



ЗЛАТЕ ДИМОВСКИ
КИРЕ БАБАНОСКИ
ИЦЕ ИЛИЈЕВСКИ



ЗАШТИТА ПРИ ТЕРОРИСТИЧКИ НАПАДИ

д-р ЗЛАТЕ С. ДИМОВСКИ
д-р КИРЕ Б. БАБАНОСКИ
д-р ИЦЕ Н. ИЛИЈЕВСКИ

**ЗАШТИТА
ПРИ
ТЕРОРИСТИЧКИ НАПАДИ**

СКОПЈЕ, 2019

проф. д-р Злате ДИМОВСКИ
д-р Кире БАБАНОСКИ
проф. д-р Ице ИЛИЈЕВСКИ

ЗАШТИТА ПРИ ТЕРОРИСТИЧКИ НАПАДИ

ИЗДАВАЧ



**КОМОРА
НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ**

ул. 50-та Дивизија, бр. 34
1000 Скопје, Република Северна Македонија
www.obezbeduvanje.org.mk
info@obezbeduvanje.org.mk

ЗА ИЗДАВАЧОТ

м-р Верица МИЛЕСКА СТЕФАНОВСКА
Претседател на Комората на Република Северна Македонија
за приватно обезбедување

РЕЦЕНЗЕНТ

проф. д-р Методија ДОЛЧИНОВСКИ

КОРИЦА

Александар СТЕФАНОВСКИ

КОМПЈУТЕРСКА ОБРАБОТКА

д-р Кире БАБАНОСКИ

ЛЕКТОР

м-р Даниела ТАКЕВА

ТИРАЖ

300 ПРИМЕРОЦИ

CIP – Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

323.284:351.746.5-051(497.7)(035)

ДИМОВСКИ, Злате

Заштита при терористички напади / Злате С. Димовски, Кире Б. Бабаноски, Ице Н. Илијевски. – Скопје: Комора на Република Северна Македонија за приватно обезбедување, 2019. – 118 стр.: илустр.; 25 см

Фусноти кон текстот. - Библиографија: стр. [99-102]. - Содржи и: Прилози

ISBN 978-608-66216-7-4

1. Бабаноски, Кире Б. [автор] 2. Илијевски, Ице Н. [автор]

а) Терористички напади - Заштита - Приватно обезбедување - Македонија - Прирачници

COBISS.MK-ID 111860490

- СОДРЖИНА -

ВОВЕДНИ НАПОМЕНИ..... 1

1. Улогата на приватното обезбедување во спречувањето и борбата против тероризмот 3
2. Изградба на јавно-приватно безбедносно партнерство за спречување и борба против тероризмот 4
3. Примена на разузнавањето во заштитата од терористички напади . 7
4. Меѓународна соработка и размена на информации во спречување и откривање терористички активности 9

ДЕЛ I

ЗАКАНА ОД ТЕРОРИСТИЧКИ НАПАДИ

1. Елементи и карактеристики на тероризмот 11
2. Терористички организации - членови, структура и идеологија 16
3. Цел на терористичките напади 18
4. Заканите од терористички напади по критичната инфраструктура. 19
5. Фази на подготовка на терористички напади 24
6. Извршување терористички напади..... 29

ДЕЛ II

ЗАШТИТА ОД ТЕРОРИСТИЧКИ НАПАДИ

1. Безбедносен оперативен план 33
 - 1.1. Идентификување закани..... 36
 - 1.2. Ранливости 37
 - 1.3. Безбедносна проценка на ризик..... 39
2. Заштитна безбедност..... 42
3. Физичка безбедност 44
 - 3.1. Закани од бомби 45
 - 3.1.1. Возила-бомби..... 46
 - 3.1.2. Закана од курир 48
 - 3.1.3. Поштенски пратки..... 48
 - 3.2. Закана од користење хемиско, биолошко и радиолошко оружје 50
4. Мерки за физичка безбедност 51

4.1. Надворешно опкружување	52
4.2. Зајакнување на имотот	52
4.3. Внатрешни области	53
5. Информациска безбедност	57
5.1. Типични методи на електронски напад	59
6. Мерки за информациска безбедност	61
6.1. Едукација на персоналот	62
6.2. Одговорно постапување со документи	63
6.3. Отстранување информации	63
7. Безбедност на персоналот	64
8. Мерки за безбедност на персоналот	65
8.1. Проценка на ризик	66
8.2. Вработување	67
8.3. Развивање добра безбедносна практика на работното место	67
9. Планирање деловен континуитет	68
9.1. Командна соба за инциденти	72
10. Комуникациски планови	74
11. Индикатори за подготвување или постоење терористички активности	76

ДЕЛ III

АКТИВНОСТИ ПО ИЗВРШЕН ТЕРОРИСТИЧКИ НАПАД

1. Реагирање при извршен терористички напад	79
2. Пружање прва помош на местото на нападот	80
3. Евакуација	85
4. Пребарување	87
5. Обезбедување на местото на инцидентот	88
6. Заштита на местото на настанот преку ограничување на пристапот	91

ЗАКЛУЧНИ СОГЛЕДУВАЊА И ПРЕПОРАКИ	95
---	-----------

РЕФЕРЕНЦИ	99
------------------------	-----------

ПРИЛОЗИ	103
----------------------	------------

ПРЕДГОВОР

Во изминатите две декади светската мапа ја обележа драматично зголемениот број терористички напади кои претставуваат застрашувачка закана по безбедноста на општата популација што побарува и сериозни капацитети за спречување и справување со нив. Со оглед дека приватното обезбедување се препознава како одговорен фактор за безбедноста на лицата и имотот во речиси секоја сфера од човековото опкружување (аеродроми, електрани, фабрики, болници, училишта, трговски центри, деловни објекти и сл.) евидентна е непосредната вклученост на овој безбедносен сегмент во генералната заложба на безбедносниот сектор за справување со заканите, нападите и последиците од терористички напади. Токму од таа причина, заканата од тероризмот, подготвување за потенцијални напади, како и справување со последиците од тероризам претставуваат проблематика од витално значење, како за државата така и за приватниот безбедносен сектор.

Комората на Република Северна Македонија за приватно обезбедување врз основа на својата законски делегирана формална одговорност за заштита на професијата и адекватен одговор на сите актуелни предизвици за приватниот безбедносен сектор, континуирано ја манифестира својата заложба за унапредување на дејноста и инвестирање во надоградување на знаењата и вештините. Проблематиката на спречување, односно соодветна реакција на терористички акти, правилно дејствување при терористички напади и, генерално, темата на подготвеност за и во врска со терористички загрозувања на приватната безбедност на лицата и имотот се наоѓаат високо на приоритетите на приватното обезбедување. Оваа област од научно-стручен аспект била повеќекратно третирана од страна на приватниот безбедносен сектор, но секогаш како дел од пошироки согледувања, анализи и генерално постапување.

Оттука, ова дело насловено „Заштита при терористички напади“ претставува пионерски обид во единствена целина да биде публикувана многу важната и актуелна тема на постапување на приватниот безбедносен сектор во случаи на терористичко загрозување на безбедноста. Во тој контекст, оваа публикација во своите воведни напомени ја аргументира улогата на приватното обезбедување во спречувањето и борбата против тероризмот, изградбата на јавно-приватно безбедносно партнерство, соработка, размена на информации и сл. Во посебен дел обработени се општите елементи, карактеристики, цели на терористичките напади, натаму фазите на подготовка и самото извршување, а посебно е третирана областа на закани од терористички

напади по критичната инфраструктура на државата што претставува сегмент во кој приватното обезбедување реализира значителен обем од своите надлежности. Оваа публикација го насочува својот фокус конкретно кон превентивниот аспект на заштитата од терористички напади, за што опширно е елабориран процесот на подготвување на безбедносните оперативни планови, безбедносната проценка на ризик, мерки, активности, задачи и работи кои треба да бидат преземени од страна на приватното обезбедување, но и другите безбедносни чинители во насока на отстранување на заканите, ризиците, опасностите и загрозувањата од тероризам. И финално, без разлика на подготвеноста, искуствата покажуваат дека терористичките напади се случуваат во реалноста, така што неминовно е работниците за приватно обезбедување да имаат познавања за активностите кои треба да бидат преземени во смисла на пружање прва помош, евакуација на простории, пребарување, обезбедување на местото на инцидентот итн. што, исто така, го нуди ова дело.

Довербата за изготвување на оваа публикација Комората на Република Северна Македонија за приватно обезбедување ја даде на потврдените автори и блиски соработници на приватниот безбедносен сектор: проф д-р Злате Димовски, д-р Кире Бабаноски и проф. д-р Ице Илијевски кои како додадена вредност на делото обезбедија и безбедносни препораки во функција на унапредување на приватната безбедност во случаи на терористички напади, но и заради генерален придонес во гаранција на безбедноста на лицата и имотот, за што сме исклучително благодарни.

Искрено се надевам дека публикацијата „Заштита при терористички напади“ ќе ја реализира својата функција во секторот приватно обезбедување и ќе ја надополни празнината во стручната литература во оваа област, а истовремено ќе го привлече вниманието и на пошироката академска и стручна јавност и ќе ја поттикне на натамошни вложувања во насока на унапредување на работењето во дејноста приватно обезбедување, но и заради општ придонес за унапредување на безбедноста во нашата држава.

м-р Верица МИЛЕСКА СТЕФАНОВСКА

Претседател на
Комората на Република Северна Македонија за приватно обезбедување

ВОВЕДНИ НАПОМЕНИ

Република Северна Македонија е дел од Антитерористичката коалиција предводена од САД која е формирана како резултат на терористичките напади на неколку локации во САД на 11.09.2001 година. Со тоа, државата покажа пред меѓународната заедница дека сака да го следи патот на цивилизираните вредности, да се вклучи во изградбата на мирот и стабилноста и да придонесе за развој на безбедни општества. Меѓутоа, од друга страна, на тој начин, практично и официјално државата стана мета на терористичките организации кои се во директна војна со оваа Антитерористичка коалиција. Државните безбедносни служби ги вложуваат сите неопходни напори за заштита на територијалниот интегритет на државата, имотот и објектите во неа, како и заштита на животот и здравјето на граѓаните.

Тероризмот е глобална закана за целото човештво која остава особено негативни и штетни последици. Терористичките организации си имаат своја идеологија и нивните цели настојуваат да ги остварат на секој можен начин. За таа цел тие врбуваат, регрутираат, обучуваат и вклучуваат погодни членови во нивната организација чии главни карактеристики со кои се одликуваат се исламски фундаментализам и радикализам. Активностите со кои се занимаваат терористите – членови на терористичката организација, се извршување терористички акти заради предизвикување страв и несигурност кај населението, во јавноста, уривање на државниот поредок, а со тоа изнудување на определено однесување од страна на власта, заради остварување на нивните политички, религиозни или идеолошки цели.

Со забрзаниот развој на приватната безбедност во државава во последните години, се зголемува бројот на јавни и приватни објекти и имот за чија безбедност се грижат агенциите за приватно обезбедување. Во рамките на делокругот на работните задачи и надлежности, работниците за приватно обезбедување ги применуваат законски дадените овластувања со цел најоптимално да го обезбедат просторот и луѓето во него од секакви внатрешни и надворешни закани и опасности. Доскорешните форми на загрозување на безбедноста на имотот, објектите и луѓето беа напади, кражби, саботажи, диверзии, уништувања, оштетувања и сл., но, во последно време се појавија и нови хибридни закани кои може значително да ја нарушат безбедноста на клиентите. Терористичките напади, инциденти и акции се форма на загрозување на безбедноста чии начини на реализирање се различни и постојано променливи. Тие се реални и доста сериозни во однос на последиците кои може да ги создадат. Нападите може да се случат на кое било место, во кое било време без предупредување кон

организацијата и луѓето во неа. Тероризмот не значи само насилнички акт кон луѓе и имот. Оштетување или уништување комуникациски системи, оштетени средства и опрема за работа и уништена репутација, може да предизвикаат брза и/или долготрајна штета на компаниите/организациите и, поради тоа, се подеднакво посакувани и применувани од страна на терористичките организации.

Борбата против тероризмот е високо зависна од ефикасноста при преземањето на мерките и активностите од страна на субјектите задолжени за спроведување на законот, нивната брзина во откривањето на терористичките организации, нивните подготвителни дејствија и делувањето по извршен терористички напад. Борбата против тероризмот бара тесна соработка меѓу ваквите субјекти заради размена на информации и навремено откривање на нелегалните активности кои се претходник на терористичките акти.

Системот на приватната безбедност има многу значајна улога и во превенирањето и во справувањето со критични инциденти вклучувајќи ги тука и терористичките напади. Тие се првите кои може да пружаат помош по случен инцидент. Затоа, работниците за приватно обезбедување треба да ги надоградуваат своите знаења, способности и вештини за заштита на имотот, објектите и луѓето од секакви современи форми на загрозување. Тие мора да знаат да препознаваат, да предупредуваат и да укажуваат на сомнителни активности кои ги забележуваат во текот на нивното работење, како и да знаат да преземат соодветни мерки и активности за спречување инцидентни ситуации, како и заштита при нивно случување. Тоа значи дека нивните работни задачи треба да се насочени пред и по извршениот инцидент.

Потребата од создавање на овој прирачник кој се однесува на практичните аспекти на заштитата на имотот, објектите и луѓето од терористички закани и активности се согледува во непостоењето на ваков тип на едукативни материјали, од каде работниците за приватно обезбедување би се запознале со конкретните упатства, насоки и препораки во вакви ситуации. Овој прирачник ќе ги прикаже токму мерките и активностите кои секој работник за приватно обезбедување треба да ги презема во текот на извршувањето на секојдневните работни задачи и обврски, а со цел превенирање на вакви напади, како и конкретните чекори кои треба да ги знае за да ги преземе во случај на извршен терористички напад во имотот или објектот кој го обезбедува.

1. Улогата на приватното обезбедување во спречувањето и борбата против тероризмот

Новите закани по безбедноста на државите создаваат нови потреби за безбедноста на лицата и имотот. Современиот тероризам, како една од тие закани создаде потреба од ново размислување и дејствување во насока на превенција и сузбивање. Поместувањето на методите на делување на терористите кон помеки цели ја поместува и борбата против тероризмот во приватниот сектор. Трендовите на закани од тероризам ја истакнуваат потребата од вложување во приватниот безбедносен сектор кој е суштински за спречување на ризиците од тероризам.

Улогата на работниците за приватно обезбедување во насока на спротивставување на тероризмот е тема за која малку се зборува и не е добро разбрана и прифатена. Сè повеќе актуелна станува по нападите на кулите близначки од 2001 година во САД, каде во сите извештаи се нагласува дека работниците за приватно обезбедување покажале голема храброст и професионализам ризикувајќи ги нивните животи за да одржат ред, да евакуираат и да помогнат во спасување на стотици животи.

Работниците за приватно обезбедување кои работат на обезбедување на критичната инфраструктура како: трговски центри, универзитети, болници и сл., објектите за јавен превоз (аеродроми, автобуски станици, железнички станици) имаат значаен придонес во контратерористичките иницијативи. Покривањето голем број оперативни позиции во објектите од страна на работниците за приватно обезбедување може да овозможи рано предупредување и препознавање ризици и закани од можни терористички акти. Тие се видлива и симболична карактеристика на заштитна мерка против тероризмот. Во случај на инцидент, тие се оние кои први реагираат: пружање прва помош, обезбедување на местото на настанот, евакуирање на лицата, известување и давање брифинг на државните безбедносни служби. Иновациите и промените на тактиките на терористите бараат соодветни мерки за превенција и заштита на клиенти, објекти, возила, авиони, итн. од страна на приватните агенции за обезбедување.

Покрај придобивката од приватното обезбедување во насока на чувството на лична безбедност, исто така, во некои инциденти може да помогне и во одвраќање на одреден напад, како и превенција од напаѓачи. Работниците за приватно обезбедување се чести жртви при терористички напади. Постојат случаи во светот каде работници за приватно обезбедување се убиени додека пресретнуваат терористи - бомбаши самоубијци, притоа спасувајќи многу животи. Парадоксот кој

се појавува, е успешно спречен терористички напад, а загинати се оние кои први реагираше. Агенциите за приватно обезбедување се позиционираат на современиот пазар на услуги за безбедност, заради нивната ефикасност, економичност, флексибилност и професионализам кој го нудат.

За таа цел потребно е подигање на свеста за важната улога која ја има секторот за приватна безбедност и јакнење на неговата заслужена позиција заедно со другите безбедносни органи во функционалноста на борбата против тероризмот.

2. Изградба на јавно-приватно безбедносно партнерство за спречување и борба против тероризмот

Службите за спроведување на законот денес се под огромен притисок да ги спроведат своите активности за спречување и реагирање на разни криминални активности, плус голем дел од работата за националната безбедност, во време на ограничени ресурси и буџети. Агенциите за приватна безбедност се под сличен притисок, но ги извршуваат своите традиционални активности за заштита на луѓето, имотот и информациите, плус придонесуваат за националните напори за заштита на државата од надворешни закани, сè додека се води сметка за профитабилноста на деловните активности кои ги заштитуваат.¹

Реагирањето на реалните терористички настани е задача на органите, институциите, телата и службите од системот за национална безбедност во државата. Генерално, јавниот безбедносен сектор е заинтересиран да добива и поседува информации за евентуални закани од подготвување и планирање терористички активности, а приватниот безбедносен сектор со покриеноста која ја има врз голем број јавни објекти и места, има контрола врз ранливите точки. Оттука, јасна е огромната потреба сите безбедносни служби во јавниот и приватниот сектор да работат заеднички, координирано и партнерски во откривањето и спречувањето на терористичките закани. Секоја страна може и ќе има корист од можностите кои ги има другата страна.²

Во интерес на двете страни е да работат заедно. На пример, службите за спроведување на законот можат:

- да ги подготват работниците за приватно обезбедување за пружање помош при итни случаи (во многу случаи, работниците за приватно обезбедување се првите реагирачи на местото на настанот),
- да ги координираат напорите за заштита на критичната инфраструктура во државата чие огромно мнозинство е во

сопственост на приватниот сектор и кои се обезбедуваат од страна на агенциите за приватно обезбедување,

- да добијат бесплатна обука и услуги,
- да стекнат дополнителни ресурси и експертиза за персоналот,
- да користат специјализација за одредени знаења и вештини од приватниот сектор (на пример, за компјутерски криминал и напредна технологија),
- да соберат докази во кривични истраги (на пример, преку снимки од видеонадзор на местото на настанот),
- да соберат повеќе информации за инцидентите (преку известување и разговор со безбедносниот персонал на местото на настанот) и
- да го намалат бројот на повици за пријавување настани.

Приватниот безбедносен сектор, исто така, може многу да извлече од заедничката соработка. Овој сектор може:

- да ги координира своите планови со службите за јавна безбедност, однапред, во врска со евакуацијата, транспортот, обезбедувањето храна и другите проблеми во итни случаи,
- да добие информации од државните безбедносни служби во врска со ризиците, заканите, опасностите, трендовите на криминалот и други безбедносни проценки,
- да развие врски за комуникација, така што практичарите да знаат со кого да контактираат кога им е потребна помош или сакаат да пријавуваат одредени информации,
- да изгради разбирање за спроведувањето на законите кои се поврзани и се однесуваат на корпоративните потреби (како што е доверливоста) и
- да го зајакне почитувањето на спроведувањето на законите во безбедносната област.

Заедничките придобивки од соработката и партнерството вклучуваат:

- креативно решавање на проблеми,
- зголемени можности за обука,
- споделување сознанија, податоци и разузнавачки информации,
- можности за „зголемување на силата“,
- пристап до заедницата преку комуникациска технологија во приватниот сектор,
- намалено време на закрепнување по катастрофи.

Способноста да се заштити критичната инфраструктура во државата и да се придонесе во напорите за унапредување на националната безбедност во одреден дел, зависи и од надлежноста на

работниците за приватно обезбедување. Градењето партнерства е од суштинско значење за ефикасна национална безбедност.

Односот помеѓу државните безбедносни служби и агенциите кои работат во областа на приватната безбедност³ може да биде повеќе негативен отколку позитивен според настанатите последици, доколку не е јасно определен. Има многу дилеми и се јавува забуна во улогата помеѓу јавниот и приватниот безбедносен сектор, особено во случаите кога нешто треба да се преземе во итни случаи.

Ако во одредена фабрика настане експлозија, таа може веднаш да биде прогласена за место на настан од страна на полицијата, па потоа безбедносниот персонал на компанијата не може да одговори по потреба. Исто така, во ерата по 11-ти септември 2001 година, службите за спроведување на законот постојано вршат безбедносни проценки на ризик, но, честопати тие не се толку одблиску запознати со нив, како што е приватното обезбедување.

Односите помеѓу државните безбедносни служби и приватната безбедност се мешани. Единиците на локалната самоуправа може истовремено да имаат некои извонредни партнерства, но и некои контрапродуктивни односи. Нападот врз кулите близначки од 11-ти септември 2001 година, помогна во градењето односи. Како и да е, вистинската мерка за успех е дали партнерството остварува нешто и колку трае.

Концептот на полициско работење во заедницата ги повикува службите за спроведување на законот да развиваат односи со различни сектори во заедницата. Претставниците на безбедносните служби редовно треба да се среќаваат со членови на верските заедници, деловни групи, спортски клубови, соседски здруженија и други формални и неформални групи на граѓани. Но, се чини дека тие не се среќаваат редовно со групи на директори и менаџери од компаниите/агенциите за корпоративна безбедност.

Со оглед на постојните ресурси и дополнителните оптоварувања на службите за спроведување на законот, се чини дека сега е најдобро време да се развијат нови односи со приватното обезбедување и да се најдат начини за заедничко работење.

Постојат некои пречки кои го оневозможуваат партнерството помеѓу службите за спроведување на законот и агенциите за приватно обезбедување.

Првенствено, размената на информации е тешка. Агенциите за приватно обезбедување не чувствуваат дека добиваат навремена информација од полицијата, а исто така се плашат дека информациите што ги даваат на полицијата може да завршат во фиока. Полицијата,

пак, стравува дека корпоративниот сектор не може дискретно да ги третира информациите кои ги поседуваат.

Другите теми вклучуваат почитување (т.е. непочитување на спроведувањето на законите од областа на безбедноста), доверба, разлики во обуката и конкуренција. Друга пречка е што двете страни можеби не го сфаќаат сериозно обемот на нивните заеднички цели.

Раководителите на службите за спроведување на законот не знаат многу за овластувањата на приватната безбедност. На пример, кога зборуваат за лицата кои први реагираат на местото на некој инцидент, тие, главно, мислат на самите нив, пожарникарите и медицинските лица од брзата помош. Зошто да не се споменуваат работниците за приватно обезбедување? Во многу итни случаи, токму тие се, всушност, први на местото на настанот и можат да им покажат на полицајците и пожарникарите каде да се упатат. Недостасува свесност за тоа што е и што прави, всушност, приватната безбедност. Делумно, ова се должи на непостоењето кохезија во безбедноста. На пример, безбедноста не е секогаш организирана како функционална група во рамките на една организација, па безбедносните служби не тренираат заеднички за заемна помош и обично немаат интероперабилност во комуникацијата.

Што би помогнало да се отстранат пречките за соработка?

И двете страни имаат одговорност за подобро партнерство.

Професионалците за безбедност треба да преземат иницијатива да организираат состаноци лице в лице со претставници од службите за спроведување на законот пред да се појави криза. Ваквите состаноци можат да помогнат во градењето лични односи и доверба.

Секоја страна треба да ја едуцира другата за своите можности, пред да избие криза, така што секоја ќе знае кога да се повика на другата и каква помош да очекува (и да понуди). Интегрираната обука може да сруши некои бариери. Агенциите за приватно обезбедување го добиваат своето место во системот и се надеваме дека во иднина претходно наведените пречки ќе се надминат.

3. Примена на разузнавањето во заштитата од терористички напади

Разузнавањето е процес, збир на активности кои обезбедуваат релевантни и навремени информации за идни планирани криминални активности, па соодветно на тоа и за индивидуалци и групи кои планираат или подготвуваат извршување терористички напади. Преку разновидни јавни и тајни методи и средства може да се откријат подготвителните дејствија кои им претходат на актите на загрозување на безбедноста на луѓето, објектите и имотот. Всушност, со тоа разузнавањето добива превентивна функција во антитерористичката

борба. Залудни се истрагите *post festum* – по извршениот терористички напад и активирањето човечки ресурси со кои располагаат безбедносните служби, заради собирање релевантни информации. Неопходно е вложување во подигнување на степенот на ефикасност, ефективност и продуктивност на разузнавачката дејност на сите субјекти во рамките на безбедносниот систем (вклучително и субјектите од секторот приватна безбедност), заради навремено откривање на терористичките цели и нивно спречување.

Дали и колку процесот на разузнавање ќе биде ефикасен во извршувањето на својата превентивна функција во однос на борбата против тероризмот, зависи од способноста за континуирано дејствување и солидно познавање на терористичките групи и поединци, нивните планови и цели, нивната политичка, економска и психолошка мотивираност и навики за лидерство/водство, членство, логистичките и финансиските можности, врските со другите домашни и меѓународни терористички организации итн.⁴

Пред сè, преку разузнавањето потребно е да се открие идентитетот на лицата кои партиципираат во одреден терористички план. Секако, мора да се дознае и која е содржината, односно целта на тој план. За потсетување, примарна задача на разузнавањето е превентивната функција или поинаку кажано, да биде чекор понапред во однос на терористите и нивните планови, така што терористичките активности да останат желба на хартија без воопшто да бидат реализирани.⁵

Огромно е значењето на разузнавањето за успешното водење на борбата против тероризмот. Разузнавањето е клучната алка во антитерористичките операции и истраги. Успешното разузнавање е најзначајното оружје во борбата против тероризмот. Способноста на државата да ја детектира, анализира и да дејствува против терористичката закана, во голема мерка зависи од ефикасноста на разузнавачкиот апарат. Секојдневното прибирање информации за идентитетот, целите, плановите и слабите точки на терористите и на терористичките организации, е најтешката област во сферата на разузнавањето. Сепак, ниту еден друг метод на антитерористичката политика не е поважен во превенцијата, попречувањето и реагирањето на терористичките напади.

Во однос на работата на разузнавачките служби и прибирањето информации за борба против тероризмот, нема да се постигне значителен успех, доколку тоа се прави само на национално ниво. Работата на регионално и на глобално ниво го надополнува разузнавачкиот процес преку меѓусебната координација и размена на разузнавачки информации.

Приватната безбедност може да даде огромен придонес во собирањето значајни информации кои ќе се искористат во антитерористичката борба. Работниците за приватно обезбедување низ секојдневната работа може да забележат сомнителни однесувања на одредени лица, нивното движење, рутински активности, специфични знаци и сл. Тие се оние кои работат на локации кои се атрактивна мета за напад на терористите, па затоа треба да бидат свесни за сите активности кои се случуваат на терен, да бараат, идентификуваат и да забележуваат потенцијални опасности и закани.

4. Меѓународна соработка и размена на информации во спречување и откривање терористички активности

Транснационалниот карактер на тероризмот ја наметнува потребата од интензивна меѓународна соработка (билатерална и регионална) за целите на размената на релевантни податоци и информации. Националните системи за борба против тероризмот би биле недоволни и нецелисходни доколку не се воспостави заедничка соработка со меѓународните тела. Меѓународната заедница поради ваквата констатација сè повеќе ги интензивира своите напори за поттикнување на определени инструменти и методи на меѓународна соработка во спречувањето на тероризмот кои би биле ефикасни за оправдување на нивното воспоставување. Ваквиот облик на меѓународна соработка претставува облик на заемна кооперативност и координираност на кој му се посветува повеќе внимание поради непроценливите резултати кои ги постигнува.

Транснационалната природа на денешниот тероризам им дава силен мотив на државите да ги разменат разузнавачките информации со цел да ги откријат терористите, да спречат идни терористички напади и да се заштитат меѓусебно. Меѓутоа, размената на антитерористичките разузнавачки информации е често тешка и комплексна. Помеѓу тајните служби на државите треба да постои размена на антитерористички разузнавачки информации и тоа со постоење на значително ниво на заемна доверба.

