**УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ, СОФИЯ**

**СПЕЦИАЛНОСТ „ИНФОРМАЦИОННА СИГУРНОСТ“**

МАГИСТЪРСКА ТЕЗА

за получаване на

образователно-квалификационната степен „магистър“

# ИЗГРАЖДАНЕ НА СИСТЕМА ЗА СИГУРНОСТ СЪС СИГНАЛНО-ОХРАНИТЕЛНА ТЕХНИКА В ЧАСТНАТА ОХРАНИТЕЛНА ДЕЙНОСТ – АКТУАЛИЗИРАНЕ И УСЪВЪРШЕНСТВАНЕ

**СТУДЕНТ:**

АЛЕКСАНДЪР ЛАЗАРОВ
Магистърска програма,
задочно обучение,
Ф№ 291 – ИСМЗ

**НАУЧЕН РЪКОВОДИТЕЛ:**

доц. д-р Г. ПЕТРИШКИ

СОФИЯ, 2016

# С Ъ Д Ъ Р Ж А Н И Е

## Увод

През изминалото десетилетие, частната охранителна дейност в България непрекъснато нараства. По последни сведения на МВР, страната ни заема челно място по престъпност и разходи за охрана.

От своя страна, развитието на частния охранителен сектор предполага разширяване на предлагания комплекс от охранителни услуги. Те са насочени в различни направления: осигуряване безопасност на граждани и икономически организациите (ИО), защита на човешко здраве и живот, опазване на имущество, гарантиране на обществения ред в охраняваните обекти и територии и др.

Охраната се осъществява на системен принцип, разгърнат в две паралелни действия – наблюдение и реагиране, които се поддържат от прилаганите при тях технически системи за сигурност и човешки ресурс. Постоянно нарастващите нужди на граждани и организации изискват, от една страна, техническите системи да осигуряват оптималното извършване на съответните действия, а от друга страна, служителите да са на необходимото ниво на компетентност и възможност за реагиране.

През последните 25 години, у нас се създадоха немалък брой охранителни фирми. Те са специфични организации с нарастващо значение в обществото. От една страна, потокът от хора и карго поражда все по-голяма необходимост от охрана и сигурност. От друга страна, терористичните прояви по света, тяхното активиране и разширяване периметъра им на действие през последните години налагат най-строги мерки при прилагане на охранителните системи във всеки тип стратегически важни обекти.

С оглед на различния вид охранявани обекти, избраната от мене **тема** *„Изграждане на система за сигурност със сигнално-охранителна техника в частната охранителна дейност – актуализиране и усъвършенстване“* стеснява периметъра на изследване до физическа охрана на карго и хора в помещения, до които имат достъп служители във фирмите, разположени на територията на обекта, и оторизирани за получаването на стоката лица.

**Обект** на настоящото изследване е пътят, по който се изгражда една система за сигурност в частната охранителна дейност, базирана на използването на сигнално-охранителна техника и съответния персонал, принципите и факторите, които влияят за създаването на проекта, и намиране на начин за увеличаване на нейната ефективност чрез

актуализиране и усъвършенстване. Използва се за примерен обект „София аерогара – център“, принадлежащ към аерогара София и изпълняващ функцията физическа охрана на карго и хора.

**Мотивите** да избера за моята магистърска теза така дефинираната тема и посочения обект са няколко. Първо, обектът „София аерогара – център“ е от стратегическо значение, заради разположението си в близост до аерогара София. Второ, той обслужва нейно карго като поток стоки от международен мащаб и опасностите от заплахи върху обекта са рефлексия на последствията от застрашеността на самата аерогара. Те са с национални и наднационални измерения, което изисква непрекъснато актуализиране и усъвършенстване на охраната и повишаване на сигурността. Трето, като бивш служител по охраната и сигурността на обекта имам лични наблюдения и известна възможност отблизо да се запозная как функционира охранителната дейност и да разграничa някои нейни недостатъци.

**Актуалността** на изследването е обвързана с непрекъснатото и ускорено развитие на технологиите и препоръките за използването им в частната охранителна дейност. Тя произтича и от развиващите се заплахи, които се базират на достиженията на науката, от слабите места на човешкия ресурс, управлението и организацията на дейността. Международната обстановка днес налага непрекъснато актуализиране, разширяване и усъвършенстване на системите за сигурност чрез техника, технологии, методи и подготвеност на човешките ресурси.

**Предмет** на магистърската теза е откриването на проблемните места в охранителната дейност на изследвания обект, начина за тяхното подобряване, както и изграждане на определена динамика на промени за защита, за постигане на необходимата ефективност.

**Защитаваната теза** е, че като стратегически обект, *„София аерогара – център“се нуждае от постоянно и динамично актуализиране и усъвършенстване на приложения проект за охрана и сигурност. Това може да стане чрез установяване на слабостите, тяхното отстраняване, подобряване на основните компоненти на организацията, най-важни от които са оптималният брой и резултатни функции на внедрената сигнално-охранителна техника, ефективността на човешките ресурси в категориите капацитет и специална подготовка, гъвкавост, адаптивност и ползотворност на мениджмънта.*

*За извършване на подобрението, в настоящата магистърска теза предлагам периодично прилагане на един неизползван досега в охранителната дейност в България* модел за системен подход на изследване, познат в бизнес средите като *„SWOT анализ“. За целта допълнително разработих ясна, функционално-приложна практическа структура на модела, разделена на диференцирани етапи, чрез които организирам работата по проучването на обекта, нейната последователност и подробна структура на извършваните изследователски действия. Чрез така доразработения от мене системен модел могат да се установят слабостите, да се определят силите и благоприятните възможности за повишаване качеството на охранителната дейност и нивото на сигурността за превенция срещу заплахите.*

**Целта** на разработката е да докаже, че чрез прилагане на разработената от мене функционално-приложна структура на модела, с ясно определени етапи на работа със “SWOT анализа”, към реалното състояние на охраната и сигурността на обект „София аерогара – център “, в даден времеви сегмент, може да се постигне актуализиране на стратегията за охрана посредством: 1) *определяне на силите, слабостите, благоприятните възможности и заплахите*, 2) *използване на благоприятните възможности за по-ефективно приложение на сигнално-охранителната техника, както и внедряване на някои допълнителни технически средства*, 3) *използване потенциалните сили на фирмата за подобряване подготовката на охранителите и повишаване мотивацията за работа,* 4) *прогнозиране с висока вероятност на заплахите и адекватно определяне на тяхното противодействие.*

**Задачата** е да демонстрирам прилагането на така обогатения и разширен от мене системен модел за анализ към състоянието и функционирането на системата за охрана и сигурност на посочения обект, *като направя пилотно проучване на*:

- принципите на изграждане на системата за охрана и сигурност на обекта,
- слабите страни на системата,
- благоприятните възможности за тяхното отстраняване,

в резултат на което да се оформи *Предложение* за подобряване на охранителната дейност.

За изпълнението на задачите и постигането на целта се приложи **методически подход**, позволяващ *съпоставяне на възможностите за реализация на преследваната цел с разполагаемите ресурси, за да се изгради бъдеща стратегия, тъй като е наложително подобряването на системата да се извършва като периодичен „нон-стоп процес“.*

**Методологията** на изследването включва: *метод на теоретичния синтез* на литературни източници по темата, *метод на анализа* приложен към проучената проблематика в охранителната дейност на обекта, *метод на наблюдението* на функциите на системата, *съпоставителен метод* приложен спрямо проученото състояние на охраната в даден времеви сегмент и нейната пригодност за противодействие на реалните и вероятностните заплахи, *анкетата като методически подход* за пилотно проучване и установяване на слабите места, *метод на синтеза на резултатите* от проучването и извличане на *предложение* за възможно актуализиране и подобряване нивото на сигурност на обекта.

**Приносът** на магистърската теза е разработената от мене функционално-приложна структура на SWOT анализа с 4 подробно описани етапа. Чрез използването на така разширения и детайлизиран системен модел доказвам, че дори при пилотното му прилагане с проучване само на един негов параметър – *слабости*, могат да се разкрият важни взаимозависимости между параметрите *сила*, *слабости*, *благоприятни възможности* и *заплахи* на изследвания обект в даден времеви отрязък, за да се направи адекватно предложение на стратегия за подобрение ефективността на сигурността. Впоследствие чрез периодично извършване на системни анализи на променящите се условия в други времеви сегменти да се очертават по-нататъшните промени в стратегията и да се правят необходимите подобрения. Така една стройна система от SWOT анализи ще поддържа стратегията на охраната актуална и ще постига нейното непрекъснато усъвършенстване.

Принос са и разработените от мене примерни взаимоотношения между отделните параметри – корелации, чиито анализ може да бъде разширяван и задълбочаван, в зависимост от конкретните характеристики на изследвания обект и поставените цели.

**Структурата** на магистърската теза включва Увод; Глава I. *Изграждане на система за сигурност със сигнално-охранителна техника (СОТ 161) в частната охранителна дейност;* Глава II. SWOT анализ – успешен подход за актуализиране и усъвършенстване на системата за сигурност*;*

Заключение: Предложение. Приноси. Приложимост; Използвана литература; схеми, таблици, илюстрации.

Уводът въвежда в актуалността на темата и запознава с моите основни мотиви да я разработя. Представя тезата, целите, задачите и приложената методология, както и подчертава нейния принос.

В Глава I представям синтезиран теоретичен обзор на литературни източници, които имат за обект принципите и етапите на изграждането на системата за сигурност със сигнално-охранителна техника (СОТ 161) в частната охранителна дейност. В нея правя преглед и на прилаганите у нас основни технически средства за защита и принципите на тяхното действие. Накрая включих някои добри европейски примери за актуални промени в охраната и сигурността на сродни обекти, които според мене, могат да послужат за ориентир в дейността по усъвършенстване на сигурността в България.

В Глава II запознавам накратко с успешния в световния бизнес, но малко известен в България системен подход за изследване, наречен *SWOT анализ*. Моето твърдо убеждение е, че той може ефективно да се използва както за въвеждане на проект за охрана, така и за периодично актуализиране и усъвършенстване на вече действащата система за сигурност. За тази цел разработих една практически ясна функционално-приложна структура на метода, конструирана в четири етапа.

Тук представям накратко и обект *„София аерогара – център“,* към който частично приложих *SWOT анализа*, с цел да направя пилотно проучване на слабостите в сигурността на обекта. За целта изготвих Анкета, специално насочена към слабите места на разглеждания обект. В тази глава представям анкетата, обобщените резултати от нея и моя подробен анализ на показателите и корелациите на компонентите, характерни за обекта. От резултатите и анализа извлякох факторите, които определят моето Предложение за подобрение на сигурността на обекта.

В Заключението включвам Изводи, Предложение за подобрение на сигурността на обекта, Приноси и Приложимост на разработената магистърска теза.

**Обемът** на работата е 80 страници, от които 75 страници текст, 3 страници схеми, таблици, илюстрации, 2 страници библиография.

**Основна трудност** при разработването на магистърската теза беше осигуряването на фактологически материал за прилаганата система за охрана и сигурност, нейните цели, задачи и стратегия, сигнално-

охранителна техника, нейното разпределение и точно местонахождение, реално функциониране на проекта към момента на проучването на обекта. Запазването на конфиденциалност не разрешава да се прави точно изброяване и класифициране на използваната сигнално-охранителна техника, ограничава достъпа до писмени материали по въпроса, стеснява информацията до минимум. Ето защо защитата на тезата е изготвена по твърде оскъдна писмена информация, предоставена и приета за разрешена от ръководството на обект „София аерогара – център“. Използвани са главно личните наблюдения на автора на магистърската теза, като бивш служител в охраната на посочения обект, наблюденията на другите охранители, както и персоналните разговори с други административни служители. Проведената *Анкета* срещна трудности за осигуряване на по-голям брой анкетирани лица охранители, тъй като числеността им е ограничена.

# ГЛАВА I

# ИЗГРАЖДАНЕ НА СИСТЕМА ЗА СИГУРНОСТ СЪС СИГНАЛНО-ОХРАНИТЕЛНА ТЕХНИКА (СОТ 161) В ЧАСТНАТА ОХРАНИТЕЛНА ДЕЙНОСТ

В тази глава правя кратък синтезиран теоретичен преглед на *методиката*, по която се изгражда една система за охрана и сигурност. Тя включва *принципите*, от които трябва да се ръководи, *етапите* и *последователността* на действията, които трябва да се следват, използваната *сигнално-охранителна техника* и ролята на *човешките ресурси*, без които е немислимо нейното функциониране.

Преди всичко е логично да започна със законовата основа, която има основополагаща ръководна роля при изграждането на система за сигурност със сигнално-охранителна техника в частната охранителна дейност. На

първо място, задължително е спазването на действащия **Закон за частната охранителна дейност** (ЗЧОД), обнародван в ДВ. бр.15 от 24 февруари 2004 г., заедно с направените изменения и допълнения през годините до 2014 г.[1] Той урежда обществените отношения, свързани с частната охранителна дейност, нейното административно регулиране и контрол.

Смятам, че при изграждането на системата за сигурност от първостепенно значение е да се конкретизира обхватът на нейното действие. Ето защо трябва да се обърне особено внимание на Чл.2, ал. 1 от **Закона**, който дава определение за частна охранителна дейност: „дейност по охрана на обекти, на мероприятия и на лица, и на техни права и законни интереси от противоправни посегателства.“[2] Същността на дейността и използваната сигнално-охранителна техника налагат съобразяването и с още два закона: **Закон за националната служба за охрана**[3] и **Закон за специалните разузнавателни средства**[4].

При пристъпване към осъществяването на конкретен проект за охрана и сигурност, трябва да се спазва и чл. 3. от ЗЧОД, който определя *принципите* при изграждане и осъществяване на частната охранителна дейност:

(1) зачитане на правата, свободите и достойнството на гражданите;
(2) взаимодействие с органите на МВР в борбата с престъпността и опазването на обществения ред;
(3) гарантиране на сигурност и безопасност в охраняваните обекти;
(4) осъществяване на превантивна дейност въз основа на анализ на причините и условията за правонарушения в охраняваните обекти.[5]

От цитираното дотук, мога да направя логичния извод, че тези ръководни принципи обхващат голям обем *информация*, която характеризира охранявания обект, охраняваните лица, охраняваната стока или информацията на организацията, но така също и тази за служителите по охраната и сигурността. Твърдо съм убеден, че *информацията се явява основен параметър за изграждане модела на охранителната система. Тя е ключов фактор от решаващо значение за постигане на определена степен на сигурност с така приложения модел*.

---

[1] http://www.lex.bg/en/laws/ldoc/2135479817
[2] Пак там
[3] http://www.lex.bg/bg/laws/ldoc/2136588571
[4] http://lex.bg/laws/ldoc/2134163459
[5] http://www.lex.bg/en/laws/ldoc/2135479817

Оттук мога да направя изключително важното заключение, че събирането на вярна и точна информация в предварителния етап на проучвателната дейност, както и нейното актуализиране след изграждане и внедряване на охранителния модел, е от първостепенно значение за успешна охранителна дейност. От своя страна, работата с информация изисква спазването на няколко закона: **Закон за защита на личните данни**[6], **Закон за достъп до обществена информация**[7], **Закон за защита на класифицираната информация**[8].

На практика, базовата информация, обхващаща жизнената сфера на даден обект, място и време, от които се изхожда за разработване на проект за охрана, не е константна величина – тя е твърде динамична и променяща се във времето. Този факт налага непрекъснати промени и в някои звена на системата за сигурност.

При изграждането на охранителна система е необходимо да се спазва определена *последователност от действия*, които трябва да бъдат съобразени с множество *фактори*, определящи окончателната оценка на съществуващия риск, обобщения образ на нарушителя, неговите очаквани действия, силите и слабостите на организацията, удобните случаи и благоприятните възможности за заплахи и за реагиране, възможните заплахи, човешкия ресурс и пр.

Оценката на съществуващия риск за сигурността на обекта се определя от вероятността от нежелано действие или угроза от него (кражба саботаж, вандализъм и т.н.) и сериозността на последиците. Необходима е и внимателна преценка за възможните нарушители, определяне на целите и начина им на действие. Важен фактор са слабостите на организацията: служителите, които биха могли да сътрудничат за враждебните действия, характеристиките на обекта и създадената организация на работа (влизане и излизане от обекта на собствения персонал и външни лица), които биха могли да улеснят потенциалния нарушител, управлението на организацията, и пр.

Сигурността е и *осъзнаване на остатъчния риск, след като са взети съответните мерки*. Съотношението сигурност–риск е обратно пропорционално, т.е. голяма сигурност–малък риск и обратно. Работата за

[6] https://www.cpdp.bg/?p=element&aid=373
[7] http://lex.bg/laws/ldoc/2134929408
[8] http://www.dksi.bg/bg/Regulatory+Framework/Law+and+Regulation/promeni+v+ZZKI_20_11_07.htm

откриване на рисковите места е работа за защита, ето защо тя има приоритетно значение. Вероятността от заплахи за фирмата е константа, изменя се само нейната величина. Това налага условията за сигурност да се поддържат и актуализират през цялото време на съществуване на охраняванията обект.

Днес сигурността може да се гарантира само чрез изграждане на *непрекъснато развиваща се комплексна система за сигурност*. Разработването и използването на тази система изисква ясна информационна стратегия и ресурсно осигурен модел на нейния жизнен цикъл, съгласувани с общата концепция за сигурност и развитие на охраняваната организация.

Теорията и практиката в сигурността са установили, че при проектиране, изграждане и експлоатация на съвременна система за сигурност би трябвало да се съблюдават следните *работни принципи*:

- Системата за сигурност е задача на ръководителя на организацията;
- Внедряване на комплексна система за сигурност;
- Развиване на системата с увеличаване на заплахите;
- Сигурността и заплахите се изграждат върху научни постижения;
- Не съществува абсолютна сигурност;
- Прилагане на принципа за икономическа целесъобразност при изграждане, експлоатация и модернизация на системата за сигурност;
- Осъществяване на динамично равновесие между оптимални вътрешни ресурси и оптималното им управление.

## 1. Същност и структура на системата за сигурност

Теорията на системния анализ показва, че ефективността и качеството на всяка система се определя не от характеристиките на най-качественото й звено, а от най-слабото. Това означава, че трябва да бъдат старателно изследвани всички звена на системата и особено внимание да се обърне на нейните слабости. Точно този възглед положих в основата на моето проучване на обект „София аерогара – център“ и специално изготвих Анкета, насочена към *слабостите* в нейната охранителна организация.

