражданщи държавна граница, рубеж направление, път и др. Външен периметър могат да бъдат и външните стени, прозорци и врати на сграда или помещение, без да има налична допълнителна площ или изградени заграждения. Външния периметър може да бъде и само една видима или невидима граница на местността. Всичко зависи от охранявания обект и условията, при които се извършва охраната.

Периметровата охрана с технически средства е най-малко прилагания вид охрана в България. Причините за това са няколко, но основната е голямата първоначална инвестиция и скъпата поддръжка. Дължините на охраняваните периметри обикновено са големи. Електронните системи за охрана на периметъра използват скъпи детектори, които от своя страна често генерират фалшиви алармени сигнали. Това налага дублирането на тези системи със системи за видео наблюдение. Освен това за правилното функциониране на електронните системи за периметрова охрана има редица изисквания към прилежащата на периметъра територия. Изискванията се изразяват в конструктивни особености на оградите и прилежащата им полоса, както и определена поддръжка на същите. Това съчетано с големите дължини означава сравнително големи първоначални и по следващи инвестиции за изграждане на периметровата охрана и нейната поддръжка. В условия на икономическа криза, а и по принцип, словосъчетанието „големи разходи" не е любимо на мениджърите и това често води до отказ от изграждане на система за периметрова охрана.

Терминът периметрова охрана обикновено предизвиква асоциации с тежки и големи индустриални, промишлени, военни или държавни обекти с



изградени заграждения. Тоест нещо скъпо, голямо, тежко и неподвижно.

В живота често се налага да се извършва охрана на временни или мобилни обекти. Може ли да се използва периметрова охрана за такива обекти, без да се извършват трудоемки и специализирани строително монтажни дейности и да се нарушава съществуваща инфраструктура, екстериор и интериор. Оказва се, че е възможно.

С напредването на войната с тероризма и сблъсъка на военни части с терористични организации и партизански способ за водене на война, възникна необходимостта от увеличаване надеждността на охраната и предотвратяване на атаки срещу обекти, персонал и техника, които се разполагат временно в полеви условия, гористо планинска местност или градска среда. Тази необходимост доведе до създаването на евтини и мобилни комплекси за периметрова охрана. Тези комплекси се развръщат бързо, без прокарване на кабели и извършване на строително монтажни работи и без високо квалифициран персонал, необходим за монтажа им.

Поради удобството за работа, бързината на развръщане и не високите цени, създадените за военни нужди комплекси се оказаха подходящи за използване от цивилни държавни и частни организации за решаване на широк набор от охранителни задачи.

Подходящи са например за охраната на временен склад със скъпи или опасни материали, прегражданe на направления или части от държавната граница, охрана на товарен автомобил или влакова композиция със скъп или опасен товар, охрана на строителна площадка, охрана на сградите и районите, в които временно пребивават охранявани VIP лица, охрана на самолетни и вертолетни стоянки, временна охрана при повреда или временно прекъсване на щатната охрана и други. Могат да бъдат използвани във всички случаи, когато се налага временно и бързо усилване на охраната, прегражданe на направления на местността и охрана на райони в градски или полеви условия, дори и там където няма налични електрозахранване и комуникации.

В мобилните периметрови охрани на практика се използват почти всички видове детектори, работещи в стандартните системи за периметрова охрана. Използват се акустични и сеизмични детектори, скрити в земята детектори с микропроводници, реагиращи при прекъсване на последните, детектори работещи при промяна на електростатично поле. Тези, които са получили най-голямо разпространение и чието използване е възможно почти във всички случай, са работещите на принципа на инфрачервените и микровълнови бариери.

Структурата и принципа на действие на един комплекс за мобилна периметрова охрана е следната:
На терена се поставят детектори, оформени в един





корпус заедно с радио предаватели и акумулаторни батерии. При необходимост се поставят ретранслатори на сигнал, като алармените сигнали от детекторите се приемат в мониторинг център. При задействие детекторите изпращат алармен сигнал до мониторинг центъра, където аларменото събитие се регистрира и се задейства реакцията на живата охрана. Мониторинг центъра има възможност да приема сигналите на множество детектори едновременно. Тази схема позволява при изграждане охраната на периметъра да се използват комбинации от детектори, работещи на различни физически принципи или да се изградят с цел защита в дълбочина няколко охранителни рубежа, наблюдавани от един мониторинг център.

Дължините на периметъра и разстоянието до мястото за разполагане на мониторинг центъра зависят от мощността на предавателите и от проходимостта на сигналите на местността. Дължините на периметъра варират от 10 метра до 10 километра за един комплекс. Отдалечеността на мониторинг центъра също варира, като може да е разположен в непосредствена близост до охранявания периметър или на разстояния от 5-6 километра.

Автономността на комплексите зависи от използваните детектори и условията, при които се използват като варират от 14 дни до 5 години. Тоест това е времето за работа с един комплект батерии без подмяна на същите.

Времената за разгръщане и събиране на мобилните комплекси също варират, но средното време е около час и половина за разгръщане на 2 километра периметър, при екип за разгръщане състоящ се от двама или трима души. При малки дължини на периметъра от порядъка на 50 – 500 метра комплексът може да бъде развърнат и от един човек.

В предвид това, че комплексите за мобилна периметрова охрана пренасят алармените сигнали чрез радио сигнали, са взети мерки срещу заглушаване на комуникационните канали, индикация при повреда, отпадане на захранването или опити за повреда и кражба на елементи от комплексите.

Физическите габарити и тегло на мобилните комплекси за периметрова охрана са такива, че позволяват лесното пренасяне от хора, автомобили или летателни средства. Необходимото оборудване за изграждане на 1000 метра периметър спокойно се пренася от двама души.