Мултилатералната размена на информации вклучувајќи ги и индикаторите за потенцијални напади, но и екстремистички и радикални дејствувања кои водат кон терористички активности, се потребни за да се спречат негативните последици. Ваквиот пристап бара развој на нови аналитички вештини, процеси и политики. Меѓувладините инструменти се потребни за во целост да се искористи споделувањето информации, заедно со развојот на дистрибуирани разузнавачки производи вклучувајќи го и развојот на механизмите за

размена на информации меѓу двата јазли - интранационален и меѓународен.

Во однос на меѓународната соработка за борба против тероризмот и организираниот криминал, Република Северна Македонија преку Министерството за внатрешни работи врши размена на разузнавачки и други податоци со соодветните безбедносно-разузнавачки служби на други земји, а соработува и со НАТО, ИНТЕРПОЛ, ЕВРОПОЛ и ЕВРОПРАВДА.

ДЕЛ I ЗАКАНА ОД ТЕРОРИСТИЧКИ НАПАДИ

1. Елементи и карактеристики на тероризмот

Тероризмот е појава која не се ограничува на територијата на една држава. Во светот не постои општо прифатена дефиниција за тероризмот. Проблемот за дефинирање на тероризмот со децении е извор на недоразбирање меѓу државите, а и денес не постои заедничка позиција. Сегашното проучување на тероризмот произлегува од две наметнати доминантни концепции за тероризмот во светот од страна на западните научници и официјалните ставови од каде произлегува и обидот за дефинирање на тероризмот.⁶

Воопштено, тероризмот се опишува најчесто како: свесна, умислена употреба на насилство од страна на организирани групи или поединци против невоени цели за да се изврши притисок врз населението преку влевање страв и заплашување или врз органите на државата за постигнување на целите кои не можат да бидат исполнети преку законски средства. Концептот на меѓународниот тероризам е идентичен – преземање на акција со политички цели против странска држава, меѓународна организација или одредени претставници во време на мир или војна што е штетно за меѓународните односи и глобалниот мир и поредок.

Терористичките активности се многу сложени и сè уште не се доволно разјаснети, особено кога се работи за нивните носители и општи причини за постоењето на модерниот тероризам. Цивилизацијата е загрозувана од непредвидливо зголемување на бројот на терористички организации во светот. Ова се должи на недостаток на сериозноста на забележаната закана од тероризмот и примена на двојни стандарди од страна на некои големи сили.⁷

Кога станува збор за антитерористичките активности, тие сега се повеќе ограничени, огромна енергија и огромни ресурси се насочени кон справување со последиците, наместо за спречување на неговите причини. Што се однесува до методите на борбата на големите сили – евидентно е ширењето на доминантната употреба на сила и воени фактори, а во заднина е разгледување на потеклото и мотивите на операциите на тероризмот од страна на терористичките организации ширум светот. Извесно е дека тероризмот не може да се искорени само со користење воена сила, туку со промена на севкупните општествени односи, развојот на демократијата и едукација на целото општество.

Експертите за тероризам и земјите кои се борат против тероризмот се согласуваат во оценката дека е многу тешко да се одреди

дефиницијата на тероризмот која ќе биде призната од страна на сите земји во светот, но тие, исто така, се согласуваат со фактот дека без тоа, не може да се води успешна борба против меѓународниот тероризам. Тероризмот не е локален проблем или проблем на одделни земји, сега е меѓународен феномен, а со тоа и за соодветен одговор на тероризмот, мора да работат заедно за да се усогласат сите земји во светот што денес се чини невозможно. Сепак, нема одговор на прашањето за тоа зошто не може да се води успешна борба против терористичките организации и нивните приврзаници, дали може да се бара отчетност на државите кои го поддржуваат и дали тие можат да ги поддржат потребните меѓународни договори чие отсуство досега се покажа како отежнувачка околност во борбата против тероризмот.

Етиолошки гледано, зборот тероризам потекнува од латинскиот збор *terror* што значи страв и трепет, начин на владеење со влевање страв и насилство, политичка борба по пат на индивидуален терор.⁸ Повеќето луѓе немаат јасна претстава за тоа што е тероризам, но им треба попрецизна и конкретна дефиниција на овој збор. Оваа непрецизност е делумно охрабрена од страна на медиумите чии напори за пренесување на често сложени пораки во најкраток можен рок доведуваат до етикетирање на цела низа насилнички дела како „тероризам“.⁹ Она што го прави сложено одредувањето на поимот тероризам е фактот дека во содржината на овој поим влегуваат повеќе карактеристики што му се својствени.

Овој процес на одредување на поимот тероризам и неговите составни компоненти дополнително го комплицира фактот дека неговата содржина се менува низ времето, станува збор за динамична компонента што ги менува своите појавни облици и форми во зависност од временските и просторните детерминанти и кои се прилично од политичка природа. Различните и бројните обиди за дефинирање на тероризмот од страна на научни институции, организации и индивидуални научни мисли, имале различно значење и употребливост во процесот на идентификација, класификација и дескрипција на поимот тероризам, во зависност од местото на настанување, степенот на научност и целите споменати во дефиницијата.

Академските дефиниции претставуваат збир на мислења и ставови кои странската и домашната наука ги забележала во процесот на истражување на тероризмот. Тие меѓусебно се разликуваат во зависност од вредносниот, концептуалниот и идеолошкиот пристап кон тероризмот и можат да се класифицираат како негативни, консензуални и апстрактни.

Големиот број дефиниции за тероризмот го покажува неговото значење, опасност, променливиот карактер и разновидната форма на

исполнување што претставува претпоставка за создавање и развој на ефикасни начини на општествена реакција на тероризмот во рамките на развој на стандардите, процедурите и механизмите што можат да се применат од страна на државите и меѓународната заедница во превенција на терористичкото однесување.

За потребите на овој прирачник, авторите го сфаќаат тероризмот, односно терористичкиот акт, како планска, организирана, групна или поединечна, незаконска употреба на сила, изразена со примена на оружје (ладно, огнено, биолошко, хемиско, радиолошко, нуклеарно) или кое било средство што може да се употреби како оружје или закана со употреба на сила, против луѓе или имот, заради принудување или заплашување, како начин за постигнување политичка, етничка, религиозна, идеолошка или друга цел.

Елементи на тероризмот

Еволуцијата на тероризмот ја отсликува неговата комплексност, динамичност и интензивност, но и неговата огромна опасност за националната безбедност на државите, како и на севкупната меѓународна безбедност. Денес меѓународните односи се карактеризираат со појавување нови поопасни форми на тероризам со можност да предизвикаат и масовни последици со што светот полека станува заложник.¹⁰

Поширокото и прецизното дефинирање на тероризмот придонесува за идентификување на неговите елементи кои константно се појавуваат во терористичките акти. Сепак, потребно е да се води сметка дефиницијата да не се конструира со едноставно набројување на доминантните елементи на тероризмот и затоа е потребно да се земат предвид одредени општествено политички прилики во кои тероризмот настанува и се исполнува.

Значаен број автори вниманието го насочуваат на основните елементи на тероризмот (со што се избегнува едностраност и површност во одредување на неговата суштина) имајќи предвид политичка и мотивирана намера, организираност, последиците од терористичките акти и исклучителна разновидност и број на можните напади, комуникативност и др. Многу автори ги констатираат следните елементи на терористичките напади:

1. Актот на насилство;
2. Политичка, верска, етничка и расна мотивираност;
3. Политички цели и пораки;
4. Создавање атмосфера на страв, ужас, недоверба;
5. Суровост и безобзирност;
6. Невини жртви;

7. Јавност/комуникативност и
8. Незаконит криминален чин.

Покрај овие елементи се наведуваат и други конститутивни елементи на тероризам: метод, средства, тактика, самоволие, безличност, учена, принуда и др.¹¹

Од анализата на дефинициите за тероризам, како и понудените елементи на тероризам може да се заклучи дека постојат 5 (пет) основни, клучни елементи на тероризам кои ги вклучуваат сите останати елементи на тероризам и се наоѓаат во сите дефиниции. Врз основа на овие елементи тероризмот може да се определи: предметно, содржински и суштински.

Секако, важна е околноста дека тие елементи се групирани по одредени битни обележја, односно дека вклучуваат повеќе слични одредувања во еден елемент. Предвид се земени основни односно одредувачки елементи на тероризмот при што се подразбира дека тие вклучуваат и останати елементи на тероризам. Значи, неспорни се следните елементи на тероризам:

- носители на тероризмот,
- цели,
- жртви,
- насилство и закана со насилство и
- предизвикување страв.

Носителите на тероризмот претставуваат групи кои извршуваат терористички напади и може да се поделат на државни и недржавни. Кога станува збор за целите, тие се најчесто од политичка природа, но може да бидат верски, етнички или национално мотивирани. Кога се зборува за жртвите се разликуваат два видови жртви и тоа: непосредна, која трпи последица и посредна, кон која е упатена пораката. Насилството и заканата од насилство е конститутивен елемент на тероризам што укажува на заклучок дека нема тероризам без насилство. Стравот е примарен ефект којшто носителите на тероризмот го предизвикуваат поради остварување на поставени терористички цели.

Од сите наведени елементи се воочува присуство на неколку битни одредници на тероризмот и терористичката акција. На нивна основа се гледа дека нема тероризам без употреба на насилство, како и без идеолошко-политички карактер на активностите што може да се каже за предизвикување страв и за организирано делување кон целта.

Карактеристики на тероризмот

Со развојот и креативноста на терористичките организации и нивните активности, се појавуваат бројни и разновидни облици на современиот тероризам, а со секој облик се појавуваат специфични

облежја и барања за уважување разновидни критериуми како би се идентификувале и формулирале заеднички карактеристики на овој, по многу карактеристики, енигматичен вид на насилство. Карактеристиките на тероризмот се врзани за неговата манифестација што го чини специфичен. Тероризмот се манифестира со вршење акти кои имаат одредени карактеристики. Носителот на секој облик на тероризам, а со тоа и на терористичкиот акт, е човекот и тоа како припадник на некоја терористичка организација или, пак, како индивидуа.¹²

Тероризмот е условен со постоење на терористичката организација како колективитет и човекот како поединец и непосредните учесници на тероризмот. Од ова произлегуваат сите останати карактеристики на тероризмот. Покрај тоа, карактеристиките на тероризмот може да се согледаат анализирајќи го сегашниот, современиот начин на постоење и исполнување на тероризмот кој одговара во моментот, при што би станувало збор за актуелни карактеристики на тероризмот. Овие карактеристики се специфични за денешните облици на тероризам. Можно е карактеристиките на тероризмот да се однесуваат, првенствено, на можноста на употребата на оружје за масовно уништување, односно хемиско, биолошко, радиолошки и нуклеарно оружје во терористички цели и можни последици кои би биле предизвикани од таквиот облик на терористичките активности.

Иако значењето на тероризмот се менувало со текот на времето, неколку карактеристики останале конзистентни и постојани. Една од карактеристиките е употребата на насилство од страна на терористите кои имаат за цел да привлечат внимание кон себеси и нивната кауза и се надеваат дека на тој начин ќе можат да манипулираат за да извлечат отстапки од одредени држави, да ги заплашат или присилуваат владите за остварување на одредени права. Исто така, стравот или теророт, вознемиреноста и загриженоста што ја создава користењето на насилството и заканата од уште поголемо насилство е непроменета карактеристика.

Врз основа на наведените карактеристики на тероризмот, може да се анализираат како основни (општи), тековни (актуелни) и можни карактеристики и тоа¹³:

1. Основни (општи) карактеристики:

- Акти на насилство (закана и примена).
- Предизвикување страв.
- Остварување терористички цели.
- Пренесување на одредена порака (медиумска експлоатација).
- Организираност (формална и содржинска).

- Бруталност, неморалност и ирационалност на терористичкиот акт.
- Избор на жртвите и објекти на напад (директни и индиректни жртви).
- Незаконитоста на терористичкиот акт.
- Осуда на тероризам (јавна).

2. Тековни карактеристики на тероризмот:

- Супстанцијална и симболична штета.
- Геноцидни намери.
- Визионерски цели.
- Безусловна мотивација.
- Порака која одекнува.
- Безбедносна криза.
- Спектакуларност.
- Глобалната природа на терористичките закани.

3. Можни карактеристики на тероризмот:

- Тајност на нуклеарниот, хемискиот и биолошкиот тероризам.
- Сеопфатност на нуклеарни, хемиски и биолошки тероризам.
- Разновидноста на средствата за извршување.
- Масовност на жртвите.
- Неселективност и случајност.
- Долготрајност на последиците.

Секако, ова не е конечна листа на карактеристиките на тероризмот, посебно не на актуелните и можните, туку напротив, секој нов терористички акт се карактеризира со нешто ново, дотогаш не видено, тоа придонесува за развој на тероризмот и појавата на нови облици, како на пример сајбер-тероризмот.

2. Терористички организации - членови, структура и идеологија

Терористичките организации вообичаено се структурираат на сличен начин, како и воените организации. Тие се различни во димензии и во дострел. Целите што ги водат варираат од специфични до премногу општи, од остварливи до виртуелно невозможни. Она што е заедничко за нив е тоа што се политички, автономни, недржавни или субнационални движења со командни и со контролни структури.¹⁴ Многу терористички организации, особено тие кои се поддржувани или раководени од странски влади или разузнавачки служби се високодисциплинирани, а задачите се организираат и извршуваат чисто, авторитетно и функционално. Водачите на терористичките групи и поголемиот број од терористите во најголема мерка се политички

мотивирани, борбено се добро обучени, често и со воена обука од сферата на тактиката и планирањето. Тие, исто така, се обучувани и на полето на разузнавачкото собирање на податоците и нивното анализирање, потоа вршат набљудување и следење, применуваат криптозаштита во меѓусебното комуницирање и располагаат со модерно оружје, опрема, возила. Покрај тоа, тие ги применуваат и сите мерки на контраразузнавање.

Сите поголеми и добро организирани терористички групи имаат хиерархиско и субординациско добро поставена мрежа, а основна единица им е ќелијата. Таа е минијатурна, многу ефикасна организациска единица. Најчесто има од 5 до 10 лица, а во зависност од акцијата може да има и повеќе. Секоја ќелија има свое конспиративно име заради препознавање и идентификација.

Врската со повисоките организациски единици најчесто се остварува преку курир или преку заштитена телефонска врска, а заради конспирација, најчесто еден од групата познава само еден од повисоката единица и ништо повеќе. Обуката на членството, посебно на оние кои непосредно учествуваат во терористичките акции, се спроведува плански и систематски. Акцент се става на техничкото и физичкото оспособување. Самото регрутирање нови кандидати го врши сектор кој го имаат скоро сите терористички организации. По правило, се бараат млади лица, цврсти во своите убедувања, спремни на саможртвување. Обуката која почнува со пишување пароли по сидовите и растурање летоци, користење на социјалните мрежи, продолжува во постојани и повремени логори за обука, каде се врши физичко - психичка подготовка и се обучуваат идните терористи да се снаоѓаат во најразлични тешки ситуации, како и да ракуваат со оружје и да поставуваат минско-експлозивни средства.

Глобализацијата и развојот на технологијата придонесоа за промени во развојот, организираноста и структурата на терористичките групи. Старите традиционални терористички групи се заменети со нови кои имаат можности да делуваат во современиот свет и демократското општество и се карактеризираат со професионалност, ефикасност и ефективност, флексибилност, користење на современата технологија и експертските познавања кои ги користат за нивните терористички цели.

На терористичките организации им се потребни пари, оружје, недвижности и, пред сè, луѓе за да можат да растат, да планираат, да тренираат и да извршуваат. Потребен им е морален легитимитет што го добиваат од лидерите во нивните заедници, а во случајот на оние што се со религиозни мотиви, од нивните религиозни институции. Последните трендови се во насока на обединување на помалите или ад хок

формираните групи во слабо поврзани мрежи под раководство на поголемите терористички организации.¹⁵

Една од поновите терористички закани претставуваат терористите поединци – „осамени волци“, феномен кој, всушност, означува поединец којшто ги спроведува терористичките цели сам, било тој да е воден од сопствени мотиви или од неговото верување дека е дел од некоја идеолошка група. Новата стратегија на дел од терористичките организации е да ги поттикне и мотивира поединците да извршат акти на насилство комплетно надвор од некаков терористички ланец на команда. Овие поединци можеби немаат вештини и обука или дејствуваат спонтано, но најважно е дека шират страв помеѓу луѓето со минимални трошоци и вложувања.

Денес се смета дека во повеќе делови од светот постојат и дејствуваат над 100 терористички организации. Иако дел од нив дејствуваат на пропаганден план, најголемиот број се мошне активни и постојано се обидуваат да го привлечат медиумското внимание. Резултат на тоа е зголемениот број терористички акти, но и сè позастрашувачките ефекти од тие акти.

3. Цел на терористичките напади

Терористите, првенствено, не целат кон остварување на физичките, туку на психолошките ефекти од нивните напади. Тие се користат со една стратегија која примарно се потпира на симболичката сила на дејствувањето, па оттука нападите се вршат со цел да се пратат пораките до таргетираниот аудиториум и да се искористи како преносител и канал за комуникација за остварување на влијанието врз претставниците на политичката власт и носителите на одлуки.

Целите на тероризмот се најчесто поврзани со крајниот ефект кој треба да се постигне со дејството, односно она што претходно било планирано и прогнозирано од страна на извршителите на актот. Како најчести цели можат да се набројат следниве:

- добивање целосна светска, регионална и национална поддршка на целта на извршителите на терористичкиот акт,
- провокација на власта и нејзините органи и предизвикување ситуација каде е неизбежна потребата од брза, одлучна и строга акција на безбедносните органи, а потоа создавање атмосфера на наклонетост кон терористите,
- преку директен напад со директни вооружени дејства да се постигне слабеење на безбедносните сили и ефект на недоверба кај населението во сопствените безбедносни органи,

- уништување стратегиски и тактички цели и инфраструктура потребна за непречено егзистирање,
- одвраќање странски инвестиции и национални планови за развој,
- остварување влијание врз решенијата на владата, законодавството, независните државни институции и наметнување насилни решенија во текот на изборни кампањи или тековни национални избори и други демократски процеси,
- одмазда и репресии,
- промена на исходот или поддршка на веќе започнати герилски, диверзантски или бунтовнички дејства на некоја држава,
- подготовка на теренот за идни поконкретни и поизразени дејства и
- поддршка и одбрана на разни криминогени операции и фактори.

Тероризмот мошне брзо го менува својот карактер, но и своите цели кои се многу поамбициозни, подраматични и веќе добиваат глобални димензии. Тој е „флуиден непријател“, но со јасно поставени цели кои секојдневно предизвикуваат шок, ужас, бес, страв, желба за одмазда и крв и нов психолошки и безбедносен амбиент во кој луѓето во светот почнуваат да се чувствуваат како да се во војна. Една од главните причини за брзо проширување на овој современ феномен како смртоносен вирус насекаде во светот е фактот дека тероризмот се покажа како евтин, нискоризичен метод кој мошне брзо носи корисни резултати во борбата на разните групи и режими.

4. Заканите од терористички напади по критичната инфраструктура

Критичната инфраструктура¹⁶ е изложена на повеќе видови опасности, како природни катастрофи, човечки грешки, технички проблеми и кривични дела, од кои последиците може да бидат огромни. Затоа е потребна нејзина посебна заштита.

Критичната инфраструктура може да се дефинира, меѓу другото, земајќи ја предвид улогата што ја има во унапредувањето и заштитата на човековите права (на пример, инфраструктура која е од витално значење за функционирање на системите за здравствена заштита, за итни услуги, за вода и отпадни води и др.), како и влијанието врз човековите права што ќе го направи штетата, нарушувањето или уништувањето на инфраструктурата (на пример, неможност за испорака на соодветни здравствени услуги, оштетување на животната средина што може да резултира со човечки загуби, присилно раселување со негативно влијание врз правото на здравје, итн.). На пример, ЕУ¹⁷ ја

дефинира „критичната инфраструктура“ како систем или негов дел што е неопходен за одржување на виталните општествени функции (здравје, безбедност, сигурност, економска или социјална благосостојба на луѓето) и чие нарушување или уништување би имало значително влијание како резултат на неисполнување на тие функции.

Хетерогената природа на критичната инфраструктура, заедно со различниот географски и институционален контекст во кој се наоѓа и функционира, ја отежнува потрагата по општи заклучоци за мотивацијата на терористите да вршат напади врз критични, наспроти некритични цели.

Објектите на критичната инфраструктура се привлечни од најразлични причини¹⁸. Прво, тие можат да бидат привлечна цел заради нивната стратегиска вредност за општествата, особено во високо индустриските земји од западната хемисфера. Мешањето во функционирањето на критичната инфраструктура, идеално со можност за генерирање каскадни ефекти, им овозможува на терористите да ја зголемат штетата само со еден истрел и да всадат страв до нивоа што не би биле остварливи толку лесно со напаѓање на „обични“ цели. Други напади врз објектите на критичната инфраструктура може да бидат насочени за да ја покажат немоќта на државните институции. На пример, терористичките организации можат да одлучат да нападнат објекти за производство на електрична енергија, гасоводи, нафтоводи, водни системи итн., со цел да го прекинат снабдувањето со основни ресурси и да се открие ранливоста на јавните институции. Трета можна мотивација, поврзана со двете претходни, би била желбата да се добие повисок степен на публицитет отколку што би било можно со фокусирање цели од „низок профил“.

Во споредба со проценките на закана од други опасности, идентификувањето и проценката на терористичките закани за критичната инфраструктура предизвикува низа специфични проблеми. Како што е забележано, основен проблем во овој контекст е тоа што терористите го прилагодуваат своето однесување. Од оваа перспектива, терористичката закана треба да се смета за динамична прилагодувајќи се кон промените во ресурсите што им се достапни на терористичките групи и на промените во безбедносните карактеристики на потенцијалната цел.

Во однос на изворите од кои треба да се извлечат елементи за проценка на заканата поврзана со тероризмот, стратегиите за критичната инфраструктура треба да ја препознаат главната улога на разузнавачката заедница. Разузнавачките служби се надлежни за заштита на националната безбедност. При извршувањето на нивните мисии, тие честопати управуваат со доверливи информации како

средства за заштита на критичната инфраструктура. Како резултат на тоа, стратегиите за критичната инфраструктура треба да воспостават механизми за справување со информации чиј опсег е ограничен. Голем предизвик е да се обезбеди споделување што повеќе информации меѓу сите засегнати страни, додека се заштитува нивната доверлива природа, од друга страна. Овие можат да бидат и чувствителни деловни информации што ги поседуваат компаниите или класифицирани информации што ги поседуваат државните служби.

Заканите поврзани со тероризмот против критичната инфраструктура имаат повеќе димензии во зависност од нивната природа (физички наспроти сајбер-напади), нивното потекло (внатрешни наспроти надворешни напади) и контекстот во кој тие се случуваат (изолирани или со повеќе цели).

Физичките закани кои се насочени кон критичната инфраструктура може да имаат различни форми. Нивната заедничка карактеристика е што тие имаат за цел да уништат инфраструктура, да ја ослабнат или да ја направат неоперативна во целост или делумно со интервенирање врз нејзината физичка структура, механички компоненти, итн. Најчестите физички закани за критичната инфраструктура вклучуваат употреба на експлозивни или запалувачки уреди, транспортни средства, ракети, гранати, па дури и едноставни алатки (на пр. прекинувачи на електрична енергија или запалки за да поттикнат подметнување пожари), итн. за да се постигне тотален или делумен колапс или уништување на инфраструктурата. Нападите може да вклучуваат и намерна модификација или манипулација со системите и процесите (на пр. вклучување и исклучување на машините во објектите, отворање и затворање на цевководните системи, потиснување на сигналите од процесите, сигнали за дефект или аларми). Распоредувањето хемиско, биолошко, радиолошко или нуклеарно оружје или супстанции претставува друг карактеристичен вид на закана за критичната инфраструктура. Ова може да се движи од ширење заразни патогени во ланци за снабдување со храна, водоводни цевки, итн., до употреба на отровен гас на клучните сообраќајни крстосници и патишта. Исто така, релевантно е да се напомене дека нападот на критичен објект кој содржи хемиски, биолошки, радиолошки или нуклеарни материјали, исто така, може да резултира во ослободување на вакви материјали.

Иако сајбер-заканите се разликуваат од физичките по природата, крајниот резултат може да биде ист. Сајбер-заканите се разликуваат, но може да вклучуваат, на пример, напади преку:

- манипулирање со системите или податоците, како што е малициозен софтвер што ги експлоатира ранливостите во

компјутерскиот софтвер и хардверските компоненти неопходни за работа на критичната инфраструктура,

- затворање клучни системи, како што се нападите на оперативните системи,
- ограничување на пристапот до клучните системи или информации, преку извршување напади со изнуда или уцена, за барање откуп и сл.

Додека заштитата на критичната инфраструктура од надворешни напади се спроведува според упатства на многу национални и меѓународни регулаторни служби, заканите од внатрешни напади, досега, биле предмет на релативно помало внимание. Во споредба со надворешните субјекти кои можат да добијат пристап до критичната инфраструктура преку насилни дејствија, извршителите на внатрешни напади (инсајдери) имаат неспорно многу повеќе предности. Инсајдерите често се вработени во компанијата или се добавувачи. Тие можат да бидат главни заговорници или да дејствуваат како соучесници (на пр. информатори) на надворешните извршители. Тие честопати се во состојба да ги набљудуваат процесите што не се нарушени во текот на еден временски период. Нивното знаење (или леснотијата со кое тие можат да се здобијат со знаење) за соодветниот објект може лесно да се искористи за криминални цели. Во оваа област, клучна превентивна улога има спроведувањето ефективни процедури за селекција на персоналот и нивна проверка.

Заканите против критичната инфраструктура може да бидат или изолирани и спорадични акти или дел од поширок план за напад на инфраструктура во истиот сектор кои припаѓаат на идентичен сопственик/оператор или се наоѓаат во истата географска област. Тука влегуваат дејствија мотивирани од терористи, насочени кон критичната инфраструктура, на ист начин, како и индустриската шпионажа, каде сајбер-нападите честопати се лансираат „кампањски“ или како сериски напади.

Идентификацијата на обрасците во слични сценарија честопати бара силни аналитички алатки и обработка на информации од огромни и хетерогени извори. Во енергетскиот сектор, на пример, повеќето сајбер-напади не се објавуваат, бидејќи операторите не сакаат да ги споделат со јавноста овие инциденти. Сепак, можноста да се препознаат основната динамика и методите што е можно порано е клучна за да им се овозможи на властите да имаат релевантни информации и да преземат соодветни активности. Ова го зголемува капацитетот за поефективно реагирање на тековните напади и претскажување непосредни напади против потенцијалните жртви.¹⁹

Во некои случаи, она што се чини како изолиран напад насочен кон релативно „неважни“ цели, во реалноста може да биде дел од поамбициозни и поединечни криминални стратегии.²⁰

Спречувањето терористички напади врз критичната инфраструктура е активност на субјектите кои се задолжени за чување на националната безбедност. Со оглед на тоа што објектите на критичната инфраструктура се обезбедуваат, чуваат и заштитуваат од страна на компаниите за приватна безбедност значи дека и работниците за приватна безбедност се директно одговорни и за заштитата на националната безбедност. Врз основа на тоа, нивната задача е да следат, проценуваат, откриваат и спречуваат планови, заговори и други подготовки за извршување терористички акти во целина. Нивните проактивни заложби за претходно преземање заштитни мерки, како и соработување со државните безбедносни служби (за разлика од едноставно реагирање по извршен терористички акт) имаат фундаментална улога во превентивните напори за спречување терористички напади врз критичната инфраструктура. Мерките кои се директно релевантни за засилување на превенцијата на терористички напади кои специфично се насочени кон критичната инфраструктура се:

- Идентификување на главните улоги и одговорности во областа на превенцијата, вклучително и на ниво на операторите со критичната инфраструктура (т.е. целокупната улога на раководителите на највисоко ниво, на безбедносните службеници и, генерално, утврдување на концептот дека спроведувањето на превентивните мерки е задача за целата компанија и бара поддршка од сите нивоа);
- Развивање работна средина и методологии за создавање прирачници, практични упатства и стандардни оперативни процедури за употреба од страна на операторите со критичната инфраструктура во областа на превенцијата;
- Методи за директно идентификување што треба да бидат широко применети или разгледани од засегнатите страни. На пример, „безбедност по мерка“ како алатка за постигнување превентивни цели или одржување ефективни безбедносни аранжмани преку извидување на областа заради зголемување на веројатноста брзо да се идентификуваат подготвителните активности за тероризам; и
- Усвојување специфични групи на превентивни мерки (меѓусекторски или во специфични сектори) од страна на операторите на критичната инфраструктура.

