ВОЕННА АКАДЕМИЯ
„ГЕОРГИ СТОЙКОВ РАКОВСКИ“

**ДИМИТЪР КАРАДЖИНОВ**
**РОСЕН ДИМИТРОВ**

# ЗАЩИТА НА ЛЕТИЩЕ

Учебник

София • 2016

*Учебникът „Защита на летище“ е предназначен за студентите от редовна, задочна и дистанционна форма на обучение във факултет „Командно-щабен“ на Военна академия „Георги Стойков Раковски“ по специалност „Сигурност във въздухоплаването“ от професионално направление „Национална сигурност“.*

*В учебника са разгледани въпросите, свързани със сигурността и защитата на гражданските и военните летища, осигуряването на физическата им сигурност, както и защитата на външния им периметър. Специално внимание е обърнато на критериите за качество на системата за сигурност на летище, оценката на способностите ѝ за наблюдение, реакция и отговор. Дефинирани са границите на външния периметър на летище и е описан алгоритъм за работа при определяне на зоните в неговия външен периметър.*

*Материалът в учебника е систематизиран и обобщен на базата на лекции, дискусии и доклади, изнесени от авторите на семинари и научни конференции. Отчетени са и регламентиращите документи в областта на сигурността в гражданското въздухоплаване.*





ISBN 978-954-9348-76-7

## СЪДЪРЖАНИЕ

*Глава четвърта*

## ДЕФИНИРАНЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ЛЕТИЩЕ КАТО СЛОЖНА СИСТЕМА



*Глава пета*

## ОЦЕНКА НА СПОСОБНОСТИТЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ЛЕТИЩЕ ЗА ЗАЩИТА НА ВЪНШНИЯ МУ ПЕРИМЕТЪР



*Глава шеста*

## АЛГОРИТЪМ ЗА РАБОТА ПРИ ОПРЕДЕЛЯНЕ НА ЗОНИТЕ ВЪВ ВЪНШНИЯ ПЕРИМЕТЪР НА ЛЕТИЩЕ / 81

# УВОД

Тероризмът е най-значимият проблем на сигурността днес. Наред с глобализацията в икономическата сфера се глобализира и самият тероризъм, т.е. добива транснационални измерения, при което нарастват неговите агресивност и жестокост. Съвременният тероризъм е проява на сблъсък между мощни икономически интереси, често прикривани с религиозна и етническа окраска.

Следователно глобализацията в икономическата сфера не носи само ползи, а създава и сериозни предизвикателства за сигурността. Ето защо сигурността се превръща в ключов фактор за осигуряването на високо качество на живот в съвременното общество и за защита на критичната инфраструктура чрез предотвратяване на общите заплахи и справяне с тях.

Защитата на летищата като елементи от критичната инфраструктура – национална, европейска и световна, е от изключителна важност за осигуряване на тяхната цялост и функциониране. Глобалното увеличаване на размерите им и тяхната икономическа дейност като силен генератор на приходи обосновават привлекателността им за терористични заплахи поради евентуалния икономически и социален ефект, пораженията върху околната среда и върху публичното здраве, до които биха довели. За обикновените хора и медиите тези заплахи обикновено се свързват със зоните за обществен достъп и по-конкретно с терминалите, в които органите за сигурност трябва да бъдат готови да реагират на всяка възникнала ситуация. Съществува обаче може би по-вероятна заплаха, която може да възникне от прилежащите райони към летищата. Докато специалистите по сигурността в терминалите се фокусират върху разкриването и залавянето на терористи, опитващи да се качат на борда на въздухоплавателно средство, осигуряването на физическата сигурност на летищните комплекси изисква предприемането на мерки за предотвратяване на незаконно проникване и саботаж в летищната инфраструктура. Сигурността на съоръженията, инфраструктурата и критичните обекти на

летищата, а също и на прилежащите райони представлява интегрална част от цялостния модел за летищна сигурност. Разширяването на периметъра за сигурност осигурява цялостна връзка и последователност на операциите, което води до значително повишаване на защитата на летищата.

Днес летищата се смятат за едни от най-сигурните места по света. За да се постигне това обаче, всички компании и държави по света налагат драконовски мерки за сигурност, изградени на базата на десетки години опит и трагични инциденти.

Разгледани са основните понятия и термини, отнасящи се до летищната сигурност, основните ѝ компоненти, системата за нейното осигуряване, а така също и въпросите, свързани с повишаване на сигурността и защитата на външния периметър на летище от терористична заплаха.

*Глава първа*

# СИГУРНОСТ И ЗАЩИТА НА ГРАЖДАНСКО ЛЕТИЩЕ. ОБЩИ ПОНЯТИЯ

## 1.1. Основни понятия

Представените определения са с широка международна употреба. Те имат за цел да опишат мерките, процедурите и концепциите по летищна сигурност и да послужат като понятиен апарат в настоящето пособие.

**Анализ на риска.** Отчитане на съответните сценарии за действие при различни заплахи с цел да се направи оценка на уязвимостта и потенциалните последици от нарушаването или унищожаването на критична инфраструктура.

**Акт на незаконна намеса.** Отправянето на заплаха, опит или действие, насочени срещу сигурността в гражданското въздухоплаване, както следва:

– незаконно завземане на въздухоплавателно средство;

– разрушаване на въздухоплавателно средство в експлоатация;

– вземане на заложници на борда на въздухоплавателно средство или в летище;

– насилствено качване на борда на въздухоплавателно средство, навлизане в летище или в периметъра на въздухоплавателна база, внасяне на оръжие или опасно устройство или материал, предназначени за криминални цели, на борда на въздухоплавателно средство или в летище;

– използване на въздухоплавателно средство в експлоатация за причиняване на смърт, нараняване или сериозно увреждане на имущество или околна среда;

– съобщаване на невярна информация, което излага на риск безопасността на въздухоплавателно средство в полет или на земята,

както и на пътниците, екипажа, наземния персонал или обществеността на летище или в периметъра на база от гражданската авиация.

**Въздухоплавателно средство.** Всяка машина, която може да се поддържа в атмосферата от реакциите на въздуха, различни от реакциите на въздуха спрямо земната повърхност.

**Заплаха.** Всяка информация, обстоятелство или събитие, които биха могли да разрушат или смутят действието на критична инфраструктура или на който и да е от нейните елементи.[1]

**Защитена зона.** Това е самият район на обекта, ограничен от външната ограда, в който опасността от въздействие върху персонала, техниката и материалните средства е необходимо да е сведена до минимум.

**Идентификация на заплахите.** Процес на разпознаване на вида опасности, установяване на възможните причини, пространствено-времевите координати, вероятността на проявление, размерите и последствията от опасността.

**Критична инфраструктура.** Система или части от нея, които са от основно значение за поддържането на жизненоважните обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни последици в дадената държава в резултат на невъзможността да се запазят тези функции.

**Опасност.** Явление, способно да нанесе вреда на жизненоважни интереси на човека.

**Оценка на риска.** Процес на идентификация, анализ и определяне на степента на риска.

**Зона с ограничен достъп.** Зони, които включват:

а) част от гражданското летище за обществено ползване, до която имат достъп проверените заминаващи пътници;

б) част от гражданското летище за обществено ползване, през която след проверка може да преминава регистрираният багаж при заминаване, или в която той може да се намира, ако не е защитен;

---

[1] *Решение на Съвета на Комисията на европейските общности относно Предупредителна информационна мрежа за критичната инфраструктура.*

в) част от гражданското летище за обществено ползване, предназначена за паркиране на въздухоплавателни средства, в които се качват пътници или се товарят товари.

**Зона за реакция на системата за сигурност.** Зоната, заключена между линията за неутрализиране на заплахата и линията на външния периметър на летището. Размерът ѝ се определя от критичността на обектите и мобилността на терористичната заплаха.

**Зона за сигурност във външния периметър на летище.** Зоната, заключена между линията на вътрешния периметър на летището и линията за неутрализиране на заплахата.

**Зона на външния периметър на летище.** Онази зона, в границите на която системата за сигурност на летището трябва да е в състояние да открие, реагира и неутрализира потенциална терористична заплаха или да минимизира последствията от такава.

**Критичност.** Ниво на загуби на хора и материални средства в следствие на външно въздействие или аварии.

**Контрол по сигурността.** Прилагането на средства, с които може да се предотврати внасянето на забранени предмети.

**Контрол на достъпа.** Прилагането на средства, с които може да бъде предотвратен достъпът на лица, превозни средства или и двете, които нямат разрешение за това.

**Летище.** Определена част от земната или водната повърхност (включително всички сгради, съоръжения и оборудване), предназначена изцяло или частично за кацане, излитане и движение по тази повърхност на въздухоплавателни средства, предназначени за търговски въздушни превози и за обслужване на техните пътници, товари и поща.

**Линия за неутрализиране на заплахата (ЛНЗ).** Мислена линия, до която силите за реакция и отговор на системата за сигурност на летище трябва да осъществят физически контакт с обекта вероятна заплаха.

**Линия на външния периметър на летището (ЛВП).** Мислена линия, до която подсистемата за наблюдение трябва да е открила заплахата (обекта), така че ССЛ да е в състояние да реагира на ЛНЗ.

**Охраняеми граници.** Терените, обхванати от периметрова ограда на летище за обществено ползване.

**Политика на сигурност.** Съвкупност от определения, изисквания към системната архитектура, заложени в системата функции и механизми на информационен обмен между тях, заедно с правилата и процедурите по организацията на сигурността и защитата на зададения обект.

**Риск.** Съчетание от вероятността и последствията от настъпване на дадено неблагоприятно събитие. Знаейки вероятността за неблагоприятното събитие, може да се определи вероятността за благоприятно събитие.

**Сигурност.** Функционалното състояние на дадена система, което осигурява неутрализирането и противодействието ѝ на външни и вътрешни фактори, оказващи влияние или можещи да ѝ въздействат деструктивно (влошаване организационното състояние на системата или невъзможност за нейното функциониране и развитие).[2]

**Система за защита.** Съвкупност от технически средства и организационни дейности, изпълнявани от назначен персонал, целящи гарантиране на функционирането, непрекъснатостта и целостта на обекта, за да възпрат, смекчат и неутрализират заплаха и риск.

**Система за сигурност.** Съвкупността от обозначен персонал, организационна структура, политики, стратегии и функции, предназначени да поддържат контролирания обект в състояние на сигурност.

**Страна „въздух".** Зоната за движение на летище, съседният терен и сградите, или части от тях, достъпът до които се контролира.

**Страна „земя".** Зоната на летището, която не е от страна „въздух" и включва всички обществени зони.

**Терминал.** Основната сграда или група от сгради, където се извършват обработката на пътници и товари и качването на борда на въздухоплавателно средство.

**Уязвимост.** Недостатък или слабост в процедурите, дизайна или вградените контролни механизми за обезпечаване сигурността на системата, които могат да се проявят в резултат на случайно или преднамерено действие и водят до нарушаване на сигурността или политиката за сигурност на системата.

---

[2] *Institute for Security and Open Methodologies (ISECOM) – Испания.*

**Физическо препятствие.** Стена, висока бариера или подобно, през което не би било възможно да се извърши прекачване или което би било пречка за преминаване без помощни средства.

## 1.2. Летищна сигурност. Елементи на летищната сигурност

*Летищната сигурност* се разглежда като елемент от системата за авиационна сигурност в гражданското въздухоплаване и като съставна част от безопасността във въздушния транспорт. Проблемите на сигурността на летищата трябва да се решават в рамките на системата за мениджмънт на качеството на авиационната безопасност като елемент на интегралната система за управление на летищата.

В общата икономическа и инфраструктурна мрежа летищата се превръщат в изключително важни комуникационни възли, част от критичната инфраструктура (КИ). Различават се по своята сложност и комплектност, но всички притежават общи физически характеристики. Някои имат опростена инфраструктура, предназначена за обслужване на ограничен брой пътници и товари, а други са с добре развита система от индустриални, търговски и обществени обекти за обслужване на интензивни потоци от пътници и товари. Всички летища обаче са еднакво изложени на опасност от възникване на кризисни ситуации.

Летищната сигурност се осигурява с помощта на комплекс от мерки, предвиждащи създаването и функционирането на летищна служба за авиационна сигурност, охрана на летището, въздухоплавателните средства, обектите на летището, проверка на членовете на екипажа, обслужващия персонал, пътниците, ръчния багаж, багажа, пощата, товарите, кетъринга, предотвратяване и пресичане на опити за завземане и отвличане на въздухоплавателни средства.

В Стандарти 3.2.1 – 3.2.4 от Анекс № 17 към Конвенцията за международно гражданско въздухоплаване са определени следните **ключови елементи** за реализиране на целесъобразни и ефективни начини за гарантиране сигурността на летищата:

- оправомощен орган по летищна сигурност;
- комитет за авиационна сигурност;

- летищна програма за сигурност;
- изисквания по отношение на проектирането на граждански летища;
- контрол на качеството в сферата на летищната сигурност;
- подготовка на персонала на летищната служба за сигурност;
- планиране в случаи на извънредни ситуации.

Всъщност това са компонентите, които изграждат сигурността на всяко летище и от които зависи нейното качество. В „Ръководство по сигурността за защита на гражданското въздухоплаване срещу актове на незаконна намеса", Документ 8973, том III – „Летищна сигурност", са посочени указанията по реализиране на тези стандарти и препоръчителните практики. Ще разгледаме всеки един от по-горе посочените ключови елементи и неговия принос за летищната сигурност.

*Оправомощен орган по летищна сигурност*. Оправомощеният орган по сигурността на всяко летище, обслужващо гражданското въздухоплаване, отговаря за координирането на всички дейности по контрола за прилагането на мерки по отношение на сигурността и на правилата за сигурност.

Като правило летищната администрация (летищният оператор) носи отговорност за организацията или координирането на дейностите на летището, включително организацията на дейностите по осигуряване на сигурността. Затова функциите на оправомощен орган по летищна сигурност изпълнява един от високопоставените сътрудници на летищния оператор – обикновено първият ръководител на летищния оператор.

По-конкретно са дефинирани функциите и задълженията на ръководителя на летищната служба за сигурност или сътрудник с аналогичен ранг:

- Осъществява основен и непосредствен контакт с летищния оператор в частта, касаеща сигурността, и съответния оправомощен орган по летищна сигурност.
- Разработва и развива летищната програма за сигурност. Съгласува я с оправомощения орган по летищна сигурност.

• Контролира изпълнението на мерките и процедурите по сигурността.

• Подържа ефективен контакт с останалите летищни структури и съответните правоохранителни органи, с авиационните оператори, а също и със службите за сигурност на другите арендатори на летището.

• Координира дейността на летищната служба за сигурност, противопожарната служба и службата за търсене и спасяване.

• Отговаря за създаването и развитието на ефективна система за реагиране и отговор.

• Участва в подбора на кадри за летищната служба за сигурност.

• Участва в работата на групата за планиране и проектиране на летището при изработване на препоръки за мерки за сигурност при модернизация на съществуващи или нови обекти на летището.

• Регистрира всички актове на незаконна намеса на летището или на въздухоплавателно средство, излетяло от летището, и ги докладва на съответния оправомощен орган. Прави запитвания по отношение на такива въздухоплавателни средства в рамките на националното законодателство.

• Осъществява текущ контрол на качеството за постигане на сигурност и предприемане на оперативни коригиращи действия.

*Комитет за авиационна сигурност.* Комитетът за авиационна сигурност (КАС) се създава на всяко летище, обслужващо гражданското въздухоплаване, за да подпомага оправомощения орган по сигурността при осъществяване на всички дейности по контрола за прилагането на мерки по отношение на сигурността и на правилата за сигурност в съответствие с програмата за сигурност на летището.

Задача на Комитета за авиационна сигурност е постоянно разглеждане и оценка на ефективността на мерките по осигуряване на летищната сигурност на основата на оценката на преобладаващите заплахи, данните за последните събития и резултатите от проверките в рамките на контрола на качеството. КАС освен това се явява форум за координиране на действията по осигуряване на летищна сигурност, обсъждане на оперативни въпроси и проблеми, свързани с осъществяването както на текущи, така и на извънредни мерки. Също така може

да консултира оправомощения орган по летищна сигурност по въпросите на сигурността.

Графикът за работа на КАС трябва да бъде обвързан с потребностите на летището. Препоръчително е да заседава не по-малко от четири пъти в годината, а при наличие на възможност да работи в състава на неголеми целеви групи.

*Летищна програма за сигурност (ЛПС).* Всяко лицензирано летище, обслужващо международната гражданска авиация, трябва да приеме, изпълнява и актуализира летищна програма за сигурност, която отговаря на изискванията на Националната програма за сигурност в гражданското въздухоплаване. Изработва се в писмен вид и обхваща всички мерки и процедури, които се изисква да бъдат приложени от летищния оператор в изпълнение на отговорностите по Националната програма за сигурност в гражданското въздухоплаване.

Този документ заема важно място в йерархията на документите по авиационна сигурност. На фигура 1 са показани различните нива в тази йерархия.


Фиг. 1. Йерархия на документите по авиационна сигурност

При разработването на документи по авиационна сигурност трябва да се отчитат потребителите, за които са предназначени, необходимото ниво на детайлизация и степента на класифицираност на информацията. Като правило по-подробна информация и с по-висока

степен на класифицираност се съдържа в документите от серията стандартни експлоатационни процедури. ЛПС може да съдържа препратки към специфични процеси и процедури за осигуряване на сигурност, но тяхното подробно представяне обикновено се дава в стандартните експлоатационни процедури.

Например в ЛПС се описват мерки за защита на периметъра на зоните с ограничен достъп, включително и патрулиране със силите за сигурност на летището, но не е задължително да се дава подробно описание на формите на това патрулиране, броя на патрулите, тяхната периодичност и т.н. Тези данни могат да бъдат третирани като информация с по-висока степен на поверителност, която не се изисква от повечето читатели на ЛПС. Този тип информация ще се съдържа в стандартните експлоатационни процедури.

Летищната програма за постигане на авиационна сигурност се съобразява с всички промени в законодателството, които засягат сигурността в гражданското въздухоплаване, и се представя за утвърждаване от главния директор на Главна дирекция „Гражданска въздухоплавателна администрация". Тя се класифицира като „Поверителна" и се третира като такава. Преглежда се и се допълва редовно на всеки 12 месеца и при всяка актуализация на НПСГВ.

Основната цел на летищната програма за сигурност, както и на НПСГВ е да осигурят безопасност на пътниците, членовете на екипажа, наземния персонал и населението по всички аспекти, свързани със защитата от актове на незаконна намеса в дейността на гражданската авиация. Затова ЛПС трябва:

– да съответства на изискванията на Анекс № 17 и НПСГВ или да ги превъзхожда по строгост и решителност на мерките;

– ясно да определя и разпределя отговорностите на лицата и организациите, които участват или са отговорни за изпълнението на мерките за сигурност, описани в НПСГВ;

– да установява стандарти за изпълнение, включително на изисквания за базова подготовка и повишаване на квалификацията, и водене на отчет на подготовката;

– да предвижда стандартизиране на мерките за сигурност;



2/1/16

– да осигурява спазване на изискванията при проектиране на летището, включително тези, които се отнасят до архитектурата и инфраструктурата, необходими за прилагането на мерките за сигурност, посочени в НПСГВ.

Документ 8973 препоръчва летищната програма за сигурност да има следната типова структура:

I. Организация
II. Описание на летището
III. Мерки за летищна сигурност
IV. Мерки в отговор на актове на незаконна намеса
V. Обучение
VI. Контрол на качеството: наблюдение и контрол
Допълнения

*Изисквания по отношение на проектирането на граждански летища.* Те включват изисквания по отношение на архитектурата и инфраструктурата, необходими за реализиране на мерките за сигурност в съответствие с Националната програма за сигурност в гражданското въздухоплаване, в процеса на строителство на нови и реконструкция на съществуващи съоръжения в летищата.

За осигуряване на летищната сигурност се използва холистичен (цялостен) подход, който оптимизира:

- проектирането на летищни обекти;
- проектирането на системи за сигурност;
- разработването на процедури при експлоатация;
- разполагането на персонал на службата за сигурност;
- системата за отчетност на целия персонал.

При проектирането на летищни обекти разработчиците трябва да използват също такъв холистичен подход за решаване на следните основни аспекти на сигурността:

а) възпрепятстване на внасянето на оръжия, експлозиви или опасни устройства по какъвто и да е начин на летището и на борда на въздухоплавателното средство чрез:

- откриване на оръжия, експлозиви или опасни устройства;

• осигуряване на сигурност на средствата, с помощта на които се осъществява достъп на борда на въздухоплавателни средства на пътници, багажи, персонал, товари, транспортни средства, пощенски пратки и други стоки;

• гарантиране на разделението между преминалите и непреминалите през проверка пътници;

• регулиране на достъпа и движенията в контролируемите зони и зоните с ограничен достъп;

б) съдействие при изпълнението на плана при аварийни или кризисни ситуации;

в) свеждане до минимум на последиците от експлозии или пожари за хората или обектите, благодарение на конструктивни особености, предназначени да ограничат броя на жертвите и щетите.

*Контрол на качеството в сферата на летищната сигурност.* Разработване и осъществяване на мерки/програми за контрол на качеството във всяко сертифицирано летище в съответствие с Националната програма за контрол на качеството за постигане на сигурността в гражданското въздухоплаване.

*Подготовка на персонала на летищната служба за сигурност.* Разработване и осъществяване на мерки/програми за подготовка на персонала на летищната служба за сигурност в съответствие с Националната програма за сигурност в гражданското въздухоплаване.

*Планиране в случаи на извънредни ситуации.* Плановете за действие при възникване на извънредни ситуации трябва да се разработват във всяко летище, обслужващо гражданската авиация, за защита на гражданската авиация от актове на незаконна намеса.

### 1.3. Защита на летище. Физическа сигурност

Под *защита на летище* следва да се разбират всички дейности, насочени към гарантиране на нормалното функциониране, непрекъснатостта и целостта на летището с цел възпиране, намаляване, смекчаване или неутрализиране на заплахите, рисковете или уязвимостта. Основни елементи от защитата на един обект са наблюдение, откри-

ване и възпрепятстване на субекти, извършващи нерегламентирано навлизане, ползване или преминаване през зони с контролиран достъп.

Понятието *физическа сигурност* в „Речник на термините и дефинициите, използвани в НАТО“ – AAP-06 е дефинирано по следния начин: „*Физическа сигурност* (*physical security*) е онази част от защитата, която касае физическите мерки, целящи да защитят личния състав, да предотвратят нерегламентиран достъп до военна техника, обекти, материални средства и документи, както и да ги предпазят от шпионаж, саботаж, загуба и кражба.“

Физическата сигурност се състои в използването на множество устройства, хардуер и технологии, които заемат важно място в контрола на достъп, видеонаблюдение и системи за откриване на нарушители (аларми). Съвременните системи за физическа сигурност са IP-базирани, като осигуряват постоянна надеждност и сигурност, премахват субективния фактор и повишават ефективността при осигуряване на сигурността. В случай на регистрирано събитие служителите по сигурността могат да бъдат своевременно алармирани, а събитието – записано в системата.

Базата от знания в тази област съдържа частично технически познания и частично познания от областта на физическата сигурност. Водещата организация по сигурността е много повече от бариери, пистолети и охранители. Тя трябва да генерира и знания, които водят до доверие и всеотдайност, което е необходимо за днешния свят.

Развитието и прилагането на физическата сигурност в дадена организация изискват прилагането на стабилен стратегически план за сигурност. Някои специалисти го наричат още *security master plan*. Той изисква от специалистите по физическа сигурност да мислят отвъд стандартите и изискванията за сигурност, както и обширно разбиране на динамиката на пазара, проблемите на служителите по сигурността и целите. Това е начинът за постигане на единомислие в моделирането на системи за сигурност между органите за сигурност и бизнеса.

Физическата сигурност се представя като забравената страна на сигурността, а тя всъщност е ключов елемент за общата стратегия

за защита. Защитата на критичните части в зоните с ограничен достъп е важна за цялостното функциониране на летищния оператор.