Разработени са и мобилни системи за видео наблюдение, пригодени за съвместна работа с мобилен комплекс за периметрова охрана.

Както всяко техническо средство за охрана и мобилните комплекси за периметрова охрана имат недостатъци и проблеми. Те обаче са добро средство за увеличаване надеждността на охраната. Незаменими са при необходимост от бързо или временно увеличаване надеждността на охраната на обекти, както и при решаване на широк кръг от охранителни задачи. Определено имат своето място в дейността на държавните и частни структури, извършващи или нуждаещи се от периметрова охрана.

Повече информация за мобилните комплекси за периметрова охрана може да се намери на **www.profisec.bg**



доц. д-р Иван Станчев,
Академия на МВР

АНТИТЕРОРИСТИЧНИ ОПЕРАЦИИ

От началото на 60-те години на XX век до днес светът е разтърсен от серия актове на организирано въоръжено насилие. Обекти на това насилие са политици, държавни служители и много често невинни хора. Жертвите се изчисляват на десетки хиляди. Материалните щети на стотици милиони долари ежегодно. За определяне на това насилие обществото използва термина тероризъм. Вълната от терористични актове, обхванала много райони по света, включително и България за известен период от време, показва, че тероризма се е превърнал в глобален проблем.

Съвременният тероризъм постоянно еволюира в развитието на своите методи на действие и мащаб на поставените цели. Докато през 70-те години на XX век целта на терористите е завоюване на обществени симпатии, а жертвите при терористична атака са ограничени, то през последните години целите на терористичните организации станаха глобални: промяна на политическата система в света или регион, унищожаване на културното многообразие, ограничаване на човешки права. Стратегията и тактиката на редица терористични организации се променя и вече е насочена към масови кръвопролития, все повече жертви в търсене на все по-голям обществен отзвук и внушаване на страх.

Днес в света не съществува единна стратегия за борба с тероризма, нито обща теория на операциите за борба с тероризма. Антитерористичните мерки и операции се реализират предимно в национален план от всяка държава, а международното сътрудничество в областта на борбата срещу тероризма е ограничено предимно в рамките на двустранни споразумения. Въпреки, че редица държави имат специално законодателство, стратегии и концепции за борба с тероризма, България не е развила достатъчно това направление.

В основата на успешната борба с тероризма стоят политически, икономически, социални мерки, ефективно антитерористично законодателство, стройна система за разузнаване, ранно предупреждение, добра координацията между държавните институции по отношение на всички аспекти на противодействието, както и провеждане на специални антитерористични операции. Тези операции се намират на границата между полицейските и военно-диверсионните операции, доколкото се провеждат в условията на сериозни правни ограничения по отношение на използването на сила (включително и въоръжена сила), но в същото



време се използват типичните за диверсионно-разузнавателните подразделения способи за подготовка и провеждане на бойни действия.

Понятието "антитерористична операция" може да има различно значение, тъй като обикновено тези операции се класифицират по редица признаци, някои от които са използваните сили и средства, място на провеждане, цели на операцията и др.

Като обобщаващо определение за антитерористична операция може да се приеме следното: "Съвкупност от съгласувани по цел, задачи, място и време тактически действия и мероприятия на държавните органи за предотвратяване на терористични актове, издирване, залавяне и неутрализиране на терористи, освобождаване на заложници и ликвидиране на последиците от терористичен акт".

Целта на операцията е неутрализиране на терористите, освобождаване на заложници или отвлечени лица (ако има) при най-висока степен за безопасност за участниците в операцията и гражданите, които се намират в района.

Съдържанието на операцията включва подготовката и провеждането на специалните тактически действия по издирване, изолиране и задържане на терористи, разузнавателна, контра разузнавателна и оперативно-издирвателната дейност за установяване самоличността на терористи и заложници (ако има.), тяхното и на техни съучастници проследяване, процесуално-следствени действия за доказване на извършени престъпления.

Съществува голямо разнообразие във видовете антитерористични операции. Могат да се направят класификации според целта на операцията, според времето

за реагиране на право охранителните органи, според територията на която се провеждат и по други критерии.

Според основната цел антитеристичните операции биват:

-операции за задържане на терористи;

-операции за освобождаване на заложници.;

-операции за унищожаване на терористи.

Операциите за задържане на терористи не се отличават по своите характерни черти, принципи, използвани способи и построение на силите от операциите за задържане на въоръжени извършители на престъпления.

Операциите за освобождаване на заложници са с най-висока степен на риск. Провеждат се след прецизно планиране и от високо подготвени специални подразделения.

Операции за унищожаване на терористи се позволяват от законодателството на редица държави.

Според времето за реагиране:



-операции при внезапно възникнал терористичен акт;

-операции, при които има предварителна информация за подготовка на терористичен акт.

Операциите, които се провеждат при внезапно възникнал терористичен акт (овладяване на сграда, транспортно средство, взривяване), се отличават със съкратени срокове за планиране, известно първоначално предимство за терористите и широко ангажиране на поделенията на охрана на обществения ред или охрана на обекти.

Операциите, при които има предварителна информация за подготовка на терористичен акт се подготвят и провеждат, следвайки общият ред за задържане на въоръжени лица и по-голямо значение на оперативно-издирвателните, разузнавателни и контра разузнавателни мероприятия.

Според територията на която се провеждат:

-операции на българска територия;

-операции на чужда територия.

Антитеристичните операции на българска територия се подготвят и провеждат от органите на МВР. При недостиг на подготвени сили и средства законодателството на Република България позволява използването на Българската армия.