5. Фази на подготовка на терористички напади

Планирањето²¹ на акциите на попознатите терористички организации се врши грижливо и во детали, како кај исклучително сложени воени операции. Користејќи го максимално факторот изненадување и иницијативата која е објективно на нивна страна, особено внимание се посветува на односот на крајната цел и непосредниот објект на напад на терористичката акција. Метата (целта) секогаш се избира поединечно и мора да биде во согласност со главните цели на организацијата. Во одредување на начинот на извршување на терористичката акција, стратезите се раководат од начелото на ефикасност и едноставност кое се заснова на претходно темелно разработени разузнавачки податоци и приспособена документација за метата на нападот. Се прибираат сите важни информации за жртвата на нападот, како што се навиките, движењето итн.

Изведувањето на терористичките акции се одвива по претходно подготвен план, со употреба на оптимални оружја, средства и учесници, потребни за реализирање на целта. Со оглед дека се исполнети сите претходни фази за одредување на членовите, обуката и добро завршените подготовки за конкретната акција, секој мора да постапува согласно со предвидениот план и на предвидениот начин, без исклучоци и по цена на жртви.²²

Прва фаза во изведувањето на терористичкиот акт е фазата на дефинирање на целта на нападот. Таа задолжително настапува по одредени промени во една држава во смисла на промена на политичкиот, односно економскиот курс или позначајни промени во односите меѓу внатрешните политички субјекти. Оваа фаза е и фаза на проценки и одлука за извршување. Многу важно прашање е што се проценува кој проценува и кој одлучува за преземање на активностите. Ако се има предвид дека терористичката организација, група, функционира на принципот на субординација, почитување на непосредно претпоставените, без да се приговара и нуди спротивно мислење и решение, тогаш иницијатива за градење проценки и одлуки, носи врхушката на организацијата. Во овој дел ќе ја согледаме поставеноста на одредени терористички групи и организации.

Организациската структура на илегалните терористички организации, според расположливите сознанија, секогаш е во функција на целите на организацијата, односно го претставува најцелисходниот, едноставен за ракување, механизам кој во зависност од целите, се служи со селективен и неселективен напад. Активноста на организациите се одвива по програмски документи во кои идеологот, создавачот и

организаторот на терористичките акции, посочува цели кои треба да се постигнат со нивната активност.

Воено-политичката команда²³ е етаблирана во поедини поголеми градови кои претставуваат ограноци и независни воено-политички организациски единици. Сите поголеми и добро организирани организации имаат хиерархиско и субординациско добро поставена мрежа, а основна единица им е ќелијата. Таа е минијатурна, многу ефикасна организациска единица. Најчесто има од 3 до 10 луѓе, а во зависност од акцијата може да има и повеќе. Секоја ќелија има свое конспиративно име заради препознавање и идентификација. На располагање имаат повеќе станovi и автомобили.

Врската со повисоките организациски единици ја остварува најчесто курир или преку телеграфска врска, а заради конспирација најчесто еден од групата познава еден од повисоката единица и ништо повеќе. Овие организации го набавуваат оружјето на најразлични начини: од пријателски држави и организации (преку нивните разузнавачки служби); преку напади во складиштата на војската и полицијата вклучувајќи ги тука и единиците на НАТО; преку купување на илегалниот пазар; некои изработуваат одредени типови за сопствена употреба и сл.

И во степенот на вооруженоста²⁴ постојат разлики меѓу терористичките организации: додека едни го немаат во доволна мерка или, воопшто, го немаат, други го имаат и повеќе од потребите. Сето тоа зависи од можностите за набавка (финансиите), поврзаноста со странска разузнавачка служба и поддршка од други странски терористички организации²⁵.

Кога постои ваков систем на функционална поставеност, тогаш секоја одлука се донесува од највисоките структури. Тие ценат кави се состојбите, можностите и потребите за акција и согласно со тоа даваат налог за почеток на подготовките на акција, се дефинираат целите и се започнува широка акција.

Втората фаза започнува кога целите се целосно дефинирани, а иницијаторите, инспираторите, се определени за извршување на терористичкиот акт. Прв чекор е определување и ангажирање на главниот организатор на акцијата – лицето кое ќе раководи со подготовките и завршната операција. Изборот на лицето го прават лица од највисокото раководство, а најчесто тоа лице е оној кој има авторитет, храброст, одлучност и докажаност. Таквото лице ќе може дополнително да ги мотивира лицата непосредни извршители, оние со кои ќе се одлучи да има непосредна комуникација, но и со ширење на информацијата кај припадниците на ќелиите, кој раководи, препознатлив преку звучниот псевдоним. Од моментот на назначување

за главен организатор тој ги презема севкупните ингеренции. Терористичката организација ќе најде некој да ја организира и да раководи со операцијата. Тоа мора да е некој целосно лојален, посветен, од доверба и подготвен да умре. Келиите и членовите се избираат, распоредуваат и им се доделуваат задачи, иако можеби веднаш не им се кажува за мисијата. Последната голема одлука е да се организира канал за пари за мисијата.

Ова второ ниво се вика и прединцидентна фаза која трае извесен период, а можеме да ја поделиме на неколку етапи.

Прва етапа во втората фаза е проучување на објектот на нападот (институција, личност, дипломатско-конзуларно претставништво и др.), преку континуиран систем на примена на методи и средства за стационарно и динамично следење, набљудување и документирање на режимот на работа, влезот-излезот, фреквентноста, патиштата кои водат до и од, обезбедувањето, сили, комуникација, контакти со други лица, протокол и др.²⁶ Во ваквите акции се применуваат сите принципи на реализација на тајната опсервација. Се ангажираат искусни припадници на терористичката организација кои за овие потреби закупуваат станбен или деловен простор, се претставуваат како деловни граѓани, обезбедуваат соодветно алиби за престојот во близина. Во оваа смисла присутни се активности за врбување луѓе вработени во институциите кои се цел на набљудувањето, воспоставување блиска комуникација со лица кои имаат директна или индиректна комуникација со нивната одредена цел и сл. Преку овие мерки и активности се дознаваат и најситните детали за целта, се проучуваат протоколарните принципи и начините на примена на принципите на обезбедување на објектот, доколку има постојано или повремено обезбедување. Од посебен интерес е дефинирањето и циклусот на промена на рутите, превозните средства, делниците на движење, брзината на движење, застанувањата, задржувањата и сл. Доколку се работи за личност која живее со фамилија се следат и проучуваат домашните лица, посетителите, периодите кога нема дома никој, динамиката и фреквенцијата на посетеност, кои се посетители, зошто, зачестеност, време на задржување и заштита на објектите (физичка или техничка). Особено се проучува личноста на лицето цел во смисла на карактерни особини, начин на комуникација со другите, вредности, морал, цели во животот, круг на пријатели, економска состојба. Сите овие и многу други податоци се основа за подготовка на детален план за изведување на една акција.

Втора етапа – планирање. За процесот на планирање може да се потребни од неколку недели до неколку месеци или дури и години. Организацијата ги бара ранливостите на целта и можното влијание од успешен напад. Потоа, таа анализира кој метод на напад би постигнал

најдобар успех за најкратко време. Дали е поефикасно експлозивната направа да се постави рачно, да ја испорача и детонира човек, возило, камион, чамец, јавен превоз, велосипед или дури и животно? Значи, планирањето претставува изградба на стратегијата врз база на добиените податоци. Сите претходно добиени податоци, анализирани, дополнети и целесообразни со потребите се основа за детално развивање на планот на акција. Планот треба да ги утврди: учесниците во акцијата (извршители), начинот за напад, средствата за извршување, местото и времето, начинот на повлекување и обезбедување на учесниците. Планот е дециден, добро разработен, со точно одредување на секој поединечен детал, време кое може да биде одредено до секунда и со напомена дека кога се реализира задачата отстапки и каење нема. Планот го разработува организаторот со најблиските соработници, докажани низ практиката која ја имале. Свкупниот план не се презентира предвреме пред другите. Тој се соопштува непосредно пред акцијата на секој кој е вклучен во акцијата, а претходно без да знае детали, секој учесник согласно со неговата улога во акцијата, активно се подготвува. Таа подготовка не се базира само на физичката подготвеност, туку и на психичката и стручната. Системот за индоктринација, подигнување на моралот и одлучноста да се делува преку примена на тероризам се стимулира кај секој учесник во акцијата од својот надреден или задолжен во групата за таквата активност. Обуката на членството, посебно на оние кои непосредно учествуваат во терористичките акции, се спроведува плански и систематски (од општо кон посебно). Акцент се става на техничкото и физичкото оспособување. Самото регрутирање нови кандидати го врши сектор кој го имаат скоро сите терористички организации. По правило се бараат млади лица, цврсти во своите убедувања, спремни на саможртвување. Обуката која почнува со пишување пароли по ѕидовите и растурање летоци, продолжува во постојани и повремени логори за обука. Во тие логори се врши физичко-психичка подготовка и се обучуваат идните терористи да се снаоѓаат во најразлични тешки ситуации, како и до ракување со оружје и поставување минско-експлозивни средства. За оваа цел, најчесто терористичките организации во своите редови имаат специјалисти, посебно за оружје и експлозиви кои најчесто експлозивите сами ги изработуваат.²⁷

Безбедносните мерки – мерките на претпазливост што ги преземаат терористичките организации фактички претставуваат правила на однесување според кои треба да се однесува секој поединец, бидејќи доколку не е доследен за брзо време ќе биде надвор од организацијата или казнет.

Во овој дел, најголем успех се постигнува преку употребата на религиските верувања и догми²⁸. Стручната подготовка се реализира со средства и методи со кои треба да биде извршена и акцијата. Така, доколку акцијата треба да се изврши со употреба на минско експлозивни средства, учесниците, колку и да се обучени, сепак, повторно работат на увежбување на припремата, поставувањето и активирањето на направата. Преку тоа се стекнува рутина, брзина и самоверба.

Планот не е флексибилен и не остава можности за корекции или одлагање на акцијата. Тој е даден круто и се очекува по започнување на акцијата во целост да се реализира и по цена на жртви од страна на терористичката организација. Ваквиот начин на практикување на акциите е во функција да се избегне каење кај извршителите, неможност да се коригира дел од акцијата, да се создава тензичност во групата изведувачи, недоверба во водачите и конфузија во делувањето. Секој учесник треба максимално достоинствено да ја заврши својата доверена задача или улога, по цена на својот живот, да се исполнат зададените задолженија до најситен детал, временски да се обезбеди точност, планот целосно да се заврши и да се поттикне потврдување на самовербата кај интергрупата и надвор кон граѓанството со ширење страв, немир и застрашеност од терористите.

Трета етапа – логистика е период на материјално обезбедување на групата која треба да ја изведе акцијата со потребна опрема и средства за реализација на нападот. Во оваа етапа се набавува сè она што е предвидено во планот. Не постои нема, не постои не можам да најдам, да донесам, да употребам. Планираното мора да се реализира и тоа максимално почитувајќи ги планските одредби. Во оваа етапа доаѓа во прашање финансирањето на терористичката организација. Финансирањето на терористичките организации за своите најосновни потреби се сведува на т.н. „самофинансирање“. Тоа значи дека се применуваат одредени методи кои се најефикасни за да се обезбедат материјални средства. Имено, одредени терористички организации се занимаваат со кражби на автомобили, фалсификување документи, опремување работилници за изработка на експлозиви и други направи и нивно продавање, набавка и трговија со оружје, провали во банки, киднапирање богати граѓани или нивни семејства, па сè до одредување задолжителни давачки за припадници на својот етнос (ако се работи за еднонационални или на верска основа поврзани организации) од дијаспората и од земјата.

Тука, пред сè, спаѓаат набавката на средствата за извршување (оружје, муницијата, експлозивот), потоа обезбедувањето на средствата за комуникација²⁹, возилата, мапите, средствата за камуфлирање на

извршителите. Транспортот и сместувањето на потребните материјали на местото на извршување, за организаторот претставува клучен проблем.

Четврта етапа е обезбедување скривалиште, отстапница за извршителите што за организаторот е, исто така, битен проблем кој мора да го испланира и реши. Реализацијата на оваа фаза започнува по извршениот терористички акт. Грижата за своето членство, посебно за оние кои се на линијата на „огнот“, е карактеристика на сите терористички организации. Ниту една организација не ги остава своите членови незащитени и без поддршка. Така што, грижата за нив, солидарното и другарското однесување, поврзување на припадниците на малите организациски единици претставува најценет дел, а, исто така, да не се изневери никој од страна на организаторите на акциите, во и пост акцијата, се вредности кои се негуваат. Дури и во моменти, кога некој член ќе заврши во затвор или ќе го загуби животот, организацијата се грижи за него или за неговото семејство. Ваквите вредности придонесуваат членовите да веруваат во организацијата, да се сигурни во делувањето и да не се плашат од репресиите кон нив или нивните блиски, затоа што секогаш постои некој кој се грижи за нив, а тоа е организацијата. Единствен случај, каде што не се размислува за скривалишта и конспиративни престојувалишта *post festum* е во случаите, кога се подготвува самоубиствен терористички напад.

Трета фаза претставува реализацијата на терористичкиот акт, фазата за напад или инцидентна фаза. На нападот најчесто му претходат две дејствија кои се изведуваат на критичниот ден или малку порано: транспорт и поставување на силите и средствата за извршување на актот и добивање почетен сигнал од организаторот дека сè се одвива по планот, па акцијата може да биде изведена.

Четврта фаза ја прават ефектите и последиците во посттерористичкиот акт.³⁰

6. Извршување терористички напади

Ако ги разгледуваме и ги анализираме тактиките на терористите, ќе заклучиме дека терористите ги напаѓаат своите цели на многу различни начини. Терористичките организации применуваат разни форми на насилство со цел да постигнат публицитет и да ги доведат до застрашување оние кон кои ги имаат насочено своите активности за да ги остварат нивните политички цели. Тековните активности вклучуваат подметнување бомби, самоубиствени напади, бомбардирање работни објекти или резиденции, вршење саботажи, сајбер-тероризам, користење оружје за масовно уништување (хемиско, биолошко,

радиолошко и нуклеарно) и сл. Исто така, терористите применуваат и други методи, како што се: атентати, убиства, киднапирања и сл. Со анализа на тековните трендови се гледа дека терористите се многу повеќе подготвени да изведуваат масовни напади на цивилни цели. Овие „меки цели“ се многу поинакви од заштитените воени или цивилни објекти. Станбени објекти, транспортни центри, киноцентри, деловни центри, хотели, банки, места за рекреација, па дури и места за верски обреди (цркви, синагоги или џамии) коишто биле цел на терористите, се места што гарантираат голем број жртви и голема симболична вредност. Тероризмот кој како поим означува владеење со застрашување, односно со насилство, претставува една од најлошите форми на криминалот. Со примената на средства за закана или за застрашување на поединци или на групи, терористите настојуваат да остварат некаква материјална корист или да постигнат одредена политичка цел. Можеби ова е една од причините поради која терористичките организации се обидуваат да ги усовршат своите оружја за напад. Неспособни да добијат, да изградат и да испорачаат модерно вооружување за борба, терористите постојано разработуваат софистицирани техники со кои широкодостапните материјали би ги претвориле во неконвенционално оружје. Трендот во насока на разработување на сè поиновативни форми на водење војна продолжува непречено со години.

Планирањето и организирањето на нападот се одвива темелно и внимателно, се анализираат ранливите места, како и оние места на кои има најголеми шанси нападот да биде успешен и да се постигне најголем успех, односно да се нанесе најголема штета. Дури откако ќе бидат организирани и добро разработени сите детали се изведува нападот.

Изведувањето на терористичкиот акт има примарно и секундарно дејство³¹. Примарно дејство е да се изврши атак на одреден објект, лице или институција и, според нивните планови, најчесто сето тоа се одвива со минимални случајни жртви. Секундарно дејство по правило е она кое според важноста за секоја терористичка организација го надминува примарното за повеќе пати, а тоа секундарно дејство е јавноста. За тој ефект, најчесто се избираат атрактивни цели, без големи последици по невини жртви. Со соопштувањето на веста во јавноста или доставување комунике или преземање на одговорност за настанот се постигнува главниот ефект и се добива публицитет, додека кај народот се јавува ефектот на страв, несигурност и недоверба во органите на власта и сл., со што се постигнува основниот елемент на тероризмот.

Откако ќе дојде до напад и инцидентот ќе се реализира, персоналот за поддршка вклучен во инцидентот ќе дојде до безбедна

зона и ќе се регрупира. Водството, командата и персоналот за акција ќе извршат анализа на целата операција забележувајќи ги грешките и извлекувајќи поуки. Овие поуки ќе се употребат во идните напади. Терористите напаѓаат со проучување и учење од претходните терористички кампањи.³²

ДЕЛ II

ЗАШТИТА ОД ТЕРОРИСТИЧКИ НАПАДИ

1. Безбедносен оперативен план

Во рамките на системот на мерки и активности за безбедносна заштита од терористички напади, се подготвуваат безбедносни планови или планови за обезбедување³³. Секој вид обезбедување има свои особености на кои треба да се посвети посебно внимание, покрај заедничките карактеристики во примената на соодветните мерки дефинирани со безбедносниот оперативен план³⁴. Тој е клучен документ во процесот на подготвување и спроведување на сите активности поврзани со обезбедувањето. Ваков документ се составува за сите места кои редовно се користат и континуирано се анализираат и дополнуваат. Сите договорени мерки утврдени со планот се спроведуваат совесно, одговорно и дисциплинирано, без разлика дали станува збор за индивидуални или заеднички активности (кои вклучуваат одредена координација и синхронизација).

Под план за обезбедување се подразбира проценка на безбедносната ситуација за загрозеноста на обезбедуваниот објект, односно личноста и мерките на обезбедување кои се подготвуваат и се преземаат.³⁵

Пред да се започне со процесот на обезбедување на лицето и објектот, мора да се направи реална проценка на податоците за појави и настани поврзани со нивната безбедност. Преку следењето на носителите на загрозувања, нивното влијание, сила и средства кои ги употребуваат, треба да се креираат и да се преземаат мерки за да се елиминираат или да се отстранат околностите во кои се создадени.

Врз основа на набљудувањето и сознанијата од безбедносната претходница, најпрво, се утврдуваат веќе постоечките носители на загрозување на животот, здравјето и делувањето на лицата, а потоа во зависност од работата со која се занимава, политичките ставови и другите карактеристични податоци, се проценува кои форми на загрозувања на безбедноста и нивните носачи би можеле да се појават во иднина.

Во рамките на превентивната дејност влегува и безбедносната проценка на степенот на ранливост на заштитеното лице и објектот и, врз основа на таа проценка и нивото на ранливост, доаѓа до изработка или модификација на постоечкиот безбедносен план.

Безбедносната проценка се определува во форма на пишан документ и е составен дел на планот за обезбедување и ја покажува моменталната безбедносна состојба, предвидување за идните настани и

ги прецизира задачите со кои треба да се елиминираат причините, методите на спротивставување, односно превенција со цел да не дојде до загрозување на безбедноста на лицето и објектот.

Безбедносниот план за заштита е сеопфатен и концизен документ кој овозможува и поддржува дистрибуција на информации до сите ангажирани работници за приватно обезбедување.

Информациите содржани во безбедносниот план за заштита се основа за оперативниот план со кој треба да се намали или да се елиминира опасноста или да се спротивстави на предвидените ризици и да обезбеди упатства за работниците за приватно обезбедување во случај на инцидент.

Видови планови:

- Постојан план;
- Привремен план.

Секој план е различен врз основа на специфичните барања на одредено место. Поради таа причина, планот треба да биде и да остане флексибилен, бидејќи, речиси, во сите случаи може да се случи нешто дополнително и во тој случај одредени мерки и активности ќе треба да се менуваат. Целите на стратешкото планирање се однесуваат на зачувување на безбедноста на заштитеното лице и објектот, а заради подобра превенција се прават планови кои се конкретни.

При изработката на планот за обезбедување секогаш мора да се води сметка дека постојат главни и резервни планови. Планот, секогаш треба да е максималистички, односно обезбедувањето да се планира со, колку што е можно, посилни мерки. Во суштина, се тргнува од планот за максимална безбедност, па потоа се коригира во зависност од: материјалните можности, постоечките потреби, слободата на приватниот живот на клиентот, одвивањето на неговите редовни активности, но никогаш не се прилагодува до степен до кој тоа драстично би ја загрозила безбедноста на лицето и објектот.

Планот мора да биде реално остварлив и по можност да е што поедноставен.

Безбедносниот план треба да биде информативен, интегриран и повеќеслоен.³⁶

Бизнис-компаниите не можат да ги отстранат сите закани со кои можат да се соочат, па затоа треба да имаат план за да ги заштитат своите најценети средства и предвреме да го планираат и да го имаат подготвено нивниот одговор на поголеми инциденти и нарушувања на нивната безбедност и сигурно функционирање.

Безбедносното планирање не смее да се развива на произволен или ад хок начин, ниту да се развива единствено од претходните грешки и пропусти. За да биде ефективен, безбедносниот план мора да биде

изграден врз основа на информации за скоро секој аспект од работното делување во сегашноста, но и во иднината. Мора да биде целосно интегриран со секојдневните операции, синџирите на снабдување и рутините. Тој треба да биде „повеќеслоен“ - каде секоја мерка е засилена од следната.

Структурата и концептот на планот се разликуваат од една до друга организација, но секој план треба, генерално, да се состои од следниве компоненти:

- Информации: проценка на деловната активност и околината во која се работи - законите, ризиците, опасностите, ранливостите, најценетите и најкритичните средства.
- Заштитна безбедност: мерки што штитат од идентификувани закани и ранливости.
- Планирање одговор: начинот на кој организацијата ќе реагира во случај на нарушување.
- Безбедносна култура: градење безбедносна свест низ целата организација.



Слика бр. 1. Структура на планот

Големите, мултисекторски организации може да креираат одделни планови за секоја локација за да ги рефлектираат локалните структури и активности, покрај сеопфатниот план кој предвидува вообичаени активности и меѓузависности.

Безбедносниот план треба да биде работен документ каде секој аспект постојано се ревидира и ажурира како одговор на организациските промени. За да биде секој план во чекор со предизвиците кои произлегуваат, тој мора да биде официјално во сопственост на одреден член од персоналот кој може да ја преземе одговорноста за надзор над аранжманите и кој има овластување да координира акции.

Во поголемите организации, ваква улога може да му биде доделена на член од персоналот кој е дел од менаџментот на организацијата или кој директно е одговорен пред менаџментот со поддршка на специјализиран тим. Во помалите организации тоа треба да биде некој со сличен статус и разбирање на бизнисот.

Кој и да управува со планот, ќе треба да биде заинтересиран скоро за секој аспект на активностите (работните процеси) во организацијата.

Без разлика на големината на организацијата, клучно е планот да има целосна поддршка од високиот менаџмент и тоа да се комуницира во текот на целиот бизнис, особено кога одредени членови на персоналот носат делегирани одговорности. Во случај на инцидент, надлежноста на одговорните за координирање на одговорот мора да биде јасно разбрана од сите вработени.

Размената на совети и информации е важен дел од сите безбедносни планови. Мислењата на менаџерите и вработените во целата организација се од суштинско значење. Но, исто толку значајни се и придонесите од оние кои се надвор од бизнисот, како што се службите за итни случаи, соседните бизниси и специјалистичките експерти (структурно инженерство, информатичка технологија и сл.).

Безбедносниот план содржи некои од најчувствителните информации што се достапни за бизнисот и затоа е важно да биде јасно кој има целосен пристап и како се дистрибуира.

1.1. Идентификување закани

Некои деловни активности се „изложени на поголем ризик“³⁷ од другите заради услугите што ги пружаат, нивниот релативно висок процент или бројот на луѓе на кои им се доделени. Организациите треба да го знаат опсегот на закани со кои се соочуваат – и директните, каде што бизнисот е цел, и индиректните, од релативно слабите, до катастрофалните закани.

Организациите треба постојано да проверуваат што е поврзано со нивното работење или, пак, кои се околностите што можат да го подложат персоналот или клучните средства директно под влијание од закани. На пример:

- Каква е природата на деловното работење или услугите што ги нуди?
- Дали има нешто на самото место што може да претставува важна цел, на пр. материјали, машини, средства, податоци, планови, техничка експертиза?

- Дали бизнисот е поврзан со високопрофесионална личност или со спорна област на работа?
- Дали организацијата одржува видливо високи стандарди за безбедност?

Накратко, колку е веројатно дека организацијата/компанијата, или персоналот, би можеле да биде директна цел на претходно планиран напад?

Исто така, можеби постојат и индиректни влијанија што се резултат од напад на друго место – каде самата организација не била цел, туку се соочила со последиците.

На пример, дали деловните простории се наоѓаат во близина на некоја поважна зграда со висок ризик? Ако е така, како би влијаело врз работењето доколку не може да се пристапи до целата површина за неколку дена? Дали персоналот ќе може да патува доколку локалната транспортна мрежа е сериозно нарушена? Дали информатичко-технолошките мрежи можат да реагираат на ненадејната појава на нов вирус или ранливост? Може ли некој инцидент во друг град или друга земја да предизвика значителни проблеми за снабдувачите, клиентите или врз испораката на основните материјали?

Другите социјални фактори, исто така, можат да ги зголемат заканите по организациите. Дали загриженоста за безбедноста на работното место го зголемува ризикот вработените да крадат или продаваат/оддаваат информации?

1.2. Ранливости

Кои области на организацијата/компанијата треба да бидат приоритет за заштита?³⁸

Кога се одлучува што треба да се заштити, следниве категории мора да се имаат предвид:

- луѓе – персонал, посетители, изведувачи, клиенти,
- физички средства - згради, содржини, опрема и чувствителни материјали,
- информации – ИТ-системи, системи за онлајн трансакции, електронски и хартиени податоци,
- процеси – синџири на снабдување, критични процедури, циклус на производство.

Потоа, на организациите им е потребен јасен консензус за оние средства што тие ги сметаат за вредни и за оние што ги сметаат за суштински.

Највредни средства во организацијата се:

1. Оние средства што организацијата има обврска да ги заштити - персоналот, клиентските услуги, системите за производство и сл.

2. Средства со висока вредност за кои се потребни дополнителни или специфични безбедносни инвестиции.

3. Единствени средства кои, иако не мора да имаат висока монетарна вредност, би било тешко да се заменат.

Некои приоритети ќе бидат очигледни со веќе воспоставените планови и одредби. Но, би било погрешно да се претпоставува дека сè е идентификувано и соодветно обезбедено. Како и со заканите, вредностите можат да се променат со тоа што некои средства продолжуваат да бидат вредни за заштитата што им се дава, додека други, во смисла на безбедносни ресурси, можеби се потценети.

Највредните средства не мора да бидат најсуштински.

Најсуштински се оние средства - опрема, информациски системи, транспорт и сл., кои се од витално значење за секојдневното работење на деловните активности кои, доколку се изгубат или компромитираат, би можеле да имаат големи импликации за другите функционални делови на бизнисот.

Задачата за идентификација на средствата кои се најважни не треба да се заврши само преку дискусии меѓу раководството. Персоналот во целата организација треба да биде консултиран за тоа како привременото губење на нивниот оддел и услуги ќе влијаат на деловното функционирање. Иако целиот персонал ќе придонесе за нормално работење, не сите ќе бидат од суштинско значење за реализација на основните услуги.

Покрај заштитата на клучните средства, исто така, треба да се утврди каде треба да се подобрат постојните безбедносни мерки. Ова вклучува искрена проценка за тоа како се извршуваат тековните безбедносни мерки и дали тие остануваат соодветни или оставаат одредени деловни области на негативна изложеност. Поставените безбедносни мерки сè уште може да им одговараат на нивните спецификации, но едноставно да се надминати од организацијата.

Некои од прашањата кои се значајни и кои треба да ги постават организациите се:

- Дали постојат нови методи или технологии кои ќе ја подобрат постојната безбедност?
- Дали постојната безбедност е соодветна за каква било планирана деловна експанзија?
- Дали вработените одговорно ги користат мобилните уреди?
- Дали во сите области на организацијата се преземаат целосни проверки пред вработување?