Фиг. 2. Примерна схема на летище и елементи от инфраструктурата му

На фигура 2 е показана примерна схема на летище с основните елементи от неговата инфраструктура и разграничаващата линия (периметрова ограда) между вътрешния периметър и прилежащите площи. На вътрешния периметър на летището, заедно с летищните съоръжения (енергоизточници, навигационни съоръжения, контролна кула и други сгради), както и на съоръженията за гориво е осигурена **физическа защита** от системата за сигурност на летището.

Летищната администрация или летищният оператор с възложени функции на летищна администрация осигурява равнището и стандартите при изпълнение на функциите, поети като задължения от

държавата, свързани със сигурността на полетите и охраната ла летището.

Съгласно чл. 16л от Закона за гражданското въздухоплаване (ЗГВ) авиационните оператори изпълняват мерките, предвидени в летищната програма за постигане на авиационна сигурност. Летищният оператор извършва:

1. Проверка за сигурност на пътниците, започващи пътуване от летището, трансферните пътници и транзитните пътници, техните ръчни и регистрирани багажи.

2. Проверка за сигурност на персонал, екипажи и моторни превозни средства за достъп до зоните за сигурност с ограничен достъп и критичните части.

3. Проверка за сигурност на товари и поща.

4. Проверка за сигурност на поща и материали на авиационните оператори.

5. Проверка за сигурност на доставки на стоки, предназначени за полета и летището.

6. Видеонаблюдение на зоните за сигурност с ограничен достъп, критичните части и други зони.

7. Контрол на достъпа и издаване на временни пропуски на лица и моторни превозни средства.

8. Охрана на въздухоплавателните средства на перона на летището.

Доставчикът на аеронавигационно обслужване разработва, прилага и актуализира програма за сигурност за недопускане на актове на незаконна намеса в дейностите и средствата за аеронавигационно обслужване. Програмата се изготвя в съответствие с изискванията на Националната програма за сигурност в гражданското въздухоплаване, на летищните програми за постигане на авиационна сигурност и се утвърждава от главния директор на Главна дирекция „Гражданска въздухоплавателна администрация".

*Обекти на летището:*

- пътнически терминал;
- административна сграда на летището;
- служебни сгради;

- ръководство на въздушното движение (РВД);
- карго терминал
- склад с гориво-смазочни материали (ГСМ).

При реализиране на физическата сигурност на летището трябва да се спазват следните принципи на защита:

- контролиране на движението на хора и МПС;
- разделяне на летището на свободни зони и зони с ограничен достъп;
- защита на летището с помощта на физически ограждания;
- организация за предотвратяване проникването през огражденията на летището.

В правилата на летището се предвиждат правила за движение на територията на летището на хора и транспортни средства, определени зони за обслужване на въздухоплавателни средства и маршрути за движение в контролираната зона. Предвиждат се и правила за безопасно пресичане на полосата за излитане и кацане и пътеките за рулиране.

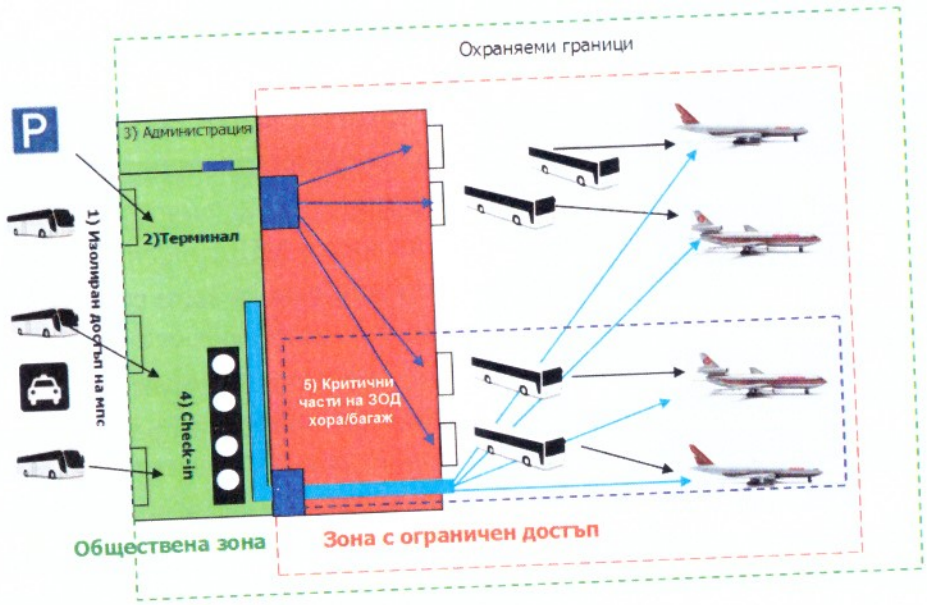
Всяко летище се разделя на зони (фиг. 3), в които правилата за достъп и мерките за сигурност са строго регламентирани. Те се разделят на свободни зони и зони с ограничен достъп.

*Свободна зона* е зона на летището, в която хората имат достъп или достъпът до която не е ограничен с други средства.

Зоните за сигурност са четири: *зона „земя“*, *зона „въздух“*, *зона за сигурност с ограничен достъп* и *критични части на зоната за сигурност*. Всяка от тях има свои собствени изисквания.

На всяко летище се установяват граници между страна „земя“ и страна „въздух“. Границата представлява физическа преграда, която се вижда ясно, има обозначения и не допуска неоторизиран достъп.

В общия план летищният оператор се състои от три района, като цяло посочени като *страна „въздух“*, *страна „земя“ и терминал*. Обикновено терминалът се намира на охраняемата границата между страна „въздух“ и страна „земя“, но може да има и други сгради, разположени по този начин. Всеки един от тези три района на летището има свои специфични изисквания.




Фиг. 3. Зони с различен режим на достъп

*1) Контролиран достъп до съоръжението за излитане и кацане. Достъпът на МПС до терминала е изолиран. 2) Терминал – извършва се патрулиране на въоръжени полицаи и видеонаблюдение. 3) Администрация – контролиран достъп чрез система за контрол на достъпа. Вратата е тип турникет за единично пропускане. 4) Check-in. 5) Критични части на зона с ограничен достъп*

*Страна „въздух“* или още *контролируема зона (зона „въздух“)* на летищния оператор обикновено включва комплексна и интегрирана система от настилки (писти, пътеки за рулиране, самолетостоянки), осветление, търговски зони, навигационни средства, средства за наземен и въздушен контрол, карго зони и други дейности, поддържащи и подкрепящи работата на летището, достъпът до които се контролира.

Международна организация за гражданска авиация (ICAO) в Анекс 17 посочва следната дефиниция: „Работна площ на летище, прилежащите територии и сгради, или части от тях, достъпът до които се контролира“. Страна „въздух“ е място, където оперират въздухоплавателните средства. Зоната започва непосредствено след граничния контролно-пропускателен пункт. Този периметър е зона с ограничен достъп, в която може да има критични части. Изборът на

място, където ще се намират преминаващата периметрова ограда или бариери, често зависи от околните пътища, осигуряващи достъп. Този избор е едно от най-важните критични решения. В допълнение към факторите за географско положение от съществено значение за страна „въздух" са:

- опасни или потенциално опасни райони, които биха могли да повлияят на безопасността или сигурността на паркирано въздухоплавателно средство;
- обраснали райони, които могат да послужат за укриване на лица или предмети, които биха могли да застрашат въздухоплавателно средство или критични летищни системи;
- съседни обекти, които имат собствени разпоредби и изисквания за сигурност, като например военни или други съоръжения, които биха могли да повлияят или да бъдат повлияни от близостта на операциите, извършвани в страна „въздух";
- природни особености, големи метални конструкции, сгради, които биха могли да повлияят на комуникацията или навигационните системи: това не само може да застраши летателните апарати, но и да ограничи възможностите за реагиране в извънредни ситуации.
- общински обекти като училища, хотели, паркове и други, които биха могли да бъдат повлияни от близостта на въздухоплавателните средства.

*Страна „земя"* е зоната на летището, която не е от страна „въздух" и включва всички обществени зони. В охраняемите граници на съоръжението за излитане и кацане няма специфично ограничаване на достъпа. В тези граници се включват местата за паркиране, обществените пътища за достъп, зоните за наемане на коли и наземен транспорт, зоните за спиране, както и хотелите, разположени на територията на съоръжението.

Някои критични зони и активи се нуждаят от особени мерки за сигурност, прилагани в охраняемите граници, като например подходи за кацане, места с навигационно оборудване или повишена сигурност в някои сгради. В тези зони се извършва наблюдение с повишено внимание. Това са места, определени като паркинги, обществена зона, зона за обществен транспорт и други. Терминалът на съоръжението за

излитане и кацане е проектиран за дейности, свързани с пътниците – като изпращане и посрещане, затова съответно той е и с най-много изисквания за безопасност, сигурност и експлоатация.

*Терминал.* Летищният терминал е проектиран да побере и подготви пътниците за качване и слизане от въздухоплавателното средство. По-големи летища често имат повече от един терминал. Терминалът обикновено е основна сграда или група от сгради, където се извършват основни процеси по обработка на пътниците и техните багажи (скрининг), качване (бординг) и слизане на пътници от търговски въздухоплавателни средства. Терминалът е районът на летището с най-засилени мерки за сигурност, безопасност и оперативни изисквания. Много от тези изисквания са тясно свързани с местоположението на зоните за сигурност в терминала и в неговата близост. При проектирането на нов обект (терминал) той трябва да бъде разположен в центъра, отстрани на съоръжението, когато това е възможно. Така се осигурява не само ефективен достъп на въздухоплавателните средства до терминала, но и преимущество за неговата сигурност. Равномерното централно разположение позволява добро изграждане на защитен буфер от бариери и реагиране на сигнали и аларми.

*Зони с ограничен достъп (ЗОД)* са онези части от контролираемата зона (зона „въздух"), определени като зони с висок риск, където в допълнение към контрола на достъпа се прилагат и други мерки за сигурност. Това са:

а) част от летището, до която имат достъп проверените заминаващи пътници;

б) част от летището, през която след проверка може да преминава регистрираният багаж при заминаване или в която той може да се намира, ако не е физически защитен;

в) част от летището, предназначена за паркиране на въздухоплавателни средства, в които се качват пътници или се товарят товари.

*Критични части (КЧ)* в зоните за сигурност се определят на граждански летища за обществено ползване, където над 40 лица притежават пропуски, даващи им право на достъп до зони с ограничен достъп. Такива са: а) всяка част от летището, до която след проверка за сигурност имат достъп заминаващи пътници и техният ръчен ба-

гаж; б) всяка част от летището, през която след проверка за сигурност може да преминава или да бъде съхраняван заминаващ регистриран багаж, ако не е бил физически защитен.

*Демаркирана зона* означава зона, която е отделена от други ограничени зони за сигурност на дадено летище чрез контрол за достъп.

*Защитена зона* е самият район на обекта, ограничен от външната ограда, в който опасността от въздействие върху персонала, техниката и материалните средства е необходимо да бъде сведена до минимум.

*Охраняеми граници* са терените, обхванати от периметрова ограда, на летище за обществено ползване.

*Оградното съоръжение (ограда)* е физическа конструкция за преграда или естествено препятствие от релефа на местността, или стена на сграда, предназначени за възпрепятстване на свободния достъп на лица и транспортни средства в зона с ограничен достъп на летище. Физическите ограждения се разполагат така, че да създадат няколко кръга на защита:

1. Външен кръг. Разполага се по периметъра на летището[3]. Всъщност периметърът на летището е границата между контролируемата и неконтролируемата зона. Състои се от ограда, система за осветление, знаци, указатели и система за сигнализация. Предназначен е за насочване потока от хора и МПС през предвидените КПП и входове. Неговата функция е да осигури определена степен на психологическо, физическо и юридическо възпиране на проникване.

2. Среден кръг на защита. Разполага се около сградите, терминалите и строежите, които се намират в границите на летището (физическа защита на вратите, прозорците, покривите). Осигурява сигурност на откритите зони (патрулиране, охрана и наблюдение) – полосата за излитане и кацане (ПИК) и перона.

3. Вътрешен кръг. Сгради, зони и въздухоплавателни средства, изискващи осигуряване на максимална защита (охрана, патрулиране и допълнителни ограждения).

---

[3] *Периметър на летище – площ от земната повърхност, оградена с периметрово оградно съоръжение, в рамките на което е разположена работна площадка на летище.*

*Глава втора*

# СИСТЕМЕН АНАЛИЗ НА СИГУРНОСТТА И ЗАЩИТАТА НА ЛЕТИЩЕ

Нито едно летище, независимо колко е голямо, не може самостоятелно да се справи с последствията на всички вероятни заплахи и рискове за сигурността. Това налага да се разчита на подкрепата и експертизата на други структури от държавната и местната власт при изготвянето на планове за действие при възникване на кризисни ситуации. Подобен подход гарантира ефективно разпределение и изразходване на наличните ресурси в полза на всички страни.

За да се изучат закономерностите на процесите, протичащи при осигуряване сигурността на летище, е необходимо да се опише средата, в която оперират субектите.

## 2.1. Анализ на средата за сигурност

Състоянието на баланс на интересите в междуобщностните, вътрешнодържавните и международните отношения, при което не съществуват нарушения на правните норми, е предпоставка за минимизиране на риска от осъществяване на терористичен акт. Нарушаването на съществуващия баланс на интереси води до появата на терористична заплаха за сигурността.

Основните критерии за оценка на средата за сигурност са потенциалните рискове и заплахи, явлението, което ги създава, и степента на тяхното разрастване. За да говорим по-нататък за заплахите, стоящи пред гражданската авиация, е необходимо да дефинираме понятията *заплаха*, *уязвимост* и *риск* и да разгледаме взаимовръзките между тях.

*Заплахата* се дефинира като „вероятност или възможност за нападение". Сериозността на заплахата е мярка за вероятността да бъде направен опит за нападение над определена цел.

*Уязвимост.* Отчитайки, че няма единно определение за уязвимост, в случая ще я дефинираме като „характеристиките на обекта, които биха могли да бъдат използвани при нападение".

Тези характеристики са:

- процедури за сигурност;
- поддържано ниво на сигурност;
- участие и осведоменост на персонала за значението на сигурността;
- обща осведоменост на служителите.

В областта на авиационната сигурност *уязвимост* е всяка слабост на прилаганите мерки и процедури, недостиг на човешки или материални ресурси, които биха могли да бъдат използвани за осъществяване на акт на незаконна намеса, с който да бъде компрометирана сигурността на гражданското въздухоплаване.

*Рискът* е вероятността конкретната заплаха срещу даден актив да се осъществи и да се предвиди колко би бил повреден той. Това е решаваща разлика между заплахата и риска: заплахите са лошите неща, които могат да се случат на активите, а рискът е възможността да се появи конкретна заплаха.

В областта на сигурността *рискът* се определя като мярка за възможността едно нападение да бъде извършено и да бъде успешно. РИСК = ЗАПЛАХА х УЯЗВИМОСТ, тоест заплахата и уязвимостта определят нивото на риска. Колкото са по-големи вероятността за нападение и уязвимостта, толкова и рискът е по-голям.

Съгласно тези критерии заплахите за сигурността на дадено летище могат да бъдат класифицирани:

а) според обхвата им като международни, национални (вътрешнодържавни), регионални и локални;

б) според сферата им на проявление като политически, икономически, природни, екологични, демографски, религиозни, социални и др.;

в) според причините, които ги предизвикват, като природни бедствия, промишлени аварии и катастрофи, действия на терористични структури, етнически и религиозни противоречия, технически и др.;

г) според средата им на проявление като физическа среда (от земята; от въздуха; от морето, ако летището има излаз на море) и информационна среда (информационно пространство).

От направената класификация следва, че терористичната заплаха реално може да бъде породена от различни явления, а нейната реализация – да се прояви от физическата или информационната среда.

В настоящия учебник се разглежда *заплахата от терористичен акт от прилежащата територия/външния периметър на летище* (повърхността на земята), без да се вземат предвид сферата на проявление и обхватът.

Гражданското въздухоплаване е потенциална мишена на актове на незаконна намеса. За да се намалят възможностите такива актове да се случат и последствията, които могат да предизвикат, от съществена важност е анализът на средата за сигурност да се основава на точна оценка на заплахата. Нивото на сигурност трябва да бъде адекватно на съответната заплаха, като се прилагат селективно интензивни мерки в зависимост от степента на риска.

Като се отчитат международната обстановка и тенденциите в областта на авиационната сигурност, е необходимо постоянно да се:

– оценява нивото на заплаха на територията на страната по отношение на българските оператори;

– оценява нивото на заплаха на територията на страната по отношение на чуждите оператори;

– провеждат обследвания на сигурността и анализ на риска на гражданските летища за обществено ползване във връзка с подобрения в методите за сигурност и настъпили физически и организационни промени по летищата;

– изпълняват искания на други държави за прилагане на допълнителни мерки за сигурност по отношение на полети със завишен риск до степен, в която това е практически възможно.

### 2.2. Обследване (оценка) на сигурността

Преди всеки план (проект) да започне изграждане е нужно да има предварително направена практическа оценка на сигурността за

защита на съоръжението. Тази оценка може да бъде наречена „обследване на сигурността", „оценка на уязвимостта" или „анализ на риска". Оценката на сигурността е цялостен преглед на съоръжението. Процедурата за летищата – в България специално, се нарича „охранително обследване на обект"[4]. Извършва се ежегодно от Главна дирекция „Гранична полиция" съгласно Наредба за граничните контролно-пропускателни пунктове, приета с ПМС № 104/20.05.2002 г., Наредба № 7/08.07.1998 г. за системите на физическа защита на строежите на Министерството на регионалното развитие и благоустройството, Регламент 300/2008 на Европейския парламент и на Съвета относно общите правила в областта на сигурността на гражданското въздухоплаване, Регламент 185/2010 на Комисията за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването, Инструкция рег. № Із-3025/21.12.2010 г. на МВР и Инструкция рег. № I-4/29.12.2010 г. на ДАНС за условията и реда за определяне на стратегическите зони на стратегическите обекти и зоните, свързани с изпълнението на стратегически дейности от значение за националната сигурност, Методически указания рег. № АМ-3135/06.04.2007 г. за извършване на охранителни обследвания на обекти и на основание чл. 7, т. 7 от Закона за МВР.

*Оценка на сигурността.* Първият въпрос, на който трябва да се даде отговор, е „Каква е заплахата?". Първата задача е определянето на потенциални заплахи и изготвянето на списък с тях: незаконно завладяване на въздухоплавателно средство в полет или на земята; вземане на заложници на борда на въздухоплавателно средство и в част от терминала; нападение над силите за охрана или служителите от администрацията на обекта; извършване на престъпления от общ характер; интелектуални кражби; посегателство над информация, свързана с външни фактори; телефонен тероризъм; природни бедствия; стачни и протестни действия; аварии или комбинация от някои от

---

[4] *Обследване по сигурност (от НПСГВ) – оценка на нуждите на сигурността, включително идентифициране на уязвимости, които биха могли да бъдат използвани за извършване на акт на незаконна намеса, и препоръка на коригиращи действия.*

тях. Тези заплахи дават насоки за съперника, определят и осигуряват разработването на една ефективна система за физическа защита.

*Идентифициране на целта* означава определяне и откриване на най-ценния актив, който трябва да бъде защитен. Активите могат да бъдат персонал, имущество, оборудване или информация. За да се определят, е най-разумно да се изработи матрица за идентифициране на актива. Тази матрица оценява вероятността от нападение или загуба и какви биха могли да бъдат последствията от това.

*Характеристиките на обекта* могат да бъдат разглеждани от гледна точка на това, дали обектът е съществуващ, или е в процес на изграждане. При изграждането на нова инфраструктура специалист по сигурността трябва да участва в строежа и преразглеждането на архитектурните планове. В случай на вече съществуващ обект е препоръчително съвместен екип от специалисти да извърши оценка на сигурността. Американският институт на архитектите е установил някои ключови въпроси, които трябва да бъдат разгледани по време на оценката на сигурността:

1. Какво искаме да защитим?
2. От кого искаме да се защитим?
3. Къде са най-уязвимите активи на инфраструктурата?
4. Какви ще бъдат последствията от загуби?
5. Какво специфично ниво на защита желаем да постигнем?
6. Какви мерки за защита са най-подходящи за дадената инфраструктура?
7. Какви мерки за защита са най-важни за дадената инфраструктура?
8. Какви са специфичните изисквания за проектиране на физическата сигурност?
9. Как интегрираните системи, обслужващият персонал и процедурите реагират на инциденти, свързани със сигурността?

Важен момент при одитирането е то да се проведе и денем, и нощем, тъй като има много особености, които не могат да се забележат през деня. Пример може да бъде поставяне или преместване на осветление за даден актив.

### 2.3. Оценка на заплахата, уязвимостта и риска

Процесът на оценка на заплахата разглежда добиването на информация и данни, които дават сведения за наличието на заплахи и възможности, за да се определят намеренията, способностите и вероятността за появата на различни инциденти. Органите, които събират и обработват информацията, са длъжни да подготвят своята оценка за заплахата, да определят степента на готовност на силите за сигурност и защита, да изследват пълния диапазон от вероятности за възникване на заплахи и да предвидят намеренията и възможностите на терористите.

Физическата заплаха за съоръжението трябва да бъде дефинирана като част от развитието на целите в системата за физическа защита. Методологията за определяне на заплахата се състои от регистър с информация, необходима за определянето ѝ. Този регистър може да включва вида и възможните ходове на противника, потенциалните му действия, мотивация и физически възможности. Заплахата невинаги е извършена или предизвикана от човек – тя може да бъде и естествена, природна.

Източниците на информация за заплаха могат да бъдат и от разузнаването. Разузнавателните източници могат да предоставят подробна информация и картина за групи, които биха могли да представляват заплаха за организацията. Събиране на информация може да се осъществява от открити източници[5] за изследване минали и настоящи престъпления. След анализ всички събрани данни могат да бъдат полезни за характеризиране на потенциалната заплаха за дадения обект. Анализът на вероятните заплахи е непрестанен процес на компилация и изследване на всяка достъпна информация, за да се определят вероятните им цели.

---

[5] *Открити източници са всички носители на информация, които не са засекретени като държавна или служебна тайна (т.нар. класифицирана информация) и достъпът до които е сравнително лесен. Сред тях са закони, вестници, списания, книги, брошури, речи, доклади, телевизионни предавания, документални филми, интернет и други.*



2/1/16

За определяне размера на вероятната заплаха се изследват факторите, които оказват влияние върху нейното разпространение. Тези фактори са:

• *Наличие.* Терористичните организации съществуват и са способни да нанесат поражение на обект от инфраструктурата на летище.

• *Способност.* Терористичните организации притежават необходимия потенциал да нанесат поражение на обекта.

• *Намерения.* Нарушаване на обществения ред, дестабилизация на държавата или демонстрация на сила и всяване на страх в обществото.

• *Поуки от практиката.* Проучване на опита и извличане на изводи от прегледа на минали терористични актове.

• *Целева информация.* Обработка на данни от различни източници и синтезиране на правдоподобна информация за дейности, показателни за подготовката на терористичен акт.

При оценката на заплахите за сигурността и защитата на обектите се използват методи, които да помагат на ръководителите и дежурните сили за реакция при вземане на решения за разпределение на ресурсите за защита от възможните заплахи. Процесът на оценка на риска дава на ръководните органи необходимата информация за заплахата и уязвимостта на обекта, персонала и пътниците и позволява вземането на решение.

*Оценката за уязвимостта* от терористични атаки на летища се извършва, без да е необходимо да се взима под внимание моментната оценка на заплаха. Тя се извършва от служители на МВР (Специализирана дирекция „Оперативно-технически операции", Главна дирекция „Гранична полиция"), летищна сигурност и инспекторите по авиационна сигурност от Главна дирекция „Гражданска въздухоплавателна администрация". Тази оценка определя възможните начини, по които може да бъде атакувано дадено летище, и върху тази основа се определят контрамерките, които ще бъдат приложени на място, за откриване, възпиране и осуетяване на подобни атаки.