Операциите на чужда територия (когато не са част от международна миро-опазваща или друга операция) се разрешават от Президента на Република България и могат да се провеждат със сили на Българската армия. Въпреки това, международната и българска антитеристична практика познават използване на сили предназначени за вътрешна сигурност в операции извън националната територия.

Какъв вид антитеристична операция се провежда и какви сили да се привличат в нея зависи от етапа, на който се намира терористичната дейност и характера на конкретния терористичен инцидент.

В районите, където терористичната заплаха е висока се провеждат "патрулни операции" (Ирак, Афганистан, Косово, Босна, Израел и др.). Целта е възстановяване на контрола над територии, които частично (за определено време) са във властта на терористични организации. За разлика от обичайната патрулно-постова дейност на полицията, патрулните операции се провеждат със сили от състава на органите за вътрешна сигурност, които се определят като „военизирани" (жандармерия, гранична полиция) и армията. Патрулите са с по-голяма численост – над 4 човека и са в постоянна готовност за използване на оръжие, построението им е с оглед отразяване на внезапно въоръжено нападение. В операциите може да се използват бронирани машини. За локализиране на отделни терористи или терористични групи и тяхното задържане специализирани антитеристични и диверсионно - разузнавателни подразделения провеждат разузнавателно-поискови операции. В тези операции широко се използват способите на тактическото разузнаване (характерно за армията) със способите на оперативното издирване (характерно за полицията).

Наред с другите видове антитеристични операции е необходимо да се провеждат разузнавателно-щурмови и разузнавателно-ударни операции.

Разузнавателно-щурмовите операции се провеждат за разузнаване (събиране на данни за терористични групи чрез наблюдение, подслушване, изучаване на документи, разпити, проверки, претърсвания и други способи) и унищожаване (чрез атака или щурмуване) на укрепени бази на терористични формирования.

Разузнавателно-ударните операции се провеждат за разузнаване и унищожаване на терористични формирования чрез мощни огневи удари за поразяване и активни бойни действия (най-често провеждане на засади и обкръжаване) срещу оттеглящи се терористични групи. Тези операции се характеризират с голяма продължителност 5-7 денонощия и повече и голям пространствен размах. Не е необходимо участието на голямо количество сили. Подготовката им и снабдяването със съвременни средства за разузнаване, оръжие и екипировка трябва да е на нивото на съвременните сили със специално предназначение. В състава на антитеристичните подразделения трябва да

се привличат специалисти не само по тактическо разузнаване, диверсии, антитероризъм, но и в агентурно разузнаване, контраразузнаване и психология.

Независимо от направената класификация и характеристика на антитеристичните операции възможно е един или друг вид да бъде приложен без да е налице силна вътрешна терористична дейност. Българската антитеристична практика показва, че операциите в нашата страна по-често са предизвикани от терористични инциденти, чиито корени са в други държави. Логично целите на конкретната терористична акция и конкретната обстановка ще изисква прилагането на различни видове операции включително и такива, провеждани със сили на българската армия на наша или чужда територия.

Разработването на съвременната теория на антитеристични операции и тяхното прилагане започва след разрастването на съвременния международен тероризъм през 60-те години на XX век. По това време национално-освободителните движения започват да изоставят тактиката на партизанските войни и се ориентират към терористични действия, с които смятат че ще привлекат международна подкрепа за своята дейност.



Паралелно с развитието на терористичната дейност се усъвършенства стратегията и тактиката на държавните институции, отговорни за борбата с тероризма.

Първата класическа операция за освобождаване на заложници извършва през февруари 1976 г френската антитеристична група GIGN. Тя унищожава 6 терористи от организация, бореща се за освобождение на френската колония Джибути, отвлекли автобус с френски деца.

През 1980 г. британско антитеристично подразделение от 22-и полк на SAS провежда успешна операция за освобождаване на заложници. На 30 април 1980 г. шестима въоръжени терористи от Демократичното революционно движение за освобождаване на Арабистан (провинция на Иран, населен с етнически араби) нахлуват в иранското посолство в Лондон и вземат 29 души заложници. С тази акция SAS, която дотогава е относително неизвестна за обществеността и медиите, придобива световна известност. Операцията в иранското посолство, наречена "Нимрод" предотвратява за доста време напред терористични действия на територията на Великобритания.

През май 1981 г. е бойното кръщение и на новосъздаденото тогава българско антитеристично подразделение СОМП (Специално оперативно милиционерско подразделение), сега Специализиран отряд за борба с тероризма (СОБТ). Това е операцията за освобождаване на заложниците от отвлечения от турски терористи турски самолет в Бургас, която завършва успешно. Благодарение на направения анализ на операцията поделението получава нова екипировка и въоръжение, които му позволяват по-бързо да усъвършенства тактико-специалната подготовка и в частност специалните антитеристични операции.

Развитието на специализираните антитеристични подразделения и техните операции от 70-те години на XX век до днес допринасят значително за превантивното ограничаване на терористичната дейност. Тези подразделения и антитеристичните операции играят основна роля в тактическото противодействие на тероризма и понастоящем, тъй като се явяват основното репресивно и относително ефективно средство на държавните институции в борбата срещу тероризма.

По отношение на въпроса – „Възможно ли е да се ликвидира тероризма?"- няма еднозначен отговор. За ликвидирането на тероризма като явление е необходимо да се отстранят причините за неговото възникване. Те най-често са политически, социални или икономически. Оттук следва, че успехът на силов вариант за унищожаването на тероризма е малко вероятен. Въпреки това, прецизно подготвените и проведени антитеристични операции могат значително да ограничат дейността на терористични групировки. Впоследствие ефективното противодействие да ги принуди да възприемат политика за промени в обществения живот без използване на насилие. Безкомпромисните удари срещу терористични организации ги лишава от важно психологическо предимство – внушаването на страх у гражданите и предизвиква в населението доверие в органите за сигурност, армията и държавата въобще, както и готовност за сътрудничество в борбата с тероризма.