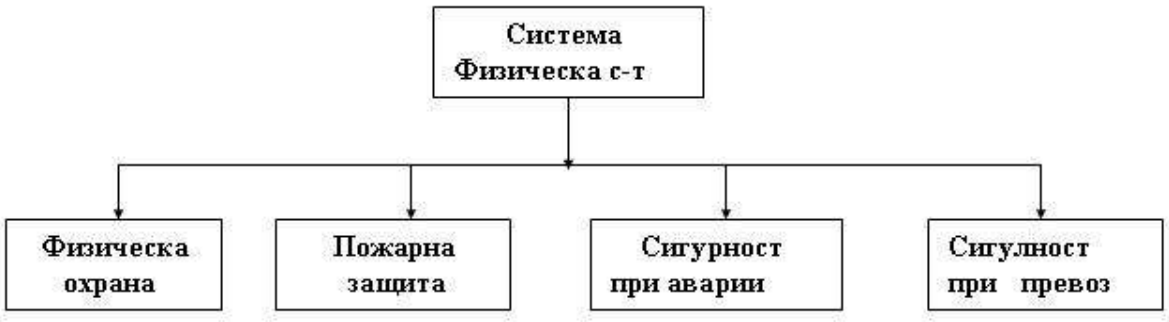
Правилната стратегия при проектиране на една система за сигурност е едновременно и хармонично изграждане на всички нейни компоненти. Това я определя като сложна комплексна система, в която трябва да се

търсят характеристиките и взаимозависимостите между нейните съставни части. Системата е структурирана от няколко подсистеми: А) *физическа сигурност и охрана*, Б) *вътрешна сигурност,* В) *външна сигурност,* Г) *сигурност на информационната система.*

А) *Физическа сигурност и охрана*

Физическата охрана е една от най-често търсените услуги. В комбинация с внедрена сигнално-охранителна техника и поддържана от развиващите се технологични иновации, тя осигурява най-високо ниво на сигурност.

Задачата на физическата охрана е да защити физически човешките и материалните ресурси на организацията. Тя има разклонена структура, съставена от четири подсистеми, ориентирани към защита от различни по характер заплахи: а) физическа защита, б) противопожарна защита, в) защита от природни бедствия и технологични аварии, г) защита при транспорт (на пари, валута, ценности, ценни книжа и стокови потоци) (фиг.1).




Фиг.1. Структура на системата “Физическа сигурност и охрана”.

Комплексното функциониране на четирите подсистеми осигурява условия за едновременност и максимална бързина за вземане на решение за адекватно реагиране срещу възникналите заплахи.

За да свържа теорията в тази глава с практиката в моето конкретно изследване, бих обобщил, че в основата на дейността на обект „София аерогара – център“ лежи физическата охрана за защита на физически човешки и материални ресурси на множество организации. Впрочем, физическата охрана се явява основен характерен белег на охранителната система като цяло. Сигурността във функционирането на посочената тук

подсистема е от изключително значение за настоящата разработка и поради това беше поставена в центъра на вниманието на проучването.

Б) *Вътрешна сигурност*

Структурата на вътрешната сигурност се определя от нейната главна задача: осигуряване лоялността на служителите, сигурност на комуникационните линии и информационните системи, сигурност на информационните потоци (вътрешни и външни, официални, служебни и поверителни, кореспонденцията на организацията) (фиг.2).


Фиг.2. Структура на системата "Вътрешна сигурност"

От схемата е видно, че компонентът „човешки ресурси" играе основна роля във взаимоотношенията на всички съставни елементи на структурата, тъй като човекът е този, който движи информационните потоци чрез съответните комуникативни средства. Това означава, че резултатът от действието на подсистемата „вътрешна защита" се определя от степента на

лоялност на служителите и тяхното отношение към сигурността в организацията.

Отчитайки този факт, смятам за важно да подчертая, че изготвената от мене Анкета проведох именно сред служителите по охраната на обекта, между които се включих лично като бивш охранител. Направи ми силно впечатление, че във всички лични наблюдения и изразени мнения личеше лоялността на служителите, от една страна, и тяхната заинтересованост от качеството на функциониране на проекта по сигурността, от друга страна. Те се оказаха изключително информативни за проучването по магистърската теза.

В) *Външна сигурност*

Системата за външна сигурност обхваща външните за организацията условия, които включват ситуацията, участниците в нея и принципите, които я движат. Задачата й е да гарантира надеждна и устойчива работа на фирмата в заобикалящата я външна среда (фиг.3).


Фиг. 3. Структура на системата "Външна сигурност"

И тук схемата показва, че лоялността на човека, в този случай външните за организацията клиенти и партньори, има преимуществено значение. Отново компонентът „човешки ресурси" се явява водещ за постигане на сигурност. Това налага да се обърне голямо внимание върху „човека" като служител, партньор, клиент, конкурент.

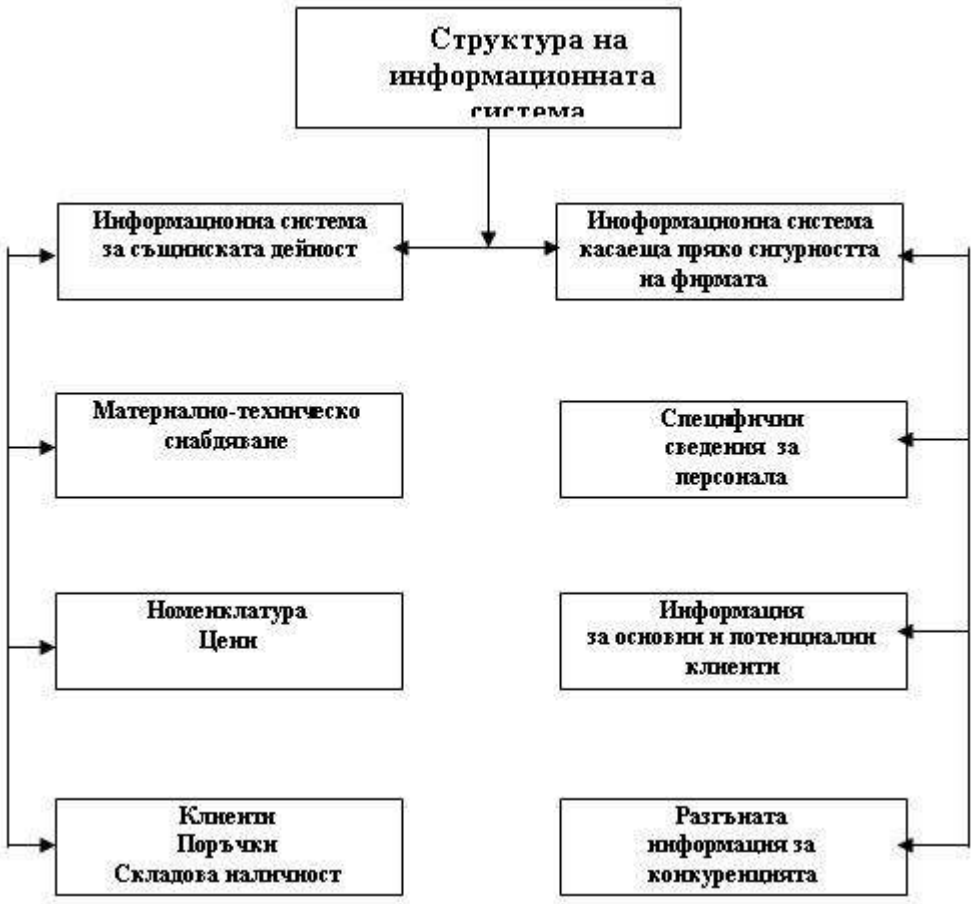
В случая с разглеждания обект „София аерогара – център", с дълбоко убеждение мога да конкретизирам, че компонентът „човешки ресурси", включващ персонал, клиенти и партньори, има лична заинтересованост от сигурността си, и поради това, те засвидетелстват необходимата лоялност към охранителната дейност. Относно конкуренцията нещата стоят по-

различно, но за разглеждания обект и периода на охраната, не са били в центъра на вниманието, поради липса на нелоялни действия или опити за подронване авторитета на организацията.

Г) *Сигурност на информационната система*

Сигурността на информационната система се отнася до сигурността на автоматизираните информационни потоци, изградени въз основа на съвременни бързоразвиващи се информационни технологии.

Структурата на информационната система на организацията е съставена от два основни градивни елемента: а) информационна система за същинската дейност на организацията (номенклатура на стоки, стокови наличности, клиенти, поръчки, срокове на доставка, цени, плащания и пр.), б) информационна система на сигурността на организацията (специфични сведения за персонала и дейността му, информация за важни партньори, клиенти и конкуренти, специфични стратегически проучвания, данни за хора „лобисти“ на фирмата, данни събирани от фирменото разузнаване, както и такива за посегателствата срещу сигурността на фирмата, анализи за състоянието на отделни сектори на сигурността на фирмата и пр.) (фиг.4).




Фиг.4. Примерна структура на система за сигурност на „Информационната система“ за фирма с производствена и търговска дейност.

По мое мнение, информационната система, която пряко засяга сигурността на изследвания обект „София аерогара – център“, има основополагащо значение за качеството на нейното функциониране. През времето на моята служба като охранител на обекта можех отчетливо да установя, че тя се отнася право пропорционално към качеството на охранителната дейност. Прекъсване функционирането на информационната система при настъпване на най-често срещаните природни условия, като например, бури, проливни дъждове, гръмотевици и пр., блокираше работата на охранителите понякога за по-дълго време. Ето защо тук обръщам специално внимание на тази част от сигурността на информационната система, която може да доведе до сериозни последици.

От така представената структура на интегралната система за сигурност отново мога да подчертая, че *човекът* е нейният най-важен компонент. Той участва във всички подсистеми и е тясно обвързан е с информацията, тъй като я създава, използва и съхранява, а освен това има

и задължението да разпространява определена част от нея. Днес все повече се налага схващането, че *сигурността не зависи толкова от техническите съоръжения, колкото от състоянието на човешкия фактор и комплексните мерки, предприемани от ръководството на фирмата по ангажиране вниманието на целия персонал с проблемите на сигурността.* Лошото управление във фирмата в съчетание с човешката алчност създават благоприятни условия за шпионаж и предателство.

Оттук мога да направя заключението, че *от гледна точка на охранителната дейност, управлението и човешкият фактор играят изключителна роля при изготвянето на проект за сигурност.* При изследването на „София аерогара – център“ на преден план излязоха недостатъци, които ще бъдат отчетени и анализирани във Глава II.

Не случайно много европейски и американски изследователи обръщат внимание на факта, че най-слабото звено в системата за сигурност е човекът. Тук ще отбележа резултатите от някои изследвания, проведени в Европа и САЩ.

Агресивната и сурова борбата за пазари и високи технологии в световен мащаб води до оформяне на една нелоялна тенденция – фирмите да набавят недостигащите им знания посредством кражба. Те използват склонността на човека към прояви на нелоялност към фирмата, за да издават и „продават“ производствени и търговски тайни. Провежданите през последните десетилетия проучвания и анализи на човешкия фактор показват нарасналата възможност собствените служители да предават фирмени тайни на други заинтересовани такива.

Така например, изследване в Италия върху защитата на фирмената тайна показва, че 25% от служителите са склонни към авантюри и шпионаж, ако заинтересовани лица се обърнат към тях за информация, а други 49%, под влияние на външните условия, биха могли да бъдат „подмамени“ да извършат предателство.

Изследвания в САЩ на рисковите групи в американското общество показват, че 13% от населението носят висок риск – от тяхната среда излизат опасни престъпници, които сами биха създали условия за престъпления, ако досега не са били налице, а други 75% не биха се поддали на различни изкушения, ако върху тях се оказва системен контрол. При условие, че такъв няма, натискът на обкръжаващата среда би довел до негативни прояви.

Според изследвания в швейцарска фирма, 25% от служителите са готови да извършат кражба при съществуващите условия, а други 25% проявяват колебание, което също ги включва в застрашаващата група. В Германия са изследвали склонността на човека да посяга към чуждо имущество: 26% са склонни да посегнат, в случай че дори един път се създаде ситуация на безстопанственост, а ако такава е налична над три пъти и те не са наблюдавани, тогава изкушените да посегнат стават 47%.

Една от най-застрашаващите прояви на нелоялност към фирмата е внезапната смяна на работното място и преминаване на страната на конкуренцията. От друга страна, все по-широкото въвеждане на информационните технологии увеличава проблема, тъй като заплахата функционално се разпределя в две направления: към информационните системи като обект и към извършителите на подобни престъпления като субект. Трудното разкриване на извършителите-специалисти в информационните технологии, както и резултатите от проучванията, че по-голямата част от заплахите върху информационната система се извършва от собствените служители, усложняват проблема. Проучване за САЩ, Англия и Австралия установява, че 80% от престъпленията са извършени от собствени служители на фирмите, докато външните потребители на информационните системи са само 8%. Това придава изключителна важност на заплахите спрямо информационните системи, и в частност, спрямо конфиденциалната информация.

С оглед на посочените явни и потенциални заплахи, произтичащи от човека, интерес представляват адекватните мерки, които се вземат за персоналната и физическата сигурност. Развитието на информационните технологии предоставя различни технически средства за изграждане на системи за защита и сигурност.

## 2. Технически средства за защита

От гледна точка на мястото и целите, за които се използват, техническите средства за защита най-общо се разпределят в четири групи:

А) *Контролно-пропускателни технически средства,*

Б) *Оперативно-технически средства,*

В) С*игнално-охранителна техника;*

Г) *СОТ и противопожарна сигнализация.*

От личните си наблюдения и направените проучвания на „София аерогара – център“ мога да изразя своето категорично мнение, че и четирите групи технически средства са от първостепенно значение при изготвянето на проект за защита. Това е така, защото по веригата от входа на потока хора (служители, клиенти или партньори), техническите средства за проследяване на случайни или преднамерени нарушения, сигнализирането и реагирането, в това число и на противопожарната система, както и човешките ресурси са тези, на които е поверена сигурността. Те изграждат едно биномно цяло – симбиоза от техника и хора – и техните взаимозависимости определят резултатите. Когато единият компонент намали качеството на своето функциониране, това се отразява на ефективността на другия компонент. На разглеждания обект имаше неединични случаи на подобни нарушения и служителите по охраната бяха свидетели на паниката и загуба на контрола в охраната.

А) *Контролно-пропускателни технически средства*

Защитата на една организация започва от входа и изхода от нея. Ето защо на първо място в системата за сигурност е изграждането на контрол на достъпа. Посредством контролно-пропускателните технически средства се изграждат различни *системи за контрол на достъпа*, които контролират движението на лица и материали на входа и изхода на организацията. Целта им е да осигурят защита на персонала и имуществото като не допускат нежелани субекти в помещенията. Така предотвратяват кражби на имущество и документи, елиминират възможности за тяхното унищожаване и пр.

Много важно е при изграждането на една контролно-пропускателна система да съществува ясна концепция и задание, както и да се привлекат добри консултанти, които да могат да дадат компетентно мнение за най-подходящия вариант. Целта е с най-малко вложени финансови средства да се постигне оптимален и гарантиращ сигурността вариант, който впоследствие може да претърпи увеличение на функциите и разширения.

Функциите на контролно-пропускателните системи са да иден-тифицират, разрешават и архивират преминаването на лица, имащи право на достъп. Тези функции се осъществяват автоматично, но на определени входно-изходни места е възможно да има присъствие и на служители от охраната.

Задължителните изисквания към една ефективна система за контрол на достъпа са:

- ✓ влизането и излизането от охранявания обект трябва да е възможно единствено чрез преминаване през пунктовете на системата;
- ✓ системата да блокира преминаването, докато не приключи проверката;
- ✓ да е предвидена възможност за вторична проверка на непреминалите през автоматизираната проверка лица и транспортни средства;
- ✓ системата да проверява както персонала и багажа му, така и транспортните средства и превозваните от тях материали;
- ✓ пропускателната способност да гарантира нормално функциониране в "пиковите" моменти;
- ✓ системата да е лесна за експлоатация и обслужване от персонала, обезпечаващ физическата охрана, като му осигурява допълнителна защита;
- ✓ системата да е под наблюдение или да е съставна част от интегрираната система за сигурност на охранявания обект.

Бързото развитие на компютърната техника и технологии даде възможност за реализиране на системи с многофункционално действие, като:

- ✓ създаване ниво на достъп (обособени като зони помещения), който е диференциран и възможен само за определени лица;
- ✓ защита от повторна употреба на един и същ пропуск (чрез дефиниран интервал от време за невъзможност от повторна употреба – "анти пас бек");
- ✓ локален "анти пас бек" (невъзможност за две последователни влизания в дадена зона, без прекъсване с излизане);
- ✓ глобален "анти пас бек" (разрешава влизане в дадена зона, само ако лицето е влизало в друга задължителна първа зона или маршрут);
- ✓ времеви зони (интервали от време, разрешени за влизане или излизане);
- ✓ контрол на броя лица в едно помещение и др.

Неразделна част от контролно-пропускателните системи са *механичните пропускателни устройства*. В зависимост от присъствието или отсъствието на служител те могат да бъдат:

- ✓ нисковъртящи се бариери (турникети);
- ✓ високовъртящи се врати;

- ✓ врати с монтирани на тях електромагнитни ключалки, управлявани от системата;
- ✓ автоматични бариери;
- ✓ автоматични електромеханични врати и др.

По мое мнение, поради възможността от техническа неизправност, спиране на електрозахранването и пр., наличието на служител трябва да бъде задължително. Първо, той може да вземе своевременни мерки за отстраняване на неизправността, второ, може да реагира на момента на пропускателния пункт, тъй като човек винаги може да замести машината и да извърши контрол на достъпа в екстремни аварийни ситуации.

За да могат системите за контрол на достъпа да функционират ефективно, от първостепенно значение е правилно да *идентифицират* преминаващите. За целта те се основават на параметрични и биометрични признаци. Известни са три начина за идентификация:

- ✓ персонален идентификационен код (въвежда се от клавиатура и почти винаги е комбинация от 4 или 6 цифри);
- ✓ легитимиране с удостоверение (класически начин, осъществяван чрез: лична карта с фотография, заменяема лична карта, сравнение със съхранявани в компютъра на системата изображения на лица);
- ✓ кодирани удостоверения (карти, пропуски).

Първият начин не е ефективен, има най-ниско ниво на сигурност и се избягва. Вторият начин е негова разновидност – преминаващият през портала дава своята карта и получава аналогична, със същата фотография и номер, но изпълнена различно. Тази карта се съхранява до неговото излизане. При третия вариант се сравнява лицето, преминаващо през портала, с неговото изображение, съхранявано в паметта на системата. Ето защо най-широко приложение намират кодираните удостоверения (карти, пропуски).

Използваните *биометрични методи за идентификация* се базират на анализа на характерни индивидуални анатомични и физически признаци (пръстови отпечатъци, големина и форма на ръката, образ на лицето, особености на ретината, тембър на гласа и др.). Прилагането на биометрични методи в системите за контрол на достъпа е свързано с преодоляване на различни трудности и се използва при гарантиране на високо ниво на сигурност.

Напоследък навлизат в употреба *небиометрични методи*, базирани на информация, известна само на определено лице (напр. изображение на

негови познати). При преминаване, след набиране на идентифициращ код, компютърната система изпраща на монитора матрица от няколко изображения, определен брой от които преминаващият ще разпознае. Има и *атрибутни методи*, които създават различни специфични за лицето признаци, за което в повечето случаи се използва персонален атрибут – идентификационна карта.