*Уязвимостта* може да бъде породена от:

• недостатъци/слабости в изисквания стандарт (това, което би могло да бъде използвано поради недостатъчно адекватна защита при съществуващите антитерористични мерки или заради сериозни пропуски в програми, мерки и процедури);

• неадекватно прилагане на мерките, които се изискват;

• комбинация от двете.

Оценката на уязвимостта трябва да бъде направена в рамките на определени заплахи, съобразени със стойността на активите. Следва да се отбележи, че оценката на уязвимостта може да промени цената на актива, т.е високото ниво на уязвимост води до снижаване цената му. В таблица 1 е показан пример за оценка на уязвимостта на някои съоръжения.

*Таблица 1*

**Оценка на уязвимостта на някои съоръжения**

| СЪОРЪЖЕНИЕ | УЯЗВИМОСТ |
|---|---|
| Вход ЗАМИНАВАЩИ | средно |
| CCTV / Видеонаблюдение | ниско |
| Контрол на достъп | високо |
| Служебен вход | ниско |
| Паркинг | ниско |
| Вход ПРИСТИГАЩИ | високо |

Основният процес при *оценката на риска* включва следните три елемента:

• оценка на заплахата;

• идентифициране на уязвимите цели;

• управление на процеса чрез развиване на съответните контрамерки и тяхното прилагане.

Оценката на риска не означава елиминирането му, а управление, което да позволява: да се изчисли, дали една атака е вероятно да бъде предприета и дали би била успешна; развитие на ефективни контрамерки, пропорционални на риска, така че той да бъде сведен до приемливо ниво. Винаги има остатъчни рискове, но трябва да има баланс между сигурността на обществото и функционирането на ефективна икономика.

Съгласно Директива 114 на ЕС (Приложение II) процедурата за изготвяне на мерки за сигурност задължава оценката да се извърши в следната последователност:

1. Установяване на важните елементи от ключовия обект, на които ще се извърши защита.

2. Извършване на оценка на риска въз основа на сценариите за действие на терористите и възможните последици за елементите на ключовия обект.

3. Установяване на мерките и процедурите за действие при защита.

Дейностите, протичащи в системата за сигурност на летище, свързани с неговата сигурност и защита, определят рамката на цикъла „откриване – отговор", състоящ се от следните условни елементи: планиране, наблюдение, откриване, локализиране, опознаване (идентифициране), предаване на информацията, обработка, анализ и вземане на решение, реакция (отговор) и оценка на получения резултат. Обединяването в единен процес на тези съставни довежда до значително повишаване на ефикасността и ефективността на извършваните дейности.

При терористично нападение е важна незабавната реакция, включваща бърза идентификация на засегнатата зона и мигновено управление на бедствието (прилагане на мерки за изолиране на хора и логистика, хоризонтална и вертикална координация и кооперирание). В голяма степен ефективният отговор зависи от ефективните комуникационни канали и бързото включване на публичните и частните актьори. Последната фаза е насочена към прилагане на мерки за минимизиране на ефекта от инцидента.

Разбира се, всички защити, разположени в зоните за сигурност, не гарантират, че никога няма да има пробив. Въпреки това е съвсем очевидно, че общата сума на всички тези защити води до много по-ефективна система за сигурност, отколкото само една защита, работеща сама за себе си. Това не означава и, че всяка една известна защитна мярка следва да бъде безразборно прилагана във всяка ситуация. Използването на риска, уязвимостта и оценката на заплахата трябва да намери баланс между сигурността, даваща отбрана в дълбочина[6], и финансовите, човешките и организационните ресурси, които ръководството на организацията е готово да разреши.

Ключът към успешна система е интеграцията на хора, процедури и оборудване в една система, която защитава цели от заплахата. Добре проектирана, тя осигурява отбрана в дълбочина, намалява до минимум последствията от пробив и дава балансирана защита. Физическата сигурност не се различава много от компютърната сигурност. В действителност завършва със съответствие на процесите. Съответствие на процесите е равно на оценка на заплаха, изработване на система за сигурност, която включва оборудване и процедури, и след това тест на цялата тази система.

---

*[6] Отбрана в дълбочина (defence in depth) – организиране на отбранителни райони, които си оказват взаимна поддръжка и чиято задача е да поемат и отслабят атаката на противника, да му попречат да събере първоначална информация за техните сили и средства и да дадат възможност на командването да маневрира с резервите.*

*Глава трета*

# ФИЗИЧЕСКА ЗАЩИТА НА ВЪНШНИЯ ПЕРИМЕТЪР НА ЛЕТИЩЕ. ПАТРУЛИРАНЕ

Защитата на летищата се осигурява чрез съчетаване на мерки за физическа защита, различни системи, операции и процедури. При проектиране на летищата трябва да бъдат отчетени мерки за сигурност в следните направления:

- защита на периметъра;
- физическа защита на зданията;
- защита на терминала;
- обекти за проверка на пътниците;
- авариен оперативен център.

## 3.1. Защита на външния периметър на летище

Превенцията на посегателства върху летищния оператор се състои от някои ключови елементи, като анализ върху функцията на актива и дизайна, противодействащ на физическата атака. За да бъде поставена и очертана границата между страна „земя“ и страна „въздух“ и да бъде ограничен достъпът на хора и превозни средства, са необходими ограда, стени, бариери, електронни технически средства (сензорна граница, радари за движение), естествени бариери (например водни обекти), както и наличие на стационарни постове и патрули.

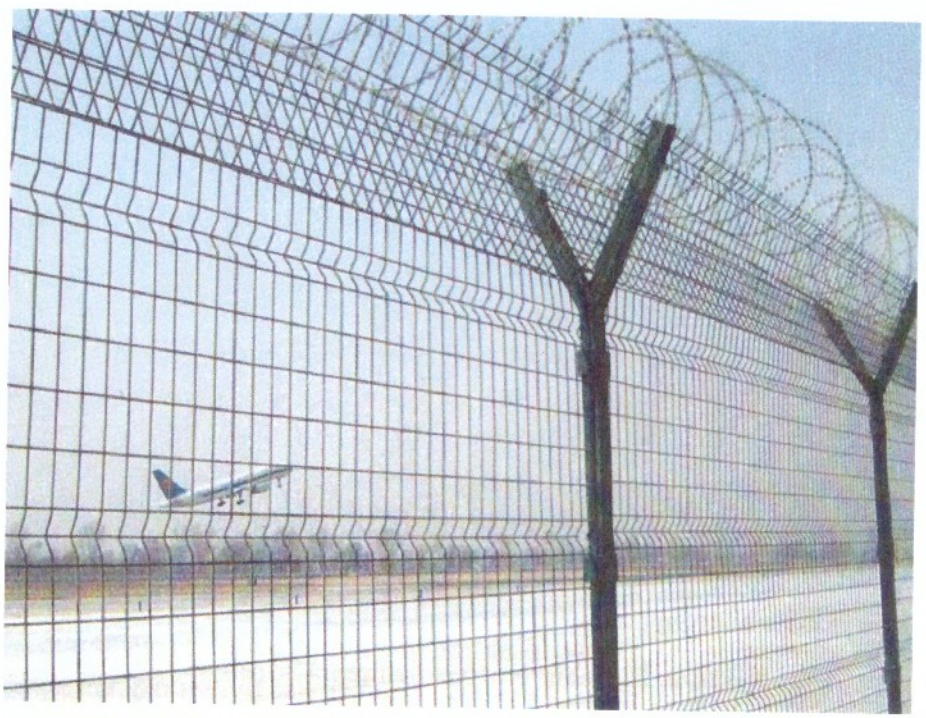
### *3.1.1. Физически бариери*

Физическите бариери се използват, за да се предотврати и забави достъпът на неоторизирани лица в зоната с ограничен достъп. Те се проектират така, че да бъдат постоянна визуална и физическа преграда. Освен това служат и за удовлетворяване на изискванията за безопасност в различни ситуации. Периметровата ограда и други физи-

чески бариери трябва да бъдат проектирани и съобразени с изискванията на Националната програма за сигурност в гражданското въздухоплаване (НПСГВ).

*Защитни ограждения (периметрова ограда)*

Защитните ограждения са предназначени за разграничаване на периметъра, възпрепятстване на несанкциониран достъп, предотвратяване на проникване и оказване на помощ при откриване на нахлуване (преодоляването на защитното ограждение представлява явно действие, видимо с помощта на системите за наблюдение). При проектиране на защитни ограждения на летищата трябва да се отчитат тези цели, а също и оценяемото ниво на риск от несанкционирано проникване.

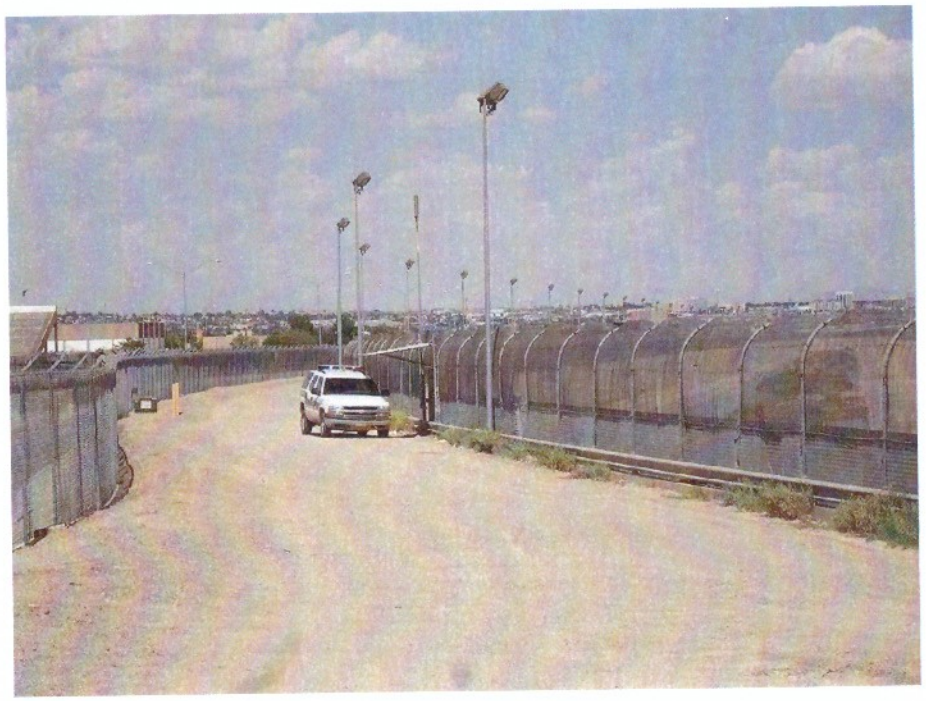


Сн. 1. Периметрова ограда на летище

Осигуряваната от оградението (от периметровата ограда) степен на защита (сн. 1) зависи от неговите височина, конструкция,

материал, от който е направено, а също и от допълнителните средства за осигуряване на безопасност, използвани за повишаване на надеждността или ефективността, като бодлива тел над оградението, периферна система, защитна сигнализация, охранително осветление или затворена телевизионна система.

Оградението трябва да е достатъчно високо, за да бъде трудно през него да се премине. Препоръчителната минимална височина е 2,44 м (8 фута) с добавяне на слой бодлива или бодливо-режеща тел, поставена под определен ъгъл. Оградението трябва да е поставено по такъв начин, че да е много трудно под него да се направи изкоп или да се премине. То може да е вкопано в земята или да е поставено на бетонен фундамент.



Сн. 2. Двойно ограждение на летище

Оградението може да бъде направено от различни материали. При избора на най-подходящите трябва да бъдат взети предвид и други компоненти на системата за осигуряване на безопасност на периметъра. Например, ако защитното ограждение се използва в комбина-

ция със защитна аларма и качествено осветление на периметъра, система CCTV, предупредителни знаци и патрулиране, то може е от най-обикновен тип. В райони, в които такива системи няма, трябва да се прибегне до ограждение от по-високо ниво, за да затрудни и увеличи времето за проникване. Необходимо е също да се вземат предвид аспектите на техническото обслужване и простотата на смяната на отделни секции в случай на повреда или непригодност за експлоатация (например поради корозия).

При наличие на необходимост и средства могат да се използват двойни ограждения (сн. 2). Обикновено представляват по-ниско външно ограждение – например телена ограда с бодлива тел с височина от 1,8 м (6 фута), допълнена от система за защитна сигнализация, която да покрива пространството между вътрешното и външното ограждение. Вътрешната ограда е по-висока – например 2,44 м (8 фута), изработена от метална мрежа с бодлива тел отгоре. Смисълът от такава схема е в това, че външното ограждение е за демаркация и предотвратяване на достъпа. Освен това то ограничава забранената зона (обикновено 3 м/10 фута ширина), в която може да функционира системата за защитна сигнализация. Ако извършителят премине през външното ограждение или проникне през направен в него отвор, ще бъде открит от системата на защитната сигнализация, която ще извести патрулите. По-високото вътрешно ограждение ще задържи и затрудни действията на нарушителя, за да може патрулите да го задържат преди да е проникнал в контролируемата зона или зоната с ограничен достъп.

Огражденията от метална мрежа в комбинация с бодлива тел или жилет осигуряват ясна видимост за патрула и може да бъдат изградени почти във всякаква среда (сн. 3).

Освен по дължината на горния край на оградението бодлива тел или концентрични кръгове от бодлива тел може да се поставят в долния край, от вътрешната страна на оградата, за да възпрепятстват проникването под оградението. Монтаж на такива средства в места, където имат достъп хора, може да има правни последици, така че използването на тази мярка изисква предварителна правна консултация.

Сн. 3. Ограждения от метална мрежа в комбинация с бодлива тел

В някои участъци – например в близост до прага на полосата за излитане и кацане, не може да се използват метални огради, тъй като могат да попречат на нормалната работа на навигационните средства. Те могат да бъдат заменени с пластмасови или дървени огради, допълнени със спирална тел и/или електронни бариери, или „живи препятствия“ – например бодлив храсталак. При избора на вида на оградението е необходимо да се вземат под внимание теренът и изискванията към системата за сигнализация и/или видеонаблюдение. Доколкото е възможно, оградението трябва да се поставя в праволинейна конфигурация за осигуряване на наблюдение и лесен монтаж. Участъците, в които се променя посоката на оградението, обикновено улесняват проникването и трябва да се свеждат до минимум. Доколкото това е възможно, трябва да се избягват стикове, насочени навън, защото в тези области е най-лесно да се премине над оградението.

Желателно е цялата площ на оградението да се намира в полезрението на служителите по сигурността на стационарните постове

или патрулите. В някои случаи може да се наложи да се намали оградението, за да се избегнат „джобове", които иначе не биха попаднали в полето на наблюдение. Това се отнася не само за стените и плътните огради, но и за прозрачните, които, гледани под ъгъл, също стават непрозрачни. Освен това като алтернатива може да се използва система за видеонаблюдение. От двете страни на защитното оградение, особено в близост до терминала и критичните части в полоса с достатъчна широчина (3 м минимално отстояние от двете страни на оградата), трябва да бъдат премахнати всички препятствия (осветителни стълбове, указателни табели, оборудване, транспортни средства, дървета), които биха могли да служат като прикритие за нарушители или да им помогнат да преминат през оградата. За целта оградението може да се измести навътре от фактическата граница на обекта, за да се получи извън заграждението, от външната страна, свободна зона. Това улеснява наблюдението и поддръжката на оградата и отказва потенциални нарушители.

Озеленяването в чистата зона трябва да бъде сведено до минимум, за да се намали потенциалът за камофлиране на обекти и враждебни лица. Има регистрирани случаи, в които лица са достигали до паркирани въздухоплавателни средства чрез прескачане или увреждане на периметровата ограда. За възпиране или забавяне на такива атаки трябва да се поддържа достатъчно разстояние между перона за паркиране на въздухоплавателни средства и периметровата ограда. Тези ясни зони не трябва да се бъркат с подобните на подходите на пистата за излитане и кацане.

По дължината на защитното ограждение трябва да се предвиди път за патрулиране с използване на транспортни средства – в идеалния вариант както от контролируемата, така и от неконтролируемата зона, но ако това е невъзможно, обезателно от страната на контролируемата. Някои обекти, разположени в нея и изискващи повишена степен за защита (например складове за гориво, складове за товари), трябва да бъдат оборудвани със специални средства за защита, отговарящи на същите изисквания като защитните ограждения по периметъра на летището.

*Сгради*

Сгради и други фиксирани застроени структури могат да бъдат използвани и включени като част от периметъра, но при условие, че са взети мерки за контрол на достъпа и ограничаване на неразрешено преминаване през тях, т.е. всяка врата и прозорец трябва да бъдат усилени и с допълнителни решетки. Тези сгради могат да бъдат най-различни в зависимост от естеството на работа и необходимостта на достъп (непрекъснат или в определено време от денонощието), но осигуряването на безпрепятствен изход от обществената страна „земя" е необходимо условие за противопожарна евакуация.

*Стени*

Стените са често срещани физически бариери, които се използват както за интериора (например за разделяне на пътникопотока), така и за екстериора.

• Вътрешни стени. Може да са от стъкло или материал, използван в строителството на терминала. Трябва да са изградени от пода по възможност до тавана или достатъчно високо, за да няма начин да се прехвърли нещо от другата страна. Вътрешните стени са подходящо решение за разделяне на пътникопотока, гранична сигурност и осигуряване на контрол на достъпа до определени зони в терминала.

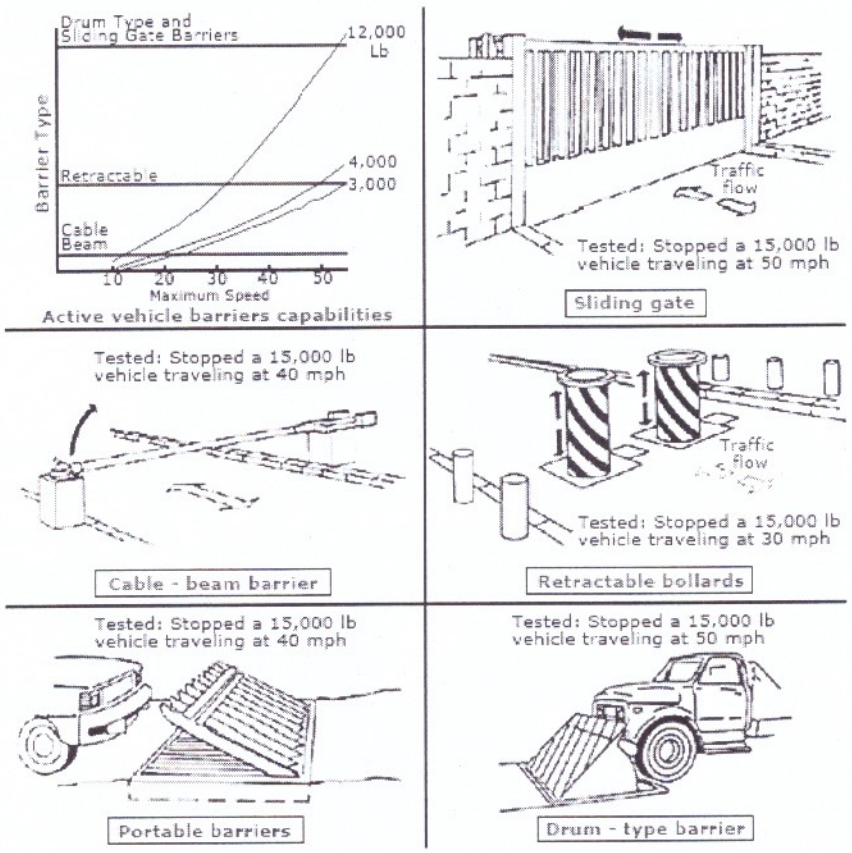
• Външни стени. Използването на външните стени не е икономически изгодно като мрежовата ограда, но често е необходимост. Стените осигуряват по-малка видимост, но могат да бъдат перфектно съчетани с околната архитектура. Изработват се от твърди материали и по тях не трябва да има възможност за катерене. Отгоре задължително се поставя бодлива тел, за да няма възможност за сядане.

*Бариери за сигурност*

Налице е значителен обем от знания за ефективна защита с бариери, които могат да стопират удар с превозно средство. BSi PAS 68[7]

[7] *BSi PAS 68 – спецификация за бариери против враждебно настроени превозни средства.*

е стандарт във Великобритания и еталон в оборудването на периметъра с физически бариери. С малки положителни разлики той е еквивалентен на американския DOS-K12. Изискването на BSi PAS 68 като стандарт е, че задължително инсталираната бариера за сигурност трябва да спре 7,5-тонен камион, който се движи със скорост 80 км/ч. Фигура 4 илюстрира видове бариери с различни приложения.




Фиг. 4. Активни бариери за сигурност и резултати от тестването им[8]

[8] *Figure E-7. Active Barrier Test Results and Examples. Transit Security Design Considerations. FTA Office of Research Demonstration and Innovation, FTA Office of Program Management. GlobalSecurity. Home page. November, 2004. http://www.globalsecurity.org/security/library/report/2004/transit-security-design_appe.htm*

Използването на естествени бариери може да стане необходимост на структурното подпомагане на физическата защита на съоръжението за излитане и кацане. Естествените бариери могат да бъдат включени като допълнение към другите видове защита. Те включват водни обекти, дървета, мочурливи места, плътна зеленина, скали и други. При тяхното използване обаче е необходимо операторите да вземат под внимание оценките на риска и уязвимостта, предварително подготвени за летищния оператор. Този тип естествени бариери са много подходящи за използване извън периметровата ограда като допълнение. Например прокопаването на канали или издигането на земна маса е много подходящо допълнение към периметъра в определени случаи. Основен недостатък е, че не могат да бъдат интегрирани към електронните системи за защита, а и в определени случаи може да пречат на видимостта.

### *3.1.2. Електронни системи за защита*

Доскоро на периметровата охрана се гледаше като на чисто пасивна физическа бариера срещу достъпа. Днес реалностите правят все по-наложително прилагането на активни средства, които да отчитат опита за проникване и същевременно да реагират така, че да предотвратят или забавят нежелано навлизане, без да се изисква постоянно наблюдение от човек.

Системите за периметрова охрана имат за цел осуетяване на опити за проникване в защитавания периметър посредством детекция на нарушителя и изпращане в реално време на информация до централен мониторингов център. Детекцията може да се осъществява по няколко начина: чрез регистриране на вибрации по оградата (сн. 4), чрез нарушение на електромагнитно поле, създадено от кабели, монтирани под земята (фиг. 5) и чрез инфрачервени или микровълнови бариери.

Преимуществото на тези системи е, че работят при всякакви атмосферни условия. Имат висока точност на локализиране на нарушението и елиминират фалшивите аларми, породени от вятър или дъжд.

Важно е да се отбележи, че редуцират разходите за жива охрана, защото мигновената и точно позиционирана детекция на нарушения в периметър от няколко километра дава възможност контролът да бъде ефективен и при ограничен персонал. Така охранителят ще бъде изпратен на нужното място само в необходимия момент.

Сн. 4. Регистриране на вибрации по оградата

Фиг. 5. Детекция чрез нарушаване на електромагнитно поле, създадено от кабели, монтирани под земята

Системата може да бъде интегрирана с други методи за защита – видеонаблюдение, осветление или гласово оповестяване. Така се осигуряват комплексни възможности за защита на периметъра. Чрез камерите за видеонаблюдение, разположени на стратегически места, се осъществява дистанционна визуална оценка на условията за аларма. В реално време или на запис изображенията от видеокамерите се анализират в центъра за координация на дейностите по сигурността. Необходимостта от видеоконтрол зависи от специфичните изисквания на летищния оператор и може да се интегрира в нови или вече съществуващи системи.