Една от основните насоки за повишаване ефективността на борбата с тероризма е създаване и развиване на нови по-успешни форми, методи и тактики. Тяхното усъвършенстване може да се извърши чрез анализиране и обобщаване на положителните и отрицателните страни на досегашния опит в тази област.

Имайки предвид участието на България в международните операции в Ирак, Босна и Херцеговина, Косово и Афганистан, както възможното участие в операции на НАТО след бунтовете и размириците в северно-африканските арабски държави, би следвало да се направи внимателен анализ на вероятността страната да стане мишена на терористични организации. Впоследствие да се направи преглед на нормативна база, касаеща борбата с тероризма и при необходимост същата да бъде осъвременена.

д-р инж. Милен Иванов

ЕЗИКЪТ НА ТЯЛОТО

Казват, че тонът прави музиката. Когато се отнася до човешките взаимоотношения, обаче, те са „правят“ не само от тонове. Мимиката, позата, жестовете – всички те съдържат голямо количество сигнали, които съобщават на събеседника информация на ниво невербална комуникация. Често ние само с помощта на не-езикови сигнали разбираме, че събеседникът ни има предвид нещо съвсем противоположно на това, което говори. Случва се така, че говорещият сам се издава. Например, иска да направи определено впечатление, но неговия език на тялото показва, че той лъже.

Обикновено в разговорната реч се ползват неповече от 3 000 – 4000 думи, докато в Българският език думите са по-вече от 30 000. По-голямата част от хората могат да контролират онова, което казват, е, не всички, но повечето могат. Докато в езика на тялото се смята, че има седемстотин хиляди знака, от които 15 000 принадлежат само на лицето. Очевидно човек не може да контролира всички тези сигнали, затова, когато изречената дума е в конфликт със сигнала, подаден от тялото, последният винаги е безпогрешен.

Всички, които се занимават с т.нар. език на тялото, се сблъскват с интересен феномен: всеки човек излъчва сигнали чрез телодвижения (в повечето случаи — неосъзнато), но рядко някой може да ги „разбере“ осъзнато (тоест да ги интерпретира). Това е така защото ние не можем да предаваме сигнали на ниво съдържание, без да „изпращаме“ заедно с тях едновременно и сигнали на ниво отношения. Никой не може да каже нещо без интонация, без мимики, без минимум жестове и ние постоянно се намираме в някаква поза, която може да се изтълкува по определен начин и т.н.

Днес много автори, в своите книги предлагат материали за езика на тялото във вид на „речници“. Според тях, ако, например искате да разберете, какво „означава“ пъхната в джоба на панталоните ръка, е достатъчно да се вгледате в нюансите - как е пъхната ръката в джоба (с цяла длан или свита в юмрук), къде се намира палеца (вътре или вън от джоба), и вие с помощта на речника ще разберете какви чувства изпитва този човек. Такива подходи са подлъгващи и не могат да служат за разбиране на езика на тялото. Първо, заради това, че, например, не се отчита модата на джобовете при тесни панталони — в тях юмрукът просто не се събира, а може даже и за палеца на не остава място! Второ, възниква реална опасност, че използващия такъв „речник“ да си въобрази, че вижда всичко ясно и нееднозначно.

Такива чувства несъзнателно възникват у много хора, ако те са уверен, че веднага правилно са



възприели неезиковите сигнали! В резултат на това у тях почти не възниква желание да си зададат контролни въпроси! А само така е възможно да се коригират или потвърдят версиите, възникнали в резултат на наблюдението.

Как се осъществява този контрол? Съществуват три възможности, като най-лесно приложима

е първата. Коя точно бихте избрали, си решавате сами, в зависимост от своя индивидуален стил и от ситуацията.

Първи метод – директен въпрос. При този случай става въпрос за въпроси, на които не може да се отговори еднозначно с „да“ или „не“. Този тип въпроси имат тактическо преимущество: те подбуждат този, към когото са насочени, към по-подробно изразяване на своето мнение — събеседникът е практически принуден да го направи. Например, могат да се формулират следните въпроси: „Какво мислите за това?“, „Какво е вашата гледна точка по този въпрос?“, „Е, а вие какво ще кажете по този повод?“, „А какво е вашето мнение?“ и т.н.

Втори метод – скрит въпрос. При този метод директно питате дали правилно сте разбрали невербалния сигнал на партньора. „Ти като, че ли се разсърди?“, „Струва ми се, че това не ти харесва, така ли е?“, „Това, май че наистина те зарад-



ва?“ и т.н. Разбираемо е, че този подход не може да се използва при всички случаи, но често именно той е най-бързия път към успеха.

Трети метод – мълчание. Мълчанието е метод, с помощта на който е възможно да се постигнат най-големи успехи, но на голяма част от хората той се удава трудно. Тъй като болшинството от хората започват да говорят когато техните партньори замълчат, този метод е по-успешен, особено в професионалната дейност, в случаите когато другите два по едно или друга причина са неприемливи. Към метода на мълчанието е отнася, също така и техниката, която понякога се нарича „активно мълчание“. При нея вие оставяте фразата незавършена, все едно е увиснала във въздуха. Например следния контролен въпрос: „Що се отнася за цените, то на вас, вероятно ще са ви нужни допълнителни данни?“.