Известни са няколко *метода за идентифициране*:

- ✓ метод на щрихови кодове;
- ✓ метод с използване на магнитни полета;
- ✓ метод с използване на радиоактивност;
- ✓ метод с използване на оптическо изображение;
- ✓ метод с използване на акустично отражение;
- ✓ метод с използване на електромагнитни вълни;
- ✓ метод с използване на магнитен цифров запис;
- ✓ метод с използване на многократно записваща се информация – smart cart.

Много от посочените методи създават различни неудобства. Напоследък се налага "Magnetic stripe" технологията, използваща кодиран цифров запис върху магнитна лента. Носителят на магнитната лента е пластмасова, водоустойчива, лека и трудно повредима карта с дебелина до 1 мм и безконтактно четене на информацията. Устройствата са два вида – с вкарване на картата и с плъзгане. Прилаганите технологии са няколко вида:

- ✓ "Wiegdnd" технология. Използва пластмасова карта с магнитни проводници за кодиране на информацията, които практически не се влияят от електрически и магнитни полета. Гарантират по-висока сигурност;
- ✓ "Infrared" технология. Отделните площи в кодовото поле на картата пропускат различно инфрачервени лъчи. При замърсени карти, обаче, е трудно, и дори невъзможно, правилно да се прочете информацията. Освен пасивната инфрачервена технология, съществува и активна – с монтиран инфрачервен предавател. Функционира на разстояние до 60 см;
- ✓ "Proximity" технология. Прочитането на информацията става при приближаване на пропуска към четеца без директен контакт. Преимущество е скриването на четеца;

- ✓ "Hands free" технология. При нея не е необходимо да се изважда пропуска, нито да се доближава до четеца. Функционира от разстояние 70 см. Тя е най-скъпа, но е предпочитана заради удобството и сигурността.

За управление на централизиран контрол на достъпа се използват и много *програмни методи*. Например, програмен модул "Digiterm" позволява контрол на работното време и изготвяне на протоколи за изчисляване на работните заплати. За хотели е разработен специализиран софтуер, който осъществява и някои допълнителни функции – регулира осветлението и отоплението, заключва и отключва входната врата, повиква персонал и др.

Много важна задача е контролно-пропускателната проверка на транспортните средства и ръчния багаж на преходните портали. Тя е с цел предотвратяване на внос и износ на неразрешени материали, оръжие, взривни вещества и пр. Проверка на ръчен багаж се извършва ръчно или с помощта на технически средства. Използва се облъчване с рентгенови лъчи, гама лъчи или с неутрони. Тук най-често използваните детектори са осцилатори, регистриращи гама лъчи, генерирани при радиоактивно разпадане.

Взривни вещества се регистрират най-често чрез обучени кучета или чрез детектори на пáри на взривните вещества. Оръжие и други метални предмети се откриват чрез портативни детектори, генериращи електромагнитно поле и регистриращи неговото изменение при движението на метални предмети между две антени, или регистриращи токове на Фуко, индуцирани в предмета от пулсиращо електромагнитно поле. Детекторите на метал са чувствителни устройства и много фактори на обкръжаващата среда могат да доведат до генериране на фалшиви алармени сигнали – метални врати и прозорци, тръби на радиатори, метални решетки, силни радиосигнали, електрически разряди и др.

Контролно-пропускателните технически системи не се изчерпват с разгледаните дотук. Има и много български разработки, а освен българското програмно осигуряване на системите, повечето фирми предлагат и изработване на контролери, а някои и четящи устройства.

Б) *Оперативно-технически средства*

Оперативно-техническите средства се използват с цел *осъществяване на негласен контрол за установяване и документиране на факти и*

*обстоятелства относно престъпна дейност, както и заплахи и опасности*.

Оперативно-техническите средства са: фотоапарати, звукозаписни устройства, телефонни и телефаксни апарати, мобилни и стационарни съоръжения, радио-микрофонни съоръжения, маркиращи средства, други специални технически средства и програмни продукти за установяване съдържанието на обработваната и съхранявана в компютрите и компютърните системи информация.

Оперативно-техническите средства имат голямо значение, но са с ограничена от закона приложимост. Само изброените в **Закона за специалните разузнавателни средства**[9] субекти могат да осъществяват негласен контрол. Но посетителите в една организация могат да се подложат на специален контрол, за което предварително се уведомяват. Това включва оперативно-техническите средства към *оперативно-издирвателната и информационно-разузнавателната дейност* в сигурността.

В) *Сигнално-охранителна техника (СОТ)*

Чрез използването на сигнално-охранителна техника за охрана на обекти се постига специализиран вид охрана. Той включва проектиране, монтаж, експлоатация и поддържане на техниката за опазване, защита и сигнализиране на обекти. Сигнално-охранителната техника *има за цел да сигнализира и предотврати нарушение или неправомерно действие*. Тя може да се разглежда и като *намаляваща или предпазваща от рисковете и опасностите от нежелани морални и материални загуби*. Към нея спадат и *пожароизвестителните средства*. Част от техническите средства, апарати и съоръжения на СОТ могат да бъдат предварително вградени. В съчетание с другите технически инсталации (електрически, телефонни) могат да се ползват и за негласно наблюдение.

Масовото внедряване на информационните и комуникационните технологии, електрониката и производството на специализирани интегрални схеми с много висока степен на интеграция доведе до развитието на *сигнално-охранителни системи*, които са съчетание на различна по функции, цели и задачи сигнално-охранителната техника.

[9] http://lex.bg/laws/ldoc/2134163459

Основен компонент на СОТ е алармената система. Нейни градивни елементи са *детекторът*, *контролният панел* (в модерните системи) и *известяващото устройство* за възникналата опасност от проникване в охранявания обект.

*Детекторът* е електронно устройство, част от алармената система, което при регистриране на нежелано проникване (или опит) на нарушител в охранявания обект или помещение, прекъсва нормалното съпротивление в електрическата верига на зоната в контролния панел.

*Контролният панел* (алармена централа, система срещу проникване) е следяща информационна система, регистрираща промените в проследяващото наблюдение на помещението за неоторизирано проникване в сградата, и информираща охранителния състав или изнесената дежурна.

*Известяващо устройство* (сирена) регистрира детектирането на злоумишлено действие или пожар, известява (алармира), задържа или спира нарушителя, изпълнява контролно-пропускателна функция, има доказателствена, информационна и самодиагностираща функция, изпраща съобщения от локални системи до отдалечен алармен център.

Съществува *класификация на техническите системи за сигурност*, определена в зависимост от вида или начина на осъществяване на регистриращата функция*:*

*а) контролно-пропускателни технически системи;*

*б) периметрови сигнално-охранителни системи;*

*в) оградни периметрови сигнално-охранителни системи;*

*г) подземни периметрови сигнално-охранителни системи;*

*д) надземни периметрови сигнално-охранителни системи;*

*е) телевизионни системи за наблюдение и контрол;*

*ж) технически системи за охрана на помещения и предмети в тях.*

Използването на определен клас системи в голяма степен се обвързва с особеностите на конкретния обект и набелязаните цели на тяхното функциониране.

*а) Контролно-пропускателни технически системи*. Вече бяха резюмирани в подточка А).

*б) Периметрови сигнално-охранителни системи (ПСОС)*. Развитието на информационните технологии позволи да се реализират устройства с много сложни функции, които намират приложение в техническите системи за сигурност. Например, модерните системи срещу проникване и

контролните им панели, системите за контрол на достъпа и интегрираните системи за сигурност. Подобни системи имат възможност за събиране и запаметяване на огромен обем информация за всички регистрирани събития, в това число и за действията на оперативния състав. Тези действия се улесняват от изграден мониторинг на входни сигнали, който позволява отличаване на алармата от техническа неизправност или опит за саботаж, придружени с видео системи за наблюдение. Много често се предвижда съвместна работа на няколко системи в икономиката и отбраната на държавни обекти, разрушаването и повреждането на които води да големи материални загуби и заплаха за здравето и живота на много хора.

Едно от средствата за намаляване на тези рискове е *охрана по периметъра* на такива обекти. Тя е скъпа система с висока ефективност. Периметровата сигнално-охранителна система регистрира въоръжено нападение, терористична акция, неоторизирано проникване, шпионаж, саботаж, кражба. Целта й е да фиксира нарушения при пресичане на периметровата граница и получената информация да спечели време за противодействие. За забавяне на нарушителя могат да се изградят периметрови съоръжения, за чието преодоляване ще е необходимо повече време. Желателно е системата да определя и посоката на проникване – отвън навътре или обратно.

Преди да се пристъпи към разглеждане на отделните системи и тяхната ефективност, трябва да се вземе под внимание, че те се изграждат извън сградите и са подложени на различни атмосферни условия – резки температурни изменения, дъждове, снеговалежи, градушки, ветрове и пр. Това налага използваните технически устройства да отговарят на високи технологически и технически критерии, за да се гарантира, че ще се намалят до минимум фалшивите сработвания от външни атмосферни влияния и радиочестотни смущения. Много често за по-ефикасно функциониране на ПСОС се използва комбинация от две или повече системи, действащи на различни принципи, което дава възможност да се компенсират недостатъците им.

От моите лични наблюдения, както и от тези на колегите охранители, установих, че охраната по периметъра е изключително деликатна система, податлива на непредвидими промени. Тя реагира при най-малките климатични изменения и често лишава КПП на обекта от видео-наблюдение и сигнализиране. Това налага нейното непрекъснато

проследяване и контролиране да влезе като неотделима част от ежедневната рутинна техническа проверка.

За реализиране на ПСОС се използват различни детектори и системи, класифицирани според типа:

✓ *Пасивни детектори* – регистрират определен вид енергия, излъчена от нарушителя или промяна на естествените енергийни полета, предизвикани от придвижването на нарушителя по или под повърхността на земята или при опит за преодоляване на заграждението с монтираната системата.

✓ *Активни детектори* – излъчват определен вид енергия и регистрират изменения в интензитета на полето или отразената вълна. Те са моностатичии и бистатични според това дали излъчвателят и приемникът са в един корпус. Практически е невъзможно да се скрият, в някои случаи могат да станат източници на смущения за други системи, но в повечето случаи се характеризират със значително по-нисък брой фалшиви аларми, тъй като излъчваната от тях енергия е сравнително голяма и измененията са по-отчетливи.

✓ *Обемни детектори* – регистрират проникване в определен обект от пространството, докато линейните реагират при опит за преодоляване на повърхност или линия (ограда, на която са поставени).

Функциите на детекторите се оценяват по няколко параметъра. *Вероятност за детектиране* – оценява способността на детектора да регистрира проникване на нарушител в охраняваната зона. Зависи от вида на технологията и конструктивните особености на сензора, начина на обработка на сигнала от него, установените настройки, характеристики на нарушителя, климатичните условия, правилното инсталиране, техническото обслужване и др. Често към тези показатели се включва и вероятността за получаване на алармен сигнал в централната станция и неговата коректна оценка. *Ниво на фалшиви сигнали* е показател, характеризиращ броя на алармите, предизвикани не от нарушителя, а по други неизвестни причини. Нормално се асоциира с шумове на сензора и детектора. *Ниво на алармите*, предизвикани от източници, които не представляват заплаха за сигурността на обект (няколко групи от фактори определят стойността на този показател: климатични условия, животни и птици, теренни особености, свързани с повърхността на земята, растителност). *Вероятност за преодоляване на системата* – чрез използване на различни технически и нетехнически прийоми, нарушителят

би могъл да проникне в охранявания обект, без да активира ПСОС. Ето защо ПСОС трябва да съдържа и средства, намаляващи тези възможности (такива са 24-часов антитампер мониторинг, самотестващи се детектори, комбинация от детектори, работещи на различни физически принципи, скрити детектори др.).

Върху тези стойности може да се влияе чрез правилен подбор на детекторите, внимателен и подробен анализ на особеностите на обекта, водещи до увеличаване на фалшиви сработвания, и добро техническо обслужване на устройствата. Сумата на фалшивите аларми и предизвиканите от източници, непредставляващи заплаха за сигурността, дава броя на невалидните аларми.

*в) Оградни периметрови сигнално-охранителни системи (ОПСОС).* Регистрират опити за преодоляване на оградата чрез събаряне, промушване между паралелните хоризонтални проводници, прерязване на проводници или част от мрежата, покатерване и прескачане. Те се различават според физическия принцип на работа на детекторите (датчиците). В много страни масово се използват системите на база опъната тел – бодлива или най-често гладка. Всяко въздействие върху оградата предизвиква опъване на един или повече проводници в хоризонтална посока. Механичното въздействие върху детектора се трансформира в електрически сигнал, който се подлага на допълнителна обработка.

Друга група ОПСОС са *вибрационните*. Детекторите реагират от механичните вибрации на оградата. Възможно е да се получат фалшиви задействания, причинени от силен вятър и боклуци, бури, градушки, сеизмични колебания, вкл. поради преминаващи наблизо тежки товарни автомобили. За да се ограничат въздействията на тези фактори, необходимо е да се направи точен оглед на изпълнението на оградата. Използват се различни методи за регистриране на вибрации, но най-разпространените са системите, използващи електромеханични детектори или специални сензорни кабели. За елиминиране на фалшиви аларми към детекторите се включва сензор за времето и "вана за вятър", а в самия детектор се осъществява филтриране на сигналите, предизвикани от вятър и градушка.

Бързото развитие на електрониката и изчислителната техника позволиха създаването на компактни компютърни системи, които

реализират много функции, визуализират огромен брой събития, групират ги по определени признаци, архивират и дават възможност за отпечатване на справки, визуална информация и др., улесняват действията на диспечера (оператора), а така също и установяват контрол върху неговите действия и пр. Неразделна част от централната алармена система са мониторите и управляващите устройства, за регулиране на осветлението и изпълнителни механизми за блокировки на врати, портали, оповестителни устройства и други технически средства.

*г) Подземни периметрови сигнално-охранителни системи* (ППСОС). Могат да се разделят на две групи: а) ППСОС използваща детектори за налягане или сеизмични детектори, б) ППСОС регистрираща промени на електромагнитното поле в пространството около детекторите.

Детекторите за налягане или сеизмичните детектори регистрират вибрации, причинени от ходещи, бягащи, скачащи или пълзящи в контролираното от тях пространство нарушители. При това детекторите на налягане регистрират преди всичко нискочестотните вълни в повърхностния слой земя, а сеизмичните – високочестотните колебания.

Намаляването на фалшивите аларми се постига при балансирани системи, използващи два шланга, включени диференциално. Детекторният блок също се заравя под земята и може да функционира при температура от - 35° С до + 55° С (примерна система "Кобра "). Сигналите от 16 броя детектори се обработват от анализатор, от който чрез интерфейс може да се изпратят в централната алармена станция. Шлангът се заравя на дълбочина от 25 до 30 см.

Сеизмичният вариант на такъв вид ППСОС се базира на свързани сеизмични детектори. Всеки от тях е изграден от постоянен магнит и бобина, като единият от тези елементи е неподвижен, а другият може да вибрира при колебания в земята За елиминиране на въздействието върху тях на отделните източници на сеизмични колебания, бобините се монтират така, че взаимно да се компенсират. Примерна система е изградена с две паралелни линии, едната от които се използва за детектиране на автомобили и хора, движещи се в непосредствена близост до охраняваното пространство (особено полезна функция при наличието на близки шосета или алеи за пешеходци). В едната линия могат да се монтират до 25 сензора, като радиусът на детектиране е 2,5 метра.

И при двата типа детектори чувствителността зависи до голяма степен от характеристиките на почвата, които от своя страна зависят от климата и сезона, което налага периодична пренастройка. Втората група ППСОС регистрират промени на електромагнитното поле в пространството около детекторите. Делят се на две подгрупи, в зависимост от това дали детекторите са активни или пасивни. Както единият, така и другият принцип имат предимства и недостатъци.

При активните системи е много важно в близост до тях да няма подвижни или неподвижни метални предмети или обекти, както и големи обеми вода. Освен източници на фалшиви аларми, те могат в някои случаи да променят "геометрията" на контролирания обем или напълно да блокират нормалното й функциониране.

При съвременните ПСОС най-често се използват *инфрачервени, микровълнови* и *видеодетектори*.

- Инфрачервен детектор (бариера). Светодиодът излъчва светлина с дължина в инфрачервения диапазон, която се оформя като лъч с помощта на леща. Излъченият лъч се приема от друга подобна леща и се фокусира върху фотодиод. Детекторът регистрира загубата на енергия на приемания лъч, когато непрозрачен обект го пресече. Конструктивно заложено е детекторът да излъчва множество лъчи, като броят на лъчите зависи от модела или се избира от проектанта. По този начин се оформя невидима мрежа и пресичането на който и да е лъч води до загуба на енергия, а оттам и до регистрирането на нарушение в охраняваната зона. Системата е на модулен принцип, позволяващ изграждане на бариери с различна височина и дължина. Влияние оказват метеорологичните условия: при ясно и сухо време – до 360 м; при дъжд и сняг до – 120 м. Системата функционира в температурния диапазон от -40°C до +60° C.

*д) Надземни периметрови технически системи*. Микровълновите детектори, използвани за ПСОС, са активни и видими, работещи най-ефективно при равни повърхности. Принципно са изградени от две антени, разположени в двата края на охраняваното пространство. Едната се свързва към микровълнов предавател, а другата – към приемник, регистриращ приемането на електромагнитната енергия. Детекторът регистрира изменението на енергията, предизвикана от движението на обекти в охраняваното пространство. Ако тази промяна надвишава предварително заложената норма, изработва алармен сигнал. За

нормалното функциониране на микровълновите системи влияят редица фактори: силен дъжд , мълнии и др.

Видеодетектори с камери се монтират на подходящи и високи стълбове. Те изискват подходящо осветление и, освен за регистриране на проникването, могат да се използват и за наблюдение на периметъра и оценка на аварийната ситуация. Видео системата трябва да отговаря на определени изисквания: препокриване на ПСОС или взаимно самонаблюдение; защита на съоръженията от умишлено повреждане; самодиагностика; защита на оборудването от мълнии.

*е) Телевизионни системи за наблюдение и контрол.* Изградени са от IP камери, т.нар. мрежови камери. За пренос на сигнала от камерата до записващото устройство се използват локални мрежи LAN или глобалната мрежа Интернет. Записващите устройства NVR (Network Video Recorder) са проектирани да приемат потоците от мрежовите камери и да ги записват във вида, в който са получени, т.е. резолюцията на записания видеосигнал зависи изцяло от камерата.

За различни случаи и приложения са възможни конфигурации. Една от тях е дистанционно домашно видеонаблюдение с IP видеокамери през високоскоростни INTERNET връзки чрез стационарен телефон. Видеокамерите и стационарният телефон се идентифицират в мрежата чрез статични IP адреси. Камерите работят като телефон и могат да бъдат търсени от всеки терминал, включен към ISDN мрежа или включен към IP мрежа.

Дистанционният видеоконтрол чрез глобалната мрежа става все по-актуален поради нарастването на достъпа до високоскоростен интернет. IP камерите могат да се наблюдават чрез клетъчен IP телефон или преносим компютър (Labtop), а също и от централна станция за дистанционно видеонаблюдение. Всички компоненти на системата за видеонаблюдение се идентифицират в мрежата чрез динамични IP адреси.