Технология от ново поколение са и системите за наземно радарно наблюдение, които са икономически изгодни и ефективни. Препоръчват се от много специалисти по физическа защита на критична инфраструктура. Голямото им предимство е, че дават възможност да се открие и проследи обект много преди да се е доближил до периметровата ограда. Обхватът им на действие включва страна „въздух“ и част от страна „земя“. Самостоятелни радарни системи вече успешно са тествани и работят на много летища. Тяхната дееспособност се изразява в следното:

- откриване на проникване по периметъра, включително извън него и по протежение на морски или водни граници;
- автоматично следене на нарушители в периметъра и зоната с ограничен достъп;
- доставка на аларми и данни в команден център, който регулира дейностите по сигурността.

Сред новите технологии е и така наречената *data fusion*, в която гама датчици, техники за наблюдение, анализ на данни, комуникация и процедури са обединени в едно цяло. Те са IP-базирани и могат да бъдат интегрирани така, че да се осигури единна система за физическа сигурност. Основната цел на това сливане е да се подобри способността на персонала по сигурността да реагира адекватно на различните видове аларми. Чрез използването на автоматизирани системи за анализ на сигнали операторът има възможност няколко пъти да увеличи своето зрително поле. Освен това те премахват субективния фактор и повишават ефективността при осигуряване на сигурността.

В случай на регистрирано събитие служителите по сигурността могат да бъдат своевременно алармирани, а събитието – записано в системата.

### 3.2. Контрол на достъпа

***Входни контролни точки***

Обикновено има повече от няколко входни контролни точки, снабдени с бариера за достъп на превозни средства, както и вход, предназначен за хора. На тези т.нар. входове също могат да се използват електронни системи за контрол на достъп, видеонаблюдение, рентгени за проверка на багаж, скенер за инспекция под превозното средство и др.

Във всички случаи в зависимост от дизайна на входната контролна точка се определя и ефективността. Желателно е броят на входните контролни точки да е сведен до минимум. При това достъпът на превозни средства и хора трябва да е разрешен за осигуряване на рутинни операции, обслужване и авариен достъп.

*Рутинни операции* са ежедневните операции в дадено летище, които се използват от персонала – полиция, патрули и екипи за реагиране, кетъринг, товарни автомобили и влекачи за гориво, насрочени превозни средства за доставка, наземни оператори и др. Входовете, използвани за рутинни операции, обикновено са с висока пропускателна способност. Те трябва да бъдат проектирани за продължително ползване и висока активност, за да се сведе до минимум забавянето на потребителите.

*Обслужващите операции* се изпълняват от персонал за извършване на редовна и периодична поддръжка. Типичните задачи включват косене, почистване, поддръжка на аеронавигационното и комуникационното оборудване и др. Тези входове не изискват бърза пропускателна способност и обикновено са неавтоматизирани.

За *авариен достъп и спешни случаи* са входове, които се използват от летището за бързо реагиране в аварийни ситуации – особено такива, които са свързани с въздухоплавателно средство. Обикновено

това са заключени портали, които не се ползват, но са в готовност да бъдат отворени по всяко време в случай на аварийна ситуация.

***Врати***

За да се предотврати неоторизиран достъп до страна „въздух", всички врати, водещи от публичните зони към терминала, трябва да бъдат сведени до минимум и ограничени. Контролът на достъп като процедура в различни части на терминала е неизбежен, затова използването на електронни устройства, като например RFID картови четци, комбинирано с видеонаблюдение, е належащо. Те могат да се използват както за контрол на достъп, така и за контрол на работното време на персонала.

***Охранителни постове***

Персоналът на охранителните постове контролира влизането в зоната с ограничен достъп. Те осигуряват контролните входни точки на периметъра. Контролират и установяват идентификация на лица и превозни средства, които преминават, в съответствие с изискванията на НПСГВ.

*Механизми*, като турникети, плъзгащи врати, падащи бариери или ролд-блокери, могат да бъдат използвани да задържат преминаващите, докато не бъдат проверени и идентифицирани. Входната контролна точка трябва да предоставя малко по-висок стандарт за сигурност от периметровата ограда. Няма смисъл да се инвестира в ролд-блокер или падаща бариера с висока сигурност, ако на десетина метра встрани може да се премине с лекота през оградната мрежа. Балансът в дизайна трябва да е съобразен с оценката на риска и уязвимостта.

*Подвижни шипове.* Това е стар вариант, използван в миналото, който вече не се препоръчва. Няма гаранция, че след спукването на гумите превозното средство ще спре и няма да продължи към въздухоплавателното средство или друга цел.

*Защита на входните контролни точки* се изразява в проектиране на достатъчна пряка видимост и безопасно разстояние в зоната,

където служителят по сигурността ще извърши проверка на превозното средство.

Достатъчно място трябва да бъде оставено за превозни средства, на които следва да бъде извършена пълна проверка, и отделно място за обръщане на превозни средства с отказан достъп. Планът трябва да отговаря на очакваните обеми от трафик, средното време за инспектиране на превозно средство и размера на възможно най-голямото превозно средство.

*Комуникация.* От съществено значение е осигуряването на комуникация във всяка контролна входна точка, която да служи за съгласуваност, подаване на сигнал или призоваване на спешна помощ.

### *Защита от коли бомби или „затрудняващи достъпа съоръжения“*

Места за проверка на превозни средства и бариери, които могат да стопират удар с превозно средство, може да са необходимост във високорискови зони на съоръжението за излитане и кацане. Може да са необходими и при въвеждане на непостоянни мерки за сигурност по време на повишени нива на заплаха, или при полети с висок риск. Този аспект на летищния дизайн трябва да започне с резултатите от оценката на уязвимостта, приети по време на планиране. Пунктовете за претърсване на превозни средства трябва да се намират на достатъчно отдалечено, взривобезопасно разстояние от обществената зона и терминала.

Обществеият паркинг също трябва да се намира на безопасно разстояние от терминала. Безопасните разстояния при експлозия на превозно средство в зависимост от мощността на взривното вещество са показани в таблица 2. Тя е изготвена по данни на Бюрото за разследване на алкохол, цигари, оръжия и експлозиви, което е отдел към Министерството на правосъдието на Съединените американски щати. Смъртоносният взривоопасен обхват е определен за открит терен. Минималното необходимо отстояние е разстояние без опасност за живота, но въпреки това може да доведе до други наранявания или временна загуба на слуха. Наличието на падащи стъкла от ударната

вълна зависи от пряката видимост от източника на експлозията до стъклото. Експлозия, извършена в затворено пространство, може да причини срутване на конструкцията на сградата. Допълнителна опасност са отломките от превозни средства.

*Таблица 2*

**Безопасно разстояние при експлозия на превозно средство**

| | ОПИСАНИЕ КАТЕГОРИИ МПС | МАКСИМАЛНА ВЗРИВНА МОЩНОСТ | СМЪРТОНОСЕН ВЗРИВООПАСЕН ОБХВАТ | МИНИМАЛНО НЕОБХОДИМО ОТСТОЯНИЕ | СЧУПВАНЕ НА СТЪКЛА ОТ УДАРНАТА ВЪЛНА |
|---|---|---|---|---|---|
|  | Лек Автомобил тип Седан | 227 кг (в багажник) | 30 метра | 457 метра | 381 метра |
|  | Лек Автомобил тип Лимозина | 455 кг (в багажник) | 38 метра | 534 метра | 534 метра |
|  | Пърнически или Карго Бус | 4,000 кг | 61 метра | 838 метра | 838 метра |
|  | Камион (4.5m каросерия) | 4,545 кг | 91 метра | 1,143 метра | 1,143 метра |
|  | Камион (цистерна) | 13,636 кг | 137 метра | 1,982 метра | 1,982 метра |
|  | Влекач + Ремарке | 27,273 кг | 183 метра | 2,134 метра | 2,134 метра |

Проектирането трябва да позволява максимална видимост на района и надеждна и бърза комуникация в оперативния център по сигурността. Освен това трябва бъде оставено достатъчно свободно място за други превозни средства с предварително разрешение, като аварийни автомобили и др.

### *Други мерки за сигурност*

*Осветление за сигурност.* Подбрано осветление в определени участъци по периметровата ограда, контролните входни точки от периметъра е препоръчително. То трябва да осигурява осветеност на ограда/вход, карточетци, телефони, клавиатури, устройства за контрол и други така, че да прави обекта видим. По подобен начин се изисква достатъчно осветление под всяка камера за видеонаблюдение, където

има активност. За областите, където има минимално движение или активност, е подходящо поставяне на осветление със сензор за активация.

*Заключващи устройства*. Осигуряването на врати от периметъра чрез използването на брави задължително включва процедурни елементи като ключова система за управление. Затруднения, като записване, използване, преиздаване, загубване, кражба на ключове са важни фактори при избора на заключваща система. Второто важно нещо след избора ѝ е съхранението на ключовете. Решение за съхранение и администриране на ключове е закупуването на органайзер, чрез който може да се задават параметри за всеки ключ и неговите ползватели, подобно на RFID система за контрол на достъпа.

*Глава четвърта*

# ДЕФИНИРАНЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ЛЕТИЩЕ КАТО СЛОЖНА СИСТЕМА

## 4.1. Структурен анализ и оценка на системата за сигурност на летище

Поради съществената относителна тежест на съставните в цикъла *откриване – отговор* – наблюдение, откриване, локализиране, опознаване (идентифициране), предаване на информацията, обработка, анализ и вземане на решение, спрямо общия брой съставни с цел да се постави основен акцент върху тях, се въвежда понятието *аналитично-мисловна дейност на системата за сигурност на летище (ССЛ)*.

Аналитично-мисловната дейност на ССЛ е съвкупност от действия на силите, провеждана по единна концепция, под единно ръководство и управление за постигане на определени цели, свързани със сигурността на летището, в рамките на дефинирани пространствени, времеви и ресурсни ограничения.

Независимо от формата, силите и средствата, участващи в тази дейност, те трябва да функционират в единна, добре подредена и целенасочено управлявана сложна система. За да се анализират протичащите процеси в системата, е необходимо тя да се дефинира и на базата на мисиите и задачите, които изпълнява, да бъде избран научен подход, чрез който те да бъдат описани.

Тъй като ССЛ представлява система от подсистеми, то за нейното описание най-подходящ е системният подход. Предимствата му са в изследването на системата в динамика, на връзките и взаимоотношенията между елементите вътре в нея и връзките и взаимоотношенията на елементите с външната среда. Основните принципи при композиране и описание на системата са:

• цялостност– разликата между свойствата на системата като цяло и сумата от свойствата на съставящите я елементи;

• взаимозависимост – зависимостта между системата и средата на нейното функциониране;

• йерархичност – всеки елемент на системата може да се разглежда едновременно като подсистема и надсистема;

• множественост – даден елемент може да бъде описан от няколко системи, като всяка отразява определен аспект от неговата дейност.

Други принципи, на които трябва да отговаря системата, са: взаимодействие, качествени определеност и разграниченост, хомеостатичност[9], константност, динамичност и откритост.

Най-общо дефиницията за *сложна система* е „съвкупност от елементи във взаимодействие". Следователно в случая може да бъде възприето следното определение: „Сложната система представлява съвкупност от взаимосвързани и взаимодействащи си обекти и процеси, наречени компоненти, образуващи единно цяло, чиито свойства са неприсъщи за съставните ѝ компоненти, взети поотделно.

Системата за сигурност на летище се характеризира с това, че:

– е изкуствено създадена и е в резултат на управленско решение на система от по-висок ранг;

– е елемент от система от по-висок ранг;

– реализира целевата си функция в специфична среда и остър дефицит от време;

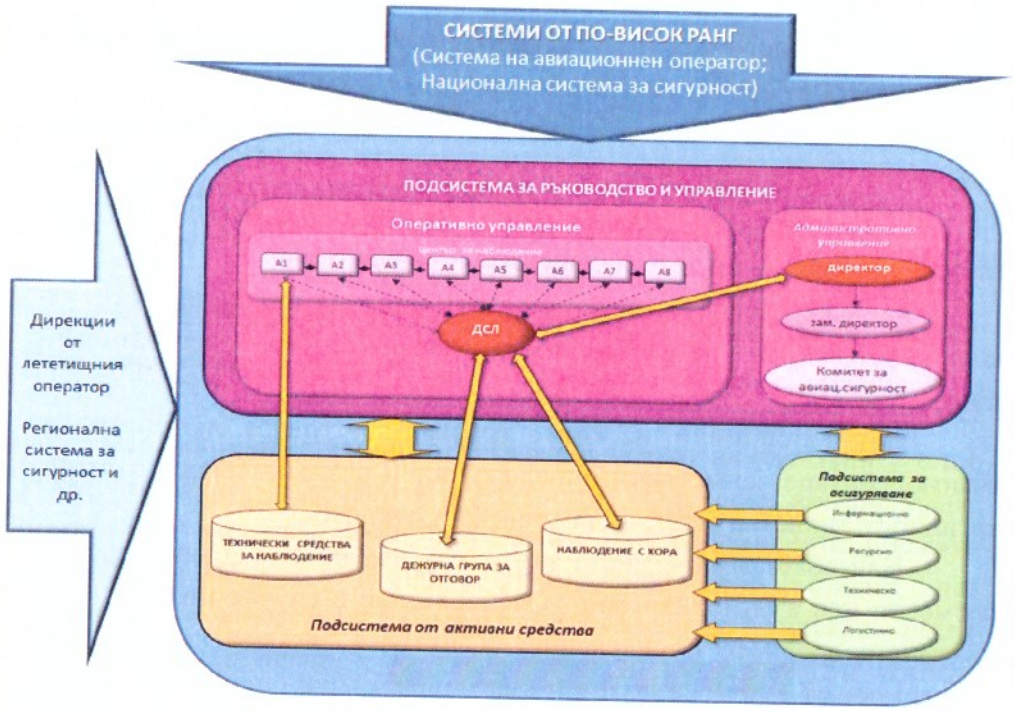
– е изградена от ограничен брой подсистеми, компоненти и функционални модули, обединени в елементи на системата (фиг. 6);

– е чувствителна на промените във външната среда;

– е система с целенасочено действие.

---

[9] *Свойство на дадена отворена система да регулира вътрешната си среда така, че да поддържа стабилно, постоянно състояние чрез многобройни корекции на динамичното равновесие, управлявани от взаимосвързани регулаторни механизми.*




Фиг. 6. Структурна схема на системата за сигурност на летище

На основата на посочените характеристики за нуждите на разработката се дава следното работно определение за ССЛ: Системата за сигурност на летище е съвкупност от елементи, функциониращи по единна концепция за сигурност, целенасочено управлявани в обща информационна среда, за осигуряване на процесите, целящи своевременно откриване на заплахи и превантивен отговор за предотвратяване на нежелани ефекти (последствия). ССЛ е отворена динамична система с възможност да включва в състава си функционални модули от подсистемите, изграждащи регионалната и националната системи за сигурност.

Способността на анализаторите в сферата на сигурността се определя като комбинация от ресурси, осигуряващи инструменти за постигане на измерим резултат при изпълнение на определени задачи в конкретни типови условия при съблюдаване на зададени стандарти.

На основата на даденото определение и в контекста на разработката *способността* може да се дефинира като качество на дадена

система, която чрез комбинация от ресурси и организираност[10] постига определен измерим резултат при изпълнение на конкретни задачи в дефинирани условия.

Сложната динамична система ССЛ може да бъде разгледана в три аспекта: компонентен, структурен и функционален. За описване на процесите, събитията и явленията в ССЛ се прилага общонаучният метод на изследване – системен анализ и синтез.

За да се изяснят характерните за ССЛ особености, е необходимо да се вникне в нейната сложност, което има двояко измерение. От една страна, сложността е свързана със системата и изграждащите я подсистеми. Нарича се статична сложност. От друга страна, е свързана с поведението на системата във времето, както и на процесите, протичащи в нея, и се нарича динамична сложност.

По системно-структурен признак ССЛ се декомпозира на подсистеми, включващи структурите (отново фиг. 6):

- обединяващи разполагаемия ресурс от активни сили и средства (Разполагаеми технически средства за наблюдение, ресурс за наблюдение с хора, групи за реакция и отговор и др.);
- за ръководство и управление;
- за осигуряване.

Всяка сложна динамична система не е просто сбор от характеристики на елементите, които я изграждат, а притежава своя качествена определеност, която е основна нейна характеристика, и за да се определи, е необходимо да се изследват функциите и взаимовръзките между елементите, техните реализация и изменение в системата.

Системата за сигурност на летище е система с целенасочено действие, която не може да се разглежда изолирано, извън външната среда[11], и е необходимо непрекъснато отчитане на влиянието на средата върху поведението ѝ.

---

*[10] Организираността е качество, което отчита степента на развитие и прилагане на концепции, нормативна база, подготовка и обучение, процедури, инфраструктура и др.*

*[11] Под „среда" следва да се разбират реални, известни обекти, процеси и явления, които могат да бъдат описани и да запазват достатъчно дълго своите характеристики (физически, вероятностни и др.).*

За анализ на динамичната сложност на процесите, протичащи в ССЛ, се използва математическо описание на процесния подход при моделиране на системата. Използвайки този подход, по системно-функционален признак ССЛ се разделя на подсистеми за:

- наблюдение и събиране на данни;
- ръководство и управление;
- реагиране и отговор;
- осигуряване.

Подсистемата за наблюдение и събиране на данни има основно предназначение да осигурява необходимата информация. Тя е елемент от националната система за сигурност, като в нея освен от източниците на обектова информация, базата данни се допълва и от всички регионални и национални структури, имащи способности да добиват информация.

Активното и всестранно добиване на информация е предпоставка за своевременно разкриване на рисковете и заплахите за сигурността, което цели да подпомагане органите, извършващи планиране, организиране и управление на действията при вземане на решение за адекватен отговор.

Класификация на добитата информация може да се извърши по различни признаци, основният от които е *важност*. Според него тя бива основна и критична. Критичната информация е с неотложно значение за безопасността/сигурността, изпраща се с най-голям приоритет, без да се предава по обичайния ред и канали за оценка. Налице е необходимост от реакция на системата в условия на дефицит от време.

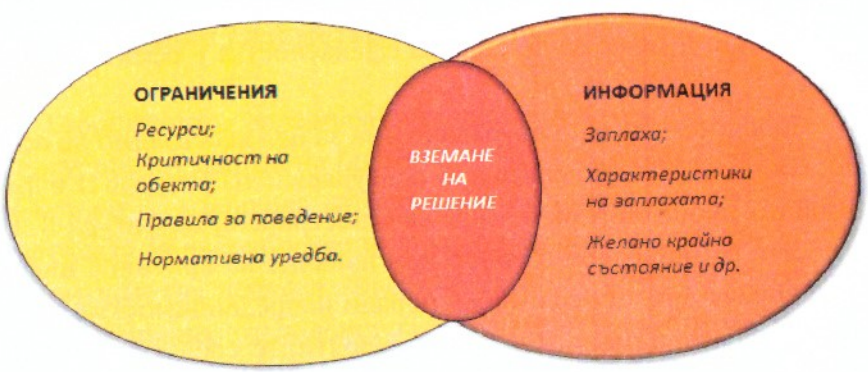
От съществено значение за процесния подход при моделиране на ССЛ е способността ѝ да изпълни задачите си при наличие на критична информация. За целта се въвежда понятието *време за реакция на ССЛ*, което включва продължителността на периода от време от момента на получаване на критичната информация до реализирането на отговор срещу дадена заплаха.

Подсистемата за наблюдение и събиране на данни генерира информация, която активира дейността на следващата подсистема и резултатът от нейното функциониране условно може да се приеме ка-

то входен параметър, определящ дейността на първия функционален модул от подсистемата за ръководство и управление.

При ССЛ тази подсистема е специализиран елемент от системата за ръководство и управление на летищната администрация или летищния оператор. Състои се от компонент за оперативно управление и компонент за административно управление на силите и средствата от ССЛ (фиг. 6). Компонентът за оперативно управление има за цел да осигурява определена последователност на действията от момента на получаване на информацията до момента на вземане на решение за отговор и самия отговор.

В процеса се интегрират текущата информация и характеристиките на заплахата с априорната информация (оперативната база данни), разполагаемия собствен ресурс и неговите способности за отговор, желаното крайно състояние, ограничаващите условия (правилата за използване на сила), регламентиращите документи и др. (фиг. 7). Тази интеграция обединява възможностите на управлението и осигуряването с възможностите на наблюдението и отговора. Непосредствените координация, взаимодействие и комуникация между тези елементи са гаранция за рационалното използване на разполагаемите ресурси.




Фиг. 7. Интеграция на процесите в модула за оперативно управление

Вторият компонент на подсистемата за административно управление е предназначен да допълва цялостния процес по вземане на

адекватно на заплахата решение за отговор и да уведомява системите за сигурност от по-висок ранг.

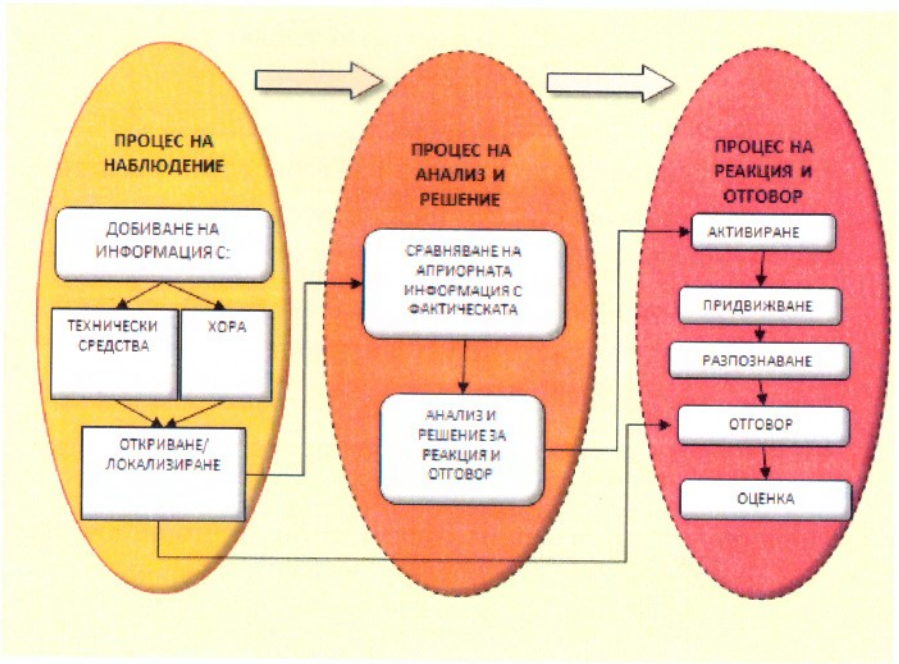
*Подсистемата за реагиране и отговор* извършва решителната фаза и има за цел да осъществи физическата реализация на вече взетото решение за реакция и отговор.

Реакцията и отговорът представляват организирано въздействие от дежурната група върху възникналата заплаха, което цели нейното неутрализиране или минимизиране на нежеланите ефекти/последствия от нея. Дейността на дежурната група за отговор представлява логическа последователност от определени действия, протичащи в условия на неизвестност и дефицит от време. Групирани са в следните етапи:

- активиране на силите;
- придвижване към линията за неутрализиране на заплахата;
- разпознаване/идентифициране на заплахата;
- решение за адекватен на заплахата отговор;
- реализация на взетото решение;
- оценка на резултата от действията.

С резултата, постигнат от подсистемата за реакция и отговор, се оценява пълнотата, правилността и коректността на дейностите, извършвани в останалите подсистеми. Чрез оценка на ефикасността и ефективността ѝ може да се съди за ефикасността и ефективността на цялата ССЛ.

Подсистемата за осигуряване има за цел всестранно да осигури дейността на ССЛ. Процесите при осигуряване на сигурност и защита на външния периметър на летище са илюстрирани на фигура 8. Необходимостта от незабавен отговор при наличие на критична информация все повече придобива смисъл поради непредвидимостта, високата мобилност и миниатюризацията на вероятните средства за осъществяване на терористичен акт, което повишава значимостта на провежданото изследване. От направения анализ на ССЛ ясно проличава, че способностите ѝ основно се генерират от нейния потенциал и се допълват от други компоненти, влизащи в състава на система от по-висок ранг.