След използването на някой от горните методи следва главното — внимателно да следите за следващите действия на събеседника. Той може да се възмути от вашето предложение/предположение и да се опита са го оспори, а може спокойно да се съгласи и да поиска разрешение да позвъни, за да направи необходимите разпореждания. Тези свои решения, действия и отношение, вашият събеседник ще изрази и с езика на тялото, което за вас вече ще е еднозначен и безспорен сигнал какво мисли, а няма да са ваши предположения за неговите намерения

Основни трудове свързани с изследване на езика на тялото:

1. Дж. Балвър – през 1644 г. пише книга, в която езика на ръцете се разглежда като природно естествено образувание, за разлика от изкуствено измислените думи на езика;

2 И. Каспар Лафатер, пастор от Цюрих, през 1792 г. публикува „Есе по физиономика”, първото систематично изучаване на движенията на тялото.

3 . К. Лихтенберг, немски учен и писател. През 1765 г. пише книга, в която критикува Лафатер за опростения подход към физиономиката и за откъсването му от реалния свят и от практическата дейност на човека;

4. Белл, анатом, нейрофизиолог, художник и хирург. През 1844 г. се занимава с изследване в областта на функционалния анализ на нервната система и за влиянието което тя оказва на физиологията на тялото;

5. Дарвин и Е. Кречмър през 1920 г. провеждат изследвания за описване на връзките между емоциите на човека, неговия характер и типа телосложение, и за връзките между израженията на човешкото лице и смисъла на данните от невербалните единици.

6. Д. Бонифацио, Д. Батиста дела Порта и Ф. Бейкън в през 1616 г. в своите трактати за невербалната комуникация твърдят, че същества универсален език от жестове, разбираем за всички народи;

7. А. Кендън, Д. Моррис, Г. Крейдлин, съвременни изследователи на езика на жестовете, които отделят голямо внимание на взаимодействието на вербалните и невербалните кодове, и особеностите на езика на тялото на отделните култури.

Д. Заяков
Управител, Риск Сълюшън ООД

СЕДЕМ СТЪПКИ ЗА ЕФЕКТИВЕН КОНКУРЕНТЕН БЕНЧМАРКИНГ

От гледна точка на конкурентното разузнаване, съществуват няколко прости инструмента, които могат да се използват за извършването на сравнителен анализ на характеристиките на преките или косвените конкуренти на фирмата. Тези инструменти могат да помогнат на фирмения „бенчмаркинг“ за формулирането на дейностите на компанията по отношение на конкурентите и, което ще и позволи да заеме по-добра пазарна позиция спрямо тях.

Бенчмаркингът обикновено се описва и използва като рамка за стратегическото планиране на фирмата. Същността му се състои в това, че след като елементите на изследването са идентифицирани, показателите могат да бъдат приложени към ключовите фактори за успех на бизнеса и пазара. Тези мерки или „критерии“ се използват, за да се развиват бъдещи качества и инициативи на пазара на фирмата за подобряване на цялостната и конкурентна позиция.

Този процес, по принцип има седем стъпки, описани по-долу. Той се прилага, както за вътрешните, така и за външните конкуренти, от гледна точка на сектора, в който работи фирмата и може да послужи като основа за по следващ конкурентен анализ, включващ целите и финансовите възможности на конкурента. Поставя се акцент на въпроса за набора от ресурси и бизнес култура на конкурента, които той би използвал в конкурирането с нас. Някои от стъпките на процеса на сравнителен анализ могат да предизвикат въпроси и идеи, свързани с определянето на допълнителни измерителни показатели за оценка.

Стъпките, за които става дума са следните:

1. Определете кои от функционалните области във вашия бизнес трябва да се подложат на сравнителен анализ, като изхождате от тяхната себестойност, значението им за бизнеса и потенциала им за промяна, след извършване на проучването. Например, налични материални и нематериални активи, наличен персонал, позициониране на пазара, доставчици, клиенти и др.

2.Идентифицирайте ключовите фактори и променливи, с които да се измерват тези функции - обикновено в общ вид на финансови средства и продуктовата стратегия.

3. Изберете най-добрите в класа фирми за всяка област, които да бъдат подложени на съпоставяне - тези дружества, които извършват всяка функция на най-ниска цена и с най-висока степен на удовлетвореност на клиентите и т.н. Най-добрите компании могат да са ваши преки конкуренти (чуждестранни или местни) и дори компании от различни индустрии (успоредни конкуренти със заменящи или заместващи продукти или услуги; латентни конкуренти, които биха могли да са интегрирани преди вас или след вас във вашия пазар, или фирми извън вашия индустриален сектор, с които не се конкурирате, но които са най-добрите в области, подлежащи на изследване, като логистиката например).



4. Проведете измерване на състоянието на най-добрите в класа фирми за всеки показател, подлежащ на сравнителен анализ – използват се източници като НСИ, публикувани финансови и други фирмени отчети на самите предприятия, статии за тях в СМИ и специализирани издания, пазарни анализи на изследователски

институти и организации, кредитни справки, клиенти и доставчици, търговски асоциации, правителствени структури. Могат да се използват и директни интервюта с други организации, готови да споделят или обменят информация с вас.



5.Проведете измерване на собствената си дейност за всяка отделна променлива, след което се пристъпва към сравняване на резултатите точка по точка. Целта е да се разкрият разликите между вашата фирма и най-добрите в класа примери. Не се колебайте да оценявате получените резултати според вашия опит и гледна точка. Много често е трудно да се получат точни мерки на изследваните функции и обикновено те не допринасят значително за стойността на проучването. Откритите диспропорции е необходимо да бъдат анализирани и да се вземе решение, кои от тях и до колко да бъдат взети под внимание в анализ.