Чрез локални мрежови конфигурации със стандартни PC е възможно да се изграждат системи за видеонаблюдение с много на брой включени в локални мрежи IP видеодетектори. Стандартният компютър играе роля и на видеосървър. Видеоинформацията от всяка IP камера се пренася чрез мрежата в паметта на диспечерски видеосървър. Чрез администрирането на IP камерите в мрежата от стандартния PC, записаната в дадена камера видеоинформация за определено време се пренася в сървъра в съответните

за всяка камера собствени пространства. Това се реализира посредством събитийно управляем запис на видеокартината в сървъра чрез рингов буфер в паметта му, организиран поотделно за всяка IP камера.

Twin-DVR е приложна програма, подпомагаща мрежовите функции на Системния файлов сървър. Инсталира се на един или повече отделни компютри в мрежата, поддържа връзка с файловия сървър и обслужва заявките на отдалечените клиенти. Twin видеосървърите са свързани в конфигурация „точка-точка" и обменят последователно видеоинформация чрез TCP/IP протокол. Един Twin-DVR видеосървър може да обслужва до 200 клиенти – Web камери. За целта на системния файлов сървър се инсталира приложен софтуер (Dinamic DNS), който следи за промените в текущата TCP/IP конфигурация и ги изпраща до специално конфигуриран сървър (Диспечерски сървър) през определено време.

IP технологиите предоставят нещо повече от по-високо качество и по-голямо удобство. Цифровата инфраструктура е основа, върху която иновативните компании ще базират бизнес процеси, които в много случаи няма да имат нищо общо с традиционното видеонаблюдение, насочено стриктно в посока сигурност и охрана.

VsaaS моделът и свързаните с него облачни инфраструктури засягат все повече ИТ и видеонаблюдението. В голяма степен тази тенденция се движи от все по-широко навлизане на мобилните устройства и възможността за бърз достъп до корпоративна информация в професионалното ежедневие. Потребителите, използващи облачни услуги като тези на Apple, Amazon, Google и Microsoft, желаят същото удобство и по време на работа, включително и за видеонаблюдение.

Видеонаблюдение като услуга (video surveillance-as-a-service VSaaS) е особено ценно при управляване и архивиране на записи от охранителни камери, тъй като чрез тях могат да се разкриват престъпления в различни организации. Наблюдава се рязък ръст в търсенето на системи за видеонаблюдение. По данни на анализатора Transparency Market Research, стойността на този сегмент, заедно със споменатите VsaaS предложения, ще достигне 24,81 млрд. долара до 2019 г., като средният годишен ръст се очаква да е 19,1%. Най-търсени ще са продуктите, свързани с IP видео, като техният годишен ръст до 2019-та се очаква да е 24,2%. Общият хардуерен пазар, включващ в себе си и аналоговите решения, през 2012 г. бе 9,49 млрд. долара и се очаква да нараства със 17,3%.

*Облачните технологии* са голяма тема в ИТ през последните години. Благодарение на тях светът навлиза в нова ера на свързаността. Независимо дали става дума за публична среда, където сървърите са на практика споделени между клиентите или собствените центрове за данни, където данните и приложенията се съхраняват изолирано, облачните инфраструктури носят предимства – резервираност, скалируемост и изместване на разходите от капиталови (CAPEX) към оперативни (OPEX).

Облачното съхранение на данни е нараснало стабилно през 2015 г. Според проучване на Centre for Retail Research сред близо 300 търговци на дребно във Великобритания (обхващащи около 20 хил. магазина), особено търсена е функцията дистанционно наблюдение на случаващото се в търговския обект. След като през 2013 г. интерес към нея са изразявали 6,5% от запитаните, само за една година техният брой е нараснал до 82%, като не става дума само за охрана на търговските обекти. Всъщност, техните мениджъри искат информация какво се случва по рафтовете и поведението на клиентите в реално време. Благодарение на нея те могат да вземат бързи и адекватни решения, чрез които да повишат доходите си. Допълнително 65% от запитаните желаят да имат възможност да получат тези данни на своя смартфон или таблет.

Скалируемостта не е само възможност за свързване на повече камери, а дава достъп до повече изчислителна мощ и пространство за съхранение на данни, ако е необходим запис с по-висока резолюция или с повече кадри в секунда. Ако са необходими анализи за поведението на клиентите, възможностите за обработка са налице и за тях може да се заплаща допълнително. Обработката и съхранението на място („on the edge") също са подходящи за критични инфраструктури и приложения. Допълнителните ресурси могат да се използват, напр., за разпознаване и съхраняване на регистрационни номера на превозни средства. Друг интересен аспект на VSaaS са възможностите за включване на допълнителни услуги към видеонаблюдението, напр., охрана или дистанционно наблюдение.

*ж) Технически системи за охрана на помещения и предмети в тях*. Имат сложно изграждане с определяне на важни фактори: техническите средства, начина на изпълнение на системата – регистрираща и сигнализираща (локална) или регистрираща и известяваща с дежурен оператор. И двата вида са свързани с *детектиране* и *алармиране* на

персонала и *охрана* при опит за неоторизирано проникване и за кражби или унищожаване на имущество.

Детекторите са голяма и разнообразна група от видове и тяхната класификация е в зависимост от вида охрана, от тяхното устройство, физически качества, принцип на функциониране и пр.

Алармените системи се изграждат по три основни метода: а) охрана по периферията на обекта (периметъра), б) обемна охрана и в) охрана на предмети. Една по-голяма и сложна охранителна система срещу проникване може да съдържа като подсистеми: телевизионна система за наблюдение и контрол, няколко участъка за охрана по периметъра, както и контрол на достъпа. Класифицирането й като комбинирана, интегрирана или друга система за охрана се прави като се отчита доколко са развити отделните подсистеми, спецификата на обекта, спецификата на реализиране чрез технически средства, на охранителни задачи и преди всичко на тези, които са най-важни или преобладават.

Техническите системи срещу проникване и охрана се характеризират с три основни показателя: детектираща способност, ниво на фалшивите аларми, възможност за проникване. В най-голяма степен тези показатели се определят от включените в системата детектори. През последните години за подобряването им се използват различни технологии. Те варират от различните прийоми за усъвършенстване на характеристиките на сензорите и специалните комбинации в един детектор на сензори, работещи на различни физически принципи, до свръхинтелигентни алгоритми за микропроцесорна обработка на сигнала от тях.

Технологиите за изработване на детектори за охрана на помещения постоянно се усъвършенстват. Понастоящем на пазара се предлагат огромен брой детектори и охранителни системи с различни физически принципи за детектиране, различна вероятност за проникване и зони за детекция. За да функционира системата ефективно, всички фактори, наред с анализа на физическите и експлоатационните характеристики на охранявания обект, трябва да се знаят и отчитат от проектантите, определящи техническите средства за охрана. По-сложните, които съдържат и други специализирани блокове, разширителни модули, CCTV подсистема и други интерфейсни устройства са само допълнения към изградената охранителна система.

Г) *СОТ и противопожарна сигнализация*

Главните компоненти на техническата сигурност са сигнално-охранителната техника (СОТ) и противопожарната сигнализация (ППС). Те имат много общо помежду си – канали на връзка, подобни алгоритми на прием и обработка на информация, подаване на сигнали за тревога и пр. Затова често се обединяват в единна охранително-противопожарна сигнализация. Тя се отнася към най-старите технически средства за охрана и досега представлява най-ефективната система за безопасност.

Използват се няколко подсистеми за сигнализация, които обхващат всякакви заплахи: *охранителна* – фиксира опит за проникване; аларма за тревога – система за извънредно повикване на помощ в случай на внезапно нападение; *противопожарна* – регистрира появата на първите признаци на пожар; *аварийна* – съобщава за изтичане на газ, вода и т. н.; *аларма за тревога* – за извънредно повикване на помощ в случай на внезапно нападение;

Задачи на ППС са получаване, обработка, предаване и представяне, в зададената форма на потребителите при помощта на технически средства, на информация за пожар в охраняваните обекти. Информацията включва: установяване огнището на пожара, определяне мястото на възникването му, подаване на сигнали към системите за автоматично гасене на пожари и отстраняване на дима. Задачата на СОТ е своевременното оповестяване за проникване или опит за проникване в охранявания обект с фиксиране на факта, мястото и времето на нарушаване на охранявания периметър. Общата задача на двете системи за сигнализация е обезпечаване на моментално реагиране с предоставяне на точна информация за характера на събитието.

Анализът на статистическите данни в много страни за несанкционирано проникване в различни обекти показва, че повече от 50% се извършват в обекти със свободен достъп за персонала и клиентите; около 25% – в обекти с неохранявани елементи на механична сигурност от типа на огради, решетки; около 20% – в обекти с пропускателна система, и само 5% – в обекти с усилен режим на охрана, с прилагане на сложни технически системи и специално обучен персонал.

В практиката на службите за безопасност и охрана на обекти се определят шест основни зони на охраняваните територии:

Зона I – периметър на територията пред зданието;

Зона II – периметър на самото здание;

Зона III – помещение за прием на посетители;

Зона IV – кабинети на сътрудници и коридори;

Зони V и VI – кабинети на ръководители, зали за преговори с партньори, хранилища на ценности и информация.

За да се обезпечи необходимото ниво на надеждност на охраната на особено важни обекти (банки, каси, места за съхранение на оръжия), е необходимо да се организира многостепенна сигурност на обекта.

Сигналните датчици на първата линия на сигурност се поставят на външния периметър. Втора защитна линия са датчиците на местата на възможното проникване в обекта (врати, прозорци, малки прозорчета и др.). Трета линия са обемните датчици във вътрешните помещения. Четвърта – непосредствено охраняваните предмети (каси, шкафове, и др.).

Всяка защитна линия задължително се включва към самостоятелна клетка на приемното устройство, така че при евентуално заобикаляне от страна на нарушителя на една от защитните линии, да бъде подаден сигнал за тревога от другата. Съвременните системи СОТ и ППС се интегрират с други системи за безопасност в единни комплекси.

Системата на СОТ и ППС включва: *датчици*, *приемни устройства* и *реагиращи устройства.*

*Датчици/периферийни устройства* са известители на тревога, реагиращи на пожар, опит за проникване в обект и пр. Характеристиките на датчиците определят основните параметри на цялата система за сигнализация.

*Приемните устройства* получават сигнал за тревога от датчиците и осъществяват управление по зададен алгоритъм на реагиращи устройства. Контролът на работата на СОТ и ППС схематично се състои във включване и изключване на датчиците и фиксиране на сигнали за тревога. В сложни, разклонени системи, контролът и управлението се осъществяват с помощта на компютри;

*Реагиращите устройства* са агрегати, които обезпечават изпълнението на зададения алгоритъм на действие на системата в отговор на едно или друго тревожно събитие (подаване на сигнал за оповестяване, включване на противопожарни механизми, автоматично звънене на зададени телефонни номера и пр.

Обикновено охранително-противопожарните системи (ОПС) се изграждат в два варианта: с локална, затворена охрана на обекта или с предаване за охрана на извънведомствени охранителни и противопожарни

служби. Цялото разнообразие на ОПС с известна условност се дели на *аналогови*, *адресни* и *комбинирани*.

*Аналоговите* системи/неадресирани се изграждат като охраняваният обект се разделя на сектори чрез прокарване на отделни кабели, обединяващи известно количество датчици. При активирането на който и да е датчик, се подава сигнал за тревога по цялата линия. Решение за възникване на събитие в този случай „взема“само датчикът, чиято работоспособност може да се провери единствено по време на техническото обслужване на ОПС. Други недостатъци на такива системи са високата вероятност от лъжливо активиране, локализация на сигнал с точност до съответния кабел, ограничение на контролираната зона. Стойността на такава система е относително ниска, въпреки прокарването на много кабели. Задачите на централизираното управление се изпълняват от охранително-противопожарно табло. Използването на аналогови системи е възможно на всички типове обекти. Но при много области на сигурност възниква необходимост от голям обем монтажни работи по поставянето на кабелни комуникации.

*Адресируемите* системи предполагат монтаж на адресни датчици на един сигнализационен кабел. Кабелната линия, на която са разположени различните устройства, започва от контролния панел и се връща в него. Линиите на адресируемите системи се наричат кръгове или контури. Такива системи позволяват да се заменят многожичните кабели, съединяващи датчици с приемника с една двойка проводници.

Адресируемите пасивни системи всъщност са допълнени само с възможност за предаване на кода на адреса на сработилия датчик. Тези системи имат всички недостатъци на аналоговите: невъзможност за автоматичен контрол на работоспособността на противопожарните датчици (при отказ на електрониката връзката на датчика с приемника се преустановява).

Адресируемите активни системи осъществяват периодична проверка на датчиците, обезпечават контрол на работоспособността им при всякакъв вид отказ, което позволява да се монтира по един датчик в помещение вместо по два. Може да се реализират сложни алгоритми на обработка на информацията (напр. автокомпенсация на измененията на чувствителността на датчиците с течение на времето). Намалява се вероятността от лъжливо активиране (напр., адресният датчик на разбито стъкло, за

разлика от безадресния, ще покаже точно кой прозорец е разбит). Решение за събитието също се взема от датчика.

*Комбинираните* (адресно-аналогови) системи са най-перспективното направление в построяване на сигнални системи. Адресно-аналоговите датчици измерват стойността на задименост или температурата на обекта. Има възможност да се включат всякакви датчици, системата е способна да определи типа и необходимия алгоритъм на работа с тях, дори ако всички устройства са на един кабел на охранителната сигнализация. Тези системи обезпечават максимална скорост на приемане на решения и управление. За правилната работа на адресно-аналоговата апаратура е необходимо да се съблюдава уникалният за всяка система език на общуване на компонентите ѝ (протокол).

Сега съществува огромно разнообразие от датчици, приемници и аларми с различни характеристики и възможности. Определящи елементи на ОПС са датчиците. Параметрите на датчиците обуславят главните характеристики на цялата система за сигнализация. Според мястото на поставяне датчиците са вътрешни и външни. Датчиците регистрират измененията в обкръжаващата среда. Те определят наличието на заплаха за техническата сигурност на охранявания обект и предават алармен сигнал за своевременно реагиране. Условно може да се поделят на: *обемни* – позволяващи контрол над пространство; *линейни* или повърхностни – за контрол на периметрите на територии и здания; *локални* или точкови – за контрол на отделни предмети.

Датчиците може да се класифицират по типа на контролирания физически параметър, по принципа на действие на чувствителния елемент, по начина на предаване на информация на централния пулт на управление. Според принципа на формиране на информационния сигнал за проникване в обекта или пожар датчиците на ОПС се поделят на: *активни* – сигнализацията генерира сигнал в охраняваната зона и реагира на изменение в параметрите му; и *пасивни* – реагират на изменение в параметрите на обкръжаващата среда. Широко се използват такива типове охранителни датчици, като инфрачервени пасивни, магнитно-контактни датчици за разбиване на стъкло, периметърни активни датчици, комбинирани активни датчици. В системите за противопожарна сигнализация се използват топлинни, димни, светлинни, йонизациони, комбинирани датчици. Типът датчици на системата се определят на физически принцип на действие. В зависимост от типа датчици охранителните системи може да бъдат:

обемни, радиоизлъчвателни,сеизмични, реагиращи на затваряне или отваряне на електрическа верига и т. н. Възможностите за инсталиране на охранителни системи в зависимост от използваните датчици, предимствата и недостатъците им, са посочени в табл. 1.

Таблица 1.

| Тип система | Тип ограда | Възможност за сигурност на неограденипространства | Преимущества | Недостатъци |
|---|---|---|---|---|
| 1.Радиоизлъчва-телни | Всяка | Да,<br>на стойки | Независимост от природни условия | Мъртви зони пред предавате-ля и приемника. Необходимост от осигуряване на пряка види-мост |
| 2.Радиовълнови | Всяка | Да,<br>под земята | Независимост от релефа и линията на оградата | Силна зависи-мост от радио-магнитната сре-да |
| 3.Инфрачервени | Всяка | Не | Прост монтаж и поддръжка | Голямо количес-тво лъжливи сигнали |
| 4.Оптични влакна | Всяка | Не | Не се поддава на електромагнитни влияния | Сложен монтаж и ремонт |
| 5.Обемни | Всяка | Не | Независимост от релефа и линията на оградата | Сложен и скъп монтаж |
| 6.Вибрационни | Всяка | Да,<br>под земята | Независимост от релефа и линията на оградата | Лъжливи сигнали при силен вятър |
| 7.Вибрационно-сеизмични | Бетонна | Да,<br>под земята | Възможност за реагиране и на копаене, и на човек | Не трябва да е близо до път и електропровод; не работи в блатисти скални почви |
| 8.Системи за активна охрана | Мрежова или метална | Не | Не вреди на хора | Смъртоносна за дребни животни и птици |

Охранителните датчици са голяма и разнообразна група, както и противопожарните. Критерий за ефективност на работата на апаратурата за ОПС е свеждането до минимум броя грешки и лъжливи аларми. Приема се за отличен резултат на работа наличието на една лъжлива тревога от една зона за месец. Честотата на лъжливи аларми е основна характеристика, по която може да се съди за устойчивостта на смущения на датчика.

Понастоящем се използва *интегрираният подход* за изграждане на проект за охрана и сигурност. Комплексното приложение на ОПС обезпечава безопасността на обекта при висока степен на интеграция с други системи за безопасност като системите за контрол на достъпа, видео наблюдението и др. При изграждането на интегрирани системи за безопасност се появяват проблеми на съвместимостта с другите системи. За обединяването на охранителни, противопожарни, алармени системи, контрол и управление на достъпа, автоматични инсталации за пожарогасене и т. н., се използват програмни, апаратурни (най-предпочитани) разработки и единни изделия.

*Техническите средства за откриване на шпиониращи устройства,* като физически обекти или електронни средства, са важен компонент на всяка ефективна система за защита на информацията. Използват се също и технически средства за създаване на смущения.

*Обобщение на някои важни наблюдения от практиката.*

От направения теоретичен преглед относно проектиране, изготвяне и внедряване на проект за охрана и сигурност със СОТ, мога да обобщя някои важни наблюдения от практиката.

В нашия модерен век на изключителен технологичен бум, изграждането на ефективна сигнално-охранителна система изисква методически подход, който да отчита тройното съотношение *преследваните цели – възможности за реализация – разполагаеми ресурси*. Налага се опитът, че слабият компонент в проекта за сигурност е човекът като носител на информация, независимо дали е външен нарушител или вътрешен служител. Това изисква предварителна професионална подготовка, задълбочена проучвателна работа преди изготвянето на проекта и строг контрол при наемане на служители, работещи с конфиденциална информация, при въвеждане на проекта, неговата поддръжка и експлоатация на охранявания обект.

Неправилното проектиране и изработка на охранителната система може да доведе до сериозно увеличаване на уязвимите места. Използването на некачествени компоненти и неподходящо програмно обезпечаване причинява чести сривове и откази в системата, паразитни електромагнитни излъчвания, загуба на информация, нарушения в комуникациите, опасност от несанкциониран достъп до информацията и проникване на нарушители, чрез заобикаляне на мерките за сигурност.