Фиг. 8. Последователност на процесите, протичащи по време на защитата на летище

### 4.2. Фактори, влияещи върху сигурността и защитата на външния периметър на летище

Теоретичното определяне на способностите на ССЛ да осигурява сигурност и защита на прилежащите площи при конкретни входни величини се извършва от управленски структури, разположени в подсистемата за ръководство и управление, които се занимават с аналитично-мисловна дейност. Фактическата проверка на качеството на извършения процес от подсистемата за ръководство и управление по оценка на тези способности при конкретни външни условия се осъществява от подсистемата за реакция и отговор. Поради тази причина независимо от подхода и метода за моделиране на целевата стратегия е необходимо да се разграничат съществените от несъществените фактори, влияещи на крайния ефект на действията.

Теоретичното определяне на способностите до голяма степен е творческо-аналитичен процес, върху който влияят следните съществени фактори:

- вид на терористичната заплаха;
- мощност (поразяващо действие) на взривното вещество;
- критичност на обектите от инфраструктурата на летище;
- възможности и характеристики на собствените сили и средства;
- подготвеност на екипите да изпълняват реални задачи;
- оперативност на системата за сигурност на летище:
- време за реакция на системата;
- мобилност (подвижност) на субекта, представляващ терористична заплаха.

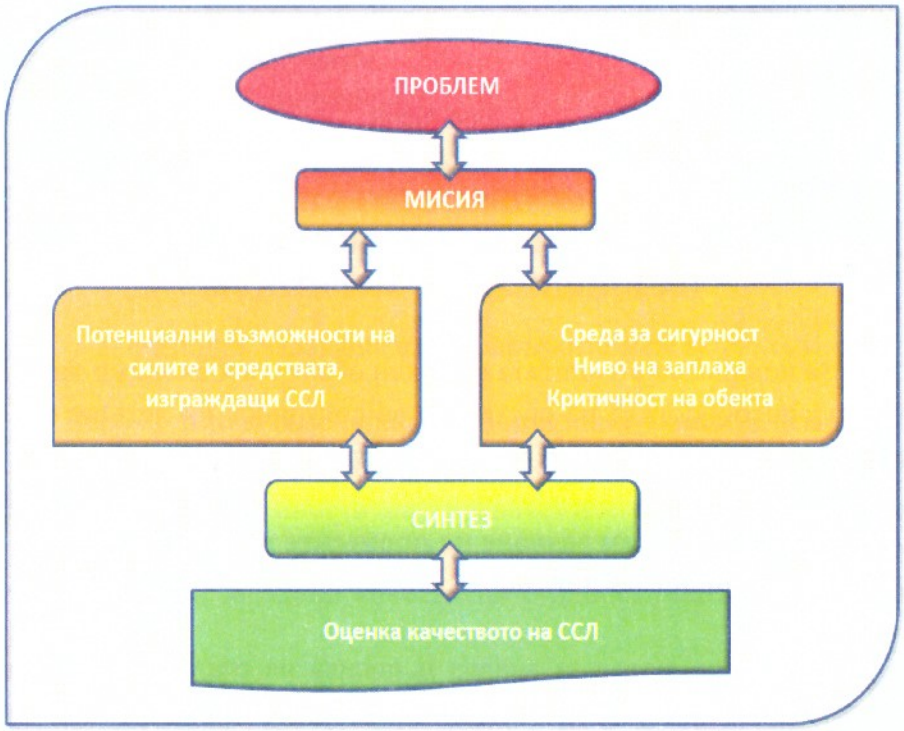
Принципното отчитане на съществените фактори, влияещи на действията на ССЛ при нейното моделиране, схематично е показано на фигура 9. Останалите фактори също оказват влияние върху крайния резултат от действията, но то може да се приеме за несъществено, т.е. влиянието на несъществените фактори върху целевата функция се доближава до единица. (Поради мултипликационния характер на целевата функция това е допустимо.)

В контекста на въведеното допускане и с отчитане на съществените фактори, влияещи на целевото функциониране на системата, е необходимо да се има предвид, че:

– моделът на сигурност и защита, както и целевата функция трябва да се формулират за конкретна задача в конкретни условия на нейното провеждане;

– моделът на сигурност и защита се изгражда на модулен принцип при комбинирано реализиране на двата подхода за декомпозиране на задачата;

– моделът на сигурност и защита и целевата функция е необходимо да са гъвкави и да отчитат динамиката на работа на системата.




Фиг. 9. Последователност на отчитане на съществените фактори, влияещи на действията на ССЛ при тяхното моделиране

След създаване на общия модел се изработват и частни модели за функциониране на модулите и компонентите, изграждащи подсистемите, като се определя спецификата на взаимовръзките между тях и техните елементи. След което се синтезират знания за цялостното функциониране на системата при зададени/дефинирани външни и вътрешни условия и се определят необходимите сили и средства за отговор или се решава обратната задача – при известни налични сили и средства, какви резултати се очакват.

*Глава пета*

# ОЦЕНКА НА СПОСОБНОСТИТЕ НА СИСТЕМАТА ЗА СИГУРНОСТ НА ЛЕТИЩЕ ЗА ЗАЩИТА НА ВЪНШНИЯ МУ ПЕРИМЕТЪР

За повишаване защитата на даден обект е необходимо да се определят способностите на системата за сигурност на летище (ССЛ), изразяващи се чрез връзката *мисия – задачи – необходими способности.*

## 5.1. Метод за изследване на процесите в системата за сигурност на летище

Подходящ метод за анализ и оценка на реално протичащите процеси и явления в ССЛ е математическото моделиране[12], чрез който с помощта на специално създаден модел се отразяват присъщите ѝ характеристики с достатъчна за практиката точност. Чрез математическия модел се получава строга, съдържателна и логически непротиворечива постановка на задачата.

Процесът на моделиране се нарича още *формализация на задачата*[13] и в общия случай е от типа:

$$F_{\max} = f(x, y), \tag{1}$$

при ограничения:

$$g_i(x, y) \le b_i, i = \overline{1, m},$$

---

[12] *Моделирането е метод за изучаване на различни процеси и явления.*

[13] *Формализацията на реален процес предполага изучаване на структурата на съставляващите го явления. В резултат се получава съдържателно описание на процеса, което представлява излагане на закономерностите, характерни за него, и постановка на дадената задача.*

където $F = f(x, y)$ е целева функция, описваща качеството на функциониране на системата;

$x$ – вектор на променливи, подлежащи на управление;

$y$ – вектор на постоянни или променливи, неподлежащи на управление;

$g_i$ – функция на необходимите $i$-ти способности;

$b_i$ – стойност на наличните $i$-ти способности;

$f$ – функция, задаваща взаимовръзките между $F, x, y$.

Необходимо е да се опишат условията и границите, в които могат да се изменят променливите величини. По определен алгоритъм се търсят наличните стойности на управляемите променливи или тези техни значения, които осигуряват най-добри показатели на изследваната система при зададени константни стойности на неуправляемите променливи.

Ако процесите, протичащи в ССЛ, бъдат разгледани от гледна точка на теоретикомножествения подход, то тя може да се представи като множество, обединяващо подмножествата на входните въздействия и на изходните реакции на системата, и да се изрази с отношението:

$$S \subset X_{вх} \times U_{изх}, \tag{2}$$

където $S$ е системата за сигурност на летище;

$X_{вх}$ – подмножество на входните въздействия;

$U_{изх}$ – подмножество на изходните реакции на системата.

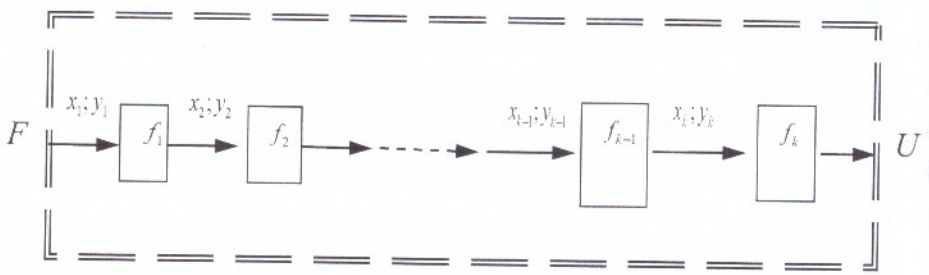
За коректно прилагане на този подход е необходимо въвеждане на ограничение, определящо способността на системата да реагира на всяко входно въздействие със съответна реакция.

*Целевата стратегия* се дефинира като „система от последователно и едновременно изпълнявани задачи", поради което е целесъобразно да се формулират два подхода при декомпозицията на общата задача:

- по етапи на действията, т.е. последователно изпълнявани задачи;

• по направление на усилията – паралелни действия или едновременно изпълнявани задачи.

За тяхното онагледяване е подходящо модулното им представяне. При декомпозиция на задачите по етапи целевата функция ( $F$ ) на системата за конкретна операция може да се представи модулно, като $k$ е броят на етапите и всеки етап се дефинира съответно от функциите $f_1 = f_{(x_1;y_1)}; f_2 = f_{(x_2;y_2)}; f_k = f_{(x_k;y_k)}$, където $x$ и $y$ са съответните входни въздействия в дадения модул, а $U$ е изходният резултат от дейността на цялата система (фиг. 10).




Фиг. 10. Модулно представяне на целевата функция при декомпозиране по етапи на действията

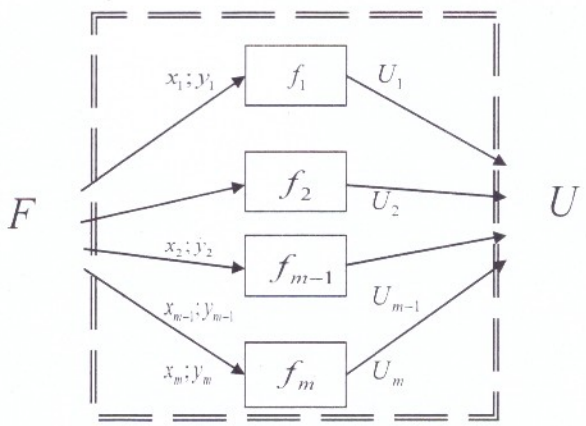
Основните предимствата при представяне на целевата функция по този начин са:

• добро онагледяване на действията чрез обвързване на етапите от дейността на системата с реалната действителност;

• удобство за работа при вероятностен характер на функциите.

Като недостатък може да се отчете, че допуснатите грешки в който и да е от етапите се „акумулират" в крайния резултат.

Декомпозирането на целевата функция на ССЛ по направления на усилията или едновременно изпълнявани задачи е представено във фигура 11, където $m$ е броят на направленията.




Фиг. 11. Модулно представяне на целевата функция при декомпозиране по направления на действията

При този подход значително по-трудно се представя целевата функция, но при него са налице следните предимства:

- дава реална представа за ред системни свойства, като сложност, взаимодействие, взаимозависимост и др.;
- онагледява участието на конкретни подсистеми за постигането на основната цел;
- в процеса на управление системата дава възможност за гъвкаво реагиране на всяка промяна в обстановката.

Недостатък на подхода е трудното проследяване на логическата последователност на действията. При конкретната декомпозиция се прилага комбиниран подход, тъй като задачите се изпълняват както по етапи и направления в даден етап, така и паралелно в едно направление. Това е от съществено значение при изследване взаимодействието между тях в цялостния процес при различна степен на застъпване във времето.

### 5.2. Определяне на критерии за качество на системата за сигурност на летище

Системата за сигурност на летище е система с целенасочено действие, която не може да се разглежда извън средата, в която функ-

ционира. За да реализира своята целева стратегия, е необходимо да притежава определени способности. Те се дефинират като качество на системата за пригодността ѝ да реализира целевата си стратегия, което количествено измерение се осъществява чрез *критерии за качеството* на системата при нейното функциониране.

Оценката по даден критерий е конкретна числена величина, наречена *показател за качество*, или показателят е числената стойност (мярката) на критерия за качеството на системата. Показателят зависи от структурата на системата, характера на връзките между елементите в нея, вида на управляващите алгоритми и закономерностите на функционирането ѝ.

Оценката на пригодността на системата да реализира целевата си стратегия, т.е. ССЛ да допринася за сигурността и защитата на външния периметър на летище, се осъществява по многокомпонентен критерий за качество, който в теорията на системите е дефиниран като *обобщен критерий за качество*.

Съставните на *обобщения критерий за качество* се наричат частни критерии за качество и служат за оценка на качеството на компонентите при последваща декомпозиция на задачата. Рационално подбраните критерии позволяват да се формулират постижими цели и изпълними задачи при отчитане средата на функциониране на системата.

За оценка на способността на ССЛ да изпълнява целевата си стратегия най-подходящи частни критерии са:

- *Резултатност* (ефикасност) – степен на достигане на целевия ефект.
- *Ресурсоемкост* (ефективност) – разход на ресурси (без времевия) за достигане на целевия ефект.
- *Оперативност* – времето, необходимо на системата да постигне целта си.

Количественo критерият *оперативност* се определя от показател за оперативност, отразяващ времето, необходимо за незабавен от-

говор, и разполагаемото време за реакция, зависещо от подвижността[14] на обектите/субектите, представляващи терористична заплаха.

След направените съдържателно описание и анализ на процесите, свързани със защитата и охраната на летище, и определяне на критериите за тяхната оценка основни моменти по-нататък са построяването на формализована схема на цялостния процес и разработването на математически модел[15] за него.

Математическият модел дава възможност да се определят числените стойности на критериите за качество, като по този начин се получи необходимата информация за определяне/прогнозиране на необходимите способности на ССЛ за изпълнение на задачата по сигурност и защита на външния периметър на летище. В обобщен вид на фигура 12 е показан процесът на изследване при преминаване през фазите *анализ*, *синтез*, *оценка и сравняване на резултатите*.


Фиг. 12. Процес на изследване на дейностите на ССЛ

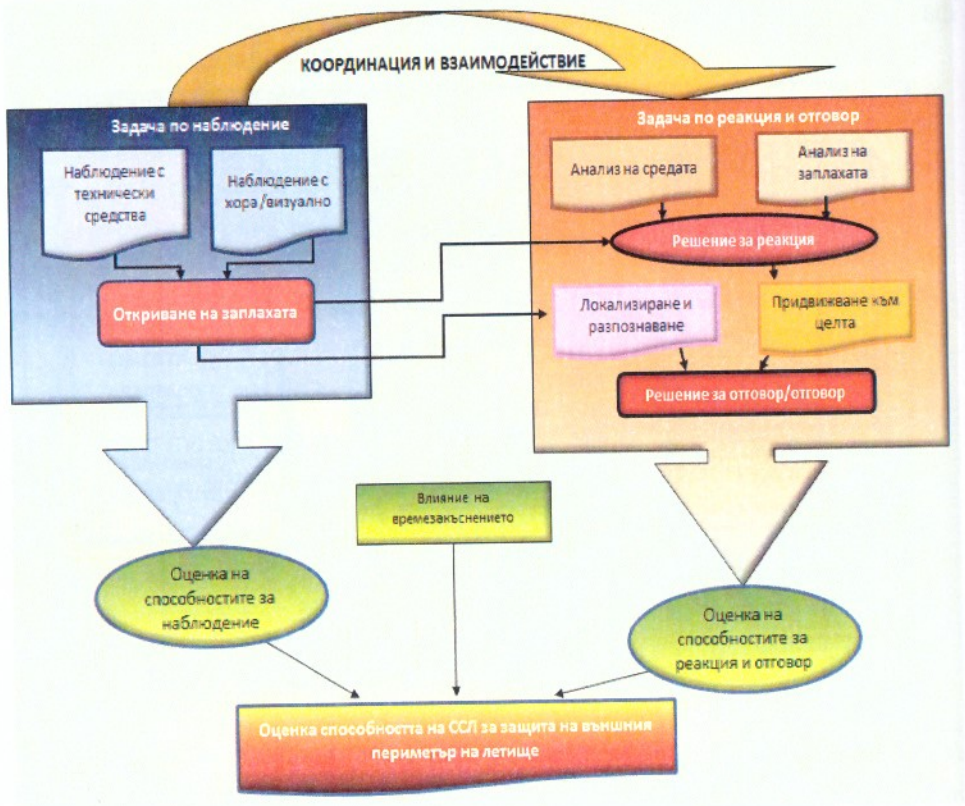
---

[14] *За подвижност на обектите виж точка 5.4. Оценка на способностите на системата за защита на летище за реакция.*

[15] *Математически модел на реална система е съвкупност от съотношения (формули, уравнения, неравенства, логически условия), които определят характеристиките на състоянието на системата в зависимост от нейните параметри, входни сигнали, начални условия и време.*

За постигане целта на изследването общата задача се декомпозира на частни задачи и подзадачи, чрез които се отчитат съществените фактори, влияещи на резултата при неговото моделиране. Последователността на тяхното решаване съвпада с последователността на дейностите, провеждани от ССЛ, и схематично е представена на фигура 13. Поради неопределеността на събитията, при които функционира ССЛ, характеризиращи критериите за качество на процесите, извършвани в системата, се разглеждат вероятностните показатели.

Оценката на способностите на ССЛ за сигурност и защита на външния периметър на летище се осъществява чрез решаване на задачите по наблюдение и отговор и чрез обвързване на техния резултат с времето за реакция в цялостния процес.




Фиг. 13. Последователност на решаваните частни задачи при оценка способностите на ССЛ за сигурност и защита на външния периметър на летище

### 5.3. Оценка на способностите на системата за сигурност на летище за наблюдение

Средствата за наблюдение като активни средства за добиване на информация участват в цялостния процес чрез събиране на данни за средата, в която функционират, като паралелно с това са и компонент от подсистемата на активните средства на системата за сигурност на летище.

За ефективни и ефикасни реакция и отговор решаващо значение имат актуалността, своевременността, достоверността и пълнотата на доставената информация, както и точността на определяне на координатите на вероятната заплаха. Поради тези причини необходимостта от водене на непрекъснато наблюдение е ключова за качеството на процесите по сигурност и защита на летище.

Според начина на добиване на информация се различават следните способи за наблюдение:

- визуално;
- с използване на технически средства:
- оптическо;
- оптико-електронно (чрез средства, използващи за добиване и предаване на информацията оптическия диапазон от електромагнитния спектър, а за преобразуване на информацията – различни електронни устройства);

➢ телевизионни прибори и системи от „клас II“ (*Image Intensification*);

➢ термовизионни прибори и системи от „клас TI“ (*Thermal Intensification*);

- фоторазузнаване;
- акустично;
- сеизмично;
- радарно/радиолокационно.

За да бъде дефиниран един обект като заплаха или не, се преминава през следните етапи:

- търсене;

- откриване;
- опознаване;
- определяне на координатите му.

Под понятието *търсене* се разбира процес на целенасочено обследване на определена област от пространството (местността) с цел откриване на намиращ се в нея обект.

Получаването на информация за мястото на обекта чрез установяване на енергетичен контакт с него се нарича *откриване*. Откриването е свързано с определяне координатите на обекта (локализиране).

*Опознаването* (идентифицирането) на обекта е процес на целенасочено определяне на неговите количествени и качествени характеристики и сравняването им с априорно зададени такива.

*Далечина на откриване на обекта* ($D_{откр}$) е пределното разстояние, при което той се открива. Детайлите му може да не се наблюдават.

*Далечина на опознаване на обекта* ($D_{оп}$) е пределното разстояние, при което обектът се опознава детайлно.

Под *обект терористична заплаха* следва да се разбира съвкупност от съществуващи самостоятелно или организационно и функционално свързани материални единици, разположени на ограничена територия, които притежават определен потенциал и представляват заплаха за сигурността.

Ключов елемент за успеха на наблюдението е откриването на обекта. Вероятността за откриване на даден обект в най-голяма степен зависи от далечината на неговото откриване, тъй като от теорията на търсенето е известно, че вероятността за откриване на обект от техническо средство $P_{тс.откр}$ се дефинира с уравнението:

$$P_{тс.откр} = 1 - e^{-\frac{L_{набл.} D_{откр.}}{S_{набл.}}}, \qquad (3)$$

където $L_{набл}$ е ширина на полосата, обследвана от техническото средство;

$D_{откр}$ – далечината на откриване;

$S_{набл}$ – площ на района за наблюдение.

Според принципа на работа основните типове технически средства за разузнаване са *оптически, телевизионни, термовизионни, радарни и др.* За нуждите на точното определяне на координатите се използват и *лазерни системи.*

Далечината на откриване се дефинира за различните типове сензори със следните зависимости:

• За лазерни системи:

$$D_{лс} = \sqrt[4]{\frac{P_{изл} S_{пр} \sigma_{ц}}{\pi \theta^2_{пр} P_{ф} q}} e^{-0.5 \mu l}, \qquad (4)$$

където $P_{изл}$ е мощността на излъчвателя, $W$;

$S_{пр}$ – площ на приемната апертура, $m^2$;

$\sigma_{ц}$ – ефективна отразяваща повърхност на целта, $m^2$;

$\theta_{пр}$ – ширина на диаграмата на насоченост на оптичната система, $rad$;

$P_{ф}$ – мощност на излъчването на фона, $W$;

$q$ – параметър на откриване;

$\mu$ – коефициент на отслабване на излъчването в атмосферата, $dB/km$;

$l$ – разстояние, изминато от лъча в плътните слоеве на атмосферата, $km$.

• За термовизионни (пасивни инфрачервени) системи:

$$D_{ич} = \sqrt{\frac{J_{чт} \varepsilon S_{ц}}{\pi \theta_{\lambda} w_{пр} q}} e^{-0.5 \mu l}, \qquad (5)$$

където $\varepsilon$ е спектрален коефициент на излъчването ($\varepsilon \approx 0{,}7$ за никелова сплав, при максимално излъчване);

$S_{ц}$ – площ на проекцията на целта, $m^2$;

$\theta_\lambda$ – спектрална плътност на излъчването на фона, $W/s\,m^2\,sterad$;

$w_{пр}$ – ъгъл на полезрение на приемника, *sterad*;

$q$ – безразмерно отношение на енергията $E$ на полезния сигнал към спектралната плътонст $N_0$ на смущенията:

$$q = \frac{2E}{N_0}, \tag{6}$$

$J_{чт}$ – интензивност на излъчването на абсолютно черно тяло:

$$J_{чт} = \frac{c_1}{\lambda^5} \cdot \frac{1}{e^{\frac{c_2}{\lambda . T}} - 1}, \tag{7}$$

където $c_1 = 3{,}74.10^{-12} W / sm^2$;

$c_2 = 1{,}4 sm.K$;

$T$ – абсолютната температура на нагрятото тяло, $K$.

• За телевизионните системи:

$$D_{TB} = \sqrt{\frac{B_\lambda S_ц r_ц S_{пр} \Delta\lambda}{\pi P_ф q}} e^{-0.5\mu l}, \tag{8}$$

където $B_\lambda$ е спектралната плътност на излъчването от повърхността на целта;

$S_ц$ – в следствие осветеността ѝ от слънцето;

$r_ц$ – коефициент на отразяване от целта;

$P_ф$ – мощност на излъчването на фона, $W$;

$q$ – параметър на откриването.

Посочените стандартни параметри в изброените формули имат следните значения:

$P_{ф} = 10^{-17} W$ ;

q = 2-3;

$B_{\lambda} = 10^{-2} W/(sm^2.sterad)$ ;

$r_{ц} = 0{,}2\text{-}0{,}8$;

$\theta_{\lambda} = 3.10^{-2} W/(sm^2.sterad)$ – за дневно небе;

$\theta_{\lambda} = 3.10^{-8} W/(sm^2.sterad)$ – за нощно небе.