6. На основата на получените при сравнителния анализ резултати, създайте програми за действие, които да залегнат в плана ви за изпреварване на конкуренцията. В тези програми се залагат действия по подобряване на онези области от вашата дейност, които са показали най-добър потенциал за промяна и които биха допринесли най-активно за подобряване на конкурентостта на фирмата ви. Могат да бъдат избрани различни подходи – извършване на промени от по-просто към по-сложно, подражаване на най-добрите фирми в сектора, промяна на основни правила в управлението на собствения бизнес или прилагането на иновативни модели и технологии от други сектори, дори от чужбина, които могат да бъдат адаптирани към особеностите на фирмата ви.

7. Пристъпете към изпълнението на тези програми като формулирате специфични цели за подобряване и срокове, в които да бъдат постигнати. В хода на изпълнението създайте мониторингова система за анализ на изпълнението, което ще ви предостави възможност да актуализирате своевременно целите във времето. На основата на резултатите от мониторинга ще получите възможност за вторичен сравнителен анализ на показателите с отчитане на вече постигнатите резултати.

Много често мениджърите на малки и средни предприятия игнорират изпълнението на тази положителна практика поради неправилната оценка на нейната ефективност. Счита се, че за осъществяването на процеса е необходим прекомерен човешки и финансов ресурс, който в условия на криза е дефицитен за повечето фирми. Освен това обикновено се очаква постигането на видими резултати в изключително кратки срокове, което е нереалистично. Ефектът от прилагането на този подход обикновено се отчита с оценка на постигнатите положителни резултати – повече подписани договори, повишаване на оборота и привличане на допълнителни клиенти, подобряване на работата с подизпълнителите и доставчиците, което очевидно изисква време. Но по-съществено е, че за осъществяването на тези стъпки не е необходимо наличието на допълнителен персонал или инвестиции на допълнителни средства. В общия случай става дума за усвояването на прости практически умения, които позволяват процесът на сравнителен анализ и оценка да се извършва текущо. Това от своя страна дава възможност да се получава натрупване на положителните резултати във времето. Същевременно той би бил изключително полезен и за своевременното разкриване на непреодолими неблагоприятни ефекти, които да изискват взимането на генерални решения от мениджърите, но във всеки случай ще предотвратят значителни загуби за фирмата.

Статията е изготвена по материали и със съдействието на Арик Р. Джонсън - управляващ директор на консултантската фирма Aurora WDC. Фирмата консултира бизнес лидерите и провежда обучение по конкурентно разузнаване на фирми и организации в здравеопазването, финансовите услуги, телекомуникации, информационни технологии, медии и развлечения, енергетиката, строителството, транспорта, индустриалното производство и търговията на дребно и едро.

д-р инж Милен Иванов

СТРЕЛБА - ФОРМИ НА ТРЕНИРОВЪЧНА ДЕЙНОСТ

Продължение от миналия брой...

Стрелкова тренировка

Тренировка - това е многократното повтаряне на действия, с цел най-доброто им усвояване и развиване на функционални възможности на организма. Под въздействието на тренировъчните натоварвания организмът се адаптира за преминаването към изпълняваната дейност. Необходимо условие за повишаването на натренираността е постоянно, постепенно, в зависимост от адаптацията, нарастване на тренировъчните натоварвания. Стереотипните натоварвания поддържат достигнатото ниво на натренираност, но не го усъвършенстват.

Насоченост на тренировките

Изпълнението на прицелен изстрел изисква съгласуваност на действията на няколко негови съставни елемента. Ролята, значението, сложността на усвояване и изпълнение на всеки от тях са различни. Някои от тях, например заемане на положение за стрелба се усвояват лесно и бързо. Други, като устойчивостта на оръжието, изискват продължителни и целенасочени тренировки. Освен чисто техническите действия при изстрела активно участват зрителната и мускулната памет, вниманието, волевия комплекс.



Насочеността на тренировъчните натоварвания често се недооценява в практиката. Предположението, че нужните качества ще се развият самостоятелно, поражда стереотипност на тренировките, което става пък спирачка на усъвършенстването. Всяко тренировъчно занятие и всяка част от него трябва да имат конкретна насоченост, конкретна цел. Това може за бъде, например развитие на физически качества, усъвършенстване на техники за стрелба, развитие на психически процеси и т.н.

Под въздействието на тренировъчната дейност, централната нервна система формира програма от двигателни процеси, която позволява да се изпълняват добре усвоени действия, без да се привлича вниманието за тяхното изпълнение. Това е навика. Формираният навик позволява на стрелеца да се съсредоточава върху най-сложни и решаващи елементи на комплексното действие, тогава, когато останалите се изпълняват автоматизирано. Закрепването на навиците зависи от количеството повторения и състоянието на възбуда на нервната система по време на изпълнението на действията. Веднъж формиран навик трудно се поддава на промяна. Затова изграждането на най-правилното действие е задължително изискване на тренировъчния процес.

В подготовката на стрелеца могат да се различат няколко етапа. Всеки от тях решава свои задачи, има свои средства и методи, но всички те трябва да са подчинени на крайната цел – формиране на умения и навици за прицелна стрелба, които да осигуряват надеждно владеене на оръжието в екстремални ситуации. Често, обаче, новакът, който е показал първоначално добри резултати, забавя своето усъвършенстване. Това се появява в момента, когато не му стигат физически сили да удържа оръжието и се налага да се приспособява и хитрува при изстрела. Стрелецът знае, как да заеме положение за стрелба, как да насочи оръжието, да задържи дишането. Знае, че усилието на показалеца трябва да нараства плавно. Много иска да улучи в центъра на мишената, а това много му пречи. Пречат също и недостатъчно усвоената стойка за стрелба и непривичната тежест на оръжието, за преодоляването, на което се налага да се напрягат мускулите. А пък недостатъчната устойчивост на оръжието се проявява във безсистемни колебания или резки движения. Също така пречи и изискването за плавно натискане на спусъка, точно когато е периода на благоприятното положение на равна мушка. Налага се да се използва всеки момент на относително подобрена устойчивост. Така възниква разпространената сред новаците грешка, наречена „дърпане“ или „кълване“. Преместването на оръжието при натискане на спусъка се среща и при стрелци, които плавно натискат спусъка, което също може да се охарактеризира като „дърпане“. То се проявява в непроизволно съкращаване на