Ето защо от голямо значение е да се възприеме схващането, че организацията е тази, която първа трябва да се погрижи за своята безопасност посредством правилна стратегия на управление и търсене на компетентно и професионално изграждане на една комплексна система за сигурност.

В Глава II разглеждам примерен обект „София аерогара – център“, принадлежащ към системата на Аерогара София, разположен недалече от нея и охраняващ помещения с нейно карго. Ето защо, в края на този кратък теоретичен обзор намирам за изключително уместно и полезно да включа някои „добри примери“ от европейската и световната практика по охрана и сигурност на аерогари. Техните проблеми отчасти се съотнасят с проблемите на разглеждания от мене обект и могат да служат като посока за следване в усилията за актуализиране и усъвършенстване на охранителната дейност в България. Европейските изисквания, посочени в редица регулаторни документи, налагат изграждането на съгласуваност и координация по сигурността между държавите членки на ЕС и нашата страна трябва да ги изпълнява.

## 3. Добри примери от европейската практика по охрана и сигурност

*Франция*

През април 2014 г., Nice Côte d’Azur става първата аерогара в континентална Европа, сканираща целия чекиран багаж чрез Стандарт 3. Marc Terraillon, началник на „Сигурност и охрана“, в обобщението си за нововъведението споделя, че заплахите на сигурността стават все по-обиграни, а чекираният багаж под постоянна щателна проверка. Това е наложило авиационната индустрия и аерогарата да установят една

Nice Côte d'Azur Airport

„направляваща рамка“ (regulatory framework) за сигурността на авиацията и аерогарата, която изпълнява постановленията на европейско, интернационално и национално ниво.“[10]

*САЩ*

За сравнение, Администрацията по сигурността на транспортирането в САЩ вече сканира 100 % от чекирания багаж в търговските превозвачи, и съгласно „Акт 11 септември“ (Акт 9/11), цялото карго, превозвано на пътнически превозвач, се проверява за експлозиви от 1 август 2010.[11]

*Европейската гражданска авиация*

Конференцията на Европейската гражданска авиация (European Civil Aviation Conference – ECAC) е създала „сили за технически задачи“ (Technical Task Force), които да се заемат с развитието на технически спецификации и тестващи методи за проверка, съгласно стандартите, изисквани за приложение в европейските аерогари. Обичайният процес на оборудване за сигурността на ECAC прилага за експлозивите проследяваща система (explosive detection systems – EDS) и скенери по сигурността.[12]

Специално внимание заслужава „Стандарт 3“ (‘Standard 3’). Той е оперативна рамка на Конференцията, която регулира и гарантира минималното изисквано ниво на проследяване в съгласие с Наредба 1087/2011 на ЕС (EU Regulation 1087/2011). ‘Standard 3’ утвърждава

[10] Виж http://www.internationalairportreview.com/advent-calendar/19-december-2014/
[11] Пак там
[12] Пак там

детайлното измерение да бъде прилагано относно основните обикновени стандарти за сигурност на въздушния транспорт, по-специално отнасящо се до проследяване на експлозиви. В Наредбата се посочва: „Standard 3 must be applied to all EDS installed as of 1 September 2014“ (Стандарт 3 задължително да се прилага към всички системи за проследяване на експлозиви – EDS= explosive detection systems, инсталирани към 1 септември 2014 г. – прев. мой Ал. Л.).

В отговор на Наредбата, много от летищата в ЕС са задвижили покупката на Standard EC 3 EDS преди крайния срок през 2014 г.

*IATA*

Международната асоциация на въздушния транспорт (The International Air Transport Association – IATA) е професионалната асоциация за световните авиолинии, представляваща около 260 авиолинии или 83% от целия въздушен трафик. През 2015 г. се провежда годишният IATA форум, на който се обръща специално внимание върху сигурността на веригата за доставки (supply chain security)[13]. Най-затрудняващото изискване, относно транспортираната стока в Европа, е Регулаторен документ ACC3 на Европейския съюз (the European Union`s ACC3 regulation), влязъл в сила на 01.07.2014 г. Това изискване се прилага към въздушния транспорт на трети страни към европейските граници. То изисква превозвачите да бъдат независимо узаконени (валидирани) за ефективността на мерките за сигурност на техните аерогари. В изпълнение на изискването, IATA основава Център за високи постижения на независимите узаконители (Center for excellence for independent validators (CEIV). CEIV дава гаранции, че членовете на IATA са 100-процентово отговорни за своите задължения по ACC3. Освен това, Асоциацията е тренирала близо 100 законни представители да провеждат изискваните проверки.

Посочените примери са само малка част от европейските и световните актуални мерки, взети по отношение на охраната и сигурността. Те са естествено следствие от пет пъти увеличилия се тонаж на карго и поща във въздушния транспорт от 1990 до 2015 г.[14] Към този факт трябва да добавим и синдрома „11 септември“, който допълнително активира дейността по охраната и сигурността на въздушните превозвачи.

[13] http://www.iata.org/2015-review/index.html

[14] http://www.statistiques.public.lu/stat/TableViewer/tableView.aspx?ReportId=7053&IF_Language=eng&MainTheme=4&FldrName=6&RFPath=7047

Тук споделям моето лично мнение, че прилаганите мерки трябва да станат ръководни и за Аерогара София в дългосрочен или краткосрочен план, най-малкото с оглед на предстоящото влизане на България в Еврозоната. България ще бъде задължена да постигне съгласуваност с европейските регулаторни рамки и колкото по-рано се координира с изискванията, толкова по-плавно биха се извършили процесите на промени.

Това естествено рефлектира и върху актуализирането и усъвършенстването на охранителната дейност на разглеждания в Глава II примерен обект „София аерогара – център“ като принадлежащ към Аерогара София. Смятам, че на фона на европейските регулаторни документи, наложително е охраната и сигурността на обекта адекватно да се координира и синхронизира с европейските изисквания, като направи това в необходимата степен и на необходимото ниво.

# ГЛАВА II

# *SWOT* АНАЛИЗ – УСПЕШЕН ПОДХОД ЗА АКТУАЛИЗИРАНЕ И УСЪВЪРШЕНСТВАНЕ НА СИСТЕМАТА ЗА СИГУРНОСТ

## 1. Същност на SWOT анализа

След краткия теоретичен обзор в Глава I, тук ще разгледам структурата на един практически модел на системен аналитичен подход за изследване на коя да е организация. Категорично съм на мнение, че той е изключително ефективен и функционален за обследване на обект, преди изготвянето на проект за охрана и сигурност. При това не е труден за прилагане дори частично, т.е. с непълно използване на заложените му параметри. В пилотното изследване по настоящата магистърска теза го приложих частично като работен модел и позитивните резултати доказаха, че трябва да стане основен компонент от дейността на всяка организация.

В нашия технологичен и информационен век функциите на анализа нарастват с невероятна скорост. Световни изследвания предвиждат през

2015-2016 г. да започне усвояване на информация от различни източници на структурирани и неструктурирани данни. Това ще става чрез средства за анализ. Възможностите на мрежовите камери да предоставят високи резолюции и да бъдат монтирани навсякъде ще се използват за черпене на все повече информация от все повече източници. Обемът на данните, скоростта на обработката и разнообразието от източници ще бъдат ключови в кризисни ситуации за вземане на бързи решения въз основа на последната налична информация. Това налага използване на по-самостоятелни и по-автоматизирани аналитични инструменти.

Аналитичният подход, известен като „SWOT анализ“ и широко използван в Европа и Америка, е доказал своята ефективност при прилагането му в различни сфери – икономика, бизнес, обществени услуги, в големи компании и малки фирми. По мое мнение, той може да има ефективно приложение и към охранителната дейност, като неговият принос може да бъде в различни посоки:

- За организация на предварителната проучвателна работа на обекта, който ще се охранява;
- за систематизиране на резултатите от анализа;
- за изготвяне на проекта;
- за поддържане функциите на внедрената система за сигурност;
- за подобряване, актуализиране и усъвършенстване на охранителната дейност.

Целта на Глава II е да защитя тезата си, че е необходимо актуализиране и усъвършенстване на приложения вече проект за охранителна система на обект „София аерогара – център“. За целта използвам SWOT анализа като системен подход, разширявам го и го обогатявам, и доказвам, че се налага непрекъснато извършване на подобрения, независимо от добре функциониращия към момента на проучването проект за сигурност.

Разположен в близост до аерогарата, обект „София аерогара - център“ изпълнява функцията да охранява част от потока на каргото на аерогарата, служителите на различни фирми, разположени на територията му, и потока от техни клиенти – собственици или получатели на охраняваната стока. Споделям моето категоричното мнение, че той потенциално и в определена степен е застрашен от характерните основни заплахи за аерогарата.

Паралелно с това, специфични и актуални за обекта са заплахите от кражби, опити за каквито са били извършвани до преди 1-2 години. Взетите мерки по охраната са предотвратили осъществяването им, но съм убеден, че работата за подобряване на сигурността задължително трябва да продължи. За тази цел, *експериментално прилагам допълнително разработения от мене SWOT анализ за обследване и изготвяне на предложение за подобрение на сигурността, което се прави за първи път в охранителната дейност в България. При това работих само по един параметър на модела – слабости, но ефективността на постигнатите резултати ми даде основание да изготвя своето Предложение за подобрение. Така стигам до своето лично заключение, че приложен в своя интегративен системен вид, анализът би бил многократно по-ефективен метод за изготвяне на цялостен проект за охрана и сигурност, както и за периодично прилагане с цел поддържане и непрекъснато актуализиране и усъвършенстване на охранителната система на обекта.*

Какво е SWOT анализ? Названието SWOT анализ е абревиатура, която произлиза от четири думи, назоваващи неговите параметри: S = strengths (сили), W = weaknesses (слабости), O = opportunities (удобни случаи, благоприятни възможности) и T = threats (заплахи).

SWOT анализът се извършва въз основа на събрана информация относно четирите параметъра, измерващи състоянието на обекта и връзката му с околните обстоятелства. От гледна точка на количествения състав на компонентите, е видно, че *SWOT анализът е системен анализ*, в чиято формула влизат параметри, характеризиращи обект, фирма, дейност. Те се намират в определени отношения и зависимости помежду си, които ги свързват в система с подвижна и динамична субординация. Анализът на *силите, слабостите, удобните случаи/благоприятните възможности* и *заплахи* и техните взаимозависимости и влияния определят съотношенията между параметрите, които са от голямо значение за ефективната дейност на една фирма, или в нашия случай, на охранителната дейност. От тях могат да се извлекат заключения за степента на развитие на лошите тенденции, както и да се обобщят стратегии за извършване на подобрение.

След направеното проучване на обекта с частично прилагане на *SWOT анализ,* стигнах до аргументираното си убеждение, че характерът му го прави преди всичко *ситуативен модел*. Това мнение досега не е споменавано от други автори. Знаем, че всяка ситуация се измерва с параметрите време, място, участници, теми, цели, задачи. Това означава, че

извършването му става в определен времеви момент, в който се изследва и параметрично измерва определена ситуация с актуални външни условия и дадено вътрешно състояние на организацията.

От гледна точка на охранителната дейност, външните условия, в които в по-голяма степен се пораждат и развиват заплахите, бързо се променят. Същевременно, организацията вътрешно остава по-тромава, по-инертна и по-бавно реагираща. Така една вътрешна, сравнително статична среда, е подложена на атаките на една външна, твърде динамична среда от променливи. Ето защо, смятам, че колкото и да е прецизен анализът, той остава ситуативен, т.е. определя взаимодействията на компонентите в дадена ситуация, т.е. в определено време, на определено място, с дадени участници и техните цели и задачи.

Моето лично убеждение за особеното на SWOT анализа, приложен в охранителната дейност, е, че е и строго времеви сегментиран. Информацията за него се събира в определен времеви сектор, в който не биха могли да се отчетат изненадите и непредвидените промени, които ще настъпят в следващия момент. Резултатите от анализа отчитат вътрешните *сили* и *слабости* на организацията, характерни за обекта, но те не са толкова динамични. Отчитат се и външните *удобни случаи/благоприятни възможности* и *заплахи,* посрещани от нея, но в даден времеви сегмент, които обаче са изключително динамични. Това означава, че разкриването на взаимозависимостите между четирите параметъра дава възможност да се изследва детайлно тяхното състояние в даден отрязък от време. От получените резултати може да се изгради обобщена картина на състоянието, от която да се извлече стратегия за подобряване на охранителната дейност за даден времеви отрязък. Ето защо тук споделям своето убеждение, че поради непрекъснато променящите се външни условия, SWOT анализът трябва да се прилага периодично, водейки се от характера и силата на заплахата и динамиката на външните промени. Така той може да поддържа динамична актуалността на своите резултати и да предлага “non-stop” адекватни на ситуацията стратегии за подобрение.

В основата на SWOT анализа лежи важната задача да се отчитат две от най-важните характеристики на една организация, или в моя случая, на една охранителна дейност на обект, а именно вътрешните *сили* и *слабости*. Същевременно моделът маркира вътрешните и външните *удобни случаи/благоприятни възможности* за промяна и вземане на мерки за преодоляване на слабостите. Измерението на външните, а както видяхме в

глава I и на вътрешните *заплахи,* изисква внимателно изследване на взаимозависимостите им, в резултат на което да се очертаят стратегиите за подобрение. Това, което открих по време на моето проучване, потвърди предварителното ми виждане, че взаимозависимостите между различните параметри съставляват сърцевината на анализа и са от изключително значение за крайния резултат.

Установих още, че приложен към охранителната дейност върху даден обект, аналитичният модел откроява потенциала и ресурсите за подобряване на сигурността в определена външна среда, характерна за обекта. Той може да бъде използван за анализ на всеки вид охрана: на организация, физически обект, личност, стока, мероприятие и пр. В зависимост от акцента на конкретно търсения ефект, се очертава и насоката за подобрение на дейността на охраняваната организация – нейното управление, административна структура, капацитет от човешки ресурси, методология за подбора им, организация на охранителната дейност, нейното качество и ефективност, модела на сигурността и пр.

В настоящата разработка доказвам своята предварително изградена хипотеза за необходимостта от актуализация и усъвършенстване на охранителната дейност на разглеждания обект, на който се използва сигнално-охранителна техника в съчетание с човешки ресурси по охраната. Те могат да бъдат реализирани чрез подобрения, изготвени въз основа на прилагането на SWOT анализа, За целта от резултатите извлякох стратегия за подобрение на сигурността до следващия SWOT анализ.

Тъй като анализът се извършва в определен времеви сегмент, твърдо съм убеден, че той може да бъде най-ефективен при периодично събиране на данни и периодичното му извършване. Периодичните анализи очертават промените, спрямо които да се извършат корекциите на стратегията, за да се подобрят резултатите. Периодите, през които да се извършва анализът, зависят от управленческата стратегия на охраняваната организация. Независимо от това каква е тя, според мене, актуализацията и усъвършенстването на охранителната дейност е задължителна, ако се мисли за сигурността на обекта в дългосрочен план.

В един съвременен проект за сигурност СОТ е неизбежен компонент. От практиката съм се уверил, че колкото и да има самостоятелна значимост в охранителната дейност, прилагането на СОТ е и функция от управлението на организацията, както и функция от компетенциите (знания, умения, вземане на решения, бързина на реакции и действия) на

охраняващия персонал. Тази взаимна зависимост се отразява във всеки отделен параметър на SWOT анализа – *сили, слабости, удобни случаи/благоприятни възможности и заплахи*. Следователно, моето обобщено виждане е, че във вземането на решение за подобрение на сигурността рефлектира състоянието на мениджмънта на охраняваната организация. Това показва колко зависима е ефективността на проекта за сигурност от управлението като компонент на всяка дейност. От друга страна, това още веднъж доказва необходимостта от системен характер на аналитичния модел, който трябва да се използва.

Моето становище е ясно определено относно темата за *подобрението:* подобрението е непрестанен процес за всяка организация и трябва постоянно да се развива. В края на Глава I споменах някои „добри примери“, които илюстрират европейското мислене по отношение на адекватността на сигурността спрямо заплахите в непрекъснато променящите се условия. Смятам, че подобрението като “non-stop” процес винаги започва от случай на подобрение в миналото, който се изследва, за да се извлекат ключови концепции и се покаже как е било намерено решението за подобрение.[15] Тук подчертавам важността да се направи първият SWOT анализ, за да се постави началото на *процес от подобрения.*

В охраната и сигурността ситуацията е много динамична. В Глава 1 подробно се очертаха движещите сили на техниката, технологията, методите, човешките ресурси. Според мене, популярната фраза „след 11 септември светът вече не е същият“ се базира на прозорлив анализ именно на *сили, слабости, удобни случаи/благоприятни възможности* и *заплахи*. Това изисква SWOT анализът да бъде прилаган периодично, като периодите се определят от самата организация, от характеристиките на конкретния обект, от динамиката на външните промени, от динамиката и агресивността на заплахите, от резултатите от съответния анализ и очертаните стратегии и цели от предишния анализ.

Дотук набелязах *същността и функциите* на SWOT анализа, както и моите лични наблюдения върху взаимовръзките и влиянията на неговите компоненти. Стигнах до заключението, че не по-малко значими са *механизмите* при прилагането му. На първо място това е *комуникацията като негов основен движещ механизъм*.

[15] Виж http://isd.engin.umich.edu/professional-programs/lean-six-sigma/index.htm#sthash.iETeNYt5.dpuf

От изследването на наблюдавания от мене обект извлякох извода, че комуникацията е най-важен източник за получаване на актуална информация в насоката, която представлява интерес за изследването. Тя е основно движещо средство за осъществяване на всеки анализ. Ако комуникативните връзки в организацията не са разработени правилно или въобще не са разработени, ако е наложен принципът „мълчиш и работиш“, за да си запазиш мястото, или цари страх от наказания при някои форми на комуникация, то събирането на информация от по-ниските нива в структурната йерархия, необходима за изготвянето на един анализ, ще бъде спъвано от страха. Подобни предварителни опасения се оказаха верни за разглеждания обект.

Информиращата комуникация може да се осъществи под различни форми: доклади, рапорти, съобщения, дискусии, семинари, анкети, мнения и пр. От една страна, тя е ключова функция на управлението, тъй като една организация не може да оперира без комуникация между своите йерархични нива, отдели и служители. Същевременно, обаче, трябва да функционира и принципът за съхраняване на поверителната информация. От това следва, че изграждането на комуникативното ниво на организацията е специална задача на управлението. В моето проучване от него зависи и успешното провеждане на анализа.

## 2. Функционално-приложна структура на SWOT анализа: Етапи на работа

По време на работата си по магистърската теза се запознах със SWOT анализа и се отнесох критично и аналитично към неговия модел. Реших, че той е подходящ не само за бизнеса, но и за охранителната дейност. Моделът предлага основните параметри за изследване, но най-важното остава как и в каква последователност на практика да бъде извършено това. За целта разработих процеса на неговото прилагане в *четири етапа*. Те го организират в последователни действия, които следват логиката на научните методи за събиране на данни, техния анализ, синтез и обобщение. Така определих методиката за работа с модела при измерване състоянието на една охранителната дейност, организирана по някакъв проект за сигурност.