• За радиолокационни средства:

$$D_{рлс} = \sqrt[4]{\frac{P_{и} G_0^{\ 2} \lambda^2 \sigma_{ц}}{(4\pi)^3 P_{пр} q K}} 10^{-0{,}005\mu l}, \qquad (9)$$

където $P_{и}$ е импулсна мощност на РЛС, $W$;

$G_0$ – коефициент на усилване на антената;

$\sigma_{ц}$ – ефективна отразяваща повърхност на целта, $m^2$ ;

$\lambda$ – дължина на вълната;

$P_{пр}$ – чувствителност на приемника;

$K$ – коефициент на загубите ≈ 3.14;

$q$ – параметър на откриване.

За да бъде надеждно открит обект, представляващ заплаха, е необходимо да се определят най-целесъобразните средства, които осигуряват откриването му за минимално време при зададени условия.

Като се използва формула 3 и се знаят характеристиките на техническите средства за наблюдение при зададен район за наблюдение, се определя необходимият им брой. Чрез решаване на тази задача се определя способността на ССЛ за наблюдение. Следващият етап в процеса на математическото моделиране е решаване на задачата за реакция и отговор.

## 5.4. Оценка на способностите на системата за сигурност на летище за реакция

За пълна оценка на способностите на ССЛ е необходимо да се определи и влиянието на времето, необходимо за реакцията ѝ като функция от мобилността на заплахата.

При класификация на терористичните заплахи се използват различни критерии, повечето от които имат физически измерения и влияят на възможностите на средствата за наблюдение.

По критерия *подвижност* обектите се подразделят на: стационарни и мобилни. Стационарните обекти са неподвижни спрямо земната повърхност и продължителността на времето от момента на откриването им до тяхното неутрализиране не влияе върху крайния резултат. Мобилните обекти, каквито обикновено представляват терористичните заплахи по своята същност, могат да бъдат *подвижни* и *движещи* се.

*Подвижността на обектите* е една от основните характеристики, определящи способностите на ССЛ за тяхното откриване и своевременно неутрализиране. Измерва се със сумарното време $t_n$ и се определя с израза:

$$t_n = t_0 + t_{ср} + t_м, \qquad (10)$$

където $t_0$ е времето, необходимо за заемане на изгодна позиция за терористична атака;

$t_{ср}$ – средно време за подготовка за извършване на терористичния акт (обектът се намира в стационарно положение);

$t_м$ – време, необходимо за напускане на района на въздействие на заплахата (ако има такова).

Тези времена зависят от тактико-техническите характеристики на обектите, както и от тактиката на тяхното използване.

Една от основните задачи на ССЛ е да неутрализира заплахата или да минимизира последствията от нея. От съществено значение за успеха при изпълнението на тази задача е времето за реакция на ССЛ, а именно способността на системата да реагира при наличие на заплаха. За изчисляване и определяне на влиянието на времето за реакция на системата върху ефикасността на изпълнената задача се използват следните зависимости:

$$P_{НЗ}(t) = 1; \qquad 0 < t_p \le t_0, \tag{11}$$

$$P_{НЗ}(t) = e^{-\frac{3(t_p - t_0)}{t_{ср} + t_м}}; \qquad t_p > t_0, \tag{12}$$

където $P_{НЗ}(t)$ е вероятността за неутрализиране на заплахата в зависимост от времето за реакция;

$t_p$ – период от време за реакция: сумарното време за анализ и решение, активиране на силите за отговор и тяхното придвижване до ЛНЗ – $t_p = t_{реш} + t_{лнз}$;

$t_{лнз}$ – период от време от момента на откриване на заплахата до пристигане на дежурната група на линията за неутрализиране на заплахата (ЛНЗ).

С цел визуализация на пространствените параметри, имащи отношение към времето за реакция на ССЛ, са дефинирани следните понятията (фиг. 14):

• *Линия за неутрализиране на заплахата (ЛНЗ)* – мислена линия, до която силите за реакция и отговор на ССЛ трябва да осъществят физически контакт с обекта вероятна заплаха.

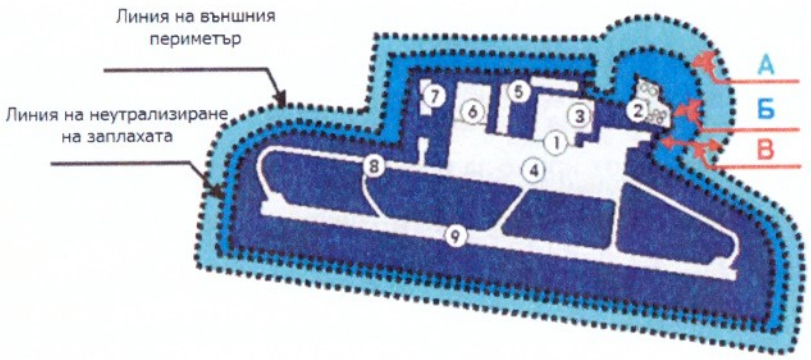
• *Линия на външния периметър на летището (ЛВП)* – мислена линия, до която подсистемата за наблюдение трябва да е открила заплахата (обекта), така че ССЛ да е в състояние да реагира на ЛНЗ.

• *Зона за реакция на системата за сигурност* – заключена между линията за неутрализиране на заплахата и линията на външния

периметър на летището. Размерите ѝ се определят от критичността на обектите и мобилността на терористичната заплаха.

• *Зона за сигурност във външния периметър на летище* – заключена между линията на вътрешния периметър на летището и линията за неутрализиране на заплахата. Размерите ѝ се определят от критичността на обектите и разрушаващите способности на заплахата.

• *Зона на външния периметър на летище* – зона, в границите на която системата за сигурност на летището трябва да е в състояние да открие, реагира и неутрализира потенциална терористична заплаха или да минимизира последствията от нея.




**А** – зона за реакция на системата за сигурност на летище
**Б** – зона за сигурност на външния периметър
**В** – зона на външния периметър на летище

Фиг. 14. Зона за сигурност и защита
на външния периметър на летище
*1) контролна кула; 2) склад за ГСМ; 3) пътнически терминал; 4) перон; 5) административни сгради; 6) база за ремонти; 7) електрическа подстанция; 8) пътеки за рулиране; 9) полоса за излитане и кацане*

## 5.5. Оценка на способностите на системата за сигурност на летище за отговор

Реакцията, респективно отговорът, при защитата и охраната на прилежащия периметър на летище са породени от необходимостта от непосредствено действие при наличие на критична информация. Реакцията и отговорът имат за цел предотвратяване или минимизиране на последствията от даден вид терористична заплаха за сигурността на летището.

Етапите след активиране на дежурните сили и средства са разгледани подробно при анализа на подсистема за реакция и отговор, откъдето може да се направи изводът, че заплахата първо трябва да бъде „намерена" и след това да се извършат необходимите действия. Като количествен показател за определяне на критерия *ефикасност* на подсистемата за реакция и отговор може да се разглежда вероятността за изпълнение на задачата от дежурните сили и средства $W_з$, която се дефинира с формулата:

$$W_з = Q_{дост} W_{откр}, \qquad (13)$$

където $Q_{дост}$ е вероятността силите за отговор да достигнат до заплахата;

$W_{откр}$ – вероятност заплахата да бъде открита от силите за отговор.

Като се има предвид, че дежурната група за отговор поддържа необходимите оборудване и възможности, вероятността силите за отговор да достигнат до заплахата за определено време след нейното откриване от подсистемата за наблюдение може да се приеме за равна на единица.

Процесът на откриване на заплахата е съпоставим с процеса на наблюдение, като за необорудвани с технически средства сили визуалното откриване остава единственият способ. Далечината за визуален контакт с обекта е ключова за неговото откриване, като тя основ-

но зависи от неговата контрастност, от индивидуалните умения на специалистите и други фактори. С достатъчна за практиката точност за определяне вероятността за откриване на заплахата от силите и средствата за реакция е приложим изразът:

$$W_{откр} = 1 - e^{\frac{nat}{kF}}, \qquad (14)$$

където $n$ е броят на хората, търсещи обекта (заплахата);

$F$ – площ на района за търсене, $m^2$;

$a$ – единична площ наблюдавана за единица време, $m^2/sec$;

$к$ – коефициент, показващ каква част от площта може да бъде използвана за разполагане на заплахата;

$t$ – разполагаемо време в *sec*.

При способа на визуалното откриване се използват възможностите за следене на заплахата от подсистемата за наблюдение и предаване на информация в реално време на заинтересованите (силите за реакция и отговор).

Като се има предвид състоянието на съвременните средства за наблюдение и комуникация, може да се приеме, че откриването на заплахата от силите за реакция е практически достоверно събитие, когато тя е явна, т.е. не е маскирана.

*Глава шеста*

# АЛГОРИТЪМ ЗА РАБОТА ПРИ ОПРЕДЕЛЯНЕ НА ЗОНИТЕ ВЪВ ВЪНШНИЯ ПЕРИМЕТЪР НА ЛЕТИЩЕ

Заради спецификата на необходимите познания, които трябва да притежава персоналът, занимаващ се с аналитично-мисловна дейност в оперативните звена на системата за сигурност на летище и субективния фактор, влияещ на процесите при формиране и вземане на решения, се поражда необходимост от наличие на обективен модел за оценка на способностите на ССЛ да извършва определени дейности (да постига желан краен резултат) при дефинирани външни условия. За това е целесъобразно да се предложи примерен алгоритъм за прилагане на разгледания модел за оценка на способностите на ССЛ за сигурност и защита на външния периметър на летище.

От разгледаните основни фактори, които оказват съществено влияние върху способностите на ССЛ, се открояват количествените и качествените характеристики на средствата за добиване на информация, времето за анализ и вземане на решение от оперативните дежурни и готовността на силите и средствата за реакция и отговор. Всички те трябва да бъдат обвързани в определен алгоритъм, който дава реална представа за способностите на ССЛ да гарантира сигурността и защитата на летище от терористична заплаха.

За решаването на конкретните задачи е необходимо определянето на редица входни параметри и данни. Основните от тях са:

- определяне на линията на вътрешния периметър на летището;
- видове, възможности, количество и тактико-технически характеристики на средствата за наблюдение (сензори, датчици и др.);
- видът на терористичната заплаха;
- времето за вземане на решение и активиране на силите за реакция и отговор;
- времето за придвижване на силите за реакция и отговор;

- скоростта на движение на потенциалната заплаха;
- разрушаващи способности на заплахата;
- критичност на разглеждания обект от инфраструктурата на летище и др.

### 6.1. Описание на задачата и предлагане на алгоритъм за оценка на способностите за наблюдение

При решаването на тази задача се извършва фактическа оценка на способността на подсистемата за наблюдение при определен наличен ресурс. При конкретни условия на водене на наблюдението физическото описание на задачата може да се сведе до: обследване на район с площ $S_{раз}$, за откриване на обект от категория $k_j$ (Трета глава – табл. 2), за периода от време $t_T$, със зададена вероятност $P_{откр.зад}$, при конкретни тактико-технически характеристики на $i$-тото техническо средство за наблюдение и параметри, характеризиращи $j$-тия тип обект (терористична заплаха).

За решаването на задачата е необходимо да са известни:

- определени физикогеографски, геоинформационни и метеорологични особености и условия на района за наблюдение, частта от денонощието и др.;
- параметри на обекта терористична заплаха;
- очаквана степен на „маскировка" на обекта;
- степента на подготвеност на екипите да оперират със средствата за наблюдение и др.

В зависимост от основните характеристики на обекта терористична заплаха, метеорологичните условия и частта от денонощието се избира подходящо техническо средство за добиване на информацията чрез определяне на максималната вероятност за контакт на различните видове технически средства.

Математическото описание на задачата се базира на израза (1) $F_{\max} = f(x, y)$, чрез който се определя целевата функция $F$, чийто максимум отговаря на способността на подсистемата за наблюдение. Векторът на променливите величини, подлежащи на управление – $x$, се определя от значенията и характеристиките на $i$-тото техническо

средство за наблюдение, а векторът на постоянните или променливите, неподлежащи на управление, се определя от характеристиките на $j$-тия обект и параметрите на средата, в която оперират средствата за добиване на информация. Показателят за качество на наблюдението се определя от вероятността за откриване на обекта $P_{откр} = f(x_i, y_j)$, като при зададени условия (неподлежащи на управление) $y_j (j = 1, m)$ е необходимо да се намерят такива стойности на управляемите променливи $x_i (i = 1, n)$, при които:

$$F = \max P_{откр} = f_{\max}(x_i, y_j). \qquad (15)$$

При това алгоритъмът за оценка на способността на ССЛ за наблюдение преминава последователно през:

- етап на намиране на рационално средство за наблюдение на дадена категория обект;
- етап на определяне количеството необходими средства за наблюдение от този тип и протича в следната последователност (фиг. 15):

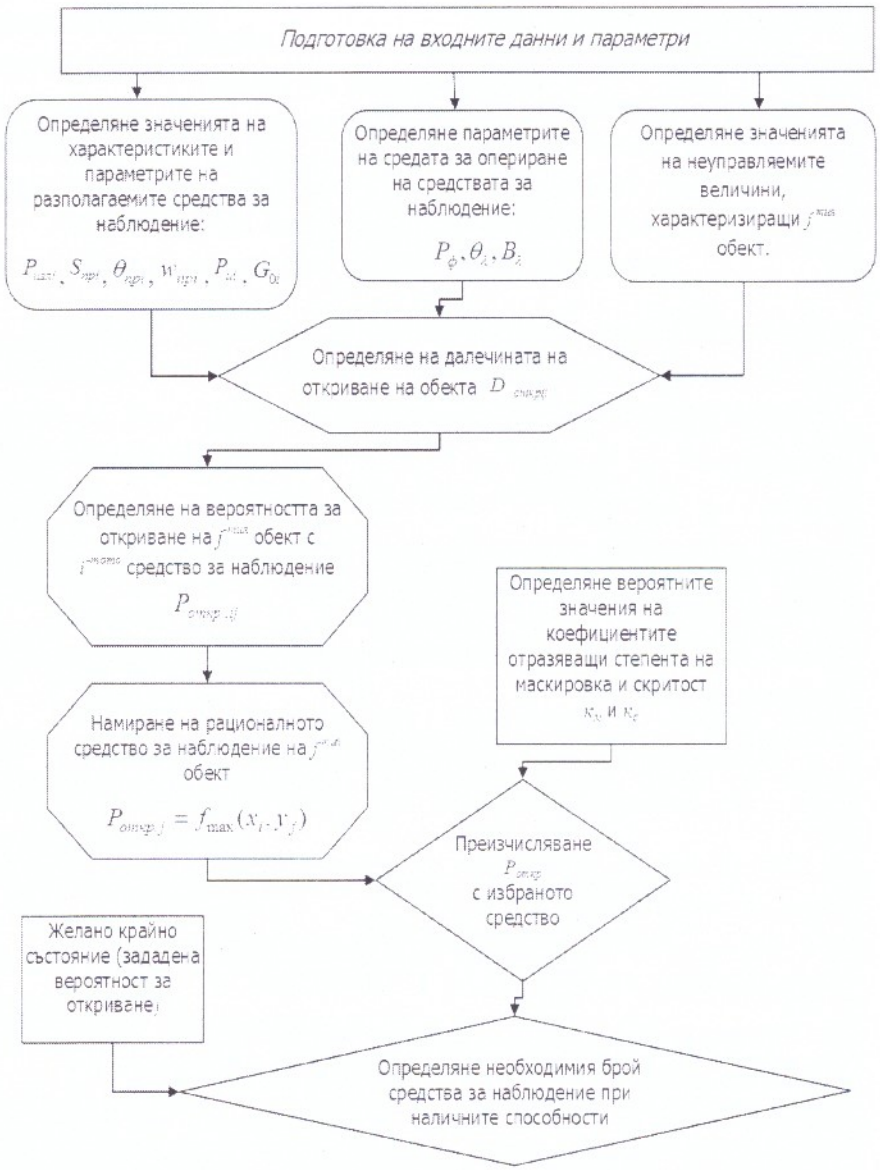
1. Определят се значенията на неуправляемите величини, характеризиращи $j$-тия обект.

2. Определят се параметрите на средата за опериране на средствата за наблюдение.

3. Определят се значенията на характеристиките и параметрите на разполагаемото $i$-то техническо средство за наблюдение.

4. Изчислява се разстоянието до далечината на откриване $D_{откр}$, (респективно ширината на обследваната полоса) на $j$-тия обект от $i$-тото техническо средство.

5. Определя се вероятността за откриване на $j$-тия обект от $i$-тото средство при липса на „маскировка“ от страна на заплахата, като там, където значението ѝ има максимална стойност, се намира най-изгодното средство за наблюдение при тези условия на външната среда.



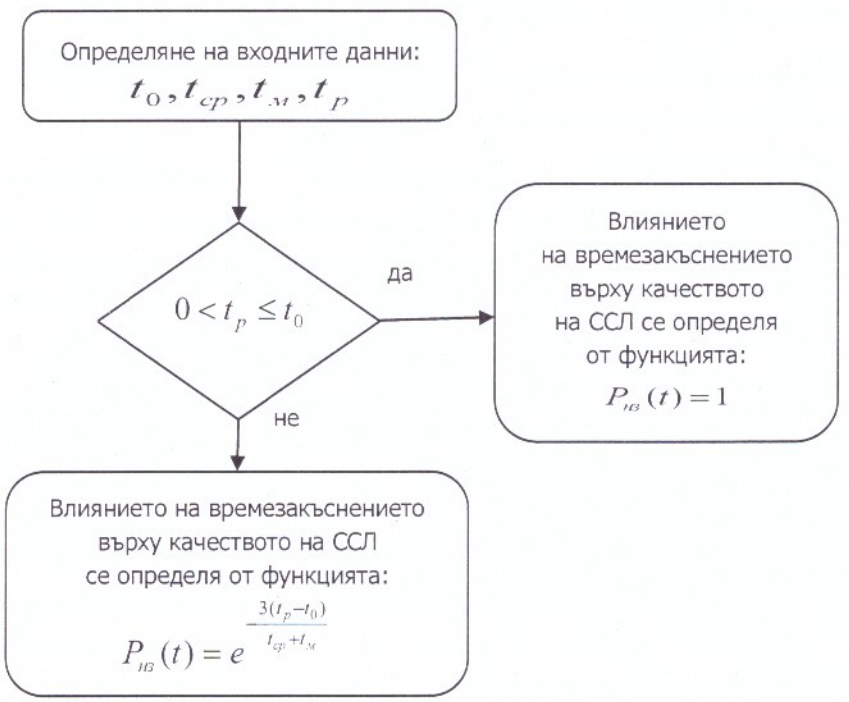

Фиг. 15. Алгоритъм за определяне на способността за наблюдение

6. При наличие на дезинформация от страна на заплахата се определят стойностите на коефициентите, отчитащи очакваните степени на маскировка на $j$-тия обект $\kappa_M$, $\kappa_C$.

7. Определя се необходимият брой средства за наблюдение, които при наличните способности биха открили *j*-тия обект с желаната вероятност.

### 6.2. Алгоритъм за определяне на вероятността за откриване на обект терористична заплаха от силите за реакция и отговор

За да се определи влиянието на времето за реакция и подвижността на обекта върху способността на ССЛ да постига дадените цели, е необходимо да се определи вероятността за откриване на обект $(P_{(t)})$ от групата за реакция и отговор като функция, отчитаща зависимостта между разполагаемото време на групата и подвижността на обекта терористична заплаха $(P_{(t)} = f(t_p, t_n))$. Редът за решаване на задачата протича в следната последователност (фиг. 16):




Фиг. 16. Алгоритъм за определяне вероятността за откриване на обекта от силите за отговор в зависимост от подвижността му и времето за реакция

1. Определя се типът на обекта по критерия *подвижност* и на базата на априорна информация за него се определят времената, характеризиращи неговата подвижност.

2. Определя се времето за реакция на ССЛ – $t_p$.

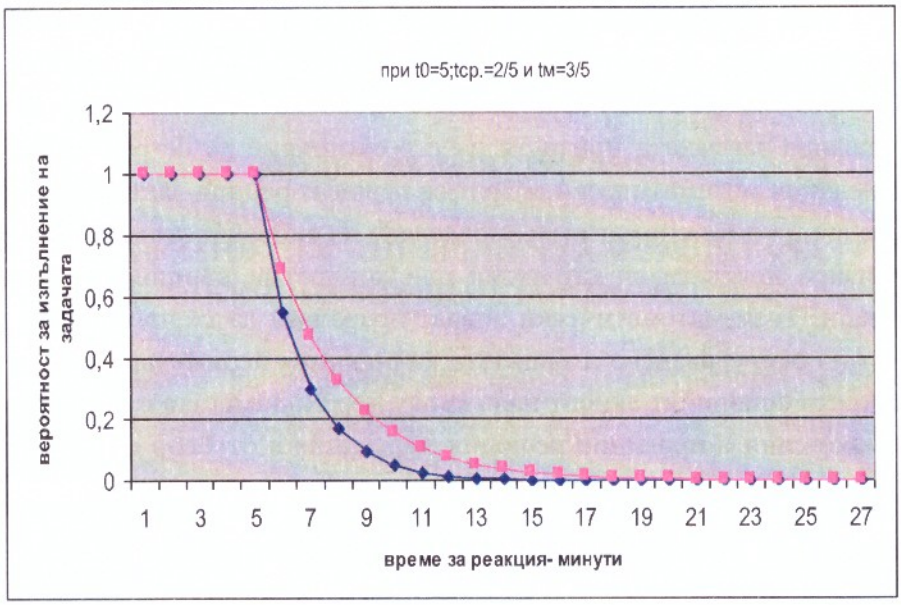
3. Проверява се условието $0 < t_p \leq t_0$ и се определя $P_{(t)}$.

### 6.3. Изследване на влиянието на времето за реакция на системата за сигурност и мобилността на обекта върху ефикасността и ефективността на защитата на летище

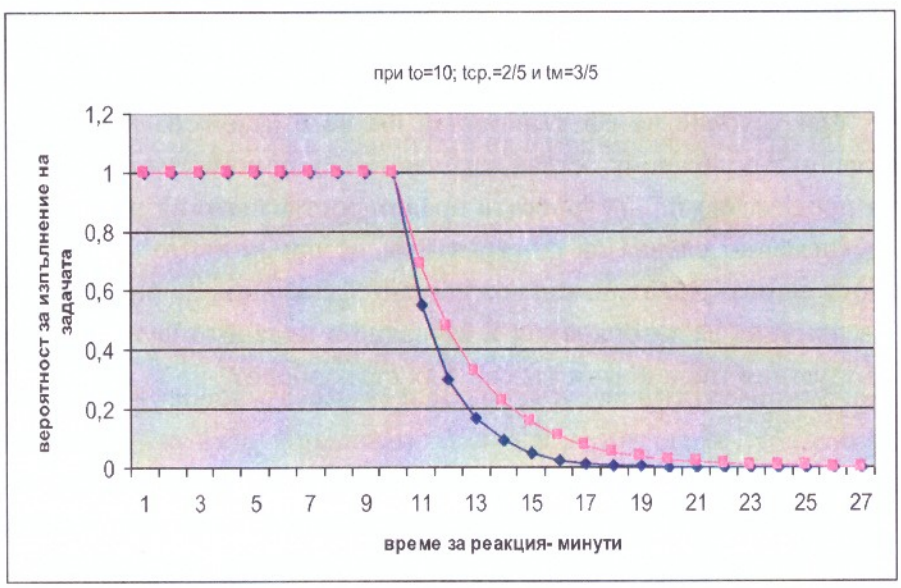
След определяне на вероятността за откриване на обекта от групата за реакция и отговор на вече разкрита позиция от подсистемата за наблюдение, израз (13) придобива вида:

$$W_з = Q_{оост} W_{откр} P_{(t)}. \tag{16}$$

Използвайки израз (12), се отчита влиянието на времето за реакция и мобилността на обекта на заплахата върху способността на подсистемата за реакция и отговор да изпълни своето предназначение. При пресмятане на тези зависимости с конкретни стойности на величините се получава резултат, графически показан на фигура 17 и 18. При анализа на резултата се вижда, че когато ССЛ е в състояние да реагира по-бързо от времето за достигане на заплахата до ЛНЗ, то практически времето за реакция на системата не оказва влияние върху резултатността (постига се чрез прилагане на способа „изнесени средства за наблюдение"). Същевременно се вижда и влиянието на подвижността на обекта терористична заплаха (при $t_0$ – 5 мин. (фиг. 17) и $t_0$ – 10 мин. (фиг. 18); $t_{ср}$ – 2/5 мин.; $t_м$ – 3/5 мин.) и времето за реакция на ССЛ върху ефикасността за неутрализиране на заплахата.