различни мускулни групи на тялото, шията, рамото, китката. Те представляват двигателна реакция на очаквания изстрел. Тази реакция най-често е предизвикана от стремежа да се ускори изстрела, от опасения от проточване на времето за изпълнение на изстрела, от спад на работните напрежения с края на обичайното време за работа над изстрела и от мисълта за очаквания резултат от попадението. Предотвратяването на тези нежелателни реакции се решава с формирането на нагласа за запазване на работните процеси в завършващата фаза на изстрела. Необходимо е да се запазва прицелването в продължение на 1,5-2 секунди след изстрела. Тъй като в основата на тези нежелателни явления лежат психологически фактори, то ефективен методически способ е стрелецът да си представи, че оръжието е заредено не с един, а с четири патрона. При натискане на спусъка ще се произведат не един, а четири последователни изстрела, и всички те трябва да попаднат в целта.



Форми на тренировъчни занятия

Формирането на технически правилни действия изисква концентрация на вниманието при тяхното изпълнение. Желанието да се попадне в центъра на мишената и очакването на изстрела стават фактори с голяма дразнеща сила, която възпрепятства запазването на вниманието върху работните процеси.

Лесно е да се мине по дъска, лежаща на пода, но възниква сериозен проблем, когато тази дъска е на височината на втория етаж. Психолозите казват, че ако дъската се вдигне не изведнъж, а постепенно, като се дава възможност всеки път да се привикне към новата височина, проблемът се решава. По подобен начин се изгражда и началната подготовка на стрелеца с пистолета.

Техническа тренировка

Това е тренировка без патрони. Известен отдавна и широко използван методически способ. Тренировката без патрони („суха тренировка“) постига високи резултати и не може да бъде заменена с друга форма на работа, в това число и практическата стрелба. Целесъобразно е тя да се нарича “техническа тренировка”, за разлика от „огневата”, която е тренировка с практическа стрелба. Техническата тренировка се провежда не за да се пестят патрони, а тя е необходима за стрелци от всички нива на подготвеност. С нейна помощ се решават следните задачи:

- развиване на силовата издръжливост на ръцете;

- усъвършенстване на устойчивостта на оръжията;

- развиване на мускулен контрол;

- разучаване на контрола на спускането;

- управление на вниманието;

- отработване на съгласуваност на действията при комплексното изпълнение на изстрела.

Огнева тренировка

Преходът от техническа към огнева тренировка при новаци има доста сложни моменти. През цялото време на обучението действията на стрелеца не се усложняват, но се усложняват условията за тяхното изпълнение, които пораждат психологически смущения. Това са очакването на изстрела, неговия звук, отката на оръжието, желанието да се порази центъра на мишената. Психологическите смущения затрудняват новаците при разучаването на техническите действия. Първата крачка за елиминиране на тези негативни моменти и прехода към практическа стрелба трябва да стане неутрализирането на самия факт на изстрела, който отвлича вниманието. Следва да се предостави възможност на новака да се „настреля“, докато изстрелът не загуби елемента на изненада, да стане привичен и непредизвикващ емоции.

Тренировка - стрелба по екран

Екранът, това е някакъв светъл фон, обикновено обратната страна на мишената. Стрелецът насочва оръжието, като се ориентира не по центъра на екрана, а просто на светлия фон, който помага да се вижда най-добре положението на мушката в прореза. Отсъствието на точка на прицелване отстранява съблазънта да се произведе изстрел в момента на най-доброто положение на оръжието и стрелецът започва да работи само върху техниката на самия изстрел.

Тренировка - стрелба по мишени

При прехода от стрелба по екран към стрелба по мишени пред стрелците възникват нови психологически трудности, свързани с появата на точка на прицелване. Възниква стремеж към възможно поточно насочване на оръжието, контрол на просвета между горната част на мушката и долната част на черния кръг на мишената, натискане на спусъка в момент на най-точно съвпадане на равната мушка с точката на прицелване. Всичко това измества от съзнанието на новака, контрола на работните процеси и с това трябва да се бори треньора.

Следва продължение...

Parabellum,
По материали от Интернет

ИЗРАЕЛСКАТА ЩУРМОВА КАРАБИНА TAVOR: СМЯНА НА КАРАУЛА

НОВОПРИЕТАТА ЩУРМОВА КАРАБИНА TAR-21 – ГОТОВА ДА СТАНЕ НОВОТО ОРЪЖИЕ НА ИЗРАЕЛСКАТА АРМИЯ? ИЛИ МОЖЕ БИ НЕ...

Винаги съм смятал, че боеспособната армия е тази, която е финансово обезпечената за дълъг период от време или накратко казано – богатата такава.

В този ред на мисли смятам, че една от най-боеспособните армии в света е армията на Република Израел, известна още като „ЦАХАЛ". Сформирана веднага след създаването еврейската държава, ЦАХАЛ се явява пряк наследник на „Хагана" – войсковите подразделения от арабско-израелската война през 1948 г.