По-долу предлагам неговите етапи, които старателно категоризирах и формулирах.

**I етап – дескриптивна статистика**.

От подробния анализ, който направих на модела, заключих, че той трябва да се прилага поетапно. Така стигнах до идеята да го разделя на 4 етапа. Първият етап логически трябва да започва със събиране на данни, описващи картината на сигурността. Нарекох го „дескриптивна статистика“, т.е. описване на данните. Събирането на статистическите данни и тяхното описание става посредством определени методически подходи и средства за целенасочени проучвания. Това могат да бъдат писмени материали от доклади, рапорти, семинари, дискусии, проучвания, анкети и пр., които имат определена тема и описват състоянието на обекта по някои от четирите параметъра – *сили*, *слабости*, *удобни случаи/ благоприятни възможности* и *заплахи*.

За един външен анализатор това е трудна за изпълнение задача, поради утвърденото в организацията специфично съдържание на понятието „поверителна информация“ и условията за нейното споделяне. За вътрешния анализатор, обаче, т.е. член на административния състав, не би трябвало да има непреодолими “тайни“. Неговата работа по анализа е поръчка на ръководния състав, който е заинтересуван от ефективно свършена работа.

В случая с разглеждания обект, анализаторът в мое лице се явявам външен човек, макар и бивш служител в състава на охраната. Поради тази причина, действието на принципите за поверителност спъваха работата ми по събиране на дескриптивната статистика. Ето защо се насочих към параметъра *слабости*, който беше най-достъпен за проучване и най-познат на колегите охранители в ежедневната им дейност.

**II етап – разчитане, разбиране и анализ на данните**.

Определям този етап като начало на същинската аналитична работа. На него се разчитат получените данни, дешифрира се тяхното значение и се определят взаимовръзките им. Именно в отношенията между показателите на параметрите се търсят причините и следствията, които определят тяхното движение в позитивна или негативна посока. Те дават яснота за вземане на аргументирано решение и очертаване на стратегия за подобрение на състоянието.

Намирам за изключително ефективна нагледната представа, която може да се добие от набора данни по всички параметри и техния анализ. Ето защо в допълнение към този етап включих изготвянето на диаграми на показателите на отделните параметри: *сили*, *слабости*, *удобни случаи/ благоприятни възможности* и *заплахи*. Диаграмите визуално представят

резултатите от анализа на статистическите данни и очертават тенденциите и степента на тяхното развитие през изследвания времеви сектор, което улеснява решенията за промяна.

В заключение бих обърнал специално внимание върху факта, че този етап уведомява административното ръководство за регистрираното състояние на охраната и с това играе роля на първи сигнал за планиране на някакви ръководни мерки.

Моята работа по обекта беше изключително върху параметъра *слабости*. Това се наложи от ограничената дескриптивна статистика, поради изяснените вече причини. Ето защо потърсих съотношенията на този параметър с другите параметри, за които можеше да се съди единствено по събраните от анкетата статистически данни за *слабостите*. Разбира се, това съвсем не е достатъчно, но беше единственото решение при съществуващите обстоятелства. Моето мнение е, че дори и при ограничено прилагане на анализа, т.е. само по един параметър, и твърде стеснена дескриптивна статистика, резултатите от неговото проучване в определен времеви сектор могат да доведат до предложение за подобрения. Макар предложението да не е изградено в резултат на системен анализ на четирите параметъра, то се явява достатъчно ефективно за вземане на някакви първоначални мерки.

**<u>III етап – групиране на променливите</u>.**

Този етап определям като аналитично най-ефективен от гледна точка на системния характер на модела. Тук целта е да се открият колкото може повече взаимоотношения и зависимости между параметрите в различни комбинация по двойки: например, между *заплахи* и *удобни случаи/благоприятни възможности,* между *заплахи* и *слабости,* между *заплахи* и *сили;* между *сили* и *слабости,* между *сили* и *удобни случаи,* между *удобни случаи* и *слабости.* Категорично съм на мнение, че определянето и анализът на взаимовръзките между параметрите са най-информативната част от системното изследване, която играе основна роля за изясняване на проблемните места и изработване на проект за подобрения.

Според мене, на първо място интерес представляват *слабостите* като базова проблемна сфера на коя да е фирма, в коя да е дейност. Поради това в моето проучване на обекта се насочих към тях. В съотношението *слабости – удобни случаи/ благоприятни възможности* изследвах възможностите за преодоляването им, от една страна, както и възмож-

ностите за поява на заплахи именно на местата или по времето на проявяващите се слабости.

В процеса на изследването стигнах до заключението, че в непосредствена зависимост от тях са *заплахите*, т.е. потенциалните извършители и техните цели. От личните си наблюдения като охранител съм се убедил, че много често голяма степен от заплахите се реализират въз основа на слабостите. От друга страна, в комбинация с *удобни случаи/ благоприятни възможности* за осъществяване на *заплахите* трябва да се търсят взаимозависимости, които очертават *възможните ситуации* за тяхното осъществяване. Те дават отговорите на класически важните въпроси „защо = поради какви причини“, „как“, „кога“, „къде“ и „при какви обстоятелства“ може да застрашат обекта.

Взаимоотношенията между *слабости* и *удобни случаи/ благоприятни възможности* могат да се разгледат и в трети аспект: да се търсят пропуснатите случаи и възможности за реагиране и вземане на превантивни мерки от екипа, отговарящ за охранителната дейност, от една страна, или от ръководителите на фирмата, от друга страна. По този начин се работи в дълбочина на анализа на взаимоотношенията между два параметъра до степен, до която анализаторът може да види причини и следствия във връзките между параметрите. Практиката затвърди моето предварително убеждение, че работата по сигурността се осъществява по всички нива на административната йерархия – от управителното тяло до охранителя, и посредством техните комуникативни взаимоотношения.

От друга страна, например, взаимозависимостите между параметрите *сили* и *слабости* могат да бъдат разгледани за цялата организация/фирмата или за един неин отдел, например, отдел охрана и сигурност. Същевременно връзките могат да се разглеждат както по отношение на слабите страни, така и по отношение на силните страни, които да се използват за намаляване или преодоляване на слабите, или за намиране на актуални подходи за отстраняването им.

По този начин групирането и прегрупирането на параметрите, прилагането им за цялата организация или за част от нейната дейност и пр. осигурява възможно най-широк поглед върху тяхното състояние и рефлектиращо значение.

Разработвайки модела на SWOT анализа, стигнах до заключението, че в резултат на сумарния анализ от групираните променливи, може ясно да се очертаят различни *стратегии* за действия: за борба със *заплахите*, за

превъзмогване на *слабостите*, за целенасочена работа по използване на *благоприятните възможности,* за начини и средства за черпене от ресурсите на *силите* с цел по-ефективни действия.

От резултатите на анализите върху различно групираните променливи мога да извлека две обобщени направления в стратегиите: ***агресивно*** – свързано с актуални и спешни действени мерки за реагиране срещу застрашеността, и ***пасивно*** – непрекъснато разгръщащи се във времето подходи и средства за актуализиране и усъвършенстване на охраната с цел повишаване на сигурността.

**IV етап – контролен анализ**

В края на аналитичната си работа върху модела на SWOT анализа установих, че има логическа необходимост от един заключителен етап, който смятам за изключително важен. Наричам го *контролен анализ*. Той не е свързан с показателите на параметрите, а с анализ на извършената от самите анализатори работа, на техните методи и средства, на пропуските и добрите им страни и пр. Обобщаващият четвърти етап се явява един вид „самоконтрол на анализаторите върху извършената от тях дейност“.

В този етап включвам два вида анализ: *количествен анализ* и *качествен анализ. Количествен анализ* наричам анализа на количеството събран изходен материал за извършване на проучването и обследване на обекта. *Качествен анализ* е анализът на качеството на работния процес, осъществен през определените от мене три етапа при прилагането на SWOT анализа. Целта на двата обобщаващи анализа е да се постигне максимална ефективност на приложената стратегия на проучванията, обработването на данните и синтезирането на резултатите от тях. Тук се отчитат всички позитиви и негативи на извършените действия.

Какво означава това? Знаем, че събирането на определено количество данни трябва да се осъществява според научния принцип за „необходимост и достатъчност“, за да се получи качествен резултат. Ето защо в този допълнителен етап предвиждам да се проследи дали събраното количество изходни статистически данни се е оказало „необходимо и достатъчно“, така както е било заложено и осъществено в проекта на I-ия етап от анализа. Количественият признак се формира от *необходимия и достатъчен брой* на: например, източници за набиране на информация – писмени материали и хора, брой набелязани подходи и средства, брой ситуации на заплаха, брой времеви отрязъци за анализ, и пр.

Съобразяването с количествения признак за „необходимост и достатъчност“ осигурява по-високо качество на резултатите от анализа. Поради тази причина, от изводите от количествения анализ започва анализът на качеството на аналитичния процес и цялостно извършената работа.

Качественият анализ задължително следва количествения. От него може да се добие представа за ефективността на извършеното, но така също и за вероятната ефективност на пропуснатите източници на информация, констатирани при количествения анализ като „необходими“, но нереализирани. Установяват се и пропуснатите възможности за реализиране на други подходи и средства за набиране на информация, ако използваните са констатирани като „недостатъчни“, и пр. Моето лично убеждение е, че определянето на качеството на извършената изследователска работа върху обекта, като цяло, и качеството на аналитичния процес, в частност, водят до неговото повишаване при прилагане на следващия SWOT анализ. Това се отразява върху ефективността на всички усилия за постигане на подобрения в сигурността на обекта.

Системният анализ по модела SWOT приключва с идентифициране на основните параметри, каквато е била и целта му: местата, степента и рефлексивната сила на *слабостите,* класическите и актуалните форми на *заплахите* върху обекта, количеството на реализираните и пропуснатите *удобни случай/благоприятни възможности* за използване на силите за противодействие. Интегрираният обобщен вид на синтеза на тълкуванията очертава стратегия за повишаване ефективността на охранителната дейност. *Предложението за стратегия за подобрения е крайната цел на SWOT анализа.*

Изводите от IV-я контролен етап строго се вземат под внимание при подготовката на следващия SWOT анализ.

Тук обръщам специално внимание на един много важен компонент, който добавям като съпътстващ паралелен non-stop процес. Това е *метод на контрол,* прилаган за проследяване правилното осъществяване на процеса „подобряващи действия“, очертани от стратегията.

Според мене, стратегията трябва да включва предложение за подобрение и трябва да предвижда методически подходи, начини и средства за контрол. Контрол е необходим да се извършва над изпълнението на подобрението. Същевременно, такъв се налага да се осъществява и над непрекъснатия процес по разлагане на причинно-

следствената връзка на външните променливи *заплахи-потенциални извършители.* Трябва да се предложи и метод на контрол над *слабостите,* както и метод на контрол за развитие на *силите*.

Контролът се извършва от съответното управляващо административно тяло: конкретно за охранителите са инспекторите по охрана, а над тях са служители от различните йерархични нива на организационната структура, които изпълняват задачи, свързани с охранителната дейност, а на върха на йерархията е ръководителят на фирмата.

В края на представянето на разработения от мене по посока на охранителната дейност и усъвършенстван модел на SWOT анализа, ще се спра накратко на един важен характерен белег. За да разберем силата на модела като системен подход за изготвяне на охранителна система, както и за нейното подобрение, актуализиране и усъвършенстване, трябва да осъзнаем необходимостта от *критическо мислене* по всички нива в структурата на охраняваната организация, както и на служителите по охраната, когато те са външни за организацията хора. Ето защо, тук отделям специално внимание на критическото мислене.

*Критическо мислене*

Критическото мислене е необходима черта на разсъждение и отношение, която трябва да характеризира процеса на изпълнение на SWOT анализа. То изисква обективно проучване на всички предположения за вероятни заплахи, които могат да направят в резултат на личните си наблюдения служителите на охраняваната организация, както и служителите на охраняващата фирма – от охранителите до най-високите нива на административната йерархия. Паралелно с това се преразглеждат и възприетите правила на управление, които са съобразени или несъобразени с тях и подчертават действащите убеждения. Проучването се прави с цел да се прецени адекватността, коректността и легитимността на правилата, и така да се потвърдят или отхвърлят определени убеждения: обикновено това са за заплахи, за използването на СОТ, за организацията на охранителната дейност, за управлението и пр.

Моето лично виждане за критическото мислене е, че е знаков фактор за служителите на всяка организация, а оттук и на организацията като развиващо се тяло. Ако липсва или е в недостатъчна степен проявено поради различни причини, това възпира развитието на организационната система. Ето защо критическото мислене трябва да съпътства

провеждането на всеки анализ. Под неговия знак трябва да се осъществява SWOT анализът и поради специфично действащи фактори в сферата на охраната. Непрекъснато изменящата се среда и обстоятелства внасят различна информация в параметрите „сила“, „слабости“, „благоприятни възможности“, „заплахи“, и ако те не бъдат отбелязани от най-строга критична гледна точка, за да бъдат взети мерки, то по-рано или по-късно ще се завърнат с „ефекта на бумеранга“.

По мое мнение, критическото мислене успешно може да се прилага и за сравняване на базата данни от предишните анализи и настоящия анализ, за да се извлекат позитивите, да се установят грешките и пропуските, и да се нанесат корекциите в избраната стратегия, която трябва да отчита старите и новите данни.

Тук искам да подчертая моето категорично убеждение, че при прилагането на системния модел за анализ критическото мислене е негово задължително качество. То е средство за категоризиране на състоянието на сигурността и охранителната дейност като процес. Дали те ще попаднат в категорията „необходимост от подобрения“ до голяма степен зависи от критическото мислене на всички служители, а не само на ръководството.

Веднага ще посоча моите лични наблюдения от примера с анкетата, която анализирам по-долу като пилотно проучване на охраната на посочения обект. Ако липсваше критическо мислене у анкетираните лица – охранители на обекта, ако те бяха сковани от страха да не загубят работните си места и бяха пожертвали обективните факти за сметка на личното спокойствие, то анкетата нямаше да може да изпълни функцията си на достоверност в проучването методическо средство.

И накрая, в относителна степен и в ограничен параметър демонстрирам действието на аргументирано допълнения и развит от мене модел на системен анализ и прилагам резултатите, анализа и синтеза на моето конкретно проучване.

## 3. Анкета за пилотно проучване на сигурността на обект „София аерогара – център“

Предвидих и изготвих анкетата с оглед на конкретния обект и обстоятелствата, при които извършвам проучването.

Обект: „София аерогара – център“, прилежащ към аерогара София, охраняващ карго и физически лица.

Обстоятелства: Извършвам анкетното проучване като бивш служител, на позиция „охранител“, към системата на охраната на посочения обект,.

Методика на изследване: Приложих методите на анкетното проучване, личните наблюдения и допълнителното допитване за извличане на информация за обекта, с цел разкриване на параметъра *слабости*. Лично изготвих анкетата и я приложих анонимно.

Анкетирани лица: Бяха анкетирани 15 охранители (настоящи и някои бивши) на обект „София аерогара – център“. Всички са от мъжки пол, на възраст между 22 и 55 години.

Съдържание на анкетата: Анкетата включва 5 въпроса, всеки от които се отнася до един от основните компоненти, изграждащи обектната охрана – *техника* (видео- и звукова), *персонал*, *мениджмънт* и *организация*, а първият въпрос изисква да се изберат най-слабите за охранителната дейност от посочените четири компонента.

Отговорите са избираеми, с четиристепенна оценка: 1) *напълно достатъчна/добра*, 2) *може да се каже, че е достатъчна/добра*, 3) *може да се каже, че не е съвсем достатъчна/добра*, и 4) *определено е недостатъчна/не е добра*. Изборът на отговорите на 2, 3, 4 и 5 въпрос очертава степента на слабостите, а отговорите на 1 въпрос посочват местата им.

Специфичното в Анкетата е, че отговорът на първия въпрос е логически обвързан с оценките в останалите 4 въпроса. Това би дало допълнителна информация дали анкетираните демонстрират критическо мислене или не, и до каква степен отговорите им са добре осмислени и дадени отговорно.

По-долу представям анкетата по реда на зададените въпроси и техните сумирани отговори. Предлагам анализ на резултатите, след което в обобщението им търся зависимостите между тях. Направеният количествен и качествен анализ дават представа за обстоятелствата, при които е осъществен разработеният SWOT анализ. Най-накрая обобщавам резултатите от анализите и предлагам четири корелации, в които в дълбочина на зависимостите да се търсят техните характеристики.

1. КОИ СА СЛАБИТЕ МЕСТА В ОХРАНИТЕЛНАТА ДЕЙНОСТ НА ОБЕКТА? – (можете да посочите повече от един отговор!):

а) техниката (видео- и звукова) – 9

б) подготвеността на персонала по охраната – 15

в) мениджмънта – 5

г) организацията – 4
д) други (отбележете кои) – 0

Анализ

Най-слабото място в охранителната дейност на обекта пада на подготовката на охранителите. 100% от анкетираните лица са показали висока степен на критично мислене към себе си на заеманата от тях длъжност „охранители –физическа охрана на стоки и хора без оръжие“. СОТ се откроява като второ слабо място с категоричните 33% „не съвсем достатъчна“ техника и 47% клонящи към изразяване на някакво съмнение за достатъчност „може да се каже, че е достатъчна“. Слабостите в СОТ са отбелязани в отговорите на 2-ия въпрос и изяснени в допълнителните проучвания по него.

На трето място като слабост е управлението с 33% и организацията на охранителната дейност с 27% като процентните разлики между тях не са значителни. Явно проблемът с „неподготвеността“ на охраната е сериозен, а в какво се изразява става ясно от допълнително събраната информация. Слабостите в СОТ бяха отбелязани в отговорите на 2-ия въпрос и отчасти изяснени в допълнителните проучвания по него.

2. ДОСТАТЪЧНА ЛИ Е СОТ В ОХРАНЯВАНИЯ ОБЕКТ?

а) напълно достатъчна – 3
б) може да се каже, че е достатъчна – 7
в) може да се каже, че не е достатъчна – 5
г) определено е недостатъчна – 0

Анализ

33% анкетирани показват критично мислене, макар и по-плахо да намират, че СОТ „не е достатъчна“, а 47% отбелязват неубеденост в нейната достатъчност. Логично е да допуснем, че първите твърдо са отбелязали техниката като слабо място и в първия въпрос, но останалите до 60%, посочили я като слабост в първия въпрос, т.е. 27%, явно принадлежат към групата на не съвсем убедените.