Фиг. 17. Вероятност за неутрализиране на заплахата в зависимост от времето за реакция на системата (Вариант 1)




Фиг. 18. Вероятност за неутрализиране на заплахата в зависимост от времето за реакция на системата (Вариант 2)

Така получените зависимости се мултиплицират с вероятността за откриване на заплахата и вероятността за отговор и реакция на ССЛ, чрез което се получава крайната способност на системата да неутрализира заплахата преди тя да е в състояние да се реализира. С разгледания математически апарат се решават редица частни задачи и подзадачи, които спомагат за определяне на способностите на ССЛ да реализира целевата си стратегия при конкретни външни условия и фактори. Този математически апарат позволява да се прогнозира успехът на осигуряването и защитата на външния периметър на летище, при което основният акцент пада върху необходимостта от вземане на своевременни и правилни решения за реакция и отговор при наличие на критична информация.

Предложеният модел позволява за кратко време и гъвкаво да се извършва комплексна количествено-качествена оценка на способностите за наблюдение и отговор на ССЛ, както и да се отчита влиянието върху тези способности на времето за реакция в цикъла „Откриване – Отговор".

Мерките и процедурите за сигурност следва да бъдат прилагани по такъв начин, че да предизвикват минимум намеса, задържане или нарушение на нормалната дейност на гражданското въздухоплаване, при условие че ефективността им не е изложена на опасност. При всички положения остава жизненоважен приоритетът да бъде даден предимство на сигурността пред опростяването на процедурите. Същевременно следва да се гарантира, че прилаганите мерки за сигурност се извършват по възможно най-ефективния начин, така че да не са причина за затруднения и забавяне в плавното функциониране на въздушния транспорт и търговския стокооборот.

*Глава седма*

# МОДЕЛ ЗА ГЕНЕРИРАНЕ НА УПРАВЛЕНСКИ (МЕНИДЖЪРСКИ) РЕШЕНИЯ, СВЪРЗАНИ СЪС СИГУРНОСТТА И ЗАЩИТАТА НА ВЪНШНИЯ ПЕРИМЕТЪР НА ЛЕТИЩЕ

Вземането на решения, свързани със сигурността, е важна, постоянна и непрекъсната мениджърска дейност. За унифициране на работата в управленските звена и за намаляване на влиянието на субективния фактор при вземане на оперативни решения са необходими оперативни процедури, които да генерират адекватни на заплахата „предложения/съвети".

За да се минимизира времето за вземане на решение и активиране на силите за отговор, е необходим определен алгоритъм за работа в структурите, изграждащи ССЛ, и прилагане на конкретни оперативни процедури при реализацията на потенциала на системата. Примерен вариант за минимизиране на времето за реакция е създаването на модел за генериране на управленски (мениджърски) решения, свързани със сигурността и защитата на външния периметър на летище.

## 7.1. Същност на управленските решения в областта на сигурността

Минимумът от мерки и процедури за сигурност е регламентиран от международните актове в областта на защитата на сигурността в гражданското въздухоплаване. В случая могат да се разгледат две положения с оглед подобряване на ефективното им прилагане, като условия и при двете са степента на риска и неговата адекватна оценка.

Първо, ако приемем една константна величина на риска, спрямо която се прилагат съответни мерки за гарантиране на сигурността (без оглед на степента на оценката – дали тя е от първо, второ или трето ниво), то вътрешните бизнес процеси, насочени към подобрява-

не на ефективността, могат да обхванат летищните дейности по планиране на действията и целия процес по сигурността, неговото ефективно управление, с прилагането на съвременни механизми и показатели, както и механизмите на контрол.

Второ, ако предположим, че степента на заплаха за даден обект от летищната инфраструктура е променлива, то насоката на вътрешните бизнес процеси би била ориентирана към прилагане на нов процес на допълнителни, усилени мерки за защита. Това налага необходимостта от адаптиране на мерките и реорганизиране на вътрешните процеси за сигурност.

Иновативният подход е насочен не само в посока усъвършенстване на технологичното ниво и развитието на ултрамодерна техника, но и към търсене на ефективност на управлението на самия процес. На базата на променящата се заплаха на преден план излиза нуждата да се работи проактивно, предшествайки събитията, като по този начин се влияе както върху формирането на решението на клиентите, така и върху формирането на решението на терористите, правейки летищата добре защитена и неблагоприятна среда за атака или трамплин към друга уязвима цел.

С много по-голяма добавена стойност могат да бъдат оценени проактивната дейност и превантивните адекватни мерки за разкриване на заплахата и осигуряване на съответна защита, отколкото действията в отговор на евентуална атака. Колкото и бързи, качествени и с голям ангажиран капацитет да бъдат те като услуга, максималният им ефект би бил единствено минимизиране на негативните последствия от инцидента. Не трябва да се чака да се случи събитието, за да се оцени постфактум обхвата на заплахата и степента на нуждата на пътниците от защита.

Затова с оглед на ефективността на гарантиране на сигурността на въздухоплаването е важно новият подход на вътрешните процеси да бъде насочен към съсредоточаване на усилията към прогнозиране на бъдещите нужди на клиентите посредством предхождащи планове и сценарии на бъдещите действия на нападателите/терористите.

Този проактивен подход изисква нови управленски методологии. Една от тях, чиято приложимост е обект на настоящата глава, е

създаването на модел за генериране на управленски (мениджърски) решения.

*Решенията, свързани със сигурността на организацията,* представляват предписание за действие към субект от системата за сигурност, като предварително е направен избор от възможни алтернативи по определен критерий.

*Процесът* на вземане на решения преминава през няколко етапа и е тясно свързан с използването на различни видове информация, от чието качество зависят резултатите от изпълнението на избраното решение.

Решенията, вземани в условия на неопределеност, каквато обикновено се проявява при потенциална терористична заплаха, спрямо елементи от летищната инфраструктура изискват незабавна реакция от страна на организацията с вътрешни и/или външни за нея ресурси. Необходимата оперативност се постига чрез превантивно разработени типови възможности за разрешаване на проблема при различни сценарии. Сценариите са комбинации от моментното състояние на организацията и средата, от една страна, и идентифицирания проблем, от друга страна.

### 7.2. Система за подпомагане на вземането на решения в областта на сигурността

Управлението на ССЛ включва управленска политика за сигурност, оценка на риска и планиране, прилагане и организационна структура, мониторинг и действия за коригиране, управленски преглед и анализ, като цялата верига е насочена към ефективност на резултатите и ресурсите. Значението на проактивните мерки е застъпено както в Европейската стратегия за сигурност във всички направления, така и в по-тесен смисъл във въздушния транспорт на международно ниво. Примери за ефективни проактивни мерки могат да бъдат взети в следните направления:

- *Планиране на летищата*: новите превантивни мерки да включват не само изискванията за физическо ограничаване на достъпа и очертаване на критични зони и зони с ограничен достъп, а и из-

бягване на концентрацията на други критични елементи от инфраструктурата в близост до летищата и по-далечна локация от населените места.

• *Контрол на достъпа* посредством идентифициращи системи, при пълно зачитане на личността и превозните средства, предотвратяване на незаконен достъп и пребиваване в демаркираните зони за сигурност.

• *Разпространение и обмяна на информация*: навременното и последователно разпространение и размяна на информация и разузнавателни данни са от съществена важност за поддържането на ефективна авиационна сигурност и дават възможност на операторите и субектите да приспособяват програмите си към променящите се условия и към специфични или генерални заплахи.

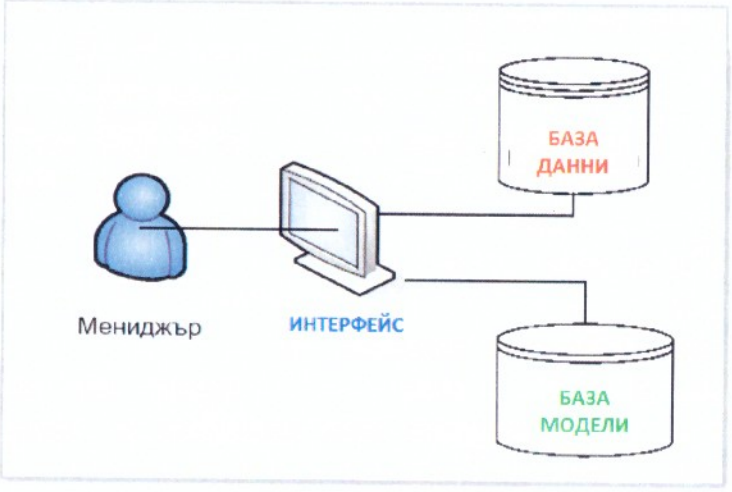
Би било грешка да разглеждаме защитата на авиационната сигурност като прерогатив единствено на летищния оператор. Успешното постигане на ефективността от прилаганите мерки силно зависи и от интегрираните действия на различните компоненти, създаващи сигурност, както в ежедневните операции, така и в дългосрочна перспектива.

Важно звено за вътрешните бизнес процеси във всеки етап на дейността по прилагане на мерките за защита е координацията на действията с всички лица, ангажирани в процеса на гарантиране на сигурността. Затова въздушните превозвачи/авиационни оператори следва да предават при поискване на органите, извършващи контрола на лицата по външните граници преди края на регистрацията, данните за пътниците, които предстои да превозят към граничния пункт, през който тези лица ще влязат на територията на дадена държава.

Тези сведения съдържат чувствителни данни, чиято сигурност в информационния поток също се нуждае от съответното ниво на гаранция: например, номер и вид на пътния документ, националност, пълно име, дата на раждане, граничен пункт, през който се влиза на територията на държавата, транспортен код, час на тръгване/пристигане. Способността и наличието на нужния капацитет за осигуряване на тази допълнителна гаранция по линия на сигурността

създават допълнителна стойност към предоставения продукт „сигурност“.

Възможностите за реален във времето пренос на данни, натрупването им в големи масиви и създаването на база данни от априорна информация са предпоставки за създаването на цифрова система за подпомагане вземането на решения, свързани със сигурността, схематично изобразена на фигура 19.




Фиг. 19. Цифрова система за подпомагане на вземането на решения

*Оценка на заплахата и мерки за предприемане*

Оценката на заплахата се извършва въз основа на данни, получени от разузнавателните служби или от Министерството на външните работи на Република България. Специализираните структури за борба с тероризма към МВР, ДАНС, ГДГВА и специалисти от МВР съвместно определят нивото на заплаха, което се приема от Съвета за сигурност на гражданското въздухоплаване (ССГВ).

При наличие на информация и необходимост от завишени мерки за сигурност, те се прилагат, когато и където това е най-необходимо, а не навсякъде и постоянно. Отговорен орган в Република България за определяне нивото на заплаха е Съветът за сигурност на гражданското въздухоплаване (ССГВ). При наличие на данни за

промяна на обстановката (вътрешна и международна) ДАНС информира субектите по нива на компетентност за промяна на нивото на заплаха. Със своите структури на гражданските летища за обществено ползване МВР осъществява превантивни мерки съгласно компетенциите си за предотвратяване на актове на незаконна намеса. Летищният и авиационните оператори/превозвачи изпълняват стриктно взетите решения от ССГВ и прилагат мерки за сигурност в зависимост от нивото на заплаха.

Когато се счете за целесъобразно спрямо оценката на нивото на заплаха от компетентните органи, в определени случаи се прилагат допълнителни мерки за сигурност за защита от неочаквани атаки или други актове на незаконна намеса. Някои полети, дестинации или въздушни превозвачи могат да бъдат категоризирани като изложени на по-голям риск. Те могат да бъдат подложени на засилени мерки за сигурност за определен или неопределен период от време. Засилени мерки могат да бъдат приложени и по искане на друга държава.

Ефективността от прилагането на засилени мерки може да бъде измерена чрез показателите:

- брой рискови полети, обслужени на дадено летище;
- срок/времеви период на приложение на засилените мерки за сигурност;
- процентно увеличение на разходите и допълнителни ресурси, ангажирани за периода на прилагането им (с оглед на оценката на тяхната пропорционалност на резултата);
- стойност на услугата;
- качество и бързина на информационния обемен;
- ефективна комуникация;
- време за реакция и способност за преминаване в „нормален“ режим на действие след отмяна на режима на прилагане на засилените мерки за защита.

За тази цел НПСГВ определя три различни категории на засилени мерки за сигурност, които могат да бъдат прилагани като цяло в

гражданското въздухоплаване или частично на летища, или дестинации, или превозвачи. [16] Тези нива са:

• *Първо ниво (основни мерки) – код „зелено"*

Това ниво би могло да се опише като нормална ситуация на заплаха, където е налична информация от разузнаване, и показва, че всяко гражданско летище за обществено ползване и всеки авиационен оператор (АО) са обект на атака. Винаги съществува *възможност* за извършване на акт на незаконна намеса от групи и индивиди, за които няма данни, или от криминално проявени, психично болни, недоволни служители и обществеността като цяло. За това ниво основните мерки за сигурност трябва да се прилагат по всяко време, за да се овладее един възможен риск.

• *Второ ниво (междинни, средни мерки) – код „оранжево"*

Разузнаването съобщава за *вероятност* за атака на определен/и авиационен оператор и/или гражданско летище за обществено ползване. За това ниво основните мерки трябва да бъдат засилени/разширени, за да се овладее завишеният риск.

• *Трето ниво (по-строги) – код „червено"*

Разузнаването има *специфични* данни за атака на точно определен АО и/или гражданско летище за обществено ползване. За това ниво основните мерки трябва да се завишат чувствително за посрещане на увеличения риск. ССГВ може да разпореди още по-строги мерки, чието определяне зависи от:

– естеството и степента на заплахата за определен авиационен оператор или гражданско летище за обществено ползване, които са обект на атака съгласно оценката на заплаха;

– очаквана или предполагаема продължителност на повишената заплаха;

---

[16] *Национална програма за сигурност на гражданското въздухоплаване. Второ издание, промяна 4, ГД ГВА, ноември, 2012.*

– разположение на сгради, съоръжения и организация на различните дейности по обслужване на даденото гражданско летище за обществено ползване (например процедури по регистриране);

– персонал по сигурност и налично оборудване;

– стандарти по сигурност, които се прилагат за полети и граждански летища за обществено ползване при завишена заплаха;

– брой полети и пътници, количество багажи и товари, обект на завишени мерки при заплаха.

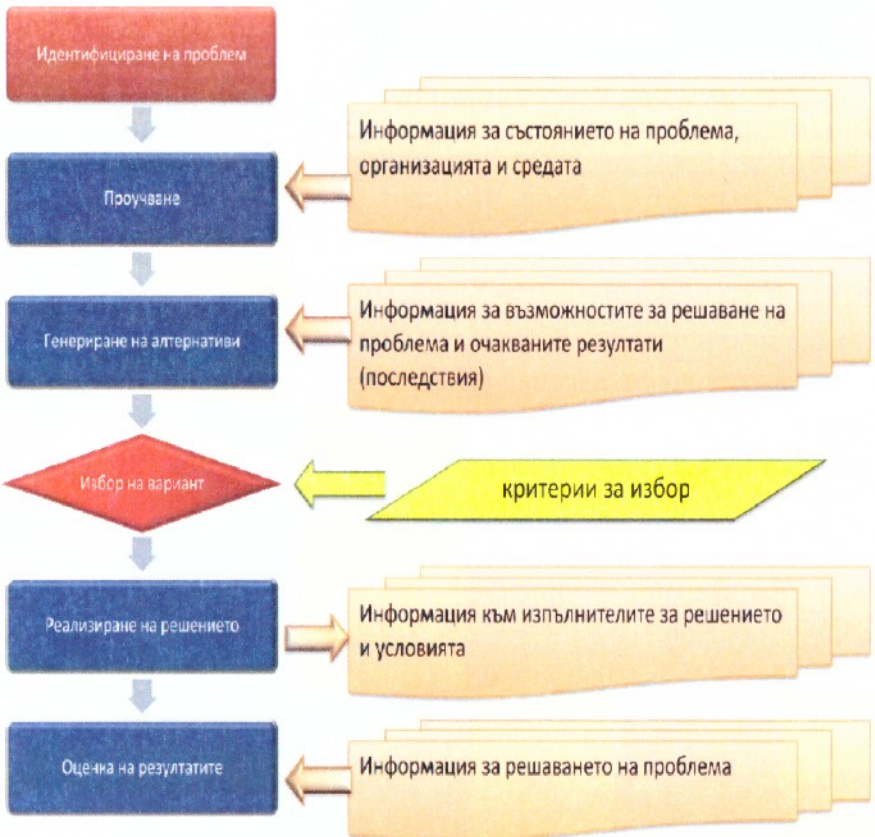
На базата на априорно заложена информация за възможностите за решаване на проблема и критерии за избор се генерира съобщение към изпълнителите за решението и условията. След реализиране на решението процесът завършва с оценка на резултатите, схематично изобразена на фигура 20.

На проведен семинар от 30 януари до 3 февруари 2012 г. в Рим, Италия, на тема „Airport Emergency Planning and Management" са дефинирани следните пет състояния на средата (нива на заплаха), в които е възможно да се намира летищният оператор във всеки един момент:

- Catastrophic;
- Hazardous;
- Major;
- Minor;
- Negligible.

Приведени към националните нива на заплаха на летище, горепосочените състояния на средата (организацията), в които е възможно да се намира летището във всеки един момент, са:

- „ЯВНА" (Catastrophic);
- „ПОТЕНЦИАЛНА – ВИСОКА" (Hazardous);
- „ПОТЕНЦИАЛНА – СРЕДНА" (Major);
- „ПОТЕНЦИАЛНА – НИСКА" (Minor);
- „БЕЗОПАСНО" – (Negligible).




Фиг. 20. Последователност на процеса на генериране на решения

В таблица 3 е разработена примерна матрица за вземане на решения при осигуряване на сигурност и защита на външния периметър на летище срещу несанкционирано проникване в охраняваните площи и обекти.

За идентифициране на даден проблем в района на охраняваното пространство са разположени съответно сензори външно на линията за неутрализиране на заплахата на минимална дистанция $D_1$, средна дистанция $D_2$, и максимална дистанция $D_3$, което е един от критериите за избор на вариант. Величината на дистанциите варира за различните обекти от инфраструктурата на летището и зависи от критичността на обекта, поразяващото действие на вероятната терористична заплаха,

времето за реакция на ССЛ и др. Друг критерий може да бъде типът на субекта/обекта нарушител (човек, МПС и др.).

В зависимост от комбинацията на моментното състояние на летището (нивото на заплаха), което се задава от подсистемата за ръководство и управление, и идентифицираната потенциална терористична заплаха в дадения момент се генерира и степента на риск, която може да бъде в едно от следните четири обозначения (зелено, жълто, оранжево или червено).

За всеки отделен риск в таблица 4 са показани примерни възможности за генериране на управленски решения, които предварително са заложени в системата и се предават към изпълнителите с цел своевременна реакция и отговор на ССЛ. В таблица 5 е даден вариант на съветваща система за оператора на летище при акт на незаконна намеса.

*Таблица 3*

**Примерна матрица за вземане на решения при осигуряване на сигурност и защита на външния периметър на летище**

| | | | | | |
|---|---|---|---|---|---|
| **E** Catastrophic Явна | 1E | 2E | 3E | 4E | 5E |
| **D** Hazardous Потенциална висока | 1D | 2D | 3D | 4D | 5D |
| **C** Major Потенциална средна | 1C | 2C | 3C | 4C | 5C |
| **B** Minor Потенциална ниска | 1B | 2B | 3B | 4B | 5B |
| **A** Negligible Безопасно | 1A | 2A | 3A | 4A | 5A |
| Ниво на заплаха / Дистанция | **1** Максимална дистанция субект | **2** Максимална дистанция хора | **3** Средна дистанция хора | **4** Минимална дистанция хора | **5** Средна дистанция МПС |

*Таблица 4*

## Примерни възможности за генериране на управленски решения

| Действия / Нива на заплаха | Действия на оператора | Действия на ДСЛ (Дежурен сигурност летище) | Действия на външни за организацията сили и средства | СИТУАЦИИ |
|---|---|---|---|---|
| | Информиране на ДСЛ и действия по указание на ДСЛ | Активиране на плана за действия при акт на незаконна намеса | ДА | **4B, 4C, 3D, 4D, 5D, 3E, 4E, 5E** |
| | Информиране на ДСЛ и действия по указание на ДСЛ | Изпращане на дежурна група от собствени сили и средства и оповестяване на горна инстанция | НЕ | **4A, 3B, 5B, 3C, 5C, 2D, 2E** |
| | Информиране на ДСЛ | Привеждане в готовност на дежурна група от собствени сили и средства | НЕ | **3A, 5A, 2B, 2C, 5C, 2D, 2E** |
| | Повишаване на вниманието към активирания сектор | НЕ | НЕ | **1A, 2A, 1B, 1C** |

*Таблица 5*

**Съветваща система за оператора на летище при акт на незаконна намеса (вариант)**

| Код | Режим на работа |
|---|---|
| **Зелено** | – Нормален режим на работа |
| **Жълто** | – Оповести дежурния по сигурност на летището и персонала по списък!<br>– Приведи в готовност дежурната група от собствени сили и средства!<br>– Регистрирай събитието!<br>– Следи с повишено внимание развитието на събитието! |
| **Оран-жево** | – Оповести дежурния по сигурност на летището и действай по негови указания!<br>– Изпрати дежурната група от собствени сили и средства!<br>– Приведи в готовност силите от гранична полиция!<br>– Оповести органите на местната и централната изпълнителна власт!<br>– Регистрирай събитието!<br>– Следи с повишено внимание развитието на събитието!<br>– Поддържай непрекъсната връзка със силите на терен! |
| **Черве-но** | – Активирай плана на обекта за действие при акт на незаконна намеса!<br>– Оповести органите на местната и централната изпълнителна власт!<br>– Регистрирай събитието!<br>– Окажи съдействие на ръководителя за управление на силите по установяване на ред и сигурност, задържане на нарушители, поддръжка и осигуряване, медицинска помощ, пожарогасене, обезвреждане на взривни устройства, евакуация, обезопасяване, ремонт и възстановяване, предаване на доклади!<br>– Окажи съдействие на ръководителя за управление на силите и други специализирани структури за извършване на разследване на инцидента и предаване на доклади!<br>– Поддържай непрекъсната връзка със силите на терен! |

Внедряването на подобна система би спомогнало за:

– решаване на комплексни проблеми за кратък период;

– възможност за тестване на различни сценарии или да се отговори бързо на спешно възникнала ситуация (при наличие на критична информация);

– намаляване на разходите на организацията и подобряване на мениджърския контрол;

– увеличава ефективността на вземане на решения и др.

Въпреки това би било неадекватно да се твърди, че мерките за защита винаги са достатъчни в абсолютна степен да предотвратят терористичните атаки.

*Глава осма*

## ЗАЩИТА НА ВОЕННО ЛЕТИЩЕ

Под *защита на военно летище* (авиационна база) следва да се разбират всички дейности, целящи гарантиране на непрекъснатостта, нормалното функциониране и целостта на летището, за възпиране, намаляване, смекчаване или неутрализиране на заплахите, рисковете или уязвимостта му. Военните летища (авиационните бази) са обекти от изключителна важност. На тях се съсредоточава огромен боен потенциал и защитата им е от първостепенно значение. Целите и задачите за защита на външния периметъра на военно летище в мирно време са идентични с тези за гражданските летища.