- Дали има зголемена стапка на обрт на персоналот - се очекува ли да се зголеми?
- Дали персоналот би можел да преземе вредни податоци надвор од организацијата, без одобрение?

Планирањето на безбедноста зависи од чесните проценки. Минатите неуспеси не треба да се тргаат настрана. Треба да се знае дали постоеле претходни нарушувања на безбедноста или евентуални „промашени“ нарушувања? Дали ова открива потенцијални прилики кога безбедносните и деловните процедури не функционирале, но притоа ништо не било направено за тоа?

Може да има и други причини зошто организацијата или дел од неа е ранлива, па групите или поединците би можеле да ги искористат. На пример:

- Дали интернет-страницата на организацијата дава премногу детали за функционирањето и работењето?
- Дали постои нешто кое ги открива инсталациите или услугите кои се витални за континуирано работење?
- Дали постои соодветно раздвојување на јавните површини и оперативните области?
- Дали услугите од надвор се во безбедни раце - кои се нивните безбедносни стандарди?
- Дали областите за испорака на стоки се изложени на одредени опасности?
- Дали постои соодветна контрола на тоа кој влегува?
- Дали безбедносните процедури за влез бараат да се вратат картичките за пристап и да се затворат корисничките сметки кога ќе заминат вработените?
- Дали некои надворешни субјекти уживаат привилегиран пристап до имотот или информациите во организацијата?

1.3. Безбедносна проценка на ризик

Одлуките за безбедноста треба да ги земат предвид заканите, ранливостите и потенцијалните влијанија. Не е практично да се посвети многу внимание за целосно да се заштити секој аспект од организацијата и тоа цело време. Наместо тоа, важни одлуки за заштитните мерки или измени во постапката треба да се донесат само по целосна проценка на ризикот. Ова вклучува стратешка анализа на заканите, ранливостите и потенцијалните последици³⁹ врз организацијата со цел да се идентификуваат најважните ризици на кои треба да се фокусираат ресурсите.

Проценката на заканата не треба да се ограничува само на информациите добиени исклучиво од внатрешните ресурси. Исто така, подеднакво треба да се искористат надворешните извори на информации.

Потребно е да се направат консултации со соседните деловни субјекти и трговските здруженија за да се одредат најголемите ризици за локалната економија. Треба да се побараат детали за безбедносните стандарди што ги применуваат клучните добавувачи на организацијата. Потребно е да се оствари и контакт со локалната власт за какви било планови за вонредни состојби и други релевантни информации за деловните активности од областа.

Процесот на проценка на ризикот вклучува логички претпоставки за веројатноста од постоење закана и нејзиното потенцијално влијание доколку актуелните безбедносни мерки не успеат да ја заштитат.

Иако не е возможно да се предвидат сите можни закани по бизнисот, преку работење со низа потенцијални сценарија и последици, станува возможно да се донесат релевантни ставови за приоритетите на организацијата.

Областите во ризик можат да бидат утврдени по неколку критериуми: население, пристапност, критичност (кон секојдневниот живот), економско влијание и симболична вредност. Идентификацијата на таквите ранливи области треба да биде координирана со државните безбедносни служби.

Постојат различни начини за да се спроведе проценка на ризикот и секоја организација треба да користи своја методологија, како што е соодветно, но процесот, најверојатно, треба да се заснова на следниве принципи:

1. Идентификување на своите клучни средства.

Првиот чекор за организацијата е да ги користи информациите собрани во проценката на заканите за да ги идентификува можните ризици со кои се соочува почнувајќи од катастрофалните до релативно ситните:

- Бомба во или во близина на влезот од главната зграда.
- Сомнителен пакет добиен преку пошта.
- Вработен кој го користи својот пристап за издавање и продажба на конкретни доверливи информации.
- Вирус внесен во главниот информатички систем.
- Вработен дискретно префрлува мали средства на неовластена сметка.

2. Составување едноставен показател за да се означи потенцијалното влијание на секој инцидент.

Ваквиот показател треба да се темели на претпоставка за последиците, односно за тоа како одреден настан ќе влијае на деловната активност (на пр. дали тоа може да предизвика повреди и жртви, влијание врз продуктивноста, оштетување на угледот и довербата на клиентот итн). Треба да се користи соодветна скала за организацијата, на пр. од резултат „5“ за најлош можен исход - скоро е сигурно дека животите ќе бидат изгубени или зградите уништени - до резултат „1“ ако е веројатно дека инцидентот може лесно да се исконтролира или да се обнови штетата со малку трошоци и без публицитет.

3. За секое сценарио да се стави втор показател – веројатност инцидентот да се случи на локацијата. Треба да се разгледа зошто и како може да се случи и како може да се реализираат постојните безбедносни мерки. Притоа се применува сличен конзистентен систем на бодување со тој погоре, како што е „1“ („исклучително неверојатно“) до „5“ („сигурно“). На пример, веројатноста за појава на ситни кражби може да достигне „5“, но шансите да се открие експлозивна направа во зградата може да достигне „1“.

Кога двете оценки за секое сценарио се споредуваат во однос на другите сценарија, започнуваат да се откриваат заканите на кои треба да се фокусира организацијата. Може да помогне ако се исцртаат точките на 5x5 матрица користејќи влијание и веројатност како оски. Најдобрата практика препорачува да се погледнат резултатите самостојно, за секое сценарио посебно - без да се множат меѓу себе, бидејќи тоа може да ги замагли резултатите (на пр. ситната кражба може да ги носи истите 5x1 поени, како и постоењето бомба 1x5).

НИВО		ПОСЛЕДИЦИ				
		5	4	3	2	1
В Е Р О Ј А Т Н О С Т	5					
	4					
	3					
	2					
	1					

Табела бр. 1. Матрица за одредување на нивото на безбедносен ризик

Овие резултати се само индикативни и евентуалните, претходно планирани активности, сè уште може да опфатат повеќе од потенцијалната веројатност или влијание, но овој процес треба да помогне во фокусирањето изнаоѓање конкретни решенија. Оваа вежба треба редовно да се прегледува за да може да се земат предвид сите промени во заканата и ранливоста.

Без разлика кој метод се користи за да се спроведе проценка на ризикот, тоа може да помогне да се категоризираат заканите во „апетит за ризик“, на пример:

- Заштита: области, каде што се неопходни промени или подобрувања во тековните мерки или преку нова опрема или преку процедури.
- Адаптација: ризици што може да се намалат преку оперативни промени, на пр. аутсорсинг, промена на рутини и сл.
- Прифаќање: ризиците се оценети како минимални кога трошоците за ублажување/промена ја надминуваат тежината.
- Непредвидливост: ризици за кои ќе бидат потребни планови за да се обезбеди алтернатива или резерви - особено средства што се сметаат суштински за работењето.

Од оваа гледна точка, организацијата треба да ги разгледа заштитните мерки што можат да ги заштитат нејзините интереси и плановите за одговор за да се осигура дека при појава на какви било инциденти, безбедносниот персонал ефикасно ќе се справи.

2. Заштитна безбедност

Мерките за физичка, информациска и кадровска безбедност треба да се надополнуваат и поддржуваат едни со други.

Најефективниот безбедносен одговор треба да вклучува комбинација на физички, информациски и мерки за безбедност на персоналот. Заедно, тие се однесуваат на обезбедување на бизнисот, компанијата и организацијата преку микс на одвраќање и откривање, или помагајќи да се минимизираат последиците од каков било напад.

Но, сите организации се различни - како и местата и локациите на кои тие се поставени – па, така соодветниот микс на мерки ќе зависи од природата на безбедносната проценка врз основа на заканите и ранливостите на секоја локација.

Физичка безбедност

Физичката безбедност⁴⁰ ги опфаќа различните инсталации, мерки и контроли кои штитат од вистински физички напад. На пример:

- Откривање на натрапникот и аларми.

- Системи за контрола на пристап.
- Чуварски места – портирница.
- Безбедносни бариери за возила.
- Заштита од експлозија.

Информациска безбедност

Мерките за безбедност на информациите имаат за цел да ги заштитат податоците на организацијата и нивните различни форми на складирање и дистрибуција. Ова вклучува заштита на информатичко-технолошките системи од електронски напад, како и мерки за обезбедување информации зачувани на мобилни уреди или хартија:

- Мерки за контрола на пристапот до мрежата.
- Откривање и спречување електронски напади на упад.
- Мерки за идентификација и автентикација (на пр. корисничко име/лозинка).

Безбедност на персоналот

Безбедноста на персоналот укажува на управување со ризикот од персоналот или изведувачите кои го користат нивниот легитимен пристап до организацијата за неовластени цели:

- Проверка на идентитет и скрининг пред вработување.
- Постапки за проценка на ризик.
- Тековни безбедносни мерки.

Нема никаква вредност во насочувањето на сите ресурси кон само еден аспект на безбедноста - широкиот систем за контрола на пристапот ќе има мала корист доколку при процесот на регрутирање не се следи на кого му се дава легитимен пристап.

Наместо тоа, безбедноста треба да се развие како „повеќеслоен“ принцип, каде што секој слој го поддржува следниот и сите заедно работат беспрекорно.

Безбедносните мерки можат да бидат интензивни во однос на ресурсите, скапи и доколку не се управуваат внимателно, можат да ги нарушат рутините и да ги оттуѓат членовите на персоналот. Ова е причината зошто е потребно внимателно размислување и планирање при изборот на вистинскиот одговор и зошто треба да се побара стручен совет.

Како генерален водич, следниве принципи треба да бидат клучни за сите одлуки:

1. Не е можно да се заштити сè, па така треба да се даде приоритет на областите за заштита.

2. Мерките треба да бидат сразмерни со заканата.
3. Не дозволувајте цената да ја надмине вредноста на средството што е заштитено.
4. Безбедноста е поекономична кога е вклучена во напредното планирање.

Воведувањето на некои мерки може да се направи поекономично преку внимателно планирање. На пример, нов систем за контрола на пристап или инсталација на армирано застаклување треба да бидат вклучени уште на почетокот во сите планови за градежни работи или реновирање. Слично на тоа, вклучувањето на соодветна безбедност треба да биде клучен фактор во развојот на сите нови информатичко-технолошки системи.

Во одредени ситуации - згради во кои се сместени повеќе компании, трговски центри или деловни паркови, на пример - можно е да се договорат аранжмани за комунална безбедност, како што се системите за видеонадзор или надворешно осветлување и уредување на земјиштето.

Преку факторите, како што се обемот на организацијата, достапните ресурси и видот на задачите што се преземаат на лице место, ќе се диктираат кои се најсоодветните и најефективните безбедносни одговори за организацијата.

3. Физичка безбедност

Мерките за физичка безбедност⁴¹ имаат за цел да ги спречат, односно одвратат директните напади и да ги намалат потенцијалните штети и повреди.

Физичката безбедност е составен дел на пошироката стратегија за безбедност и во себе вклучува неколку компоненти како: контрола на пристап, надзор и тестирање на безбедноста со цел објектот кој се обезбедува да го направат посигурен.⁴²

Контролата на пристап може да започне на надворешниот раб на безбедносниот периметар. Може да се користи ограда и видеонадзор за да се следи пристапот до објектот и да се обезбеди областа на отворено. Сеопфатниот систем за контрола на пристап вклучува и употреба на напредни брави, картички за контрола на пристап или биометриска автентикација и овластување.

Надзорот е уште една важна компонента која треба да се разгледа. Современите безбедносни системи ги користат сензорите за откривање упад, топлинските сензори и детекторите за чад за заштита од упади и несреќи. Стратегијата за безбедност, исто така, треба да

предвиди поставување камери за набљудување и системи за известување.

Кога ќе се случи одреден инцидент или катастрофа, треба да се дејствува брзо и во согласност со усвоените процедури. Затоа претходно треба да се тестира планот за опоравување при катастрофи на редовна основа. Вежбите треба да ги тестираат способностите на безбедносниот персонал и вработените лица во организацијата/компанијата за начинот на реагирање при природни катастрофи и при итни случаи предизвикани од внатрешни или надворешни закани. Треба да се проверат и слабите точки во врска со пристапот до критичните деловни ресурси, како што се сервер-собите, центрите за податоци, производствените линии, опремата за енергија и слично.

Физичкиот напад може да вклучува некоја форма на импровизирана експлозивна направа.

3.1. Закани од бомби

Повеќето закани за бомби се прават преку телефон, а голем дел од нив се лажни, честопати дело на злонамерни шеги, иако терористите знаат да направат лажни повици со намера да предизвикаат тревога и нарушување. Секое лажно пријавување за бомба е кривично дело и, колку и да е смешно или неубедливо, мора да биде пријавено во полиција.

Повиците можат да бидат од два вида:

1. Лажни закани наменети за нарушување, тестирање на реакциите или пренасочување на вниманието.
2. Предупредувачки закани од постоење вистинска бомба: овие може да бидат обиди да се избегнат жртви или да се овозможи терористот да ги обвинува другите доколку има жртви. Сепак, оригиналните закани можат да обезбедат неточни информации за тоа каде и кога може да експлодира уредот.

Основните процедури за постапување по закана со бомби се според следниве принципи:

- Осигурете се дека целиот персонал кој може да добие закана од бомба е обучен за постапување или има подготвен пристап до инструкциите. Ова особено се однесува на судовите, банките, хотелите, болниците, информативните агенции, организациите за јавен превоз и оние што нудат секаква услуга за итни случаи. Операторите за разводни табли треба да бидат запознати со процедурите.

- Составете јасен список со активности што ќе следуваат по приемот на повик. И покрај тоа што персоналот не може да ја процени

точноста или потеклото на некоја закана, нивните впечатоци од повикувачот би можеле да бидат важни.

Сметајте дека членот на персоналот кој ја прима заканата можеби не е подготвен - примањето таква закана може да биде најблизу до кое многу луѓе некогаш доаѓаат до акти на тероризам - затоа понудете неколку основни совети за вработените за справување со закана, на пример:

1. Останете смирени и слушајте.
2. Добијте што е можно повеќе информации - обидете се повикувачот да биде прецизен за локацијата и времето на наводната бомба и кого тие ја претставуваат. Ако е можно, одржувајте го повикувачот да зборува.
3. Осигурете се дека е вклучен кој било објект за снимање.
4. Веднаш пријавете го инцидентот до надлежниот менаџер или безбедносниот тим за да одлучите за најдобриот тек на дејствување и да ја известите полицијата. Ако не можете да најдете никого, па дури и ако сметате дека повикот е измама, информирајте ја директно полицијата. Дајте ги вашите впечатоци за повикувачот и точни информации за тоа што беше кажано.
5. Доколку не сте успеале да го снимите повикот, направете белешки за безбедносниот персонал или полицијата. Не оставајте ја вашата објава - освен ако не е наредено да се евакуираат - сè додека не пристигне полицијата или безбедносните тимови.

3.1.1. Возила-бомби

Возилото-бомба е едно од најефикасните оружја во арсеналот на терористот, поради потенцијално големите количини на експлозив што може да се насочат кон целта со разумна прецизност. Експлозивната направа, обично, се подготвува однапред и се крие во возилото.

Безбедносните закани од возилото може да се појават на различни начини:

- Паркирано - таму каде што возилото е поставено близу или под целта (во подземна гаража).
- При движење - кога возилото навлегува преку какви било нецелосни или погрешно распоредени постојни безбедносни бариери или следи легитимно возило, па навлегува низ активниот систем на бариери во просториите.
- Преносно - кога возилото е удрено во неговата цел.
- Со измама - кога сторителите се користат со измама, со употреба на подготвена лажна приказна, лажна документација или „тројанско возило“.

- Со принуда - кога чуварот што ја контролира контролната точка е принуден да го пушти возилото или возачот на легитимното возило е принуден да носи импровизирана експлозивна направа.

Неколку тони експлозив можат да бидат натоварени во поголеми возила што би се користеле за да предизвикаат жртви и структурни оштетувања во опсег од стотици метри.

Постојат три нивоа на заштита од возила-бомби и тоа: ниско, средно и високо ниво.⁴³ Примарните разлики помеѓу нивоата на заштита се огледаат во степенот на дозволена штета на објектот што се штити, како и степенот на оштетување на средствата во објектот.

- Ниско ниво - Објектот или заштитениот простор ќе претрпи голем степен на оштетување, но нема да се уништи целосно. Можеби нема да биде во можност повторно да се употребува.
- Средно ниво - Објектот или заштитениот простор ќе претрпат значителен степен на оштетување, но структурата ќе биде повторно употреблива.
- Високо ниво - Објектот или заштитениот простор ќе претрпат само површни оштетувања и веднаш ќе може да се користат.

При спротивставувањето на возила-бомби потребно е да се посвети внимание на оддалеченоста на возилото-бомба од обезбедуваниот објект, бариерите кои треба да се постават за да се спречи возилото-бомба, како и брзината на возилото која мора да се има предвид.

Во однос на оддалеченоста на возилата од објектот што се обезбедува треба да се утврди периметар кој ќе гарантира заштита на објектот од корисетење експлозив. За таа цел, сите возила треба да бидат паркирани надвор од тој периметар, освен неопходните возила кои треба да бидат пропуштени откако врз нив ќе биде извршен преглед и претрес.

Во практиката се користат два типа препреки, односно бариери кои служат да се заштитат објектите од возила-бомби. Типот бариера што се користи зависи дали возилото-бомба е во движење или е стационирано (паркирано) во непосредна близина. Бариерите што се користат за стационирани возила-бомби имаат за цел да не дозволат пристап во заштитената зона и да ги регистрираат сите движења во таа зона. Бариерите кои се користат за возилата-бомби во движење треба да го запрат движењето на возилото и тие мора да бидат многу посуштински. Активните бариери најчесто се поставуваат на отворите во периметарот каде возилата треба да влезат или излезат. Овие бариери мора да бидат во можност да се подигнат и спуштат или да се поместуваат на страна.

Од големо значење во спротивставувањето на возилата-бомби има ограничувањето на движењето на возилата во периметарот кој се обезбедува. Најдобар начин да се ограничи брзината на приближување на возилото до периметарските бариери е да се постават или задржат пречките во можните патеки за пристап. Поставувањето пречки во форма на змија на патот го принудува возилото да ја намали својата брзина. Исто така, може да се предвидат остри свртувања или поставување кружни текови.

3.1.2. Закана од курир

Уредот што се носи на лицето/курир, обично, се сокрива под облеката на лицето или се носи во вреќа, торба или чанта. За да остане преносно, обично, тежината му е помалку од 15 кг (количина што е сè уште соодветна за да предизвика сериозни структурни оштетувања).

Овие уреди се користат во самоубиствени мисии, но исто така, се дизајнирани да може да бидат оставени без надзор, да бидат сокриени зад мебелот или екраните и да се активираат без предупредување. Во секој од случаите, влијанието се зголемува со пакување на уредот со фрагментациски материјали: завртки, навртки, клинци, штрафови, лагери и слични предмети што делуваат како шрапнели што може да има разурнувачки ефект на мал простор.

Подметнувачкиот уред - кој е наменет да запалува, а не да експлодира - обично е помал предмет кој, затоа што не бара експлозив, е поедноставен. Обично тие се наменети да предизвикаат оштетување и нарушување, со предизвикување повторен удар или, на пример, со активирање на системот за прскање, наместо да предизвикува жртви.

3.1.3. Поштенски пратки

Писмата, пратките или пакетите што содржат експлозивно, запалливо или хемиско средство, може да бидат конструирани во најразлични облици и големини. Тие се дизајнирани да изгледаат прилично вообичаено, но, сепак, постојат одредени знаци што сугерираат кога треба да се покаже дополнителна претпазливост при ракувањето со нив:

- Пакетот е од неочекуван или непознат испраќач.
- Слабо е напишано, неточно адресирано или напишано во необичен стил и има повеќе од соодветна вредност на марки за неговата големина и тежина.

- Тоа е обвиткан плик или гломазен предмет кој е невообичаено тежок за неговата големина (повеќето писма тежат до околу 30 грама, додека заканувачките писма тежат 50-100 грама).
- На пликот или пакувањето има една или повеќе дупки направени со игла.

Иако секоја сомнителна пратка треба да се третира сериозно, повеќето случаи се лажни аларми и затоа постапките за ракување со вакви сомнителни предмети треба да се спроведуваат на тој начин да не предизвикаат какво било нарушување.

Некои поголеми приватни компании и корпорации не дозволуваат доставување лични пратки на вработените на работното место, за да се намали бројот на испораки. Исто така, тие практикуваат користење услуги од една компанија за доставување која ќе биде проверена. Овластените доставувачи на пратки треба да треба да бидат во системот за контрола на пристап, за да може да се идентификува лицето и пратката.

Во зависност од проценката на ризикот и фреквенцијата на примање на поштата и пратките, а да не влијае на динамиката на работата, потребно е пратките да се проверуваат рачно и при тоа да се препознае некој од клучните знаци при идентификување сомнителни предмети.

Најчесто треба да се имаат предвид следните знаци:⁴⁴

- Облик на пакетот: Импровизираните експлозивни направи и уреди за запалување може да имаат неправилен облик поради постоење на напојување, експлозив, детонатори, фрагментациски материјал и сл. Исто така и тежината може да предизвика сомневање за содржината на пакетот.
- Мирис: Одредени експлозивни имаат карактеристичен мирис и одредена арома која може да продуцира силен мирис. Таквите миризби треба да се третираат како сомнителни.
- Мрсни дамки: Експлозивите при промена на температурата може да остават мрсни траги и дамки на пакетите во кои се испорачуваат. Доколку се забележат такви знаци треба да се реагира навремено и внимателно.
- Адресирање и печат: Најнапред треба да се провери од каде потекнува пакетот и да се внимава на користењето на марките кои се употребуваат во зависност од тежината. Исто така, треба да се внимава и на оригиналноста и автентичноста на одредени печати и жигови кои постојат на надворешната страна на пратката.

Тука се нагласува и потребата од постоење пишан акциски план во случај на откривање на импровизирана експлозивна направа. Таквиот

план треба да го знаат вработените на сите нивоа, во случај да се појави потреба од реакција и евакуирање.

3.2. Закана од користење хемиско, биолошко и радиолошко оружје

Оружјето за масовно уништување, само по себе, претставува закана по глобалната безбедност. Опасноста, терористичките групи и нивните приврзаници, да добијат пристап до оружје за масовно уништување е сериозен ризик за загрозување на меѓународниот мир и безбедноста. Традиционалните методи престанаа да бидат психолошки ефикасни и доволни за да го привлечат вниманието на јавноста, така што новите терористи го препознаваат оружјето за масовно уништување како нова можност и реална закана. Влијанието на напади со користење хемиско, биолошко, радиолошко и нуклеарно оружје зависи во голема мерка од успехот на избраниот метод и временските услови во моментот на нападот.

Поттикнувачките фактори за терористите да употребат оружје за масовно уништување се предизвикување на една или повеќе цели:

- масовни жртви;
- преоптоварување на системите за реагирање во итни случаи;
- нарушување на нормалниот живот во градовите;
- затворање и загадување на објекти;
- паника и збунетост;
- предизвикување губење на довербата во државните органи дека може да го заштити населението и да спречат терористички активности;
- предизвикување губење на довербата во системот за реагирање во итни случаи.

Првите индикатори за напад со оружје за масовно уништување (хемиско, биолошко и радиолошко) може да бидат ненадејно појавување прав, течности или чудни мириси во објектот, со или без непосреден ефект врз луѓето кои се присутни на местото на инцидентот.

Во случај таквиот напад да доаѓа од надвор, потребно е да се преземат следните мерки:⁴⁵

- останете внатре во објектот;
- известете ги и помогнете во евакуација на другите лица во објектот;
- затворете ги и запечатете ги вратите и прозорците со поставување влажна крпа;
- исклучете ја климатизацијата, вентилацијата и затворете ги другите отвори за воздух.

Заштитата од можноста за користење хемиско, биолошко и радиолошко оружје во терористички активности⁴⁶ е приоритетна цел на секоја држава. Најголемо внимание треба да се посвети на:

- Превенција: се однесува на разбирање и спроведување на мерки за намалување на потенцијалните несреќи или безбедносни инциденти. Тоа подразбира заштита од кражба на хемиски, биолошки и радиолошки агенсии како и намерно испуштање во околината.
- Откривање: се однесува на системи и процеси кои овозможуваат рано откривање на одредени загуби во системот или утврдување степен на сомневање за намерно ослободување на одредени агенсии.
- Реагирање: се однесува на навремена реакција на ниво на објектот или на национално ниво по случен инцидент од ваков ранг. Системот за реагирање вклучува ангажирање, опремување и обука на сите засегнати страни кои први реагираат.

4. Мерки за физичка безбедност

Обезбедувањето и заштитата на приватните и деловните објекти подразбира преземање на севкупни мерки, активности, задачи и работи кои претходно се планираат и преземаат од надлежните органи и агенциите за приватно обезбедување во насока на отстранување на ризиците, заканите, опасностите и загрозувањата кои постојат кон нив.

Објектите може да бидат загрозени на многу начини, со различни средства и методи, а преземањето на мерките и активностите за нивно обезбедување зависи од повеќе фактори. Најсериозно е загрозувањето од извршување терористички напади.

Специфична карактеристика кај овој вид обезбедување е тоа што преземените мерки за заштита не се однесуваат само на објектите, туку и на сите лица кои се нивни корисници или престојуваат во овие објекти од различни причини. Затоа, ваквите мерки имаат поширок опсег во нивната примена.

Најчестите мерки за заштита кои се применуваат во процесот на обезбедување на приватните и деловните објекти се мерките за физичка, техничка, противпожарна заштита, како и мерките за санитарно-технички, биолошко-хемиски и мерките за здравствена заштита.

Како се заштитуваат компаниите од напад, зависи од индивидуалните околности. За повеќето организации одговорот вклучува мешавина на добро раководење заедно со соодветни инвестиции во видеонадзор, аларми за натрапници и осветлување што може да ги одврати, но и да ги открие заканите. Всушност, многу

препорачани мерки кои се однесуваат против тероризам помагаат компаниите да се заштитат и од други кривични дела како што се кражби и вандализам, а исто така можат да им помогнат на компаниите да се справат со здравствените и безбедносните проблеми на нивните вработени.

Како и да е, одредени ситуации може да бараат повеќе специјализирана опрема (технологија за скенирање на поштата, на пример) и компаниите треба да побараат професионален совет за проценка на нивните барања и опции, пред да донесат големи одлуки.

4.1. Надворешно опкружување

Ако постојат закани и загриженост за евентуални напади со возило-бомба, тогаш приоритет треба да биде сигурноста, односно сите неовластени и/или непрегледани возила да се чуваат на безбедно растојание, идеално, да се држат возилата на растојание од најмалку 30 метри од зградите, а поголемите комбиња и камиони, на растојание од најмалку 90 метри.

Пристапните правци, паркиралиштата и околните отворени области треба да се проценат за нивната пропустливост на непријателски возила. Треба да се инсталираат соодветни мерки за смирување на сообраќајот, како што се свиоци и острови и успешно тестирани безбедносни препреки за возилата, за да се создадат и да се одржуваат соодветни растојанија во случај на експлозија. Овие безбедносни бариери за возила, можат да вклучуваат активни (подвижни) мерки, како што се повлечени столбови, растечки бариери за заградување и влезови или лизгачки порти, како и пасивни (статички) мерки, како што се структурни сидови, препреки и жардинери.

Ако се дозволува влез на возила во рамките на безбедносната зона, тие треба да бидат прегледани на контролниот пункт дизајниран така што неовластените возила можат да бидат одбиени без да се пуштат да влезат во зоната.

4.2. Зајакнување на имотот

Врати и прозорци

Надворешните врати треба да бидат цврсти, правилно осветлени и опремени со брави со добар квалитет. Сите врати што ретко се користат треба да бидат внатрешно обезбедени (осигурувајќи почитување на соодветните регулативи за безбедност). Пристапните прозорци, исто така, треба да бидат обезбедени со брави со добар квалитет.

Ако веќе не постои систем за аларм, тој треба што поскоро да се инсталира на надворешните прозорци и врати.