Допълнителните проучвания извлякоха на повърхността както причините за съмненията на неубедените в достатъчността на техниката, така и осъзнатите проблеми със СОТ на по-критично мислещите:

- Общият брой на камерите е 72 и 4 монитора: 3 монитора обхващат 20 камери и 1 монитор – 12;
- Отвън са разположени около 50 камери, а останалите около 22 са вътре;
- Въпреки че въртящи се камери има на всеки ъгъл на сградата, някои от които се задействат при сигнал, няма видимост на някои ъгли и чупки на сградите отвън (4 сгради с по 4 входа), което оформя „сенчести“ места, необхванати от видеонаблюдението;
- Липсват въртящи се камери на някои места отвън, за да обхванат периметъра – сигналното устройство, което реагира при допир;
- Случва се две съседни камери да не засичат обхвата си и също да оставят „сенчести“ места между тях за периметъра;
- В складовите помещения и рампите няма камери за наблюдение от охраната на КПП, но няма и информация дали някои друг, освен дежурните на КПП, наблюдава тези помещения;
- Камерите са некачествено монтирани: при силен вятър и други атмосферни условия, позицията им се измества от първоначално монтираното положение;
- Ефективността на камерите намалява в резултат на изместването им;
- Чести сривове в сървъра, някои за дълго време, сриват и ефективността на СОТ.

В резултат на събраната информация, можем да заключим, че има вероятност 72 да не е оптималният брой камери, поради което 33% отговарят за СОТ „може да се каже, че не е достатъчна“. Явно местата без видеонаблюдение смущават една трета от охранителите. Разбира се, само при детайлно обследване на обекта може да се установи дали причината е в неоптималния брой камери или по-скоро в некачественото им монтиране, периодична поддръжка и наложителен допълнителен оглед на монтажа след определени атмосферни условия, влияещи върху тяхното ефективно функциониране.

От така набелязаните проблеми в анкетата можем да обобщим, че дори само една трета от служителите по охраната ако мислят критично, SWOT анализът ще разкрие реални слабости и ще доведе до реални подобрения.

## 3. КАК ОЦЕНЯВАТЕ ПОДГОТОВКАТА НА ОХРАНИТЕЛИТЕ?

а) напълно достатъчна – 0
б) може да се каже, че е достатъчна – 0
в) може да се каже, че е недостатъчна – 6
г) определено е недостатъчна – 9

Анализ

По мнението на анкетираните служители, охраната реагира на всичко нередно, случващо се на обекта, включително и на аларми. Ето защо фактът, че 60% от анкетираните оценяват подготовката на охранителите като "определено недостатъчна", а 40% не толкова категорично я определят като „може да се каже, че е недостатъчна", говори за две неща. От една страна, за липси в професионалните компетенции на охранителите – знания, умения, мотивация, действия. Това буди съмнение, че подборът на тези служители става по определени критерии. От друга страна, липсата на утвърден „компетентностен модел", който задължително да се прилага към заетите в сектора, девалвира професията и уронва авторитета й на частен вариант на правоохранителна структура.[16]

От допълнителните запитвания става ясно, че оценката е дадена на база лични наблюдения по време на обучението при постъпването им на работа и впоследствие по време на изпълняване на задълженията като охранители. Всички анкетирани бяха категорични в следните слабости:

- предвидените 3-4 часа за теоретична и практическа подготовка за работа и запознаване с обекта са определено недостатъчни;
- интензитетът на подаваната информация многократно надхвърля времето, поради което тя не може да бъде пълноценно възприета, осмислена и запомнена;
- „на бърз ход" се показва само една част от местата на обекта, което оставя служителите неинформирани и впоследствие постепенно да се запознават с обектите и условията на терена, който охраняват;
- недопустим е фактът, че „обучението" на охранителите става 1-2 седмици след постъпването им на работа;
- при тази подготовка напълно неаргументирани са очакванията за „отлични" резултати;

От събраната информация може да се заключи, че има проблем в организацията на подготовката на новопостъпилите охранители. Тук

[16] http://www.bia-bg.com/service/view/14416

проблемът опира до мениджмънта на охранителната фирма на разглеждания обект. След което на най-ниско ръководно ниво отговорността пада върху инспекторите по охраната и сигурността, които са „низови ръководни кадри“ и трябва да отговарят на определени критерии: „5 г. стаж е необходим, според световните концепции за управление на специалните служби, на низовите ръководни кадри в службите за сигурност и обществен ред.“[17] Следователно, за постигане на максимално подобрение, трябва да се започнат действия по уточняване и решаване на проблемите както отгоре надолу, така и отдолу нагоре по административната йерархия на фирмата. За това могат да помогнат и отговорите на следващите 4-и и 5-и въпрос.

4. КАК ОЦЕНЯВАТЕ МЕНИДЖМЪНТА?

а) определено добър – 2
б) може да се каже, че е добър – 7
в) може да се каже, че не е добър – 6
г) определено не е добър – 0

Анализ

Радостно е, че 40% от анкетираните показват критическо разбиране на въпроса, за разлика от стоте процента отговорили критично, макар и в различна степен, на 3-ия въпрос за подготвеността на охранителите. Вероятно не се прави логическа връзка между проблема с подготовката на охранителите и управлението на охраняващата фирма.

От допълнителните запитвания стават ясни някои важни детайли, определили отрицателната оценка:

- няма изградена политика за подбиране на персонала: изразите, че за охранители се назначават хора „събрани от кол и въже“, „смотаняци“, се употребяват в смисъл на необразовани, нискокултурни, некадърни, неспособни, със слаба психика, с неподходящи физически качества, с липсващи умения за бързо реагиране и пр.;

[17] Радулов, Николай, бивш главен секретар на МВР. Предаването „МВР и отговорността“, НОВА ТЕЛЕВИЗИЯ, 20.00 ч., 15.01.2016.

- няма изграден стил на тип охранител, към който да се стреми всеки служител;
- няма подходящ човек, който да замени отсъстващия по здравословни или други причини;
- липсата на оптимален брой охранители (напр. на КПП, за което вече стана дума, 4 души наблюдават 4 сгради или 16 входа!) води до невъзможност за своевременно реагиране на даден код и дадена аларма и настъпва пълен хаос, (напр. за 2 минути пада електрическото напрежението, започва да изплува вода от водния резервоар, защото реагира като на пожар).

Резултатите от направеното пилотно проучване внасят известна яснота относно слабостите в управлението на охранителната дейност. От анализа може да се извлече стратегия за тяхното преодоляване и подобряване на охраната. Със сигурност, обаче, при едно щателно проучване и цялостно прилагане на SWOT анализа, ще се проявят много повече детайли, характеризиращи слабите места, за да може мениджмънтът да се актуализира в посока към по-голяма ефективност на охранителната дейност.

## 5. КАК ОЦЕНЯВАТЕ ОРГАНИЗАЦИЯТА НА ОХРАНИТЕЛНАТА ДЕЙНОСТ?

а) определено добра – 3
б) може да се каже, че е добра – 7
в) може да се каже, че не е добра – 2
г) определено не е добра – 3

Анализ

Тук отговорите са разнопосочни. В процентно отношение оценката на организацията на охраната клони към добра – 67%, макар че 47% от тях не са съвсем убедителни с мнението „може да се каже, че е добра“. Въпреки всичко 33% критични оценки са достатъчни, за да се заключи, че и тук има слабости.

При търсене на корелация с първия въпрос, където 27% са определили организацията като слабо място, тук се отбелязва преориентиране на 6% от анкетираните към по-критично отношение. Това означава, че в процеса на анкетата лицата търсят по-голяма определеност и яснота. Информацията от допълнителните запитвания показва, че вероятно анкетираните не са много

наясно кои дейности се отнасят до организацията на охраната. Въпреки това от личните наблюдения и практика на охранителите се посочиха конкретни примери за порочна организация:

- Служителите на КПП формално се водят 5, но редовно работят 4 души: един почти винаги е в отпуск или отсъства по здравословни, семейни, лични или др. причини;
- В КПП има разположени ДМС, видеонаблюдение, периметър, звуков сигнал, белезници, палки, радиостанции и с тях работят само двама дежурни охранители;
- От общо 4-мата охранители двама остават в КПП, а другите двама са разпределени в две от четирите сгради;
- Две от сградите остават без дежурен охранител, което говори за неефективност на организацията на охранителната дейност;
- Не се разпределят охранители не само във всички сгради на обекта, но и двама охранители се грижат за сигурността на 4 сгради с 4 входа всяка = 16 входа!;
- Двама охранители на 16 входа не могат да осъществят никаква охранителна дейност;
- Не се разпределя подходящият човек за сградата, т.е. с необходимите физически и психически качества;
- Не се разпределя подходящият човек за дадена позиция по време на дежурството (по същите критерии);
- На КПП са необходими минимум трима служители, а не двама, каквато е порочната практика понастоящем;
- При работата с кодове и ДМС на КПП, се налага моментално разчитане на алармата и незабавно реагиране: единият охранител има 3 минути да отиде до сървърното и да напише кода за спиране на алармата и отстраняване на проблема, докато другият охранител остава сам, което е нежелателно, за да наблюдава камерите и държи връзка с колегата си по радиостанцията;
- При междувременно настъпване на втора ситуация за бързо реагиране, КПП остава без физическо наблюдение от дежурен охранител, което е недопустимо;
- Разпределението на двамата охранители в КПП за обход и стационар не се ръководи от определени критерии (физически данни и умения,

психически качества, моментно състояние на лицето и пр.), а е водено от механичния принцип на редуването;

- Липсата на оптимален брой охранители лишава организацията от системност и принципност на нейното функциониране;
- Всеки срив в сървъра се следва от пълен срив и в организацията на охранителната дейност.

Една разработена анкета с тематично целенасочени детайлни въпроси би разкрила още много факти от организацията на охраната. Засега посочените слабости се обединяват от параметрите *стратегия* (място и време), *тактика* (начин и средства) и *човешки ресурс*.

Интересен е фактът, че в отговорите на 1-ия въпрос 27% отчитат слабост в организацията, докато на 5-ия въпрос процентът на критичните оценки нараства на 33%. Много е вероятно това съотношението да показва известно „съзряване“ на критическото мислене в процеса на анкетата, когато въпросите стават по конкретни. Дори да не се разбира добре ролята на организацията, от допълнително събраната информация става ясно, че организационните слабости се явяват значими за ефективното функциониране на проекта за сигурност, въведен на посочения за пример обект. Тяхната корекция би подобрила самата охранителна дейност и същевременно би туширала някои слабости в управлението. Задължително е, обаче, щателното проучване на състоянието на организацията на дейността, защото от него зависи елиминирането и на много други недостатъци.

В този заключителен етап анализирам количествения материал и качествения процес, протекли при SWOT анализа. Предварително направих уговорката, че задачата е да осъществя пилотно проучване на обекта с цел да потърся подобрения в сигурността, демонстрирайки действието на SWOT анализа. Принципите на поверителността не разрешиха да разполагам с необходимата информация, която ми се искаше, тъй като съм вече външен за фирмата анализатор. Въпреки това, обаче, ефектът от резултатите даде основание да завърша пилотното проучване с предложение за подобрение.

*Количествен анализ*. Направеното пилотно проучване обхваща информацията само за един параметър от SWOT анализа – *слабости.*Следователно, не може да се реализира третият етап „групиране

на променливи“ и да се търсят съотношенията между четирите параметъра. Т.е. в количествено отношение се извърши една четвърт от анализа, която също трябва да продължи да бъде разработвана в дълбочина и детайли. За да стане това, от една страна, въз основа на събраната информация трябва да се предвидят различни средства за извличане на детайлите относно проблема слабости, както и да се приложат адекватни на получената вече картина методи и подходи. От друга страна, количественият принцип за „необходимост и достатъчност“ изисква да бъдат обхванати не само конкретните охранители на КПП и четирите сгради, а възможно най-голям брой служители на охранителната фирмата, ако не всички, включително и работещи в другите фирми, разположени в четирите сгради. Следователно, количественият материал от пилотното проучване е съвсем в начален стадий. Това обаче не означава, че получените данни са по-малко значими. Те са необходими, които могат да очертаят основната картина на слабостите, но са недостатъчни.

*Качествен анализ*. Качественият анализ изисква достоверни статистически данни в количествено и качествено отношение. Качеството на изходните данни се базира на тяхната количествена „необходимост и достатъчност“, но също така и на достоверност при попълване отговорите на анкетата. Направеното пилотно проучване само открои посоките, в които да се търсят методи, средства и подходи за набиране на допълнителна и по-детайлна информация. Ето защо мога да кажа, че то постави началото на един анализ с анонимна анкета и допълнително проучване чрез срещи, разговори, мнения и лични наблюдения на най-важния контингент – охранителите.

Резултатите от анализите могат да се обобщят в четири корелации:

- ✓ I корелация*: СОТ – подготвеност на охранителите/персонала по охранителната дейност*

В отношението *СОТ – подготвеност на охранителите* разкрилите се слаби качества на някои служители в охраната доказват как може да се намали ефективността на използваната добра сигнално-охранителна техника. От менталните, психическите и физическите качества на персонала зависят бързото вземане на правилно решение, адекватни и съобразени реакции, ефективност на действията за изпълнение на конкретната задача. Проучването на слабостите показа, че някои от охранителите не отговарят на изискването за съобразителност и правилна

преценка на възникналата ситуация, както и на необходимостта от спешни действия. Теглото и възрастта, по-слабият физически статус на част от тях пречи на бързината на реагиране. Неспособността за бързо реагиране обърква. Поддаването на паника драстично намалява самоконтрола. В следствие на това, в спешните случаи „младите“ и „можещите“ изцяло поемат изпълнението на задачата и „изземват“ функциите на останалите дежурни. Така една част от охранителите се натоварва много повече за сметка на останалите, което довежда до преумора, но също и рефлектира в оценката и отношението на служителите към управлението и организацията.

Тази корелация може да се разглежда и в отношението *СОТ – подготвеност на персонала по охранителната дейност.* Тук спада *персонала по поддръжката на сигнално-охранителната техника*, които спадат към системата на охранителната дейност. Отбелязаните чести сривове в сървъра блокират сигнално-охранителната техника, а чрез нея и свързаната със СОТ охранителна дейност като цяло. Получават се краткотрайни и дълготрайни сривове, които са недопустими и категорично се явяват повод за задълбочено проучване на техния произход. Причините са различни, като най-чести са сривовете поради драстични промени в атмосферните условия. Не липсват и такива поради неправилна поддръжка на техниката, по-висока температура в помещението и пр., които причини биха могли да се изяснят при допитване до самите специалисти по поддръжката. В случая, според мене, възниква логическият въпрос дали има целенасочени действия за постигане на срив, като например, съучастие към престъпно деяние, саботаж и пр. Това би трябвало да подлежи на допълнително проучване.

В заключение за тази корелация бих обобщил, че от гледна точка на качеството на охранителната дейност, резултатите тук демонстрират правопропорционални отношения в двойката *СОТ–подготвеност на охранителите/персонала по охранителната дейност*: т.е. колкото по-усъвършенствано е технологичното оборудване, толкова по-високо ниво на подготвеност на персонала изисква. В противен случай не биха могли ефективно да се използват високотехнологичните качества на оборудването. Под думата персонал включвам, техници по поддръжката на техниката, специалисти по поддръжката на сървъра и сървърното помещение.

- ✓ II корелация: *СОТ – мениджмънт и организация*

Резултатите от I корелация между *СОТ* и *подготовката на охранителите/персонала по охранителната дейност* са функция от управлението на охраняваната фирма и от организацията на охранителната дейност. Тук корелацията показва нивото на управлението по посока на внедрената СОТ и организацията на охранителната дейност, свързана с нея. Доброто управление включва оптимално използване на ресурсите на фирмата за постигане на оптимална защита и сигурност. Така се връщаме към един от принципите за създаване на система на сигурност, а именно че тя е задача на ръководителя на организацията. Същевременно, обаче, сигурността изисква непрекъсната поддръжка и актуализиране, което показва дали така създадената организация на охранителната дейност функционира добре или е налице необходимостта от нейното преорганизиране.

В разглеждания случай с нашия обект, отбелязаната необходимост от още няколко камери за наблюдение на определени места по периметъра трябва да бъде взета под внимание от ръководителите, за да се избегне съмнението за слабост в наблюдението по периметъра. Тази слабост би могла да се използва по различен начин: от една страна, за оправдание на охранителите, че „техниката не показва нарушение“, или „броят на камерите е по преценка на ръководството“, „ръководството решава, не ние“. От друга страна, дава се възможност за спадане на отговорността на охранителя и прехвърлянето й към ръководството. Това от своя страна рефлектира в отношението на персонала към организацията на сигурността и управлението на фирмата.

Организацията по поддръжката на сървъра и оптималните условия за неговото функциониране е другото открoено слабо място. То е от първостепенно значение, тъй като причинно-следствената връзка между СОТ и работещия с нея персонал може да доведе до възпрепятстване и поредица от грешки в работата на останалите служители.

В заключение относно тази корелация, бих казал, че внедряването, поддръжката и функционирането на СОТ зависи от управителното тяло на фирмата като цяло, и от методите и средствата на организиране на охраната, в частност. В крайна сметка, лошото е, че отговорността се носи от всички, конкретно заети в охраната – от охранителя до ръководителя. Ето защо трябва да се избегне тази „колективна“ отговорност и тя да стане „персонална“.

- ✓ III корелация: *подготвеност на охранителите – мениджмънт на фирмата*

Съотношението в тази III корелация показва зависимостта на подготовката на охранителите от готовността на мениджмънта на фирмата да реагира за повишаване на тяхната квалификация. Логиката на корелацията е при по-ниска подготвеност да има по-висока степен на готовност на управлението да повиши компетентностите на служителите, което ще доведе до по-качественото извършване на охранителната дейност. В случая, обаче, съотношението между склонността на анкетираните към оценка „недостатъчна подготвеност“ на охранителите и колебанието между „добър и „недобър“ мениджмънт прогнозира, от една страна, слаба реакция на управлението за повишаване подготовката на охраняващия персонал, а от друга страна, говори за недостатъчно разбиране на анкетираните за ролята на управлението на фирмата за нивото на охраняващия персонал.

Моето категорично убеждение е, че *подготвеността на охранителите* изцяло зависи от *мениджмънта на фирмата.* Управителното тяло решава дали са налични необходимите качества на кандидатите, за да инвестира в тяхната подготовка. Когато тези функции се изпълняват от отговорника по организацията на охранителната дейност, какъвто е случаят в разглеждания обект, тогава неговите персонални качества рефлектират в нивото на организацията на охранителната дейност, а оттук в мениджмънта на фирмата. Причинно-следствената връзка по административната йерархия „отгоре надолу“ и „отдолу нагоре“ е явна и отчетлива. В този случай предложенията могат да идват и „отдолу“, докато решенията се вземат само „отгоре“.

- ✓ IV корелация: *подготвеност на охранителите – организация на охранителната дейност.*

Също толкова нелогична корелация се получава и в оценката на анкетираните при съотношението „недостатъчна“ подготвеност на охранителите (около 100%) и преобладаваща „добра“ организация на охранителната дейност (75%). Ако организацията на дейността е на ниво, това би означавало, че е изпълнено нейното задължение да се грижи за добрата подготовка на охранителите. Това отново води към извода, че повечето анкетирани не правят връзка между компетенциите на

охранителите и организирането им за изпълнение на различни задачи, което се отразява на ефективността на охраната.

Както вече казах в предишната корелация, предложенията за подобрения могат да идват и отдолу, т.е. от охранителите, и ако отговорникът по организация на охранителната дейност не реагира, върхът на йерархията е ръководителят на фирмата. Тази комуникация може да доведе до подобряване на организацията на охраната, от която всички са заинтересувани, защото от нея зависи качеството на сигурността.