От създаването си до днес, израелската армия е голямото „изключение от всички правила" по отношение на концепциите за въоръжени сили, през последните 60 години. Това се отнася с пълна сила и относно на въоръжението на въпросната армия, по-конкретно – лекото стрелково оръжие. Израелската армия е може би единствената армия в света, която може да си позволи за 60 години три пъти изцяло да замени лекото си въоръжение. При създаването ѝ, като основна щурмова карабина на въоръжение стои белгийската FN FAL, която след Шестдневната война е заменена изцяло от автомата „Галил", в последствие заменен (почти) изцяло от американските карабини M16, Car-15 и M4. Всичко това е свързано с огромни финансови разходи – както за закупуването на самите оръжия, така и за ново обучаване на военнослужещите.

И ето, че през последните десет години отново започва превъоръжаване, като този път ситуацията е още по-интересна: на въоръжение се приема щурмовата карабина „TAVOR", компановката на която е по системата „булпап" – различна от всичко, стоящо на въоръжение до този момент в ЦАХАЛ...

Но нека да разгледаме и самото оръжие:

Още през 1991 година в Израел била започната разработката на ново поколение леко стрелково оръжие в перспективната „булпап" компановка. Целта била новата карабина да замени стоящите на въоръжение M4/16, CAR-15 и „Галил". Поръчката за разработката на новото оръжие получила държавната тогава компания Israel Military Industry – IMI (понастоящем частна IWI - Israel Weapon Industry), като процесът по разработката вървял в тясно сътрудничество с военните.

Новата щурмова винтовка за пръв път била показана през 1998 година и получила обозначение Tavor TAR-21 (Tavor Assault Rifle, 21), като името идвало от планитата Тавор в Галилея, а индексът „21" означавал, че новата карабина е оръжие от 21-ви век.

Корпусът на оръжието се състои изцяло от удароустойчив полимер, като ръкохватката и спусковата скоба на оръжието не са отделни детайли, а са интегрирани в него, а на местата, в които е необходимо, в корпуса са поставени стоманени волжки.

Газоотводният механизъм на оръжието е изцяло скрит в корпуса, газовото бутало е с дълъг ход, а затворът е ротационен, като заключването му става посредством 7 бойни упора. Затворната рама заедно със затвора се движи вътре в корпуса на оръжието по направляваща ос, а над нея е разположена възвратната пружина. Затворът може да бъде изпълнен в два (взаимозаменяеми) варианта, според това от коя страна на оръжието ще се изхвърлят гилзите на изстреляните патрони. Разбира се, за тази цел и от двете страни в корпуса на оръжето са предвидени „прозорци" за гилзите, като боецът може да избере страната, на която ще се изхвърлят те, в зависимост от това дали прикладва на ляво или на дясно рамо. Достъпът до механизмите на



оръжието с цел разглобяване и обслужване се осъществява посредством отваряне на задтилъка на приклада.

Ръкохватката за презареждане е разположена над цевта, обикновено от лявата страна на корпуса, но може да бъде преместена и от дясната, според това дали боецът е десняк или левичар, като при стрелба тя остава неподвижна. Селекторът за режим на

огъня е палцов, разположен над ръкохватката, като се движи в три позиции – за поставяне на оръжието на предпазител и съответно единична и автоматична стрелба. Също както ръкохватката за зареждане, и той може да бъде преместван и от двете страни на корпуса на оръжието.

Поставянето на пълнителя се осъществява стандартно за „булпап" компановката, като той се поставя в задната част на корпуса, зад пистолетната ръкохватка. Основно оръжието е под патрон 5.56x45 NATO, като може да бъде зареждано със стандартни пълнители за американските карабини M4/16, тъй като заключването на пълнителя става по същия начин, както при тях. Скорострелността на карабината в калибър 5.56x45 NATO е между 750 и 900 изстрела в минута, а посредством специални адаптери някои модели могат да бъдат преконвертирани в картечен пистолет в калибър 9x19.

Фамилията стрелкови оръжия Tavor TAR-21 се състои от карабини, базирани на една и съща основна конструкция и различни модификации по нея:













След като разгледахме оръжието, в заключение може да се каже, че щурмовата карабина Tavor е една изключително авангардна оръжейна концепция, която без съмнение притежава предимствата на съвременните „булпап" системи: компактни размери, но дълга цев; адаптивна конструкция и ниско тегло (оръжието в най-дългия си вариант тежи само 3,30 кг.), но и имаща по-голямата част от недостатъците им. Един от тях например е, че не може да се стреля и от двете рамена (което в условията на градски бой е ключово при прочистване на сгради). Има, разбира се, и други: сменянето на пълнителя е затруднено от факта, че той е в задната част на карабината. Също така, намирайки се в там, той силно разваля баланса на оръжието...

И все пак в днешно време армиите на много държави вече са възприели „булпап" системите като сериозна част от своето въоръжение. Но дали това е оръжейната концепция на бъдещето? Ще имаме възможност тепърва с интерес да разберем...

ТИ!

СТРАЙКБОЛ ИГРАЕШ ЛИ?



“ВИТОША” СТРАЙКБОЛ КЛУБ

ВОЕННИ ИГРИ

ПРИКЛЮЧЕНИЯ

ТИМБИЛДИНГИ

ЗАБАВЛЕНИЯ

http://teambuilding-vitosha.com/



ГЕЛАК ООД

СТРОИТЕЛСТВО НА ОБЕКТИ ОТ ТЕХНИЧЕСКАТА ИНФРАСТРУКТУРА:

- Преносни и разпределителни водопроводи, канали и съоръжения;
- Обекти от транспортната инфраструктура;
- Ремонт на проводи и съоръжения от техническата инфраструктура;
- Проучване и проектиране на обекти от техническата инфрастурктура;
- Строителство на сгради.

АДРЕС:
гр. София
ул. Люба Величкова № 24
тел. 962 25 35
факс 962 22 25
e-mail: office@gelak.net



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