Квалитетот на заштита со застаклување е важен затоа што до 95% од сите повреди со бомба се предизвикани од летање или паѓање на скршено стакло. Панцирната фолија за стакло е релативно евтино и брзо подобрување, додека ламинираното стакло треба да се користи доколку прозорците треба да се заменат со нови или кога се работи за нови градби, затоа што нуди повисоко ниво на заштита.

Заштитени простории (области за засолништа при напад со бомба)

Во одредени ситуации може да биде побезбедно да се премести персоналот на одреден внатрешен заштитен простор, наместо да се евакуира зградата. Заштитениот простор треба да биде конструиран од соодветно тестирани материјали и, генерално, да не се наоѓа на приземје или на првите спратови, а исто така, да е оддалечен од надворешните сидови. Можеби ќе биде неопходно да се сместат групи луѓе во неизвесни периоди, затоа овие простории треба да бидат во можност да обезбедат простор за седење, вода за пиење, електрична енергија за итни случаи и надворешни комуникации (процедурите не треба да се потпираат на мобилни телефони), како и пристап до тоалети.

При ваквото сместување може да недостасуваат внатрешни сидови што можат да заштитат од експлозија или коридори што можат да обезбедат патеки за евакуација. Во вакви случаи, важни се мерките, како што е застаклување отпорно на експлозија и јасно обележани, редовно проверувани излезни правци.

4.3. Внатрешни области

Мерки за внатрешно обезбедување

Мерките за внатрешно физичко обезбедување ги преземаат работниците за приватно обезбедување во рамките на објектот и тие се состојат од:

- Непосредна заштита, контрола и надзор на објектот, просториите, имотот, уредите, средствата, опремата, ресурсите и инсталацијата во него;
- Спречување потенцијални напади (физичка сила, закана и сл.) врз вработените лица, клиентите и други лица кои по различна основа престојуваат во објектот и совладување на напаѓачите;
- Вршење работи на пријавница и водење уредна евиденција за сите посетители;
- Легитимирање и контрола на сите лица кои доаѓаат во објектот што се обезбедува со користење на одредени расположливи

системи за техничка заштита, како што се метал-детекторска врата и рентген апарат;

- Привремено одземање и задржување на предметите кои би можеле да бидат потенцијални загрозувачи на безбедноста на лицата во објектот.

Доброто управување во компанијата може да помогне во намалувањето на можностите за оставените предмети од сомнителните лица и да се олесни забележувањето на персоналот (и дополнително ќе помогне да се намали бројот на лажни аларми). Од персоналот треба да се побара:

- Да ги чуваат надворешните, јавните и комуналните области (излези, влезови, места за прием, скали и ходници, перални и сл.) - чисти и уредни.
- Да се заклучуваат празните канцеларии, простории и шкафови за чување.
- Минимизирање на мебелот и растенијата во влезовите и јавните места, за да се намалат местата каде што би можеле да се сокријат сомнителни уреди.
- Отстранување на отпадоците од корпите за време на зголемена закана - користење чисти просирни пластични ќесиња, како привремена алтернатива.

Видеонадзор, аларми и осветлување

Современиот начин на функционирање на приватната безбедност укажува на можноста од вградување различни безбедносни технички системи и уреди во објектите заради нивна заштита. Видот на системите и уредите, нивниот распоред и местоположба, зависат од видот на обезбедуваниот објект и од безбедносната проценка на ризикот.

Алармите за упад може да бидат пречка, како и средство за заштита. Алармните системи за заштита заземаат значајно место во процесот на обезбедувањето на објектите кои може да бидат мета на терористички напади, а нивната основна функција е да детектираат неовластен пристап во внатрешниот или надворешниот простор на обезбедуваниот објект или присуство на извесни надворешни опасности и да алармираат до конкретниот субјект кој се грижи за заштита на објектот. Тие може да бидат противпровални системи, противпожарни системи и системи за предупредување. Денес, масовно се применуваат алармните системи за заштита кои се состојат од повеќе потсистеми во одредена меѓусебна корелација и функционална меѓузависност. Тие се состојат од алармни централи, сензори, сирени, магнетни контакти и алармни дојавувачи.⁴⁷

Техничките системи за снимање од затворен тип се компонента од интегралниот систем за техничка заштита на објектите. Видеонадзорот треба редовно да се следи за да се разјасни дали безбедносното предупредување е реално. Снимањето (архивирањето) овозможува репродукција на настаните што е од исклучително значење за дополнителна анализа на информациите од надгледуваниот простор. Честопати, во истрагите за инциденти, од суштинско значење е користењето на снимките, за да се идентификува што и како се случило. Основните елементи на овие системи се камерите, преносните кабли, мониторите и уредите за снимање и репродукција на слика. Видеонадзорот, исто така, треба да се испланира заедно со нивото на осветлување што може да се обезбеди.

Области за прием на странки

Ефикасната област за прием е неопходна за следење на пристапот во и надвор од просториите. Кога е можно, влезовите и излезите треба да се искористат со квалитетен систем за контрола на пристап кој користи магнетни чипови или контактни картички, поддржани со верификација со ПИН. Посетителите треба да бидат придружувани од членовите на персоналот и, исто така, да носат јасно обележани бецови за привремени посети што се враќаат при заминување.

Воведувањето на ваквите системи ја зголемува безбедноста на објектот, а воедно, го намалува и бројот на ангажирани работници за физичко обезбедување.

Системот за контрола на пристапот го регулира движењето на лицата во рамките на одреден објект, односно во неговата внатрешност, но и во подрачјето околу објектот. Контролата се применува на луѓе, транспортни средства и материјали. Притоа, постојат три видови⁴⁸ системи за идентификација на пристапот (контролата) до одреден објект и тоа: шифриран (кодиран) влез, влез со идентификациски картички или бецови и биометриски пристап (врз основа на препознавање на некои физички особености на лицата - папиларни линии од прсти, дланка, лице, мрежница од око и сл.).

Основен начин за контрола на пристапот на лица до објектот е нивно легитимирање. За странки, посетители, новинари, технички персонал итн., се предвидени пропусници, а за одредени моторни возила, за користење на одредени паркинг-места, се доделуваат налепници. Посебни значки, бецови се издаваат на лица кои имаат неограничени права во поглед на влезот, движењето и задржувањето во објектот што се обезбедува.

Преглед и пребарување

Случајниот преглед на рачниот багаж може да дејствува како спречувач, а редовното скенирање на багажот треба да се земе предвид во време на зголемена закана. Компаниите имаат право да одбијат влез на секој што не дозволува да се пребарува неговиот/нејзиниот багаж; но, сепак, претресот може да се изврши само со согласност на поединецот.

Рутинското пребарување и патролирање на просториите, исто така, претставува видлив застој. Затоа, патролите треба да се практикуваат редовно, но, да не бидат премногу предвидливи.

Исто така, потребно е повремено да се прегледува и пребарува и самиот објект. Прегледот на објектот се врши од надворешната и внатрешната страна.

Од надворешна страна прегледот и контролата за овој вид заштита подразбира преглед на објектот, дворот и околниот простор вклучувајќи ги тука сите подземни и надземни инсталации (електрична инсталација, водоводна мрежа, парно греење, гасна инсталација, канализациска мрежа, телефонски и останати сигнални кабли и инсталации), притоа вршејќи контрола над нив за пронаоѓање и отстранување на можни поставени експлозивни материи.

По извршениот преглед на надворешниот дел од објектот се пристапува кон преглед на внатрешноста на објектот. Прегледот на внатрешниот периметар на објектот се започнува од долу-нагоре или од горе-надолу почнувајќи со подрумските постории (котлара, гасна станица, резервоари за течно гориво, резервоари за вода, генератори за електрична енергија) и останати делови и предмети во подрумските простории. Потоа се преминува со преглед на приземјето заедно со влезовите и излезите, заради поголема и поефикасна контрола на сите пристапи кон објектот, а ако за тоа постои можност се врши редуцирање на влезовите на главни и споредни (влез за вработени и техничкиот персонал), преглед на просторот под скалите, скалилата, лифтовите (нивна исправност и носивоста) и просториите на катовите сè до поткровјето.

Доколку при прегледот се забележат одредени недостатоци, оштетени предмети, прегорени електрични апарати и техника, се известува одговорното лице на објектот за благовремено отстранување на недостатоците. Во случај при прегледот да се забележи присуство на експлозивна материја или направа или друг вид на сомнителен предмет, прегледот се прекинува, се известува локалната полициска станица, објектот се напушта и се чекаат понатамошни инструкции.

Сандачиња за пошта

Експлозијата на бомба во зградата има многу поголеми и потешки ефекти од истата експлозија надвор од зградата. Поради тоа потребно е да се предвиди посебна просторија каде ќе се прима поштата и ќе може да се пребаруваат сомнителни пакувања кои може да имаат експлозивни материји или запаливи уреди. Најчесто таквите простории треба да бидат лоцирани на надворешноста на објектот и да бидат изградени на начин што ќе ги задржат ефектите на експлозијата надвор од објектот.

Дојдовната пошта и испораките треба да бидат обработувани на една локација, идеално надвор од просториите на компанијата или во област што лесно може да се изолира. Испораките треба да се третираат без да се донесат преку други делови од зградата. Треба да се осигура дека сите вработени кои управуваат со поштата (вклучително и персоналот за прием) редовно се брифираат и обучуваат. Треба да се охрабрат редовните дописници да ја стават својата адреса за кореспонденција на секоја пратка.

Откривањето на поштенските пратки зависи од нивото на заштита. На пониските нивоа на заштита се користат едноставни процедури за преглед. Како што расте нивото на заштита, се зголемува софистицираноста на откривањето. На повисоките нивоа на заштита, може да се користи опрема, како што се уреди за испитување на х-зраци, детектори за метали и детектори за експлозиви. Кога е неопходно може да се користат и кучиња за откривање експлозиви.

Ако постои загриженост од прием на сомнителни писма или пратки, особено, ако рутински, при работата на компанијата, секој ден се примаат големи количини пратки, тогаш треба да се побара совет од локалната полициска станица.

Големите компании и корпорации, своите вработени кои работат на прием на пошта и пратки, ги праќаат на соодветни акредитирани курсеви за препознавање сомнителни пакети. Ваквите обуки треба да се посетуваат редовно со што вработените ќе бидат во тек со најновите уреди и методологии од закани со импровизирани експлозивни направи.

5. Информациска безбедност

Во денешното современо општество, кога е потребна брза комуникација и размена на информации, сите сфери на живеењето се зафатени од дигитализацијата и зависат од информатичката технологија. Нејзините предности се огромни и помагаат за висок степен на напредок на човештвото. Но, ниту новите технологии не се имуни од криминалните активности на современите криминалци.

Компјутеризацијата и префрлањето на целокупните животни и работни процеси преку интернет-технологијата, истовремено си има и свои негативни страни. Компјутерските напади и компјутерскиот криминал сè повеќе стануваат актуелни и се закануваат во иднина да заземат високо место во рамките на целокупниот криминал, со особено штетните последици кои произлегуваат од нив, по националната и глобалната безбедност. Токму затоа, безбедноста и заштитата на компјутерските бази, програми и системи, се наметнува како главен проблем на иднината.⁴⁹

Во безбедносно-правна смисла, сајбер-тероризмот претставува намерна злоупотреба на дигиталниот информациски систем, мрежа или компонента за исполнување на целите за потребите на терористичката борба. Последица од злоупотребата на системот нема да биде директно насилство против луѓето (што не е исклучено, на пример, со паѓање авиони, хаос во болниците, хаварија во системот за снабдување со електрична енергија и слично), но, сепак, ќе предизвика страв, зголемување на светскиот криминал со најбрзо темпо, најголема стратешка ранливост на сите витални општествени функции, огромни човечки страдања, но и жртви како „колateralна штета“. Во овој контекст, уште пострашен е и фактот што овие суптилни дејства може да иницираат и кибернетичка војна или да „наместат“ определени држави да отпочнат класична војна, како одговор на сајбер-контрамерките „преземени од другата страна“.

Меѓутоа и покрај економските и другите штетни консеквенци од компјутерскиот криминал, општеството се потпира на компјутерските системи за, скоро, сè во животот, од воздушна, железничка и автобуска сообраќајна контрола до координација на медицински сервиси и национална безбедност. Потребна е мала грешка во работењето на овие системи за да се стават човечки животи во опасност. Брзата експанзија на големите компјутерски мрежи и можноста да се пристапи до многу системи преку обична телефонска линија ја зголемуваат ранливоста на овие системи и ја отвораат можноста за злоупотреба и криминална активност, како и нарушување на националната и глобалната безбедност.

Начинот на користење, складирање и дистрибуирање на информациите⁵⁰ е голем предизвик за сите организации.

Бидејќи деловните субјекти се потпираат сè повеќе и повеќе на нивните информациско-комуникациски системи за подобрување на ефикасноста и обезбедување поголема функционалност, така и информациите што ги задржуваат стануваат поранливи на намерни и случајни напади.

Без разлика дали се зачувани како хартиена евиденција или во електронски системи, безбедноста на информациите на една организација мора да биде фундаментална за какво било безбедносно планирање и планирање на вонредни состојби. Клучните прашања што треба постојано да се поставуваат се:

- Кој би сакал пристап до нашите информации и како би можеле да ги добијат?
- Каква придобивка може да имаат од нивната употреба?
- Дали можат да ги продадат, да ги изменат, па дури и да спречат пристап на персоналот или клиентите до нив?
- Колку е штетна загубата на податоците? Кој би бил ефектот врз работењето или угледот на компанијата?

Одредени функции, како што се обработка на податоци, администрација на системи или хостинг на сервери, веќе се рутински аутсорсинг и однапред договорени што значи дека безбедноста и интегритетот на податоците стануваат зависни од стандардите што ги имаат воспоставено другите организации.

Додека инвестициите во софтвер и контролите на пристап помагаат во намалувањето на одредени закани, човечкиот фактор кој е вклучен е, исто така, многу значаен. Многу инциденти на загуба или злоупотреба на податоците произлегуваат од погрешна проценка или момент на негрижа од страна на член на персоналот.

Без разлика дали некој член од персоналот е принуден да воведува малициозен (злонамерен) софтвер во мрежата или да поврзе неовластен подвижен медиум, како што се USB-стиките на системи, или да се игнорираат постапките за постапување со доверливи документи надвор од компанијата, најголем предизвик може да биде обучувањето на персоналот за да знае како се појавуваат слабостите и ранливостите и како, ставовите и навиките на персоналот, прават разлика.

5.1. Типични методи на електронски напад

Во суштина постојат два основни методи⁵¹ преку кои терористите ги извршуваат компјутерските терористички напади.

Првиот метод е кога самата информациска технологија претставува цел на терористичките напади. Со изведување на определени саботажи (електронски и физички) врз информацискиот систем, ќе се обидат да го уништат или да извршат прекин во функционирањето на информацискиот систем и информациската инфраструктура, во зависност од самата конкретна цел.

Вториот метод е кога информацискиот напад претставува средство-чекор за спроведување на една поголема операција. Овој чин имплицира дека терористите ќе прават напори за манипулација и експлоатација на информацискиот систем, кражба на информации како алтернатива или принудување – „програмирање“ на системот да врши функција за која не е наменет.

Малициозен софтвер

Малициозен (злонамерен) софтвер се однесува на која било датотека или програма која е штетна за компјутерот, како што се вируси, црви, тројански коњи и шпионски софтвер (програма што собира информации на корисникот без дозвола). Обично се шири преку е-пошта или компромитирани веб-страници, па заразениот компјутер има потенцијал да му овозможи на напаѓачот да собира лозинки, да скенира дискови, да испраќа и да презема податоци или да шири нарушувања низ целата мрежа.

Овој софтвер, испратен како прилог на е-пошта директно до примателот, се чини дека потекнува од легитимен испраќач. Предметот на е-поштата и прилогот ќе имаат за цел да го привлечат интересот на примателот и при отворањето на ваквиот малициозен софтвер, тој да навлезе во компјутерот и мрежата на компанијата.

Другите рути во мрежата вклучуваат преносни уреди за складирање и медиуми, како што се ЦД-РОМ кои жртвата може да ги вметне директно во нејзиниот компјутер - особено прашање за организации со голем број персонал што работи од далечина и соработува преку мрежни системи.

Хакирање

Хакирањето се однесува на секој обид да се добие неовластен пристап во компјутерскиот систем. Постои голем број на можни мотивации кои се движат од нарушувачка или криминална намера до поединци кои покажуваат техничка моќ. Хакерите може да имаат техничка експертиза, но достапноста на „алатките за хакерство“ го направи хакерството помалку специјализирана активност.

Покрај вообичаените напади врз поединци, софистицираните координирани хакерски напади се насочени кон владите и високопрофесионалните деловни организации.

Фишинг

Нападите со фишинг користат мешавина од техничка измама и социјален инженеринг, за да ги стават во искушение жртвите да вршат

серија активности што ќе овозможат пристап до конкретни или чувствителни информации.

Во повеќето случаи, напаѓачот имитира доверлив извор, како што е банка или доставувач на информатичка технологија, во форма на официјална порака преку е-пошта, веб-страница или поп-ап реклама за да привлече внимание кон некоја итна случка за која примателот е притиснат да обезбеди одредени чувствителни податоци како повратен одговор.

Нападите со фишинг стануваат посоефистицирани и заштитата од нив, исто, како и кај малициозниот софтвер за е-пошта, се однесува повеќе кон свеста на поединецот отколку кон безбедноста на централната мрежа.

Одбивање на услугата

Станува збор за обиди со кои се оптоварува системот со тоа што се натрупува со несакани податоци. Некои вакви напади се дистрибуирани, во кои голем број на необезбедени, „невини“ компјутери/машини (познати како „зомби“), се регрутираат за да извршат понатамошни поголеми напади.

6. Мерки за информациска безбедност

Генералните совети кои организациите треба да ги земат предвид при работењето заради зајакнување на безбедноста на информациите и базите на податоци со кои располагаат се:

- Набавете ги сите информатичко-комуникациски системи од реномирани производители и добавувачи.
- Сите компјутери поврзани на интернет треба да бидат опремени со антивирусен и антишпионски софтвер и да бидат заштитени со т.н. заштитен сид. Новите компјутерски вируси секојдневно се испуштаат во интернет-просторот, па антивирусните компании постојано ги детектираат слабите страни на компјутерските софтвери и изработуваат надградби за нивните клиенти, па затоа често проверувајте ја оваа корисна алатка.
- Информации за резервна копија - по можност чувајте безбедна копија од сите податоци на друга локација и проверете дали редовно се тестираат сите постапки за резервна копија и обновување на податоците.
- Осигурете се дека сите изведувачи/трети страни се придржуваат кон истите безбедносни политики и стандарди користени од организацијата.

- Доколку се користат даватели на услуги однадвор, треба да се воспостават договори за зачувување на податоците.
- Размислете за пакетите за криптирање на изваден материјал надвор од локацијата. Кога е можно, заклучете ги или оневозможете ги дисковите, USB-портите и безжичните врски.
- Осигурете се дека постојат соодветни стандарди за дигитални медиуми. Кои било дигитални медиуми треба да бидат преснимани неколку пати за да се направат нечитливи и кога ќе стигнат до крајот на својот животен век да се уништат за да не може лесно да се реконструираат.
- Придржувајте се до принципот дека целиот персонал и/или надворешните контакти започнуваат со минимално ниво на пристап. Продолжувањето и проширувањето на правата на пристап треба да се извршат следејќи специфични барања за управување со нив - осигурете се дека истите тие права се укинати во случај на промена на улогата или лицето, за да нема пристап до податоците кога лицето ќе биде преместено на друга работна позиција или ќе го напушти работното место.
- Наметнете политика за задржување и бришење на заштитата на податоците. Постојат законски услови за заштита на податоците што една компанија ги задржува и одговорност е на бизнисот да обезбеди дека ги исполнува своите обврски.
- Чувајте ги сите информации во врска со други компании под постојан преглед. Бидејќи односите со деловните субјекти или клиентите се менуваат, можеби е неопходно да се откажат привилегиите, како што се пристапот до екстранет или да се отстранат од конкретните списоци за испраќање.

6.1. Едукација на персоналот

- Охрабнете ја безбедносната свест кај вработените. Бидете сигурни дека тие ги разбираат проблемите околу нападите со малициозен софтвер или фишинг или откривање информации што можат да се користат за да се добие пристап до одреден систем.
- Дајте насоки за безбедно користење на е-поштата на работа. Барајте нивната е-пошта да се користи претежно за кореспонденција поврзана со работата и приватните е-пошти да не се користат за контактирање со клиенти или испраќање/примање информации.

- Ограничете го пристапот до одредени веб-страници кои не се поврзани со работата; ова вклучува какви било страници за социјално вмрежување и веб-пошта каде безбедносните стандарди не се загарантирани.

6.2. Одговорно постапување со документи

Многу приватни или чувствителни записи, сепак, се чуваат на хартија и затоа е важно да се обезбедат објектите и процедурите за нивно безбедно чување и отстранување.

Чувствителните, доверливите или комерцијалните документи треба да бидат соодветно обележани со јасни упатства издадени на персоналот за ракување, кога се надвор од работното место. Вработените треба да бидат целосно свесни за нивните одговорности кога располагаат со вакви документи, на пример, никогаш да не работат јавно на нив, никогаш да не ги оставаат во паркирано возило и да ги чуваат во сефови или други безбедносни кутии кога престојуваат во хотел.

Персоналот треба да биде охрабрен да одржува „чисто биро“ со заклучување на сите документи и преносни медиуми кога се далеку од работните места или кога заминуваат на крајот од работниот ден. Ова треба да вклучува какви било оставени хартии на печатачи, фотокопири или во простории за состаноци. Особено вредните или чувствителните документи не треба да се оставаат наоколу или да се прикажуваат во секое време. Затоа треба да се обезбедат соодветени безбедни ормари или заклучени места за складирање.

6.3. Отстранување информации

Некои од материјалите што бизнисите рутински ги фрлаат можат да бидат од корист за различни групи, вклучително и деловни конкуренти, крадци на идентитет, криминалци и терористи. Имињата и адресите на персоналот, телефонските броеви, информациите за производите, техничките спецификации итн., можат да им бидат од корист на одредени луѓе. Хартиените документи треба да бидат уништени со безбедни средства. Персоналот треба да се обезбеди со лесен метод за уништување, согорување или сечење, така што вредните документи нема да се фрлаат со останатото ѓубре.

7. Безбедност на персоналот

Безбедноста на персоналот⁵² е систем на политики и процедури кои имаат за цел да го намалат ризикот на вработените кои го искористуваат нивниот легитимен пристап до средствата на една организација за неовластени цели.

Безбедноста на луѓето се однесува на обликување и контролирање на околината за промовирање будност и ефикасна безбедносна култура и за влијание и одвраќање на оние што сакаат да предизвикаат штета. Пристапот кон подобра безбедност на персоналот и луѓето е насочен кон три главни области на активност околу луѓето, како елемент на заштитната безбедност:

- Намалување на ризикот од инсајдери - оваа област им помага на организациите да го намалат ризикот од инсајдери преку преземање добри практики за безбедност на персоналот, како што се проценка на ризик, скрининг пред вработување и тековно обезбедување на персоналот.
- Оптимизирање на луѓето во безбедноста - како да извлечете максимум од релативно неискористениот безбедносен ресурс - персоналот и посетителите? Оваа област им помага на организациите да ја разберат важноста за градење добра безбедносна култура и како да преземат кампањи за промена на однесувањето на персоналот. Тука се разгледуваа начините за зголемување на можностите на безбедносниот персонал за мотивација и проактивно откривање.
- Нарушување на непријателските извидувања - оваа област разгледува како да се ублажат заканите од надворешните посетители преку разбирање на свеста и активностите на оние што планираат напади и непријателско извидување.

Поставувањето или вработувањето на „инсајдер“ - некој што го искористува или има намера да го искористи својот легитимен пристап до една организација за нелегитимни цели - го користеле терористички и криминални мрежи, како и активисти, новинари и конкуренти.

Инсајдер⁵³ е лице кое го искористува или има намера да го искористи неговиот легитимен пристап до средствата на организацијата за неовластени цели, односно да наштети на безбедноста на организацијата или со намера или несакајќи, преку шпионажа, тероризам, неовластено откривање информации и загуба или деградација на ресурси или капацитети. Тој може да биде постојан, привремен, повлечен од друга организација, ангажиран по договор или работник од агенција. Бидејќи организациите спроведуваат сè посоефицирани физички и информациски безбедносни мерки за да ги

заштитат своите средства од надворешни закани, регрутирањето инсајдери станува поатрактивна опција за оние кои се обидуваат да добијат пристап до капацитетите и ресурсите во организацијата.

Засега се идентификувани повеќе причини/мотиви и начини поради кои инсајдерот може да ја наруши безбедноста на организацијата.⁵⁴

Вообичаените причини/мотиви поради кои инсајдерот може да ја наруши безбедноста се:

- одмазда против работодавецот или колеги,
- неизвесност за неговото континуирано вработување,
- алчност или финансиска добивка,
- политичка или верска идеологија,
- его или озлогласеност,
- принуда, манипулација или експлоатација од надворешна трета страна.

Исто така, постојат примери на постојни вработени кои доброволно се пријавиле да им помагаат на трети лица или да се вклучат во инсајдерски активности за нивна лична корист.

Вообичаени начини на кои инсајдерот може да ја наруши безбедноста:

- неовластено откривање деловни, приватни или комерцијални информации,
- измама или поттикнување корупција,
- неовластен пристап до информатичко-комуникациските системи во организацијата,
- економска или индустриска шпионажа,
- кражба, насилство или физичко оштетување на објектите, капацитетите или средствата на организацијата.

Затворањето на можностите за оние што сакаат да го злоупотребат својот легитимен пристап е сложен предизвик. Засега не постои точен метод за идентификување на персоналот кој може да претставува закана за безбедноста, прекумерното компензирање со дополнителни мерки може само да троши ресурси, да ги наруши рутините и да ги остави вработените да чувствуваат недоверба.

8. Мерки за безбедност на персоналот

Безбедносните мерки за персоналот⁵⁵ им помагаат на организациите да ги намалат можностите персоналот да го злоупотреби нивниот легитимен пристап.

Од процесот на пред селекција за вработување, па сè до финалното интервју, организациите мора да демонстрираат конзистентен, транспарентен и недискриминирачки пристап кон безбедноста на персоналот кој се однесува на сите членови на персоналот, без разлика дали се постојано или привремено вработени или се изведувачи, без разлика дали се работи за висок менаџмент или асистенти со скратено работно време.

Режимот на ефикасна безбедност на персоналот треба да се смета за континуиран циклус на идентификување и проценка на ризици, селекциска проверка заради вработување, процедури за проценка и подигнување на свеста кај сите вработени (безбедносна култура) и добро управување со безбедноста во организацијата (безбедносен менаџмент).



Слика бр. 2. Режим на ефикасна безбедност

8.1. Проценка на ризик

Проценката на ризикот е од клучно значење за формирање добар режим за безбедност на персоналот помагајќи им на менаџерите да ги фокусираат ресурсите на областите од најголема загриженост, да обезбедат сегашните мерки да бидат пропорционални на заканите и да обезбедат услови за донесување нови мерки, доколку тоа се бара.

При спроведување на проценката на ризик, постојат низа методи кои организациите можат да ги применат и кои во зависност од природата и големината на бизнисот, може да имаат вредност во спроведувањето на ваквите проценки на различни нивоа соодветно, на пример:

- Проценката на ризикот во организацијата го идентификува широкиот спектар на инсајдерски закани со кои се соочува една организација и приоритети во однос на нивната веројатност и влијание.
- Проценката на групно ниво ги идентификува оние групи на вработени со потенцијал да извршат закани од најголемо влијание и утврдува дали тековните контрамерки се соодветни и каде се потребни дополнителни мерки.
- Проценката на индивидуално ниво го испитува ризикот од индивидуалните вработени или малите групи со висок ризик, засновани врз комбинација на нивната улога, нивото на пристап и постојните слабости во работната средина.

8.2. Вработување

По процесот на селекција, од сите потенцијални вработени треба да се побара да обезбедат доказ за нивниот идентитет, право на работа, доказ за претходни вработувања и доказ за стекнато образование. Одлуката за барање дополнителни проверки треба да се заснова на специфичностите на индивидуалната улога и одговорности кои се очекува да ги имаат на работното место. Па, така, треба да се направи и проверка за претходно изречени санкции и финансиска проверка.