Дотук мога да обобщя, че в основата на несполуките в охраната на разглеждания обект лежи *човешкият фактор*. Именно на него неслучайно европейските организации обръщат специално внимание в търсене на начини за подобрения. Човешкият фактор се проявява в *комуникацията*, която може да е под формата на интервю при постъпване на работа, споделено мнение от гледна точка на работната позиция, съобщение за наблюдавана нередност, предложение за избягване на недостатък, и др., като всички те са форми на *критично мислене*. Така затварям кръга на проблематиката като стигам до това, от което започнах – ролята на човешкия фактор и неговия отличителен белег критическото мислене.

Заключение от анкетните резултати

Резултатите от Анкетата демонстрират, че при прилагането на част от SWOT анализа, т.е. на един негов параметър, моделът ефективно служи като методическо средство за предварително базово проучване. То може да се провежда преди изготвянето на актуализиран проект за защита на организация със сигнално-охранителна техника, както и за извличането на предложение за подобрения на изградена вече система за сигурност.

Цел на Анкетата беше проучване на най-значимият, по мое мнение, параметър от SWOT анализа, а именно *слабости*. Въпросите в анкетата пилотно потърсиха слабостите в основните конструктивни елементи, изграждащи една охранявана организация – сигнално-охранителна техника, охранители, организация на охраната, управление на охраняваната фирма. Получените резултати разкриха слабости, за ефективното отстраняване на които трябва да продължи да се проучва по посока на всички компоненти на SWOT анализа. Това доказва, че моделът работи, дори когато е обследван само един параметър сред ограничена еднородна група служители (охранители).

За демотивирания служител от охраната фактите, свързани с техниката, персонала на охраната, мениджмънта и организацията на охранителната дейност не означават нищо. В този случай той не разсъждава и за взаимоотношенията на въпросите от анкетата и тяхната взаимна логическа връзка. Ето защо не е ясно какво логическо обяснение може да се даде при сравнението на отговорите на въпрос 1 и 5: на първи въпрос 13% от анкетираните посочват организацията като слабо място, докато на пети въпрос – 20% дават оценка на организацията като „определено недобра“. Това демонстрира нелогическо и безкритично мислене и едва ли от такъв немотивиран служител охранителната дейност има полза.

Резултатите от направения дотук анализ водят към оформяне на стратегия за подобрение на организацията на охраната и управлението на фирмата, като предложението се посочва в Заключението на магистърската теза. Тук ще обобщя негативните елементи, които играят роля за оформянето на предложението.

На първо място се откроява фактът, че броят на охранителите не е оптимален и при критична ситуация за бързо реагиране решенията за изход от нея са три: 1) първият охранител е в обход и при подаване на сигнал реагира вторият, който е получил сигнала на КПП, и то остава без охрана, 2) при нов сигнал реагира отново вторият охранител, но в ущърб на първата или втората сигнализирана ситуация, 3) не се реагира своевременно на втория сигнал. И трите решения са недопустими за охранителната дейност, а последствията могат да бъдат с големи материални и човешки загуби.

През последната година на разглеждания обект е имало подобни ситуации. По-често е избирано второто решение, но то винаги е било за сметка на бързината на реакцията или на качеството на изпълнението на задачите. В екстремни случаи е избирано и първото решение и КПП е оставало без дежурен.

Като обобщение от проведената анкета на обект „София аерогара – център“ мога да се извлекат някои изводи, които е много вероятно да не са валидни за други охранявани обекти на аерогарата. Значимостта на обект „София аерогара – център“, обаче, ми дава основание в някаква степен като цяло да отнеса резултатите към характеристиката на управлението и организационната структура, които явно търпят сериозна критика.

## 4. Фактори, определящи предложението за подобрение на сигурността на обекта

В резултат на направените пилотни проучвания за слабостите на обект „София аерогара – център“, мога да обобщя някои фактори, които определят предложението ми за подобрение на сигурността.

Първо, ***СОТ*** е базов фактор, който беше разгледан в Глава I. В съвременния технологичен век сигнално-охранителната техника е средството, без което е немислимо осъществяването на проект за охрана и сигурност. Ето защо тя трябва да бъде непрекъснато актуализирана и усъвършенствана, паралелно с човешкия фактор, каквато е защитаваната от мене теза. Това трябва да се извършва като се съобразяват последните достижения на науката, тъй като и заплахите се развиват, основавайки се на нея.

Второ, системата за сигурност на един обект, обаче, не е само техника и технология, а функционира на основата на ***комуникация*** между техниката и човешкия ресурс, комуникация между шефове и служители, комуникация между служители, както и между служители и клиенти. Постигането на растяща класа на комуникация е необходимо за изграждане на растяща класа на защита и сигурност, която от своя страна да съответства на растящата класа на контингента на нарушителите и извършителите на престъпления. Моето твърдо убеждение е, че един от важните фактори за изграждане на комуникативната среда е постигането на ***конструктивна обратна връзка***, която да подпомага охранителната дейност на обекта. За целта е необходимо шефовете да дадат начален тласък и да поддържат обратната връзка, за да ускорят метаболизма на вътрешната комуникация. Това изисква желание за комуникация и желание за разпространение на информация.

Трето, в основата си човешкият ресурс се ръководи и е ръководен от присъщата за човека ***психология***. Тя задължително включва психологически подход в комуникацията между охранители, шефове и клиенти. Той определя типовете поведение, необходими за постигане на поставените цели. Има изградени критерии за поведение за охрана и сигурност на служителя и на компанията, които трябва да бъдат представени, изяснени, разработени и прилагани в работните колективи.

Въз основа на тези три фактора, изградих предложението си за подобрение на охранителната дейност на обекта.

## ЗАКЛЮЧЕНИЕ

Основавайки се на теоретичния обзор относно сигнално-охранителната техника в Глава I на магистърската теза, на прегледа на характеристиките на предложения в Глава II SWOT анализ и основно на неговата разработена от мене поетапна функционално-приложна практическа структура, както и на пилотното проучване на параметъра „слабости“ на обект „София аерогара – център“ посредством анкетата, мога да направя някои заключения относно защитаваната тук теза за необходимостта от актуализиране и усъвършенстване на охраната и сигурността.

Факторите, с които трябва да бъде съобразено изграждането на една система за сигурност, всъщност определят крайните резултати. Те се регистрират чрез проучване по параметрите на предложения системен анализ: *сили, слабости, удобни случаи/ благоприятни възможности* и *заплахи*. От извлечените взаимозависимости между тях, изразени в няколко корелации, които включват и личния опит, споделените впечатления и дадените мнения на човешкия ресурс, пряко ангажиран в охраната на обекта, могат ясно и убедително да се открояят проблемите и техните места.

Изключително важен фактор за ефективността на една система за сигурност с използване на сигнално-охранителна техника е методическият подход при изграждането ѝ. SWOT анализът предоставя този подход, тъй като е системен анализ, включващ най-важните компоненти на една система за сигурност. Нещо повече, разработената му от мене и представена в тази магистърска теза функционално-приложна структура организира и систематизира работата в един продължителен процес на подобрения. Ясно и убедително подчертах необходимостта от изследване на няколко корелации между параметрите *сили, слабости, удобни случай/благоприятни възможности* и *заплахи*. От тях само на база слабости в настоящото проучване, с особена значимост се проявиха съотношенията между *разполагаеми ресурси* (техника и хора) и *възможности за реализация на целите*.

От направените пилотни проучвания върху обект „София аерогара – център“ относно параметъра *слабости* на посочения и доразработения от мене системен аналитичен модел, се установи, че връзката *СОТ – човешки*

*ресурси – управление* видимо се е „пропукала“. Откроi се необходимостта от строг контрол при наемането на охранители, сред контингента на които беше направено проучването. Подчерта се необходимостта от добра организация на охранителната дейност както спрямо техниката, така и спрямо персонала, работещ и отговарящ за нея.

Неправилното проектиране, изработка и монтаж на охранителната система може да доведе до сериозно увеличаване на уязвимите места. Използването на некачествени компоненти и неподходящо програмно обезпечаване води до чести сривове и откази в системата, нарушения в комуникациите, опасност от несанкциониран достъп до информацията и проникване на нарушители, чрез заобикаляне на мерките за сигурност.

Работата по актуализирането и усъвършенстването на охранителната дейност на обекта трябва да продължи с оглед на европейските регулаторни документи, отнасящи се до аерогарите, както и по посока на синхронизацията на сигурността на обекта с тази на аерогара София.

Изложените анализи в настоящата работа насочват към определени направления в охранителната дейност, които изискват внимателно преразглеждане за постигане на нейната основна цел – повишаване на качеството и ефективността.

Моите убедителни заключения са, че основните направления, по които охраната и сигурността трябва да се актуализира и усъвършенства, са няколко:

- *Техника*: постигане оптимален капацитет на сигнално-охранителна техника и оптимизиране на резултатите от нейните функции;
- *Човешки ресурси*: достигане оптимален капацитет и качества на охранителите за осъществяване на баланса между охранители и вид конкретни задачи;
- *Мениджмънт*: мениджмънт на СОТ и мениджмънт на човешките ресурси – развитие по йерархични нива.

За постигането на основната цел, поставена в магистърската теза, правя конкретно предложение и съм дълбоко убеден, че то би повишило ефективността от действащата в момента охранителна система на обекта.

**Предложение за подобряване на охранителната дейност със СОТ на обект „София аерогара – център“**

След направения теоретичен преглед в Глава I и анализ в Глава II, се очертаха два основни фактора, които определят конкретните предложения за актуализиране и усъвършенстване на охранителната дейност на обект „София аерогара – център“.

*А. Мениджмънт на техниката и технологията*

- Да се поставят допълнителни въртящи се камери по необходимите ъгли на сградите отвън, за да се обхване изцяло сигналното устройство периметър, реагиращо при допир;
- Да се проследява застъпването на обхватите на съседни камери и покриването на „сенчестите“ места между тях;
- Да се извършва по-качествено монтиране на камерите;
- Да се правят периодични проверки на позициите и функционалността на камерите, както и задължителни такива по време на и след по-бурни метеорологични условия;
- Да се минимизира броят на сривовете на сървъра чрез извършване на по-честа профилактика на сървъра и непрекъснато следене на температурата на сървърните помещения.

*Б. Мениджмънт на човешките ресурси*

- Необходимо е организационно, методическо и психологическо подобрение на управлението на човешките ресурси;
- Да се набират служители за длъжност „охранител“ по система от критерии, уредени в Държавното образователно изискване (ДОИ) за придобиване на квалификация по професия 861010 „Охранител“ от област на образование „Обществена сигурност и безопасност“ и професионално направление 861 „Защита на собствеността и личността“ [18], съгласно списъка на професиите за професионално образование и обучение по чл. 6, ал. 1 от Закона за професионалното образование и обучение. Съдействаща за целта би била и

[18] Наредба № 9 от 04.12.2006 г. за придобиване на квалификация по професията "Охранител", в сила от 09.02.2007 г., издадена от Министерство на образованието и науката, обн. в ДВ, бр.13 от 09.02.2007 г. - http://www.security.bg/polezno/normativni-aktove/naredbi/naredba-9-ot-4-dekemvri-2006-g-za-pridobivane-na-kvalifikatsiya-po-profesiya-ohranitel-2

Националната изпитна програма, определяща единни критерии за оценка на професионалните компетенции на обучаваните, изискващи се за придобиване „Четвърта степен“ по изучаваната специалност “Организация на охранителната дейност“, разработени във връзка с чл. 36 от Закона за професионалното образование и обучение (ЗПОО), обнародван в ДВ, бр. 68 от 30.07.1999 г. и заедно с измененията и допълненията през годините до 13.10.2015 г. включително; [19]

- Да се изгради стил на тип охранител на фирмата по специално разработена за целта длъжностна характеристика;
- Да се подобри организацията на охранителната дейност като по определени критерии се разпределя подходящия човек за обход и подходящия за стационар, като критериите са изградени съобразно професионалните компетентности, физическите и психическите качества и умения на служителите за двата вида действия;
- Да се разпределя подходящия човек за дадена позиция в охраната, както и подходящия за даден обект, съобразно с индивидуалните професионални компетентности, физически и психически качества и умения;
- Да се постигне оптималния брой охранители на обекта чрез съобразено увеличение на персонала;
- Да се увеличат часовете на обучение – теория и практика, при приема на нови охранители, от 3-4 часа (по времето на направеното проучване) на 12-15 часа;
- Обучението да се провежда преди постъпване на работа, (а не след постъпване и започване на работа, каквато е практиката понастоящем).

Трябва да не се забравя, че актуализацията и усъвършенстването е постоянен и продължителен процес, съпровождащ техническите иновации.

## Приноси и приложимост на резултатите

### Приноси

- Основният принос на настоящата магистърска теза се състои в *оригиналното авторско поетапно разработване на функционално-*

[19] http://lex.bg/laws/ldoc/2134673921

*приложния характер на SWOT анализа и неговото прилагане като модел за системен подход за организация, разработване, поддържане и развиване на един охранителен проект*. Доколкото ми е известно, именно в моето проучване на обект „София аерогара – център“, SWOT анализът се прилага за първи път към охранителната дейност в България.

- Постигнатите резултати изтъкват ефективността на защитаваната магистърска теза за системен подход на работа при извличане на Предложение за средства и начини за актуализиране и усъвършенстване на сигурността.
- Направеното пилотно проучване само на един от параметрите допринася за доказване на резултативността от прилагането на разработеният от мене системен анализ за реализиране на подобрения в няколко направления – внедрената СОТ, охраняващия персонал, управлението на фирмата, организацията на охранителната дейност.
- От своя страна, всяко подобрение в охраната допринася за по-добра мотивация на персонала да развива своите качества, за да е адекватен на новите внедрени техники, технологии или подходи на работа. По този начин СОТ и човешките ресурси взаимно се обвързват с управлението и организацията.

От резултатите от направеното пилотно проучване мога да заключа, че приносите на моята магистърска теза биха имали голяма ефективност при прилагането им в охранителната дейност на коя да е фирма в страната и това ще допринесе за повишаване качеството на сигурността, категорично необходимо във време на национални размирици, бунтовни движения и терористични действия, на каквито сме свидетели днес.

**Практическа приложимост**

Основна цел в охранителната дейност е повишаване на сигурността. За тази цел функционално разработеният от мене SWOT анализ има ясна и доказана практическа приложимост и в двете страни на биномната връзка *охранявана организация – охраняваща фирма*. Чрез неговото прилагане могат да се търсят слабости и възможности за подобрение на охраната както в дейността на охраняваната организация, така и в дейността на

охраняващата фирма. Това води до повишаване ефективността на управлението на сигурността и в двете организации/фирми.

Практическото приложение на разработения системен анализ може да се реализира в няколко мащаба. Най-мащабният е да се използва за повишаване ефективността на работата по изготвяне на проект за сигурност. Неговият системен характер обхваща и добре организира предварителната проучвателна дейност, като направлява нейното извършване по параметрите и функционалните етапи на модела.

Моделът може да бъде използван и за периодични вътрешни анализи на неговите параметри *сили, слабости, възможности* и *заплахи* на всяка от обвързаните в действащия вече проект организации. Чрез тях могат да се извлекат нови стратегии за подобрения на по-нататъшното управление на охранителната дейността, които водят до повишаване степента на сигурност.

И не на последно място, анализът дори на един параметър след всяко подобрение води до ново подобрение, което осигурява продължителен и непрекъснат процес на актуализиране и усъвършенстване функциите на системата за сигурност.

**В заключение мога да кажа, че широката практическа приложимост на SWOT анализа, и особено неговата разработена от мене поетапна функционално-приложна структура, убедително защитава магистърската теза, че настоящото проучване предоставя ефективен подход за актуализиране и усъвършенстване на охранителната дейност.**

ИЗПОЛЗВАНА ЛИТЕРАТУРА


1. **Бойчев**, Петър. Техническо разузнаване. Оперативни способи и противодействие.
2. **Беджев**, Борислав. Технически средства в системата на национална и корпоративна сигурност. – Учебник за дистанционно обучение.
3. **Закон за ДОИ.** Закон за достъп до обществена информация. http://lex.bg/laws/ldoc/2134929408
4. **Закон за ЗКИ.** Закон за защита на класифицираната информация. http://www.dksi.bg/bg/Regulatory+Framework/Law+and+Regulation/promeni+v+ZZKI_20_11_07.htm
5. **Закон за ЗЛД.** Закон за защита на личните данни. https://www.cpdp.bg/?p=element&aid=373
6. **Закон за НСО.** Закон за националната служба за охрана. http://www.lex.bg/bg/laws/ldoc/2136588571
7. **Закон за СРС.** Закон за специалните разузнавателни средства. http://lex.bg/laws/ldoc/2134163459
8. **Закон за ЧОД.** Закон за частната охранителна дейност. http://www.lex.bg/en/laws/ldoc/2135479817
9. **Наредба за реда**… http://www.lex.bg/bg/mobile/ldoc/2135764722
10. **Начев,** Атанас Иванов. Технически средства и системи за защита на информацията.
11. **Энциклопедия** промышленого шпионажа. Авт. Каторин, Ю. Ф., Куренков, Е. В., Лысов, А. В., Остапенко, А. Н.. Санкт-Петербург, 2000.
12. **Sennewald**, Charles**.** Effective Security Management, 5th Edition.

**Електронни източници:**

13. http://www.bia-bg.com/service/view/14416
14. http://cfo.cio.bg/724_konkurentnoto_razuznavane__strategiya_i_ezhednevna_rabota
15. http://computerworld.bg/47528_video_oblaci_video_analizi_video_uslugi
16. http://www.iata.org/2015-review/index.html
17. http://www.internationalairportreview.com/
18. http://www.internationalairportreview.com/advent-calendar/19-december-2014/

**19.** http://www.internationalairportreview.com/19809/airport-news/airspace-trial-launched-at-edinburgh-airport/
**20.** http://www.internationalairportreview.com/19736/airport-news/dfs-signs-contract-with-frequentis-to-install-remote-tower-technology/
**21.** http://www.internationalairportreview.com/directory/company-details/?c=351-cem-systems
**22.** http://www.internationalairportreview.com/18739/airport-news/worlds-busiest-airport-keeps-people-safe/
**23.** http://isd.engin.umich.edu/professional-programs/lean-six-sigma/index.htm#sthash.iETeNYt5.dpuf
**24.** http://www.lex.bg/en/laws/ldoc/2135479817
**25.** http://lex.bg/laws/ldoc/2134673921
**26.** http://www.schneiderelectric.bg/documents/downloads/Global_Detection_Catalogue.pdf
**27.** http://www.sectron.com/bg/grid/21/videonabludenie-21
**28.** http://www.sensomat.info/sensors.htm
**29.** http://www.statistiques.public.lu/stat/TableViewer/tableView.aspx?ReportId=7053&IF_Language=eng&MainTheme=4&FldrName=6&RFPath=7047
**30.** http://isd.engin.umich.edu/professional-programs/lean-six-sigma/index.htm