Организациите не треба да прифаќаат дупликати или фотокопирани документи и треба да се проверат очигледните празнини и недоследности во историјата на претходни вработувања или живеалишта на апликантот. Апликантите треба да се потсетат дека доставувањето лажни информации или необјавување релевантни информации може да биде основа за разрешување и да претставува кривично дело.

Во прилики, кога кандидатот треба да биде назначен брзо, треба да биде јасно дека задоволителното завршување на проверките е услов за вработување.

Кога се регрутираат кадри од агенции или изведувачи, треба да се провери дали можат да го потврдат идентитетот на нивниот персонал и предвреме да обезбедат автентична фотографија.

8.3. Развивање добра безбедносна практика на работното место

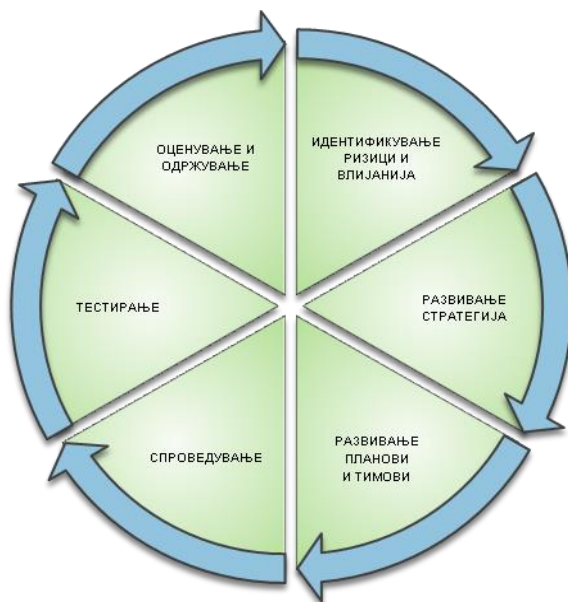
Персоналот треба да се охрабри да го прифати принципот „безбедноста на прво место“ како навика во и надвор од работното место:

- Кога се издаваат пристапни дозволи во вид на картички, тие треба рутински да се носат од страна на персоналот кога се наоѓаат во просторијата и да ги остават при напуштање на просторијата. Исто така, персоналот треба да се чувствува охрабрен за да реагира кога некој не носи пропусница и да пријавува секаква загриженост.
- Да се одржува политика на „чисто биро“ каде што сите документи, листи, клучеви и сите други подвижни вредни предмети да можат да се заклучат, дури и кога просториите остануваат без надзор. Треба да се обезбедат средства за отстранување/уништување на отпадот (како што се шредерите), така што чувствителните или комерцијалните документи да можат да бидат уништени, наместо да се остават за собирање, а печатачите и фотокопирите секогаш да бидат расчистени од хартиите.
- Да се обезбеди пристап до чувствителните области - на пр. серверски простории - само за оние на кои вистински им е потребен, со менаџери одговорни за издавање и отстранување на правата за пристап.
- Да се воспостават јасни правила за прилики, кога персоналот може да земе комерцијално чувствителен материјал и да ги изнесе надвор од просториите/канцелариите на организацијата. За највредните предмети може да биде соодветно да се бара претходна согласност од управителите со формален запис за нивното изнесување и враќање назад.
- Воспоставување доверлива телефонска линија или е-пошта каде вработените можат да известуваат за евентуални загрижености, а во согласност со тоа треба да се понудат и внатрешни и надворешни телефонски броеви за оние кои работат од далечина.
- Да се бара сите посетители да се регистрираат на приемот и да бидат придружувани во секое време. Пропусниците издадени на посетителите треба да ги нудат само најосновните права за пристап и мора да бидат вратени на излез. Во зависност од природата на организацијата, можеби е најсоодветно посетителите да ги оставаат мобилните телефони и сличните уреди уште на главниот влез.

9. Планирање деловен континуитет

Планирањето на деловниот континуитет⁵⁶ е процес преку кој организацијата/компанијата настојува да создаде систем за превенција и закрепнување од потенцијални закани, како што се внатрешни или

надворешни напади, функционални пропусти и проблеми, природни непогоди, катастрофи или сајбер-напади. Ваквиот процес е дизајниран за да ги заштити персоналот и имотот и да осигури дека тие можат да функционираат повторно ефикасно во случај на катастрофа. Развиените планови треба да се тестираат и ажурираат за да се провери дека немаат слабости и недостатоци, а доколку се утврдат и идентификуваат, тие треба и да се коригираат.



Слика бр. 3. Процес на составување план за деловен континуитет⁵⁷

Планот за деловен континуитет⁵⁸ е, всушност, план за одржување на операциите и враќање на деловните активности во нормала како резултат на терористички напад или поголемо нарушување.

Планот за деловен континуитет е суштински дел од планирањето на мерките и активностите како одговор при потенцијален напад на организацијата. Во него се утврдува како ќе продолжи да функционира организацијата по некој случен инцидент и како се очекува да се врати во нормала во најбрз можен рок.

Овој план не мора да биде специфичен за терористички инциденти и треба да се однесува на какви било поголеми нарушувања, како што е пожар, поплава или проблем со струјата.

Подготовката на планот бара важни одлуки за средствата во рамките на организацијата кои, без разлика на околностите, не смее да се изгубат и временските рамки во кои операциите мора да продолжат.

Самиот план ги утврдува договорените аранжмани за ставање под контрола на ситуацијата, потребните ресурси за одржување на

критичните деловни функции и персоналот потребен за координирање на активностите.

Достапен е широк спектар на совети за развој и одржување на планот, но следните принципи се највообичаени.

Првиот чекор е да се идентификуваат средствата и процесите кои се клучни за деловното работење, со цел полесно да се разбере деловното функционирање:

- Кои улоги и поединци се неопходни за извршување на деловните обврски?
- Каква опрема, транспорт и слично ќе му треба на персоналот за да ги одржува активностите?
- Кои оддели се неопходни за спроведување на активностите и договорните обврски?
- Кои добавувачи и други трети страни се составен дел од секојдневните рутини?

За секое идентификувано средство, треба да се земат предвид три клучни прашања:

1. Кое би било кумулативното влијание врз организацијата доколку ова средство биде нарушено за одредени периоди на време, како што се почетните 24 часа, 48 часа, неколку дена и така натаму?
2. Колку брзо мора да се врати?
3. Кои алтернативни ресурси се достапни?

Процесот на подготовки за континуитет ги потенцира активностите што може да се преземат предвреме за да се подобри отпорноста, како на пример:

- Вкрстена обука за вештини меѓу работната сила.
- Процедури за документирање, така што делегираниот персонал може да изврши непознати задачи.
- Договорена опција за преместување во и надвор од просториите (на пр. простории за состаноци кои можат брзо да се претворат во работни места).
- Далечински пристап до информатичко-комуникациските системи во номинирани локации за резервна копија.
- Алтернативни извори за производство на опрема.
- Безбедно чување резервни копии на податоци и вредна документација.
- Договорени методи за вонреден контакт со вработените, добавувачите, клиентите итн.

Потоа, планот треба да ги претстави сите чекори што вработените се очекува да ги следат по инцидентот со цел да се одржат

основните активности и да се вратат во „нормално деловно работење“ колку што е можно поскоро.

Структурата и деталите на планот варираат од бизнис до бизнис и од локација до локација, но, генерално, треба да ги вклучат:

- Околностите/условите за воспоставување просторија за инциденти и кој треба да го пријави тоа.
- Планови за одговор и комуникација за справување со првичното закрепнување.
- Јасни улоги и делегирани одговорности.
- Фактори кои одредуваат делумна или целосна евакуација на просториите.
- Како ќе се обезбеди прва помош и насочување на толпата.
- Поддршка за лица со посебни потреби, ограничена подвижност или други потреби.
- Кога и како ќе се користат алтернативни сместувачки капацитети и објекти.
- Аранжмани за вонредни состојби за критични трансакции и операции - нарачки за клиенти, прием на испорака, производство и др.
- Договорени процедури за повторно започнување со рутинските операции.

Сите вработени нема да бидат во можност да добијат нови инструкции среде инцидент. Во одредени ситуации, на некои вработени може да им се доделат одговорности што претходно не ги извршувале. Затоа, планот треба да биде инклузивен и достапен ресурс насочен кон сите страни, вклучително и оние надвор од организацијата. Тој мора да биде јасно претставен, да се избегнуваат нејасни внатрешни референци и кратенки и да се структурираат на таков начин што луѓето можат брзо да најдат и да разберат што се очекува од нив.

Планот треба постојано да се ажурира како одговор на промените во рамките на организацијата. Организирањето редовни проби и вежби ќе помогне во запознавањето на персоналот со процедурите и доуредување на деталите во рамките на планот. На пример, звукот за алармирање во случај на бомба може да се разликува од звукот на алармот при пожар, па точката на собирање може да биде подалеку за да се избегнат околните оштетени згради и така персоналот треба да ги разбере разликите и зошто е тоа така.

Претходните подготовки, вежби и проби значително може да помогнат во реагирањето на персоналот во организацијата во случај на инцидент.

Среде голем инцидент може да има малку време да се размисли за тоа какви активности е потребно да бидат преземени. Овие моменти може да бидат стресни и напнати, евентуално влошени од недостаток на информации за тоа што се случило и ако се очекува понатамошно нарушување. Медиумите ќе се обидат да го утврдат обемот на инцидентот, додека службите за итни случаи ќе ги следат нивните сопствени процедури додека не добијат дополнителни детали.

Кога планот за деловен континуитет ги утврдува дејствијата, одлуките и аранжманите за вонредни состојби за закрепнување на операциите, планот за одговор помага да се формира првичното постапување сè додека не станат достапни следните факти: како ќе се управува со инцидентот, од кого и од каде и како, ресурсите и информациите, ќе бидат достапни за оние кои ќе управуваат со ситуацијата.

Аранжманите во планот за деловен континуитет може да бараат одреден персонал да преземе одговорност за првичниот одговор помогнат од номинираните членови на персоналот со релевантно знаење за производството, односите со засегнатите страни и поддршка за информатичко-комуникациската опрема.

Сепак, мора да има одредена флексибилност - присуството за време на инцидентот може зависи од пристапот, особено ако инцидентот се случи надвор од работните часови, а некои вработени може да бидат номинирани едноставно затоа што живеат доволно блиску за да обезбедат поддршка.

9.1. Командна соба за инциденти

Во поголемите организации можно е да се обезбеди област во која брзо може да се постави просторија за инциденти (или, ако просторот дозволува, таа трајно да се одржува). Ова е достапна и сигурна просторија во која номинираниот персонал ќе се состане за да собере информации, да ги следи случувањата и да ги координира упатствата веднаш по настанот. Секундарна локација, идеално надвор од организацијата, може да не се земе предвид, во случај ако претпочитаната просторија е недостапна.

Меѓу задачите што треба да се извршат во просторијата за инциденти е водењето дневник во кој се евидентираат времето и релевантните активности редоследно како што се случуваат. Ова не само што ќе помогне при примопредавањето, за да се следи генералниот напредок, туку може да помогне и како информација за анализата по настаните.

Собата за инциденти во случај на вонредна ситуација може да работи 24 часа и затоа треба да биде опремена со соодветен мебел, информатичко-комуникациска технологија, канцелариски материјал, ТВ и радио и, доколку е можно, сместување. Претходно подготвениот пакет за одговор, исто така, треба да биде достапен за персоналот во ваквата просторијата за инциденти.

Пакетот за одговор треба да содржи клучни документи и предмети што може да им бидат потребни на оние кои ќе управуваат со просторијата за инциденти или ќе работат со службите за итни случаи. Содржината на овој пакет е дадена во продолжение, но, сепак, овие списоци не се исцрпни и треба да се додадат други предмети по потреба.

Документи:

- План за деловен континуитет и планови за комуникација.
- Контакти со детали на номинираниот персонал за одговор, плус список со сите вработени, нивните адреси и мобилни броеви.
- Контакти со детали на службите за итни случаи.
- Детали за какви било локални комунални претпријатија, организации за спасување, градежни изведувачи, локални власти надлежни за планирање на вонредни состојби.
- Планови за градење вклучувајќи ја локацијата на местата каде се складираат енергенси, електричната енергија и водата и контролите за греење и вентилација. Исто така, сите заштитени подрачја каде што ќе биде евакуиран персоналот.
- Ажурирана листа на залихи и опрема.
- Финансиски и банкарски информации.
- Списоци со производи и спецификации.

Опрема:

- Самостоен лаптоп-компјутер, компатибилен со локалната мрежа.
- USB мемориски стикови.
- Резервни клучеви / безбедносни шифри.
- Факел и резервни батерии.
- Лента за опасност и кордонска лента.
- Мал паричен ресурс.
- Картички и маркери за привремени знаци и друг канцелариски материјал (пенкала, хартија, итн.).
- Активен мобилен телефон со полнач.

10. Комуникациски планови

Комуникациите⁵⁹ се од суштинско значење при случен инцидент. Со цел пораките да бидат точни - и да се избегне забуна или ширење на дезинформации - специфичните задачи треба да бидат распределени на релевантен, искусен персонал.

Во случај на сериозен инцидент, ќе има потреба што поскоро да се известат персоналот за тоа што се очекува од секого да направи. Ова треба да биде преку тестирани канали за внатрешна комуникација, како што се системот за јавни адреси, сигнали за е-пошта, интранет или какви било табли/патокази за известување во комуналните области.

Сите пораки треба да бидат јасни и содржајни. Ако има какви било упатства за персоналот да ги следи, важно е да не се бараат премногу активности одеднаш. Луѓето со поголема веројатност ќе одговорат на едно или две упатства отколку на цел список.

Брзиот одговор може да биде од суштинско значење (особено ако персоналот ги следи медиумските извештаи), затоа треба да се постават претходно подготвени обрасци за соопштенија на персоналот.

Треба да се искористат целосно внатрешните комуникации за да се информираат вработените за каква било истрага која е во тек, како и за евентуални застои и блокади на локалните патишта и јавниот превоз.

Во случај на целосна или делумна евакуација, во одредена фаза ќе има потреба да се ажурираат оние што се собрани во заштитените подрачја или местата за евакуирање, па затоа е неопходно да се има соодветна комуникација до овие точки.

Доколку веќе не е вклучен во плановите за вонредни состојби, треба да се размисли за уредување на одреден договорен модел за вонредни каскадни пораки кај вработените. Каскадата подразбира секој менаџер на тимот да биде одговорен за контактирање со неговите директни вработени. Персоналот треба да биде запознат со тоа како ќе работи каскадата и како ќе се обезбедува редовно ажурирање на нивните контакт детали.

Планот за деловен континуитет и планот за одговор го идентификуваат водечкиот контакт за службите за итни случаи, но може да има потреба да се контактира со други надворешни чинители за да се понудат ажурирања, на пример:

- Централна и/или друга локација во рамките на деловното работење.
- Просторија за планирање вонредни состојби.
- Соседни организации.
- Комунални компании.
- Друштво за осигурување.

- Клиенти и добавувачи.
- Големи акционери.

Во секој случај, комуникацискиот план треба да даде до знаење кој е одговорен за одржување контакт. Во некои случаи, тие ќе бидат координатори на просторијата за инциденти, но во други може да биде соодветно тоа да бидат вработените со релевантни работни односи, знаење или овластување. Контактите со детали треба да се чуваат во кутијата за итни случаи.

Целокупната координација со службите за итни случаи треба да оди преку претходно номинирани лица со соодветна надлежност во рамките на организацијата. Службите за итни случаи може да бараат детали од плановите за пребарување и детали за какви било познати жртви или области на локацијата што може да станат опасни. Исто така, како практика треба да се прифати дека на местото на настанот се следат упатствата на службите за итни случаи.

Доколку самата организација е вклучена директно или се наоѓа во близина на голем инцидент, разбирливо е дека ќе има загрижени роднини и пријатели кои бараат информации. При големи инциденти, може да се постави телефонска линија за врска со службите за итни случаи и секоја јавна веб-страница треба да се ажурира со детали за овие броеви.

Можеби е соодветно да се обезбеди листа со овие телефонски броеви за вработените.

Во зависност од сериозноста на инцидентот, можеби е неопходно да се биде во контакт со локалните или дури и националните медиуми кои можат да вршат притисок за итна информација и реакција.

Доколку одредени вработени во организацијата се запознати со односите со медиумите, сите вакви прашања треба да продолжат да бидат насочени кон нив, за да се избегне ризикот од објавување и пренесување неточни детали. Можеби е тешко да се спречи персоналот или заинтересираните за настанот да даваат коментари или да користат мобилни уреди, да споделуваат слики, но, што се однесува до сопствениот официјален одговор на организацијата, информациите треба да бидат точни и соодветни колку што дозволува ситуацијата.

Треба да се дистрибуираат низа одобрени одговори на медиумите со релевантни надворешни страни, за да помогнат во координирањето на пораките. Доколку е потребно, треба да се даде формална изјава за медиумите, за да се обелоденат фактичките информации и, што е можно повеќе, да се разјасни што се случило, што се презема и кога ќе бидат достапни дополнителни информации.

11. Индикатори за подготвување или постоење терористички активности

Како и организираните криминални групи, така и терористичките организации треба да планираат и подготвуваат, купуваат и складираат материјали и да најдат начини за финансирање на нивните активности. Голем дел од овие активности се прават пред очите на јавноста. Затоа, доколку работниците за приватно обезбедување забележат или слушнат нешто невообичаено и сомнително, потребно е да го пријават и да ја известат локалната полициска станица. Секоја информација што може да биде директно или индиректно поврзана со одредени терористички активности може да им помогне на безбедносните органи да спречат извршување терористички акт и да спасат одредени животи.

За таа цел, постојат одредени индикатори за препознавање знаци и однесување на сомнителни лица кои може да бидат поврзани со терористички активности:⁶⁰

- **Складирање:** Одредени објекти, како што се гаражи, бараки, подруми и сл., може да бидат искористени од страна на терористите за складирање оружје и опрема. Доколку се сомневате и забележите некој да изнајмува вакви објекти потребно е да се пријави.
- **Хемикалии:** Доколку некој купува специфични хемикалии во поголеми количини во одреден временски интервал без некоја очигледна причина, тогаш тој може да биде на листата на сомнителни лица.
- **Заштитна опрема:** Ракувањето со хемикалии или изработка на импровизирани експлозивни направи е опасно без заштитна опрема. Доколку забележите оставена или расфрлена заштитна опрема, тогаш може да се заклучи дека таа била користена токму за таква намена.
- **Финансирање:** За извршување на терористичките напади потребни се финансиски средства кои терористичките организации ги обезбедуваат на различни начини. Измамата со кредитни картички е еден од тие начини. Во случај да забележите сомнителни трансакции од страна на одредени лица, потребно е да го пријавите.
- **Документи за идентификација:** Терористите најчесто користат лажни лични документи. Доколку познавате некого кој има повеќе лични документи со различни имиња и фотографии, автоматски влегува во кругот на сомнителни лица.

- Надзор: При планирање и подготовка на терористичките напади, терористите често вршат надзор над потенцијалните објекти на напад. Доколку забележите некој да фотографира одредени заштитени објекти или објекти од критичната инфраструктура потребно е да го пријавите.
- Патување: Состаноците, обуката и планирањето на некој терористички напад може да бидат на различни локации во една држава или во повеќе држави. Од таа причина доколку воочите некого кој патува често, а има сомнителна работа и остварува приходи, може да предизвика одредено сомневање.
- Комуникација: Комуницирањето помеѓу членовите на некоја терористичка организација најчесто се врши телефонски, но често тоа се при-пејд телефонски броеви или украдени телефонски уреди. Во случај некој често да го менува неговиот телефонски број или да поседува повеќе телефонски апарати без некоја посебна причина, влегува во сомнителна активност. Исто така, ако некој често посетува веб-страници кои се поврзани или споделуваат одредени содржини со тероризам или активно промовираат или воздигнуваат терористички активности, тогаш постои опасност да западне под одредени влијанија.

Исто така, при извршување на секојдневните рутински задачи, работниците за приватно обезбедување треба да забележуваат одредени сомнителни однесувања како:

- Луѓе во стационирани возила што набљудуваат одредени објекти од критична инфраструктура.
- Возила што се движат полека во близина на одредени објекти и се паркираат во сомнителни околности.
- Луѓе што користат опрема за фотографирање и снимање или прават одредени белешки или скици за одредени безбедносни детали на некој објект.
- Луѓе кои се сомнителни, а користат специфични места за влез и излез, како скали, ходници или места за евакуација.
- Луѓе кои подолго време се задржуваат во определен објект без некоја причина и евидентираат персонал, посетители, испораки и сл.
- Луѓе коишто поставуваат детални или невообичаени прашања во врска со распоред на објекти, безбедносни планови, користење паркинг и сл.

ДЕЛ III

АКТИВНОСТИ ПО ИЗВРШЕН ТЕРОРИСТИЧКИ НАПАД

1. Реагирање при извршен терористички напад

Терористичките напади не се исклучени во работењето на работниците за приватно обезбедување. Никој не сака да размислува за терористички напад, но важно е работниците за приватно обезбедување да бидат подготвени доколку се случи таков настан. Терористички напади може да вклучуваат употреба на вооружени напади, експлозиви, запаливи материи, биолошки и хемиски агенси кои предизвикуваат штетни влијанија во повеќе области. Несаканите ефекти врз здравјето на лицата присутни на местото на инцидентот може да бидат катастрофални и зависат од видот на нападот, а работниците за приватна безбедност треба да бидат обучени да одговорат на ваквите видови напади.

Во случај на терористички напад во објектот што се обезбедува, одговорот на работниците за приватно обезбедување треба да биде најжесток и со сите расположливи средства.

Во случај на напад, првиот чекор е објавување тревога, односно најитно треба да се информира одговорниот за обезбедување на објектот и веднаш да се информира полицијата, за да се побара помош. Доколку одговорниот за непосредно спроведување на обезбедувањето е времено или трајно онеспособен, тогаш тоа треба да го стори некој од останатите членови на тимот.

При терористички напад, покрај тоа што е загрозувана безбедноста на објектот, загрозувани се и животите на припадниците на безбедносниот персонал кои вршат обезбедување, животите на луѓето кои се вработени во објектот, како и животите на луѓето кои случајно се нашле на местото на инцидентот. Работниците за приватно обезбедување во вакви ситуации согласно со законите и подзаконските акти, можат да употребат оружје во самоодбрана и да го заштитат објектот што го обезбедуваат, но секогаш мора да внимаваат да не пукаат кон нејасна мета. Затоа терористите во вакви ситуации се во предност, бидејќи сакаат да ја остварат нивната цел без разлика на сè.

Употребата на огнено оружје е најтешка и најнепопуларна мерка. Работникот за приватно обезбедување може да употреби огнено оружје кога на друг начин не може да одбие непосреден противправен напад со кој се загрозува неговиот живот или животот на лицето или имотот што го обезбедува. Она што е важно е дека пред употребата на огнено оружје, работникот за приватно обезбедување гласно го предупредува лицето за намерата за употреба на огнено оружје. Доколку е неизбежна

примената на огнено оружје се инсистира, доколку е можно, да се испукаат еден до два куршуми во воздух, за да се покаже сериозноста на работникот за приватно обезбедување и неговата решеност да пристапи кон гаѓање во жива цел. Употребата на огнено оружје е забранета:

- доколку со тоа се доведува во опасност животот на други граѓани;
- против бремена жена чија бременост е видлива, дете и старец, освен ако овие лица со огнено оружје или со други опасни средства непосредно го загрозуваат животот на работникот за приватно обезбедување или на лицето кое се обезбедува; и
- при обезбедување јавни собири и други настани.

2. Пружање прва помош на местото на нападот

Обезбедувањето на работното место или областа која се заштитува е многу важна работа. За да се реализира ефикасно, работниците за приватно обезбедување треба да бидат подготвени за вонредни ситуации. Во рамките на обуката за оспособување и полагање за лиценца за приватно обезбедување има и обука која се однесува за пружање прва помош и заштита⁶¹. Со неа работниците за приватно обезбедување треба да се стекнат со индивидуална сигурност, знаење и подготвеност доколку некогаш треба да пружат прва помош. Важно е да се биде подготвен за медицински итни случаи и инциденти во секојдневниот живот, но особено е важно во работна позиција, каде што треба да се помага и да се служи на јавноста. Бидејќи може да се случи работниците за приватно обезбедување да бидат единствените лица со обука за прва помош во близина, кога ќе се појави некој итен случај, тие треба да можат да дејствуваат брзо и да им помогнат на сите оние на кои им е неопходна таква помош.

Знаењата од прва помош и нудењето третман на повредено или болно лице во случај на напад пред да бидат повикани и да пристигнат медицинските лица, може да го зачува животот и да спречи понатамошни повреди кај жртвите. Персоналот на брзата помош, полициските службеници и пожарникарите повикани на местото на вонредната состојба се познати како „лица за прва реакција“, но сè додека не пристигнат, работниците за приватно обезбедување се единствените на местото на настанот кои може да пружат прва помош. Исто така, работниците за приватно обезбедување кои се обучени за прва помош, не само што можат да обезбедат грижа пред да пристигне медицинската екипа, туку можат да споделат информации за текот на настаните и состојбата со жртвите заштедувајќи драгоцено време на медицинските екипи.

Според тоа, првата помош е непосредна, почетна нега на лице кое е повредено пред пристигнувањето на квалификуван медицински тим. Тоа е помошта дадена на секое лице кое претрпело ненадејна повреда со грижа за да се зачува животот, да се спречи влошување на состојбата и да се овозможи опоравување.

Во случај на вонредни ситуации - напади, работниците за приватно обезбедување треба да ги преземат следните чекори:

- Потврдете дека службите за итни случаи (полиција, прва помош и противпожарна екипа) се известени.
- Набљудувајте го местото на настанот заради очигледни опасности, како што се: пожар, чад, паднати електрични водови, поплава и нејасни опасности.
- Внимавајте на опасните ситуации: несоодветни временски услови, компромитирано возило или структура и пожар што не е ставен под контрола. Знаењето како да се одговори во вакви случаи, е многу важно.
- Управување со местото на настанот.

Пред да пристапат кон пружање прва помош⁶² на лицата на кои им е потребна, работниците за приватно обезбедување секогаш треба да бидат претпазливи за каква било опасност која е во тек, која може да им го загрози и нивното здравје. Тие треба да се обидат да им помогнат на другите луѓе, само ако е тоа безбедно и возможно.

Пружање прва помош при извршени напади со опасни хемикалии

- Бидете внимателни да не пренесете никаква хемиска супстанција на себе.
- Повикајте брза помош или побарајте некој друг да повика ако вие веќе помагате на жртвите.
- Побарајте од жртвата да ја отстрани контаминираната облека и накит од зафатените области на телото.
- Исплакнете ги изгорените места на телото со многу вода - ако немате вода, тоа може да се направи и со безалкохолен пијалок.

Пружање прва помош при напади со прободување или пукање

- Прво, проверете дали е безбедно да им помагате на другите.
- Започнете со упатување на жртвите кои се подвижни на безбедно место.
- Ако жртвата е свесна, диши и крнави, прво, треба да се одвлече на безбедно место, а потоа да се направи обид да се сопре крварењето.

- Ако жртвата не е свесна, треба да се постави во положба за опоравување.
- Не треба да се допира или преместува оружјето на местото на настанот.
- Не треба да се извлекува нож или друг предмет од која било рана на жртвата, бидејќи тоа може да предизвика поголемо крвање и оштетување.
- Покријте ја раната со нешто чисто.
- Чувајте ги жртвите затоплени - покријте ги со ќебе или со палто.
- Не им давајте ништо да јадат или пијат.
- Разговарајте со нив тивко и смирено за да ги смирите.

Ако сте повредени:

- Секогаш треба да бидете сигурни дека сте безбедни.
- Притиснете ги раните ако крвавите или нека ви помогнат другите околу тоа.
- Исто така, можете да им посочите на другите луѓе што да прават и како да си помогнат самите на себе.

Пружање прва помош при напади со горење

- Бидете претпазливи од каква било опасност од пожар, топлина, хемикалии или електрична енергија.
- Третирајте ги изгореницата со ладна истечна вода најмалку 10 минути.
- Отстранете ги накитот или тесната облека во близина на изгорениците.
- Не нанесувајте облека или креми.
- Побарајте медицински совет и чекајте ја екипата на првата помош да пристигне.

Пружање прва помош при напади со експлозија

- Местото на настанот може да претставува опасност предизвикана од оштетувањето на објектите, од пожарот, електричната инсталација, гасот и сл. Во најбрзо време треба да се напушти областа.
- Ако не можете да заминете, внимавајте на каква било опасност во тек.
- Ако постои можност експлозијата да е дел од терористички напад, не треба да се користи мобилен телефон, бидејќи може да активира секундарна направа.

- Ако е безбедно и возможно, тогаш треба да се започне да им се помага на жртвите.
- Започнете со упатување на жртвите кои се подвижни на безбедно место.
- Ако жртвата обилно крвави, тогаш обидете се да го контролирате крвавењето.
- Ако жртвата не е свесна, треба да се постави во положба за опоравување.

Доколку жртвата крвави обилно:

- Најпрво заштитете се - ставете ракавици или користете пластични ќесиња или крпи за да избегнете контакт со крв, доколку можете.
- Врзете ја или покријте ја раната со облека, крпи или слично.
- Притиснете на раната или кажете ѝ на жртвата да врши притисок врз неа - и продолжете да притискате додека не пристигне помошта.
- Држете ја жртвата свесна и одржувајте ја топла, покриена со палто или со ќебе.

Ако жртвата не може да го напушти местото на инцидентот:

- Ако жртва не се движи, нежно треба да се протресат рамената за да се утврди дали ќе реагира.
- Ако е безбедно да се зборува тивко со нив, замолете ги да направат нешто - на пр. „отвори ги очите“ и видете дали ќе реагираат. Ако одговорот, проверете дали нивните дишни патишта се функционални и побарајте знаци на крварење.
- Ако жртвата не е свесна, треба да се постави во положба за опоравување и да се продолжи со пружање помош на следната жртва.

Проверете ги дишните патишта на жртвата:

- Ако жртвата зборува нормално, тогаш нејзините дишни патишта се во ред.
- Ако не зборува нормално или се бори да диши:
 - Поставете ја едната рака на челото на жртвата.
 - Поставете два прста под брадата на жртвата.
 - Подигнете и ја брадата и наведнете ѝ ја главата нежно спрема тилот.

Проверете дали диши:

- Ако не сте сигурни дека жртвата диши, погледнете, слушајте и чувствувајте дишење до 10 секунди.
- Дали може да го почувствувате нивниот здив на образот?
- Дали може да видите движење на градите или на абдоменот?
- Ако жртвата диши, треба да се постави во положба за опоравување.
- Ако жртвата не диши - за жал, нема многу што да се направи во тој случај.
- Треба да се премине со пружање помош на следната жртва.

Пружање помош и справување со шок

- Помогнете на секоја жртва да седне или да легне.
- Уверете ги дека помошта доаѓа.
- Чувајте ги жртвите затоплени.
- Не им давајте ништо да јадат или да пијат.

Настаните, како овие, се многу стресни за сите инволвирани лица. Повеќето ги надминуваат многу добро, но некои лица се здобиваат и се соочуваат со одредени психички стресови, трауми или подолги проблеми. Затоа, важно е, за настанот да се разговара со некој близок, со пријател, колега или да се побара помош од психолог, ако сте загрижени или исплашени поради тоа што се случило.

Исто така, за потребите на пружање прва помош, во објектите кои се обезбедувани од работници за приватно обезбедување, неопходно е да постојат соодветни планови во случај на терористички напад. Планот треба да го содржи следното:⁶³

- Однапред да се разгледаат и координираат договорите за заемна помош и локациите за медицинско постапување земајќи ги предвид проценките за посетеност на објектот;
- Обука и подготовка на персонал и волонтери кои може да бидат повикани во случај на напад да пружаат прва помош и да ги пренесуваат повредените во медицинските установи;
- Организирање и развивање програми за обука на обични граѓани кои како случајни минувачи може да помогнат за време на инциденти со голем број на жртви;
- Пренесување на повредените со нетрадиционални превозни средства до медицинските установи без притоа да ги блокираат влезовите на нивните објекти или местата за итни случаи;

- Во случај на напад да се повикаат сите најблиски медицински установи да помогнат со приемот на жртвите, иако можеби тие не се надлежни.

3. Евакуација

Постапувањето во итни случаи е специјализирана работа наменета за професионалци. Работниците за приватно обезбедување треба да бидат подготвени и да постапуваат во итни случаи со давање соодветен одговор во зависност од нападот.

Може да се бара евакуација на просториите заради:

- Закана насочена директно кон просториите.
- Закана или инцидент на друго место што е известно од страна на полицијата.
- Откривање на сомнителен предмет во или во близина на зградата.

Во зависност од големината и локацијата на бизнисот, плановите за евакуирање на просториите треба да ги опфатат и околностите и аранжманите за спроведување целосна евакуација, делумно евакуација или евакуација во внатрешно безбедно подрачје, како што е заштитниот простор.

Најголемата дилема со која се соочува секој одговорен за план за евакуација е како да се оцени каде е најбезбедното место. На пример, ако трасата за евакуација ги тера луѓето да минуваат во близина на сомнителниот уред надвор од зградата или преку област за која се смета дека е контаминирана, евакуацијата можеби не е најдобриот тек на дејствување и треба да се земат предвид внатрешните заштитени простори.

При планирањето на патот за евакуација, важно е да се обезбедат луѓето и да се држат настрана од другите области, каде што би можело да дојде до детонација на втор уред.. Активностите треба да вклучуваат брзо пребарување на точката за собирање, за да се осигури дека е ослободена од сите други уреди.

Општиот принцип е ако уредот е во зградата, тогаш размислете за евакуација, ако уредот е надвор од зградата, можеби е побезбедно да се остане внатре. Без разлика на околностите, кажете им на надлежните во полицијата за акцијата која ја преземате што е можно поскоро.

Во случај на сомнително писмо или рачно направена бомба, евакуирајте ја просторијата, засегнатиот кат и двата ката над и под засегнатиот кат.

Упатствата за евакуација треба јасно да бидат дефинирани и претставени на патиштата. Сместувањето на поширок простор може да

нема сидови што можат да заштитат од експлозии и фрагменти или ходници кои нудат патеки за евакуација, па затоа се важни мерките, како што се застаклување со непробојно стакло и јасно дефинирани, редовно проверувани излезни правци. Назначете лица да постапуваат како маршали и како контакти, откако ќе се достигне збирната точка.

Може да бидат потребни посебни ангажмани за секој персонал со инвалидитет, бремените жени и посетителите.

Збирните точки треба да бидат оддалечени најмалку 500 метри од зградата. Општо, се советува дека две збирни точки се идентификуваат - во спротивни насоки - кои, веројатно, ќе бидат подалеку од зградата од која било одредена точка за собирање при аларм за пожар. Во случај на повеќе возила-бомби, на пример, ова растојание треба да го одведе персоналот безбедно зад полициските кордони - иако би било препорачливо да се има алтернатива оддалечена околу 1 км. Избегнувајте користење на паркиралишта како места за собирање.

Секој план за евакуација треба да биде договорен со службите за итни случаи, локалните власти и соседите и да се обезбеди дека секој припадник на службата за обезбедување со специфични одговорности е соодветно обучен и плановите редовно се проверуваат.

Најважното прашање кое треба да се реши е кој да нареди евакуација во ситуации на висок ризик. Најчесто, доколку постојат планови, е одредено кој може да нареди. Меѓутоа, во поново време бојазливоста од одговорност за преземање евакуација која може да предизвика застој во процесот на работа и позначајни материјални штети, заради прекилот, е голема одговорност. Поради таквата ситуација ретко кој би си дозволил да повика на евакуација, ако не е стриктно овластен тоа да го направи, нормално до доаѓање на полициските сили или на јавниот обвинител, зависно од конкретната ситуација. Во институциите кои се под ингеренции на владата, најчесто највисокиот по звање може да нареди евакуација. Меѓутоа, можно е тој да не биде во можност да биде информиран за состојбите, па затоа мора да се предвидат алтернативни решенија кои јасно ќе бидат одредени во плановите за вонредни ситуации. Тој којшто наредува евакуација која би можела да биде и со можен ефект на губење на муштериите во подолг временски период (хотели, ресторани, институции од културно забавниот живот - кина, театри), создавање паника, можни повреди при санацијата, оштетување имот и средства во позначителен обем, треба да е свесен за последиците посредно и непосредно. Меѓутоа, доколку ситуацијата налага задолжителна евакуација, а не ја нареди, поради бојазливост од губење профит и создавање чувство на несигурност кај вработените и клиентите - посетителите, муштериите, околината или

предизвикување на потешки, па и фатални последици, одговорноста повторно е негова. Поради ваквите ситуации, лицата од обезбедување посакуваат лицето кое ќе нареди евакуација да биде од највисоките менаџерски редови. Менаџерските тимови, пак, секогаш сакаат одговорноста да ја префрлат кон пониските ешалони на вработени, заради избегнување на товарот на одговорност. Во вакви случаи, најдобрите практики покажуваат дека потребно е формирање кризни тимови или штабови кои ценејќи ја објективната ситуација колективно носат одлука за евакуација и ја делат одговорноста. Тој начин, можеби е најдобар и поради избегнување на субјективноста и егоизмот во сите ситуации на зголемена опасност по безбедноста. Согласно со тоа, потребно е да се формираат тела или овластат поединци кои ќе можат да наредат евакуација.

4. Пребарување

Редовните прегледи на просториите треба да бидат дел од секојдневната рутина.

Редовните прегледи се важен дел од секојдневното добро раководење со организацијата. На пример, целото пребарување може да се вклучи како дел од деловната рутина секој ден. Особено, пребарувањата треба редовно да се вршат кога има зголемено ниво на одговор или безбедносно предупредување во областа.

Подготовка на план за пребарување

Планот за пребарување ќе зависи од околностите на секоја посебна локација, но целта е секогаш да се обезбеди дека целата област редовно се пребарува. Покрај главните јавни и оперативни области, планот треба да обезбеди дека се вклучени околните терени и паркиралиштата, како и скалилата, излезите во случај на пожар, ходниците, тоалетите и лифтовите итн.

За да може пребарувањето полесно да се управува, поголемите организации би можеле да размислат да ги поделат своите простории во посебни сектори и да им обезбедат на работниците за приватно обезбедување списоци со проверки - потпишани по завршувањето - за да обезбедат дека ниедна област не останала непроверена.

Пребарување за време и по евакуацијата

Во случај да бидат евакуирани просториите, однапред треба да се направат претреси на уредените места за собирање, насоките кон нив и околните области за да се обезбеди дека нема некакви секундарни опасни уреди.

Исто така, треба да се изврши целосен преглед на просториите пред повторното враќање на персоналот на деловните активности. Ова е одговорност на деловната активност, а не на службите за итни случаи. Полицијата притоа ја презема одговорноста за пребарувања во кои било соседни јавни места.

Правила за вршење пребарување:

- Назначете координатор за пребарување за надгледување на постапката и врска со лицата задолжени за пребарување.
- Започнете со пребарување преку издавање порака преку систем на договорена комуникација (можеби кодирани за да се избегне непотребно нарушување и тревога), преку текстуална порака, преку лично радио или преку телефонска врска.
- Поделете ги приоритетните локации на области со управлива големина за еден или двајца пребарувачи. Идеално, персоналот треба да пребарува во парови, за да се осигура дека ништо не е пропуштено.
- Обезбедете дека оние кои вршат преглед се запознати со подрачјата и за она што вообичаено би очекувале таму. Тие не треба да бидат експерти во експлозивни или други уреди, но можат да препознаат сè што не треба да биде таму или не е на местото на кое треба да биде.
- Да развијат соодветни техники за персоналот да може рутински да пребарува јавни области без да ги алармира присутните посетители или клиенти.
- За време на пребарувањето, посебен фокус се става на: области што се отворени за јавноста; какви било затворени области како што се кулоари, скали, ходници и лифтови; какви било патеки за евакуација и места за собирање; паркиралишта и други надворешни области, како што се стока или места за товарање.
- Под никакви околности не треба да се допира или преместува на некој начин сомнителниот предмет откриен при претресот. Полицијата треба да биде веднаш информирана и тие ќе обезбедат соодветен одговор.
- Да се провери планот за пребарување со локалната полиција и редовно да се вежба.

5. Обезбедување на местото на инцидентот

Терористички напади продолжуваат да се случуваат на настани со отворен пристап, масовни собири и надвор од периметарот на обезбедените настани, евентуално заради перцепираниот недостаток на

безбедност, достапноста на објавените распореди и во голема мерка неограничен прием. Примери на настани со отворен пристап се маратони, паради, протести, митинзи, фестивали, пазари на земјоделци и сл. Терористите, исто така, би можеле да изберат места во близина на големи спортски настани или концерти. Преку напредно планирање и разбирање на вообичаени заговори и тактики за напад кон јавни настани, работниците за приватно обезбедување и оние кои ги организираат настаните, треба да бидат подготвени да ги спречат, да одговорат на нападот и да ги ублажат ефектите од можни терористички напади. Без разлика на големината на настанот, местото и локацијата, соработката на сите засегнати страни, како и споделување на информациите ќе ја зајакне безбедноста и ќе ја подобри реакцијата во итни случаи.⁶⁴

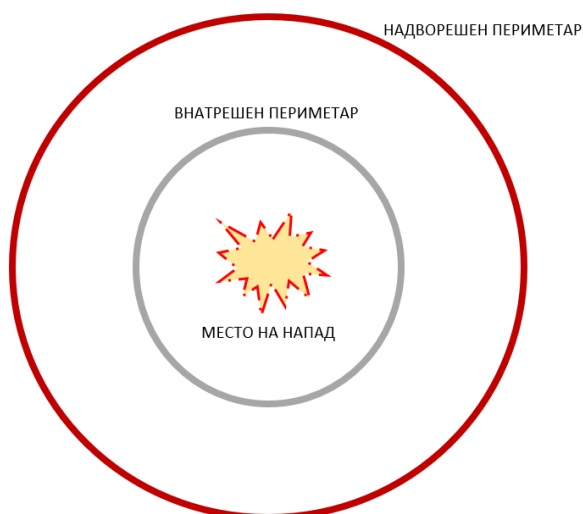
Критичката инфраструктура стана мета на нови форми на терористички закани, познати како сајбер-тероризам, биотероризам, екотероризам, нуклеарен-тероризам и други. Ова укажува на можности и зголемени ефекти на терористички закани кои потешко се контролираат и управуваат.

Работниците за приватно обезбедување кои први реагираат на местото на инцидентот, потребно е личната безбедност да ја третираат како најважна. Доколку се извршил терористички напад, тие треба, прво, да се заштитат себеси за да можат да ги заштитат останатите. Постапувањето на местото на ваков настан може да вклучува влегување во опасна зона. Опасноста постои, бидејќи терористите на тоа подрачје може да имаат поставено секундарни уреди наменети да ги убијат или повредат оние кои први реагираат на местото на настанот.

Обезбедувањето на местото по извршен терористички напад се спроведува, како и кај останатите извршени кривични дела. Разликата е во итната состојба и брзото реагирање кое се бара од страна на работниците за приватно обезбедување.

Физичките докази може да бидат клучни за поврзување на сторителот со местото на настанот. Препознавањето, собирањето и зачувувањето на физичките докази може да биде единствениот начин за идентификување и успешно гонење на одговорните за терористичкиот напад.

Утврдувањето на безбедносниот периметар е од големо значење за постапување по извршен терористички напад. Безбедноста на периметарот опфаќа изолација и контрола на пристапот на сите лица поврзани со реагирање при итни случаи. Основни елементи на безбедносниот периметар се процедурите за надворешниот периметар и процедурите за пристап до внатрешниот периметар.



Слика бр. 4. Приказ на местото на настанот

Надворешниот периметар опфаќа физички бариери составени од ограда, бетонски сидови или некој друг вид бариера која не го дозволува или го ограничува пристапот до местото на инцидентот. Утврдувањето на надворешниот периметар го заштитува местото на инцидентот од надворешно влијание овозможувајќи целосна контрола на пристапот под раководство на една служба за безбедност. Постапките за ограничување на пристапот и контролата на влезот на местото кој е ограден со надворешниот периметар и обезбедуваат механизам за контрола на пристапот во внатрешниот периметар.

Ефективната периметарска безбедност на местото на инцидентот е од суштинско значење при итна реакција од терористички напад. Основни елементи во оваа фаза се:

- Заштита на службите кои први реагираат и јавноста: Брзата и ефикасна контрола на местото на инцидентот ги штити службите кои постапуваат во итни случаи од опасностите кои постојат од потенцијални секундарни напади. Безбедноста на периметарот, исто така, ја спречува јавноста да не нанесе штета на местото на инцидентот, односно да се спречи негова контаминација.
- Зачувување на доказите: Постапувањето на периметарот им помага на безбедносните служби во зачувувањето на доказите за истрага за терористичкиот напад.

6. Заштита на местото на настанот преку ограничување на пристапот

Активностите за контролирање, идентификување, отстранување на лица од местото на настанот и ограничување на бројот на лица кои влегуваат во местото на настанот и нивното движење, претставуваат важна одговорност на работникот за обезбедување кој прв пристигнува на местото на настанот. Изгубени или компромитирани докази значат изгубени можности. Газењето по просторот на местото на настанот, а кое често се случува, докажано е дека секогаш е многу штетно за истрагата. Често, овие упаѓања резултираат со тоа поосетливите судско-медицински техники, како што се анализа на траги и споредба на ДНК, да не се откријат или да не се развијат успешно за употреба. Ова може сериозно да попречи на процесот на спроведување на истрагите и на конечниот исход на гонењето. Форензичарите одговорни за собирање на доказите на местото на настанот ја знаат безвредноста на постапката на собирањето доказен материјал од местото на настанот, ако во тој простор се движеле голем број лица. Затоа, лицата за обезбедување кои први ќе пристигнат на местото на настанот, веднаш по пристигнувањето вршат идентификација на сите лица присутни на местото на настанот и го контролираат нивното движење. Работникот за обезбедување кој е поставен на предниот влез на местото на настанот, мора да ги евидентира сите посетители вклучувајќи име и организациска единица на која ѝ припаѓаат, чинот или официјалниот статус или дозвола за влез, причината заради која се тука и времето на пристигнување и напуштање на местото на настанот. Апсолутно ниеден незапишан посетител не смее да влезе во местото на настанот.

За да се зачува интегритетот на местото на настанот и за да се зачуваат доказите и да се минимизира нивната контаминација, од суштинска важност е да се спроведе контрола на движењето на лицата на местото на настанот и ограничување на бројот на лицата кои влегуваат внатре. Притоа, се легитимираат сите лица на местото на настанот и со поседувањето список со имиња на лица чиј влез е дозволен, преку кој се врши проверка на идентитетот, се утврдува целта на влезот на местото на настанот, како и видот на влезот (привремен, селекционен и сл.).

Осомничените може да бидат на местото на настанот ако е потребно, но на сигурно место, одделно во присуство на полициска, вооружена заштита.

Сведоците исто така може да бидат присутни на местото на настанот, само ако тоа е потребно, но на сигурно место, одделно и под придружба.

Со случајните минувачи треба да се изврши разговор со цел да се одреди дали тие можеби се потенцијални сведоци за да се продолжи постапување со нив на начин предвиден со закон, а ако пак не се потенцијални сведоци, тогаш да се отстранат од местото на настанот.

Пристапот на жртвите, членовите на семејствата и пријатели треба да се контролира (да се држат понастрана од местото на настанот), или се дозволува нивно присуство на местото на настанот само тогаш кога треба да им се искаже помош или сочувство.

Медицинскиот и друг помошен персонал треба целосно и накратко да се информира во врска со процедурите за влез и пристап на местото на настанот, а по потреба се придружуваат. Никој освен медицинскиот персонал под придружба, нема пристап до местото на настанот, значи потребно е да се чека за одобрување или пристигнување на назначениот одговорен инспектор. Постојат точно определени основи за присуство на полицаец, без разлика на неговиот чин, а истото важи и за претставник на цивилната власт поради официјално информирање или поради други утврдени причини. Нема да се дозволи влез на кое и да било неовластено лице, без разлика на личната желба да се присуствува на местото на настанот (пр. службени лица за спроведување на законот, но кои не работат на случајот и без разлика што се старешини, политичари и претставници од медиумите).

Информирањето во врска со местото на настанот е единствен начин, можност, одговорниот инспектор да биде запознат со сите релевантни информации кои може да имаат директно влијание врз тоа како понатаму ќе се постапува во истрагата.

Правилната процедура за ова известување вклучува:

- Користење белешки за забележување на преземените дејствија на работникот за обезбедување кој прв пристигнал на местото на настанот, за да се обезбеди подробна евиденција на сите случувања сè до пристигнувањето на одговорниот надлежен инспектор.
- Опис на сите дејствија преземени од страна на одговорниот работник за приватно обезбедување заради обезбедување и зачувување на интегритетот на местото на настанот; укажување помош на жртвите; белешките кои се направени за релевантните надлежни лица; проценка на расположливите факти; легитимирање; лоцирање и обезбедување на достапност на која и да било жртва или сведоци кои имаат сознанија во врска со кривичното дело; какво и да било информирање во врска со положбата и местото на живеење на жртвите; идентификација и опис на осомничениот.

- Помагање во определување на официјални параметри на местото на настанот.
- Предавање одговорности во врска со документацијата која се однесува на влез и излез на местото на настанот;
- Останување на местото на настанот сè до целосно завршување на увидот.

Сублимирано, работникот за приватно обезбедување при обезбедување на местото на инцидентот потребно е да ги преземе следните дејствија:

- да го задржи сторителот ако е затекнат на местото на настанот или ако е фатен од други лица;
- да преземе мерки и активности за укажување прва помош на настрадани лица;
- да ја ограничи привремено слободата на движење на затекнатите лица со цел да го обезбеди местото на инцидентот;
- да издаде соодветни предупредувања и наредби;
- да го прегледа визуелно објектот, просторот и предметите кои се наоѓаат на местото на инцидентот;
- да ги прегледа лицата, предметите и превозните средства;
- да го провери и утврди идентитетот на затекнатите лица и предмети;
- привремено да ги одземе предметите кои може да послужат како доказ во соодветна постапка;
- да ги заштити трагите и предметите од значење за разјаснување на инцидентот; и
- да забрани снимање на местото на инцидентот.

По пристигнувањето на увидната екипа, работата на работникот за обезбедување на местото на настанот не престанува, само што веќе раководната функција за сите дејствија од тој момент ја има јавниот обвинител. Доколку јавниот обвинител не е присутен, а им дал овластување - наредба за вршење увид на местото на настанот на овластените службени лица на Министерството за внатрешни работи, улогата на раководење со местото на настанот ја презема одговорниот на увидната група. Тој ја води целата ситуација и издава јасни наредби на сите овластени службени лица. Работникот за приватно обезбедување постапува согласно со наредбите и укажувањата на одговорните лица од безбедносните служби, контактира со своите претпоставени и постапува согласно со нивните укажувања. Не е дозволено да го напушти местото на настанот пред за тоа да добие јасни насоки од своите претпоставени, затоа што мора и натаму да го заштити објектот кој му е доверен за обезбедување. Доколку настанот

се случува надвор од местото кое го обезбедува, тогаш може да го напушти објектот кој го обезбедува и да помогне само по консултации и добивање инструкции од своите претпоставени, затоа што може случајот да е монтиран за да го одвлече неговото внимание и да се предизвика отсуство на местото кое го обезбедува што може да претставува замка за да се нападне неговиот објект на заштита и да направи непоправлив пропуст кој може многу да ја чини неговата институција, но и него самиот. Затоа, потребно е секогаш да се одржува врската со своите претпоставени кои мора да бидат запознати со специфични ситуации кои можат да се случат во текот на работењето. Местото на настанот се напушта кога ќе завршат сите активности од страна на увидната и на другите екипи.

По извршеното обезбедување, работникот за обезбедување кој го обезбедувал местото на настанот изготвува службена белешка која покрај податоците од усното известување, содржи и податоци за: работникот за обезбедување и местото кое е обезбедувано; причините поради кои се извршени овие дејствија; времето за известување и пристигнување на местото на настанот, како и за затечените лица на местото на настанот. Во неа се опишуваат преземените дејствија по аналоген ред и со временска рамка и се наведуваат дејствијата кои се преземени како легитимирани лица, евидентирани присутни, состојба при доаѓање и сл. Увидната екипа од Министерството за внатрешни работи, пак, составува записник за извршен увид во кој се наведуваат сите детали на затекнатата состојба, траги и потенцијален доказен материјал, каде сигурно ќе биде наведен и работникот за обезбедување кој прв пристигнал на местото на настанот и неговите преземени дејствија на имотот кој е под надлежност за физичко обезбедување.

Сите наведени документи треба да бидат објективни, со точни податоци, навремени и целосни, затоа што претставуваат илустрација на местото на настанот, додека целосна слика на состојбата и начините на пронаоѓање, фиксирање и подигнување на доказниот материјал изготвуваат одговорните лица од Министерството за внатрешни работи. Мора да се опишат и надворешните временски услови, доколку местото е на отворен простор заради точна илустрација на условите кои биле во тој момент. Службената белешка за преземените дејствија од работникот за обезбедување се дел од документите кои може овластените службени лица да ги побараат и да ги приклучат кон кривичната пријава и главен документ доколку се нареди реконструкција на настанот, а работникот за обезбедување можно е да добие статус на сведок на главната расправа.

ЗАКЛУЧНИ СОГЛЕДУВАЊА И ПРЕПОРАКИ

Генералната цел на трудот беше да се даде теоретски приказ и конкретно објаснување на мерките, активностите и постапките кои се преземаат при заштита на луѓето, објектите и имотот при терористички напади. За таа цел, најпрво беа прикажани индикаторите за заканите, опасностите и ранливостите, со сите нивни специфичности, преку кои може да се идентификуваат подготвителни терористички активности. Понатаму беа прикажани и мерките за заштита од терористички напади, а на крајот беа прикажани и активностите кои се преземаат од страна на работниците за приватно обезбедување во случај на извршен терористички напад.

Во текот на работата на работниците за приватно обезбедување се случуваат итни случаи - вонредни настани, напади, инциденти и сл. Подготвеноста за постапување во вакви случаи е сигурен начин да се реагира ефикасно и да се остане смирен. Поседувањето на потребните вештини овозможува да се биде подготвен доколку се појави итен случај. Знаењата и вештините како да се обезбеди местото на настанот, да се процени ситуацијата, да се испитаат алтернативите за реагирање, да се изберат и спроведат стратегии за одговор, да се распределат ресурси, план за експанзија и демобилизација на настанот и да се повикаат националните безбедносни служби, првата помош и пожарникарите, се клучни аспекти за успешно справување со ваквите настани.

Следните генерални безбедносни препораки⁶⁵ се само неколку активности кои националните безбедносни служби и агенциите за приватна безбедност можат и треба веднаш да ги преземат:

1. Подобрување на заедничката реакција при критични инциденти. Во реалноста, во многу кризи, работниците за приватно обезбедување, а не полицајците, пожарникарите или медицинскиот персонал, се првите лица кои се присутни и одговорни на местото на настанот. На пример, токму работниците за приватно обезбедување, најверојатно, ќе донесат брзи одлуки и решенија за евакуација на згради, ќе активираат безбедносни системи или бариери или ќе ги затворат изворите на хемикалии што протекуваат по извршен терористички напад. Јавниот и приватниот безбедносен сектор треба да соработуваат во обука, планирање на закрепнување и споделување информации. Командните центри за инциденти кои здружуваат различни претставници од владите безбедносни институции треба да вклучат и претставници од приватниот безбедносен сектор.

2. Координација за заштита на критичната инфраструктура. Приватниот сектор ја поседува или штити поголемиот дел од

критичната инфраструктура на државата. Заштитата на таа инфраструктура е совршена задача за јавно-приватна соработка. Службите за спроведување на законот може да споделат разузнавачки информации за евентуални закани, да обезбедат информации за контакт и да предложат постапки за одговор/реакција. Приватните безбедносни компании може да извршат анализа на ранливоста и да ги информираат државните безбедносни служби за местата на кои можеби ќе треба полицијата да одговори.

3. Подобрување на комуникацијата и интероперабилноста на податоците. Секој субјект поседува богати податоци и информации кои може да бидат од голема важност за другиот. Ако државните и приватните служби за обезбедување не можат, воопшто, да ги вмрежат нивните гласовни и податочни системи или ако не можат да го сторат тоа додека ги заштитуваат своите информации, тогаш комуникацијата и соработката ќе бидат сериозно нарушени.

4. Зајакнување на размената на сознанија и информации. Голем дел од соработката лежи во размената на информации. Понекогаш пречката е технолошка (како во претходната точка), но честопати таа е процедурална, правна или само прашање на навика или заинтересираност. Безбедносните служби треба да им дадат на располагање повеќе информации на работниците за приватно обезбедување и да одговорат на нивните легитимни прашања. Од друга страна, работниците за приватно обезбедување треба да ги споделат со државните безбедносни служби информациите за закани, опасности и нелегални активности што ги откриваат во текот на нивното работење. Споделувањето на ваквите информации ќе го подобри развојот на планирањето за постапување во случај на инциденти и катастрофи во заедницата. Нивоата на предупредување од терористички закани од државните безбедносни служби треба да доведат до специфични сигнали за закана врз работењето на работниците за приватно обезбедување. Локалните заедници треба да бидат охрабрани да развиваат јавно-приватно меѓусебно разбирање на влијанието и очекувањата, бидејќи се менуваат нивоата на закана. Треба да се креира систем со кој ќе се обезбедат релевантни разузнавачки информации кои ќе им бидат од корист и на работниците за приватна безбедност.

5. Спречување и испитување на високотехнолошки криминал. Ова подрачје на криминал има значителна вклученост на странски елемент, важност за националната безбедност и националниот економски систем. Најголемиот дел од стручноста за справување со високотехнолошки криминал е токму во приватниот сектор. Тоа е всушност терен за најсилна соработка за јавна - приватна безбедноста соработка и партнерство.

6. Постојана надоградба на постојните и добивање нови сознанија. Криминалитетот, како и тероризмот, секојдневно ја менуваат својата форма, методите, средствата, како и целите на напад. Поради тоа треба постојана надоградба, размена на искуства и рефреширање на вештините, знаењата и стекнатите искуства.

Без разлика дали се креира, разгледува или ажурира безбедносниот план, работниците за приватно обезбедување треба да ги имаат предвид овие генерални безбедносни правила⁶⁶:

- Спроведете безбедносна проценка на ризик за да се идентификуваат заканите со кои може да се соочи организацијата и колкава е нивната веројатност да се случат. Идентификувајте ги постојните и потенцијалните слабости и нивното влијание врз какви било нарушувања на безбедноста.
- Ако се доградуваат или прошируваат простории, разгледајте ги барањата за физичка безбедност веднаш, уште во фазата на планирање. Поевтино и поефективно ќе биде тоа, отколку додавање мерки подоцна.
- Направете ја безбедносната свест да биде дел од културата на организацијата. Овозможете персоналот да биде редовно информиран и осигурајте се дека безбедносните стандарди се целосно поддржани од повисоко ниво.
- Обезбедете добро управување низ просториите. Чувајте ги јавните места уредни и добро осветлени, отстранете го непотребниот мебел и одржувајте ги надворешните области чисти.
- Чувајте ги точките за пристап до објектот на минимум и издајте им на членовите од персоналот и посетителите посебни пропусници, односно картички за евиденција на влез. Кога е можно, не дозволувајте неовластени возила близу до зградата.
- Инсталирајте соодветни физички мерки како што се брави, аларми, надгледување со видеонадзор, дополнително осветлување и заштита со застаклување.
- Одржувајте соодветни процедури за ракување со поштенските пратки, размислете за воспоставување на поштенските сандачиња надвор од главните простории.
- Кога регрутирате персонал или изведувачи на одредени работи и услуги, проверете ги нивните идентитети и препораки.
- Размислете како најдобро да ги заштитите информациите и да преземете соодветни мерки на претпазливост за информатичко-комуникациска безбедност. Осигурајте се дека постојат соодветни одредби за отстранување на доверливиот отпад.

- Планирајте ги и пробајте ги плановите за деловен континуитет и плановите за одговор при инциденти. Проверете дали клучните деловни функции можат да продолжат да опстојуваат за време на разни видови нарушувања.

РЕФЕРЕНЦИ

- ¹ National Policy Summit, Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder, Vital Issues and Policy Recommendations, 2004, p. 14-15
- ² National Policy Summit, Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder, Vital Issues and Policy Recommendations, 2004, p. 5
- ³ National Policy Summit, Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder, Vital Issues and Policy Recommendations, 2004, p. 12-13
- ⁴ Котовчески, М., Борба против тероризмот, Македонска цивилизација, Скопје, 2004, стр. 176
- ⁵ Дојчиновски, М., Оџаков, Ф., Разузнавачки операции, Соларис принт, Скопје, 2010, стр. 178
- ⁶ Милошевић, М., Одбрана од тероризма, Свет књиге, Београд, 2005, стр. 5
- ⁷ Гаџиновић, Р., Тероризам у политичкој и правној теорији, Еврођунти, Београд, 2010, стр. 12
- ⁸ Вујаклија, Лексикон страних речи и израза, Београд, 1954, стр. 947–948
- ⁹ Hofman, B., Unutrašnji terorizam, Narodna knjiga Alfa, Beograd, 2000, стр. 9
- ¹⁰ Bockstette, C., Jihadist Terrorist Use of Strategic Communication Management Techniques, George C. Marshall European Center for Security Studies, Number 20, December, 2008
- ¹¹ Бајагић, М., Основи безбедности, Криминалистичко-полицијска академија, Београд, 2007, стр. 211, Пашански, М., Савремене камиказе – транснационални тероризам и дипломатија, НИРО "Књижевне новине", Београд, 1987, стр. 38–40, Димитријевић, В., Тероризам, Радничка штампа, Београд, 1982, стр. 122–149 и Гаџиновић, Р., Како против тероризма, Младост, Београд, 1996, стр. 26
- ¹² Мијалковски, М., Тероризам, Факултет цивилне одбране, Београд, 2004, стр. 5
- ¹³ Мијалковић, С., Милошевић, М., Обавјештајно-безбједносна дјелатност и службе, Висока школа унутрашњих послова, Бања Лука, 2011, стр. 301
- ¹⁴ Ташковски, И., Танески, Н., Разрешување конфликти и меѓународен тероризам, Скопје, 2018, стр. 45
- ¹⁵ Ташковски, И., Танески, Н., Разрешување конфликти и меѓународен тероризам, Скопје, 2018, стр. 52
- ¹⁶ CTED and UNOCT, The protection of critical infrastructures against terrorist attacks: Compendium of good practices, CTED, UNOCT and INTERPOL, 2018, https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf
- ¹⁷ чл. 2, Council Directive 2008/114/EC
- ¹⁸ Ackerman, G., Assessing terrorist motivations for attacking critical infrastructures, Centre for Nonproliferation Studies, Monterey Institute of International Studies, 2007, <https://e-reports-ext.llnl.gov/pdf/341566.pdf>
- ¹⁹ OSCE, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, 2013, www.osce.org/atu/103500?download=true
- ²⁰ DHS, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, 20 October 2017, www.us-cert.gov/ncas/alerts/TA17-293A
- ²¹ Димовски, З., Тероризам, Графотранс, Скопје, 2007
- ²² Пашански, М., Современи камикази, Књижевне новине, Београд, 1987

-
- ²³ Кеча, Р., Тероризам – глобална безбедносна пријетња - Европски дефендологија центар за научна, политичка, економска, социјална, безбедносна, социолошка и криминолошка истраживања, Бања Лука, 2012
- ²⁴ Кронин, К., О., Лудс, М., Џ., Напад на тероризмот: Елементи на грандиозна стратегија, Скопје, Нампрес, 2009
- ²⁵ Dimovski, Z., Ilijevski, I., Babanoski, K., Intelligence as a key link in the fight against terrorism, International scientific conference Security in the post conflict (Western) Balkans: Transition and challenges faced by the Republic of Macedonia (Security Studies and the Science of Security), Ohrid, 27-28.05.2011, pp. 268-281
- ²⁶ Доревски, З., Атентати - анализа, Безбедност бр. 3, Скопје, 1997
- ²⁷ Велјанов, С., Експлозии и траги од активирана експлозивна направа, Безбедност бр. 4, Скопје, 1996
- ²⁸ Laqueur, W., The New Terrorism – Fanatism and the Arms of Mass Destruction, London, 1998
- ²⁹ Bockstette, C., Jihadist Terrorist Use of Strategic Communication Management Techniques, George C. Marshall European Center for Security Studies, Number 20, December, 2008
- ³⁰ Пашански, М., Современи камикази, Книжевне новине, Београд, 1987
- ³¹ Димовски, З., Илијевски, И., Меѓународен тероризам, Факултет за безбедност, Скопје, 2011
- ³² Hoffman, B., Inside Terrorism (Revised and Expanded Edition), New York: Columbia University Press, 2006
- ³³ Белић, М., Васић, М., Историјско-правни аспект послова обезбеђење одређених личности и објеката, Безбедност, часопис Министарства унутрашњих послова Републике Србије, Београд, 1-2/2009, стр. 114 и Павловић, Н., Модели праћења и процењивање безбедносне ситуације у функцији обезбеђења и заштите одређене личности, специјалистички рад, Криминалистичко-полицијска академија, Београд, 2013, стр. 19
- ³⁴ Jakić, M., Preventivna delatnost u zaštiti lica, 18.01.2012, преземено од <http://vipprotection-miloradjakic.blogspot.com/2012/01/>
- ³⁵ Станковски, Љ., Планови за обезбедување и процена на безбедносната ситуација, Меѓународно научно списание за одбрана, безбедност и мир, Современа македонска одбрана, Министерство за одбрана, Скопје, 2013, стр. 138
- ³⁶ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 5-6
- ³⁷ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 7-8
- ³⁸ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 9-10
- ³⁹ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 11-12
- ⁴⁰ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 13-14
- ⁴¹ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 15-18
- ⁴² Terrorist threats, преземено од https://www.fema.gov/media-library-data/20130726-1455-20490-3893/fema427_ch2.pdf
- ⁴³ преземено од <https://www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch3.htm>
- ⁴⁴ Postal threats, City of London Police, преземено од:

<https://www.cityoflondon.police.uk/advice-and-support/countering-terrorism/Pages/postal-threats.aspx>

⁴⁵ Procedures in case of emergency and terrorist attack, преземено од: [https://www.ed.umed.wroc.pl/sites/default/files/jan.wojna/files/PROCEDURE_IN_CASE_OF_EMERGENCY_AND_TERRORIST_ATTACK_wersja_angielska\(1\).pdf](https://www.ed.umed.wroc.pl/sites/default/files/jan.wojna/files/PROCEDURE_IN_CASE_OF_EMERGENCY_AND_TERRORIST_ATTACK_wersja_angielska(1).pdf)

⁴⁶ CTED and UNOCT, The protection of critical infrastructures against terrorist attacks: Compendium of good practices, CTED, UNOCT and INTERPOL, 2018, p.137, https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf

⁴⁷ Даничић, М., Стајић, Љ., Приватна безбедност, Висока школа унутрашњих послова, Бања Лука, 2008, стр. 120

⁴⁸ Даничић, М., Стајић, Љ., Приватна безбедност, Висока школа унутрашњих послова, Бања Лука, 2008, стр. 128-136

⁴⁹ Dimovski, Z., Krstevska, K., Ilijevski, I., Babanoski, K., Cyber attacks and their real threat for modern world, International scientific conference: The Balkans between Past and Future: Security, Conflict Resolution and Euro-Atlantic Integration, vol. I, Ohrid, Republic of Macedonia, 05-08.06.2013, pp. 634-648

⁵⁰ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 19-22

⁵¹ Dimovski, Z., Ilijevski, I., Babanoski, K., Security-criminalistics dimensions of cyber-terrorist attacks, Thematic proceedings, International scientific conference, Preventing crime and European integrations, with special overview on the hi tech crime, Colege for interior affairs, Department of police education, Ministry of interior of the Republic of Srpska and Hanns Seidel Stiftung, Laktashi, Banja Luka, 28-30.03.2012, pp. 65-77

⁵² Centre for the Protection of National Infrastructure, Personnel and People Security, <https://www.cpni.gov.uk/personnel-and-people-security>

⁵³ Centre for the Protection of National Infrastructure, Ongoing Personnel Security, A Good Practice Guide, edition 3, April 2014, p. 3, <https://www.cpni.gov.uk/system/files/documents/d0/d2/ongoing-personnel-security-a-good-practice-guide-edition-3.pdf>

⁵⁴ Protective Security Requirements, Guide to personnel security for your organisation, February 2018, p. 4, <https://www.protectivesecurity.govt.nz/assets/Personnel-security/e63eedae7c/Guide-to-personnel-security-for-your-organisation.pdf>

⁵⁵ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 23-26

⁵⁶ Kenton, W., Business Continuity Planning (BCP), 01.06.2019, <https://www.investopedia.com/terms/b/business-continuity-planning.asp>

⁵⁷ ICAEW Crisis Management Handbook, <https://www.icaew.com/about-icaew/regulation-and-the-public-interest/business-continuity-plan>

⁵⁸ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 27-30

⁵⁹ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 31-32

⁶⁰ преземено од: <https://www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch3.htm>

⁶¹ SCG Team, Security Guards and First Aid Training, 07.03.2019, <https://securityguardcourse.ca/security-guards-and-first-aid-training/>

⁶² St. John Ambulance, Counter Terrorism Policing, Action Counters Terrorism,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742418/SJA_Public_Advice.pdf

⁶³ Crisis management for terrorist related events, преземено од

https://www.cpni.gov.uk/system/files/documents/de/eb/Crisis_Management_for_Terrorist_Related_Events.pdf

⁶⁴ First responders toolbox, преземено од

<https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/First-Responders-Toolbox---Planning-Promotes-Effective-Response-to-Open-Access-Events.pdf>

⁶⁵ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 26-27

⁶⁶ Centre for the Protection of National Infrastructure, Protecting against terrorism, third edition, 2010, p. 2

- П Р И Л О Ж И -

ПОТЕНЦИЈАЛНИ ОБЛАСТИ ВО РИЗИК

ОБЛАСТ	МЕРКИ И АКТИВНОСТИ
СООБРАЌАЈ	- Утврдете по кои патишта/тунели/мостови се одвива поголем обем на сообраќај. - Идентификувајте ги точките на метеж кои можат да го спречат реагирањето или да ги внесат граѓаните во ранлива област. - Забележете го времето од денот и денот во неделата кога ваквите појави се случуваат.
ТРАНСПОРТ	- Идентификувајте ја локацијата на капацитетите за утовар/истовар на опасни материи за транспорт. - Забележете ги ранливите области како што се мерните станици и местата за одмор низ кои што овој товар може да транзитира.
ВОДЕН СООБРАЌАЈ	- Мапирајте ги цевководите и објектите за обработка/третман на вода (покрај веќе мапираните брани). - Идентификувајте ги летувалиштата и пристаништата за бродови за крстарење, капацитетите за утовар/истовар на товарни бродови и бродови со контејнери. - Забележете какви било меѓународни (странски) бродови (и товарот што го носат) кои вршат бизнис дејност во областа.
АЕРОДРОМИ	- Обезбедете информации за авио превозниците, патеките на летовите, распоредот на аеродромите и типовите на летала што ги користат аеродромските објекти. - Забележете ја локацијата на кулата за контрола на воздушниот сообраќај, пистите, патничкиот терминал и местата за паркирање.
ЖЕЛЕЗНИЦА	- Идентификувајте ја локацијата на шините, клучките, терминалите, тунелите и патничките и карго терминалите. - Обезбедете информации за опасни материи што може да се транспортираат преку железницата. - Забележете ја локацијата на станиците, пристапот до нив и системите за контрола на вентилацијата.
ВЛАДИНИ ОБЈЕКТИ	- Идентификувајте ја локацијата на државните органи и на канцелариите на локалната самоуправа. - Обезбедете информации за локацијата на поштата,

	полициската станица, против пожарната екипа, екипите за заштита и спасување, управување со кризи, радијациона сигурност, градската управна зграда, резиденции на градоначалникот, министерствата, амбасадите итн. - Обезбедете информација и за правосудните објекти. - Мапирајте ги локациите на спомениците, меморијалните центри и истакнатите владини симболи.
РЕКРЕАТИВНИ ОБЈЕКТИ	- Мапирајте ги спортските арени, терени, театри, трговски центри, капацитети на разни здруженија на граѓани и локациите за посебни настани.
СИМБОЛНИ ЗГРАДИ И ЛОКАЦИИ	- Мапирајте ги националните споменици, капацитетите и локациите кои ги преферираат странците итн. - Мапирајте ги потенцијалните области на метеж поврзани со ваквите објекти и локации.
ДРУГИ КАПАЦИТЕТИ	- Мапирајте ја локацијата на финансиските институции и деловните области. - Направете какви било белешки за распоредот на настани во деловната/финансиската област. - Утврдете дали трговските центри или густо населените места во центарот на градот се зафатени од гужва во одредени периоди. - Забележете ја локацијата на специјалните настани кои се од национално значење. - Забележете ја локацијата на истакнати високи згради.
ВОЕНИ ИНСТАЛАЦИИ	- Забележете ја локацијата и типот на воените инсталации.
КАПАЦИТЕТИ ЗА ОПАСНИ МАТЕРИИ	- Мапирајте ги локациите на овие капацитети (како на пример електрани, рафинерии за нафта, магацини за складирање на опасни материи и сл.).
ОБЈЕКТИ ЗА СНАБДУВАЊЕ СО ВОДА	- Забележете ги локациите на станиците за довод на вода од езера или реки. - Забележете ги локациите на цевководи за водоснабдување и местата каде што се резервоарите. - Забележете ги локациите на постројките за третман на вода.
ХРАНА	- Забележете ги локациите на клучните земјоделски капацитети, како што се големите силоси за жито и фарми со добиток.
КОМПЈУТЕРСКИ СИСТЕМИ	- Идентификувајте ги владините и деловни компјутерски системи меѓусебе поврзани и утврдете го нивното ниво на заштита од терористички сајбер-напад.

ПРЕГЛЕД НА ПОЗНАЧАЈНИ ТЕРОРИСТИЧКИ НАПАДИ ВО ЕВРОПА

ДАТУМ	МЕСТО	НАЧИН	ПОСЛЕДИЦИ
26.10.2002	театар во Москва, Русија	земање заложници во театар од страна на терористи	загинати 129 лица повредени 150 лица
15.11.2003	двете најголеми синагоги во Истанбул, Турција	истовремени експлозии на повеќе автомобили-бомби	загинати 23 лица повредени околу 300 лица
20.11.2003	британски конзулат и британска банка во Истанбул, Турција	бомбашки напад извршен од страна на 73 терористи	загинати 33 лица повредени преку 400 лица
11.03.2004	Мадрид, Шпанија	бомбашки напад на возови за локален превоз	загинати 191 лице повредени повеќе од 1.800 лица
02.11.2004	улица во Амстердам, Холандија	убиство на режисер и сатиричар по премиерата на неговиот филм	убиено 1 лице
07.07.2005	Лондон, Велика Британија	четворица атентатори- самоубијци во автобуси и во метрот го активирале речиси истовремено бомбите во нивните ранци	загинати 52 лица, повредени стотици
30.07.2007	аеродром во Глазгов, Велика Британија	цип влетал во хала на аеродромот	повредени 5 лица
11.12.2010	центар на Стокхолм, Шведска	автомобил-бомба експлодирал, а атентатор- самоубиец се разнесол во центарот на градот	повредени неколку лица
02.03.2011	аеродром во Франкфурт, СР Германија	атентатор пукал врз невооружени војници на САД во автобус на аеродромот	загинати 2 лица повредени 3 лица

02.11.2011	редакција на весник во Париз, Франција	фрлени молотови коктели преку прозорите во канцелариите на редакцијата на францускиот сатиричен магазин “Шарли Ебдо”	материјална штета
11-15. 03.2012	Тулуз, Франција	убиства на војници со пукање	загинати неколку лица
19.03.2012	училиште во Тулуз, Франција	убиство во еврејско училиште	загинати 4 лица (3 деца)
18.07.2012	Бургас, Бугарија	напад врз автобус со туристи	загинати 7 лица повредени 30 лица
22.05.2013	Лондон, Велика Британија	прегазен британски војник со автомобил и убиен со ножови и мачета од страна на две лица	загинато 1 лице
24.05.2014	музеј во Брисел, Белгија	вооружен терорист нападнал 4 лица во влезниот простор на Еврејскиот музеј	загинати 4 лица
07.01.2015	редакција на весник во Париз, Франција	двајца атентатори ги нападнале редакциските простории на сатиричниот магазин “Шарли Ебдо”	загинати 12 лица
13.11.2015	Париз, Франција	речиси истовремено на 6 места низ Париз повеќемина атентатори извршиле напади врз барови, ресторани и концертна хала	загинати 130 лица повредени околу 300
12.01.2016	историскиот центар на Истанбул, Турција	напаѓач самоубиец се разнесол со бомба среди туристичка група	загинати 12 лица
22.03.2016	меѓународниот аеродром и метро станица во Брисел, Белгија	напаѓачи со повеќе бомби го нападнале меѓународниот аеродром и метро станица	загинати 32 лица
14.07.2016	шеталиште во Ница, Франција	напаѓач со камион влетал во група луѓе на шеталиштето	загинати 86 лица

19.12.2016	центар на Берлин, СР Германија	напаѓач со камион влетал во група луѓе на Божиќниот панаѓур	загинати 12 лица
22.03.2017	пешачка зона во центарот на Лондон, Велика Британија	напаѓач со автомобил влетал во пешачка зона и избодел еден полицаец	загинати 4 лица
07.04.2017	шопинг-зона во Стокхолм, Шведска	напаѓач со украден камион удрил во толпа луѓе, а потоа и во трговски центар	загинати 5 лица повредени 15 лица
22.05.2017	Манчестер Арена, Велика Британија	експлозија на импровизирана експлозивна направа во салата пред крајот на концертот	загинати 22 лица повредени 60 лица
17.08.2017	улица Лас Рамблас, Барселона, Шпанија	напаѓачи со комбе влетале во толпа луѓе	загинати 13 лица повредени стотина лица
29.05.2018	центар на Лиеж, Белгија	вооружен напад врз полициска патрола	загинати 2 лица
28.09.2018	плоштад во Маријампол, СР Германија	напад со нож на плоштад	повредени 3 лица
11.12.2018	центар на Стразбур, Франција	напаѓач пукал врз група лица за време на Божиќен панаѓур	загинати 4 лица повредени 12 лица
18.03.2019	Утрехт, Холандија	четворица напаѓачи пукале на плоштадот и избегале	загинато 1 лице повредени неколку лица
24.05.2019	Лион, Франција	експлозивна направа поставена пред пекара	повредени 13 лица
05.07.2019	Рејхан, Турција	импровизирана експлозивна направа поставена во автомобил	загинати 3 лица
29.11.2019	Лондон, Велика Британија	напаѓач кој кај себе имал лажна бомба со нож нападнал неколку лица на мост	загинати 2 лица повредени 3 лица

**КОМПАРАТИВЕН ПРИКАЗ
НА ОСНОВНИТЕ ПОДАТОЦИ ЗА ТЕРОРИСТИЧКИТЕ НАПАДИ
ВО ЗЕМЈИТЕ ЧЛЕНКИ НА ЕУ ВО ПЕРИОДОТ 2012-2018**

	2012	2013	2014	2015	2016	2017	2018	просек	ВКУПНО
терористички напади (земји членки на ЕУ)	219 (7)	152 (5)	201 (7)	211 (6)	142 (8)	205 (9)	129 (9)	180 (7)	1.259
повредени	46	9	6	350	379	844	53	241	1.687
настрадани	17	7	4	148	142	68	13	57	399

*(Извор: Извештаите TESAT на Европол,
кои се однесуваат на состојбите и трендовите на тероризмот во Европската Унија)*

**КОМПАРАТИВЕН ПРИКАЗ
НА ОСНОВНИТЕ ПОДАТОЦИ
ЗА ЛИЦАТА ПОВРЗАНИ СО ТЕРОРИСТИЧКИ АКТИВНОСТИ
ВО ЗЕМЈИТЕ ЧЛЕНКИ НА ЕУ ЗА ПЕРИОДОТ 2012-2018**

	2012	2013	2014	2015	2016	2017	2018	Просек	ВКУПНО
приведени лица (земји членки на ЕУ)	537 (17)	535 (14)	774 (16)	1077 (19)	1002 (17)	1.219 (19)	1.056 (18)	886 (17)	6.200
обвинети лица	400	313	444	514	580	565	653	496	3.469
осудени лица	437	336	452	527	587	569	664	510	3.572

*(Извор: Извештаите TESAT на Европол,
кои се однесуваат на состојбите и трендовите на тероризмот во Европската Унија)*

ИЗВАДОК ОД РЕЦЕНЗИЈАТА

Трудот „Заштита при терористички напади“ од авторите **д-р Злате Димовски, д-р Кире Бабаноски и д-р Ице Илијевски** е конципиран како прирачник за работниците за приватно обезбедување, кадрите од областа на јавната безбедност, како и за пошироката заинтересирана јавност. Методолошкиот и предметниот пристап се карактеризираат со настојувањата на авторите целокупната материја да ја приближат кон поновите тенденции за спречување и сузбивање на тероризмот. Во трудот, авторите успеале да ги исполнат основните критериуми за изготвување на еден прирачник и тоа, структурата на содржината на ова автентично и оригинално дело има јасна композиција што значи дека има вовед (проследен со јасен предговор) и содржини (развиени согласно со целите во програмата) кои вклучуваат автентичен наративен дел и практични примери. Содржината е научно заснована и нуди потврдени знаења и информации.

Материјалот претставува основа во проучувањето на постапувањето на работниците за приватно обезбедување, има посебна вредност, разработува актуелна материја и настојува преку научниот пристап и соодветен дидактичен начин да ја претстави материјата која е основа за постапување во функција на откривање, попречување и постапување при терористички напади. Трудот ја одразува својата оригиналност преку фактот дека постои малку литература од оваа област која ја разработува предметната материја, усогласена со позитивната законска регулатива и актуелните начини на реализација на оперативната функција на агенциите за приватно обезбедување.

Користената литература ги задоволува потребите за материјалот, има соодветна застапеност на актуелни наслови, бази на податоци, како и електронски едиции. Тоа укажува дека материјалот е опсежен и искористени се познавања, знаења, вештини и мислења од автентични дела од автори кои ја познаваат материјата и кои имаат издадено соодветни публикации кои се во корелација со разработените тематски целини и содржини.

Авторите употребуваат научно-стручна терминологија во разработуваната материја, употребуваат и презентираат јасна мисла, разбирлив текст и јазик, како и адаптиран израз за работниците за приватно обезбедување кои сакаат да се образуваат, усовршуваат и надоградуваат во оваа област.

проф. д-р Методија ДОЈЧИНОВСКИ

- АВТОРИТЕ -

д-р ЗЛАТЕ ДИМОВСКИ

Злате С. Димовски е роден на 02.10.1966 година во Битола. Докторирал на Институтот за социолошки и политичко-правни истражувања при Универзитетот „Св. Кирил и Методиј“ – Скопје и се стекнал со научна титула доктор по социолошки науки. Во моментот е редовен професор на Факултетот за безбедност – Скопје при Универзитетот „Св. Климент Охридски“ – Битола.



д-р КИРЕ БАБАНОСКИ

Кире Б. Бабаноски е роден на 05.03.1987 година во Прилеп. Докторирал на Факултетот за безбедност – Скопје при Универзитетот „Св. Климент Охридски“ – Битола и се стекнал со научна титула доктор на науки од областа на безбедноста. Во моментот е национален проектен координатор во ДЦАФ Центар за управување со безбедносниот сектор Женева – подружница Скопје.



д-р ИЦЕ ИЛИЈЕВСКИ

Ице Н. Илијевски е роден на 29.06.1986 година во Битола. Докторирал на Факултетот за безбедност – Скопје при Универзитетот „Св. Климент Охридски“ – Битола и се стекнал со научна титула доктор на науки од областа на безбедноста. Во моментот е доцент на Правниот факултет – Кичево при Универзитетот „Св. Климент Охридски“ – Битола.