В условия на военен конфликт или опасност от възникване на такъв освен усилване на мерките по защита на външния периметър са необходими допълнителни мероприятия по организиране и осъществяване на защита на летището от въздушна заплаха, т.е организиране на противовъздушна отбрана (ПВО) на летището (авиационната база).

Организиране на противовъздушна отбрана на военно летище е задължително изискване и при възникване на вероятност от осъществяване на терористичен акт от въздуха както на територията на Република България, така и при участие на въоръжените сили в многонационални съюзнически и коалиционни операции в отговор на кризи по мисия „подкрепа на международния мир и сигурност".

Решаването на задачата за рационално построение на групировка за ПВО за прикриване на войски, обекти или направления е пряко свързана с определяне на взаимните връзки, които съществуват между трите основни фактора на противовъздушната отбрана: обекти с техните две страни, като обекти за атака от страна на въздушния противник и като обекти за прикритие от системата за ПВО, въздушен противник (заплаха от въздуха) и сили и средства за ПВО.

Задачата може да бъде решена по два начина. Първият е на базата на анализа и оценката на заплахата и риска да се търси оптимал-

но разпределение и използване на наличните ресурси (сили и средства за ПВО). Вторият е на базата на зададено ниво на ефективност на системата за ПВО да се определи колко и какви средства за ПВО са необходими за изпълнение на задачата.

### 8.1. Обекти за поразяване на военно летище (авиационна база) и техните характеристики

Летищата (авиационните бази) се разполагат в равнинна местност, осигуряваща открити подходи за излитане и кацане и съответно удобни направления за нанасяне на въздушни удари. Освен това е трудно или почти невъзможно да бъдат „скрити“ от противниковото разузнаване.

Основните демаскиращи признаци на летищата са характерните очертания на полосата за излитане и кацане (ПИК), пътеките за рулиране, самолетите на открити стоянки и зоните за разсредоточаване, наличието на „глухи“ железопътни и автомобилни пътища, работата на свето-технически средства през нощта и при намалена видимост, наличието на антени на радио- и радиолокационни станции (РЛС), рулиращи, излитащи и кацащи самолети, движение на специални самолетообслужващи автомобили и др.

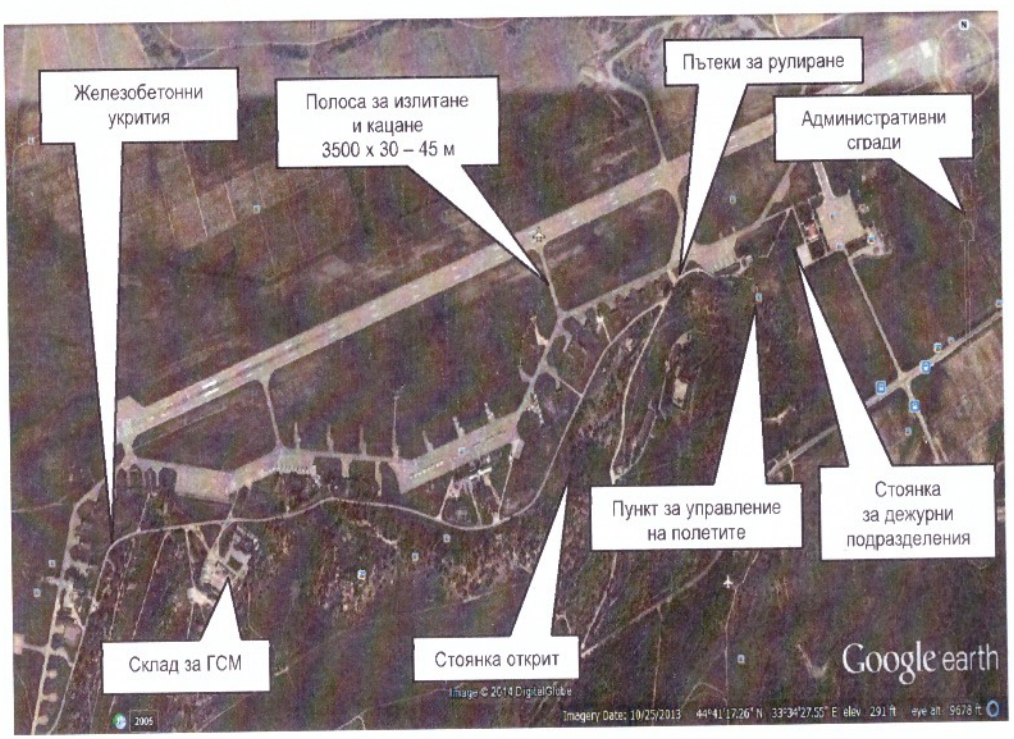
От друга страна, нанасянето на удари по летищата не е лесна задача. В зависимост от това какъв род авиация е базиран на тези летища, те се намират на отдалечение от 100 до 300 км от границата (линията на съприкосновение с противника). Поради това средствата за въздушно нападение трябва да преодолеят големи разстояния над противникова територия, при което времето за въздействие на противниковата ПВО е значително. По-голямата част от обектите за поразяване на летищата са устойчиви цели и, за да бъдат разрушени, е необходимо пряко попадение на определен тип боеприпас, т.е. нанасянето на удари от големи разстояния и височини невинаги е достатъчно ефективно.

Летищата (авиационните бази), като обекти за прикритие от системата за ПВО, представляват площна цел с квадратура около

10 км$^2$, състояща се от голямо количество разсредоточени обекти с различна уязвимост.

На летищата са разположени (фиг. 21):

- полоса за излитане и кацане (ПИК);
- пътеки за рулиране;
- две или три групови самолетни стоянки с укрития (открит или закрит тип);
- стоянки за дежурни подразделения;
- пункт за управление на полетите;
- система за осигуряване на полетите;
- складове за боеприпаси;
- складове за гориво-смазочни материали;
- административни сгради и укрития за личния състав и др.




Фиг. 21. Авиационна база – общ вид

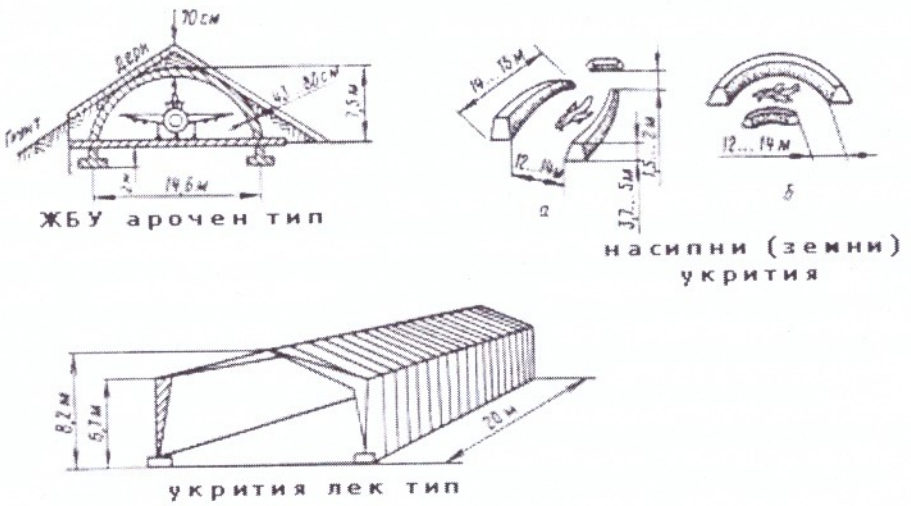
*Полосата за излитане и кацане и пътеките за рулиране* са високоустойчиви линейни, тесни цели. Размерите на ПИК са от порядъка 3500 м на 30 – 45 м с бетонно или асфалтобетонно покритие. На летища за базиране на три ескадрили обикновено има паралелна магистрална рульожка с размери 2400 м на 25 м, която може да се използва като запасна ПИК.

Полосата за излитане и кацане и рульожките визуално, при добра видимост, се откриват на разстояние 10 – 15 км при полет на средни височини и на 6 – 8 км при полет на малки височини. В лунна нощ ПИК се открива на дистанция 3 – 5 км. Работата на РТС позволява да се открие летището на дистанция 6 – 7 км и повече.

При удар по ПИК е необходимо разрушаване на полосата, така че останалите изправни участъци да не позволяват излитане на базираните на летището самолети. Изваждането от строя на ПИК, рульожките и участъци от магистрали се постига чрез използване на фугасни авиационни бомби (ФАБ), управляеми авиационни ракети (УАР) и неуправляеми ракетни снаряди (НУРС) от голям калибър. За минирането на летищата се използват ФАБ, снабдени с взриватели с различно закъснение.

*Самолетите, разположени на открити стоянки,* са единични, малоразмерни, леко уязвими, периодично подвижни цели. Имат възможност за кратко време да излязат изпод удара на авиацията на противника. Това време зависи от степента на готовност или етапа на подготовка за излитане и е от 5 до 30 минути.

Самолетите се разполагат в специални зони, отдалечени от ПИК на различно разстояние (от 600 м до 2 – 3 км). Зоните за разсредоточаване са свързани с ПИК чрез рульожки. За поразяване на самолети на открито и в укрития от лек тип, а така също и на летателния състав в местата за разполагане се използват ракети „въздух – земя", стрелба с оръдия, осколъчно-фугасни авиобомби и запалителни средства. Самолетите се вкарват като правило в укрития, които по конструктивните си особености могат да бъдат *тунелни (арочни)*, *усилени*, *хангарен* и *открит тип* (фиг. 22). Самолетите в железобетонни укрития се унищожават с ракети и ФАБ от голям калибър, а при отворени врати на укритията – със стрелба от оръдията и НУРС.




Фиг. 22. Схема на укрития за самолети

*Складовете за боеприпаси* са на различни разстояния от ПИК (от 600 м до 2 – 3 км) и са разположени на площ с приблизителни размери 500 м на 600 м. На нея се намират няколко хранилища *подземен* или *полуподземен тип* с железобетонна или стоманена конструкция, защитени с насипи и покрити с грунд. За всяка ескадрила може да има до три склада за боеприпаси.

Складовете за гориво-смазочни материали (ГСМ) са подземни и са разположени разсредоточено в района на летището. Запасите от гориво трябва да осигуряват воденето на бойни действия от летището в продължение на няколко денонощия. За унищожаването на складовете за ГСМ и боеприпаси обикновено се използват ФАБ, УАР и НУРС от голям калибър.

## 8.2. Характер на действие на средствата за въздушно нападение при нанасяне на удари по авиационна база в условия на военен конфликт

Мащабът и характерът на действие на въздушния противник зависят от редица фактори, по-важни от които са:

- типове разполагаеми средства и техните характеристики;
- въоръжение и неговите характеристики, в това число и системи за радиоелектронно противодействие;
- подготовка на летателния състав – възможности за изпълнение на задачи във всякакви условия;
- наличие на средства за ПВО и техните характеристики;
- поставени задачи.

За удари по летищата и площадките за базиране на тактическата авиация противостоящата страна основно използва ударна авиация, въоръжена с многофункционални тактически изтребители.

Съвременните многофункционални тактически изтребители притежават способности за поразяване на различни типове обекти, при това могат да използват голям брой разнотипни авиационни средства за поразяване (АСП), в това число управляеми ракети (УР) и подвижни оръдейни установки.

Планирането на удари по военно летище (авиационна база) е дейност, при която детайлно се анализират и отчитат всички фактори, оказващи влияние върху успешното изпълнение на задачата. При подготовката за нанасяне на удар по летище подробно се изучават броят на стоянките за самолети, наличието и типът на укритията, броят и разположението на ПИК и рульожките, пунктовете за управление, складовете, зенитните средства, местата за разполагане на летателния състав. Детайлно се разработва редът за действия на групите с различно тактическо предназначение.

Оценявайки летището като обект за удар, се определят очакваният брой самолети и характерът на неговото функциониране. На основата на този анализ се определя времето за нанасяне на удара.

Ако целта на действията по летището е унищожаване на самолетите, разположени на него, времето за нанасяне на удар се избира

така, че всички или голяма част от самолетите по време на удара да се намират там. За възпрепятстване на възстановителните работи и недопускане функционирането на летището за продължителен период от време се нанасят последователни удари с използване на обикновени АСП.

При планиране на удара особено внимание се отделя на оценката на възможностите на системата за ПВО на летището. С отчитане на разположението на средствата за ПВО се избират направленията и вида на първата и следващи атаки. Опитът показва, че при наличие на различни зенитни средства и невъзможност за нанасяне на удари извън зоните им за поразяване, атаките се изпълнят през зоните на тези установки, ефективността на които е по-малка.

Тъй като на самолетните стоянки има укрития от различен тип, то средствата за поразяване, направленията на атаките, точките за прицелване и способите за атака се определят от характера на укритията. При това целта е да се нанесе удар по укритието така, че намиращият се в него самолет да бъде поразен с максимална вероятност.

Самолетите, разположени на открити стоянки, могат да бъдат поразени с огъня на оръдейното въоръжение, осколъчно-фугасни авиационни бомби (ОФАБ) с малък калибър или неуправляеми авиационни ракети (НАР).

### 8.3. Анализ на въздушните заплахи за военно летище (авиационна база) в мирно време и при участие на въоръжените сили в многонационални съюзнически и коалиционни операции в отговор на кризи

До началото на XXI век се смяташе, че основни заплахи от въздуха за отделните страни в мирно време могат да бъдат конвенционалните въздушни средства преди всичко на съседните държави, военни коалиции или съюзи. Към тези средства се включваха преди всичко различни типове самолети, вертолети, балистични и крилати ракети, т.е. големи въздушни обекти, летящи на малки, средни и големи височини, със сравнително голяма ефективна отразяваща повърхност. В отговор в различни страни по света се създадоха редица сис-

теми за ПВО, по-голямата част от които бяха проектирани за отбрана срещу този тип заплахи.

През последните години обаче конвенционалната въздушна заплаха се разви към асиметрична заплаха, която се насочва преди всичко към достигане на голямо количество жертви при ограничен брой на „ударите“ от въздуха. Съвременната асиметрична въздушна заплаха може да включва всякакви въздухоплавателни средства и летателни апарати, които летят във въздуха и са предназначени да унищожават или да убиват. Към тях се отнасят както изстреляните от самоделно направени установки ракетни, артилерийски и минохвъргачни снаряди (т.нар. RAM заплахи), така и оперативно-тактически балистични ракети с малък, среден и голям обсег (70 – 3500 км), крилати ракети (КР), безпилотни летателни апарати (БЛА), а така също малки и големи пилотируеми летателни апарати. След 11 септември 2001 г. въздушната опасност придоби и ново измерение – т.нар. самолети нарушители, тип „Ренегат“, които най-често са отвлечени авиолайнери от гражданската авиация, превърнати във въздушно оръжие.

Характерни черти на асиметричните заплахи от въздуха:

- появяват се и се променят много бързо (действат за много кратко време);
- не включват само конвенционални оръжия, а всякакви въздухоплавателни средства и летателни апарати, които летят във въздуха и са предназначени да унищожават или да убиват;
- в повечето случаи стойността на този тип средства е твърде малка, вследствие на което те лесно могат да се закупят или да бъдат придобити; в някои от случаите не са необходими специални технически умения и познания за използването им.

През последните години технологиите за производство на безпилотни летателни апарати направиха възможно създаването на относително малки апарати (до 3 м разпереност на крилата), способни да доставят от 2 до 20 кг полезен товар на разстояния от регионален до интерконтинентален мащаб. Пример за такива системи са *Aerosonde* и *Scan Eagle*. Оборудвани с висотомер и сателитна навигация, те имат способности да доставят малки количества оръжия, в това число и за масово унищожение на голямо разстояние, летящи на много малка

височина. Освен това са евтини (от порядъка на няколко десетки хиляди долара) и се нуждаят от относително просто наземно оборудване. Този тип БЛА могат да дублират някои от способностите на пилотируемите летателни апарати по отношение на наблюдение/разузнаване и нанасяне на удари от въздуха. Могат да бъдат достатъчно малки или достатъчно бавни, за да не бъдат открити от системите за ранно предупреждение, което ги прави сериозна заплаха. Налице са индикации, че през следващото десетилетие тези системи ще бъдат широко разпространени по целия свят.

Безпилотните летателни апарати притежават следните характеристики като въздушни цели (ВЦ):

- възможност да се използват практически при всякакви метеорологични условия;
- изработват се от композитни материали и пластмаси със специално покритие и специална комбинация от слоеве, което ги прави трудни за откриване, идентификация и унищожаване, т.е. системата за ПВО има изключително малко време за реакция;
- полет към целта по единично на малки и пределно малки височини с максимално използване на маскиращите и защитните свойства на местността;
- внезапност при атаката на целта – намират се в зоната за откриване от порядъка на 20 – 50 секунди;
- нискоскоростни цели, т.е. малка доплерова съставна на отразения сигнал;
- БЛА с малки бензинови двигатели излъчват малко топлина и работят почти безшумно, а за БЛА с електродвигатели това важи в още по-голяма степен;
- при дължина на радиовълните 5 – 10 см ефективната отразяваща повърхност е от порядъка 0,01 – 0,1 $м^2$;
- възможност за нанасяне на удара едновременно от няколко направления.

Дистанционно управляемите авиационни модели са една от разновидностите на безпилотни летателни апарати. В наши дни наличието на високотехнологични компоненти позволява практически на

всеки любител да създаде въздушна платформа с потенциално унищожителен ефект. В действителност ентусиастите в областта на авиомоделизма могат да създадат съвременни въздушни модели, които да бъдат оборудвани с навигационни системи, позволяващи дистанционно управление. Такива примери могат да бъдат намерени дори и в интернет мрежата.

Сериозни разрушения, ранявания и смъртни случаи на военни и цивилни в операции по поддържане на мира могат да бъдат следствие на атаки с ракети, артилерийски и минохвъргачни (RAM) снаряди, изстреляни от самоделни установки. Най-често точността им на насочване и резултатите са незадоволителни, но при попадение опасността за мироопазващите сили е значителна.

По своята същност терористичният акт от въздуха е вид терористичен акт, извършен от пилотиран, безпилотен или овладян летателен апарат, или целенасочено използване на оръжие или материално тяло, изстреляни или пуснати от летателен апарат, и преднамерено действие, отличаващо се с внезапност, неопределеност и сложност за вземане на решение, често съпроводено със значителни човешки загуби и стрес.

Терористични актове от въздуха срещу обекти на територията на Република България могат да бъдат резултат от:

- използване на летателен апарат (самолет, вертолет, делтапланер, балон и други), овладян или пилотиран от терорист камикадзе;
- целенасочено използване на оръжие от летателен апарат;
- ракетен удар;
- стоварване (хвърляне) на диверсионно-подривни групи в района на важен обект. За тази цел могат да се използват малогабаритни лекомоторни летателни апарати, балони, мотоделтапланери, парапланери и вертолети;
- електронно проникване в комуникациите или в управленската информационна система на обекта с цел нарушаване на неговата работа с използване на технически средства от летателни апарати във въздуха.

## 8.4. Варианти за ПВО на авиационна база

От направения анализ на типовете обекти за прикриване от състава на военно летище (авиационна база) и възможните заплахи от въздуха може да се направят някои изводи, свързани с изграждането на системата за ПВО на авиационна база.

*Първо,* системата за ПВО на военно летище трябва да бъде изградена от средства, способни да унищожават средствата за въздушно нападение до рубежа за изпълнение на задачата (рубежа, от който средствата за въздушно нападение нанасят удари – извършват бомбопускане или пуск на ракети по прикривания обект). В зависимост от целите, които си е поставил противникът, избраните обекти за поразяване и АСП рубежът може да отстои на значително разстояние. Тъй като тези средства за ПВО са достатъчно скъпи, те обикновено не се използват за непосредствено прикритие на летища, а последните се прикриват зонално от системата за ПВО на територията на страната или в зоната на операцията.

*Второ,* значителното количество СВН, които противникът може да задели за нанасяне на удар по военно летище (авиационна база), изисква броят на средствата за ПВО (целевите канали) да не бъде помалък от едновременно нанасящите удар цели. Имайки предвид броя на обектите и размерите на авиобазата, вероятното количество едновременно действащи цели може да бъде от порядъка на 4 – 6 двойки, което предполага наличието на 8 – 12 целеви канала.

*Трето,* възможността да бъдат използвани разнотипни авиационни средства за поразяване от сравнително големи разстояния и височини, в това число и разгледаните асиметрични заплахи, изисква използваните средства за ПВО да притежават способности да унищожават както носителите, така и самите АСП. Тоест необходимо е изграждането на така наречения „близък рубеж за ПВО". Тези средства трябва да притежават способности да откриват и идентифицират АСП, RAM заплахи, малки БЛА. Освен това трябва да притежават малко време за реакция, висок темп на стрелбата и висока вероятност за поразяване. В тази ситуация е желателно използването на комбинация от зенитноракетни и зенитноартилерийски комплекси и системи.

Особеността на тези средства е в това, че пред тях не се поставя (за разлика от останалите средства от групировката) задача за оказване на въздействие по атакуващите средства на максимално отдалечение от прикривания обект. Напротив, рубежите за въздействие се приближават до пределите на допустимата (гарантираната) безопасност, която може да е от порядъка на няколко километра до няколко стотици метра. Благодарение на това, възниква възможност за концентриране на целия енергиен (информационен, огневи, функционален) потенциал в непосредствена близост до прикривания обект и той да се съсредоточи в полусферата, от която са възможни атаките на тези средства. Тоест необходимо е да бъдат създадени предпоставки за осъществяване на ефективна всеракурсна отбрана на малоразмерни обекти при осигуряване на подвижност, многоканалност и производителност на специализирани средства с удовлетворяване на изискванията за тяхната малка маса, габарити и относително невисока цена. С други думи, трябва да им се противодейства на всички етапи от подготовката и използването им и поразяването на крайния участък от траекторията на полета им.

Процесът на унищожаване на въздушни цели преминава през няколко основни етапа:

- откриване на целта;
- идентификация на целта;
- захващане и съпровождане на целта;
- изстрелване на ракета (стрелба с оръдия);
- поразяване на целта.

За да се противодейства на RAM заплахи и малоразмерни безпилотни летателени апарати, преди всичко те трябва да бъдат открити и идентифицирани. Основното средство за откриване и идентифициране в съвременните системи за противовъздушна отбрана са радарите. Те са в състояние да откриват самолети и вертолети на разстояние до няколко десетки километра в зависимост от характеристиките на целите и особеностите на терена. В много от случаите RAM заплахите и безпилотните летателни апарати – и по-специално тези от най-лекия клас, са достатъчно сложни цели за съществуващите радари поради малката ефективна отразяваща повърхност.

Въпреки това конструкторите на системи за ПВО се опитват да подобрят характеристиките на своите разработки за откриване на малоразмерни цели. За ефективно противодействие на леките БЛА на противника създателите на РЛС трябва да решават няколко задачи. Първо, подобряване на характеристиките на станцията, което да позволява откриването на малоразмерни цели с много малка ефективна отразяваща площ (ЕОП), и второ, правилното идентифициране на целта. Леките БЛА, освен че имат малка ЕОП (не повече от 0,1 м$^2$) се движат и с относително ниска скорост. По този начин апаратурата може да обърка БЛА с птица, което да доведе или до пропускане на целта или до ненужно изразходване на боекомплекта.

Както всеки материален обект БЛА имат демаскиращи признаци, които ги правят откриваеми в една или друга степен. Степента на откриваемост се определя от тяхната сигнатура[17] в радио-, инфрачервения, видимия и акустичния спектър. Както вече бе подчертано, съвременните леки безпилотни апарати имат малки сигнатури.

Изпитанията на съвременни радари през последните години показват, че откриването на обекти с ЕОП 0,1 м$^2$ не е проблем. Истинското предизвикателство е в тяхната идентификация и различаването им от птици, смущения и други отразени сигнали, които обикновено се филтрират от радарите.

Решението на подобни проблеми специалистите виждат в радарите с изменяща се разделителна способност през цикъла на откриване. Такива радари са способни надеждно да откриват и идентифицират обекти с малка радиолокационна сигнатура, движещи се по нелинейна, трудно прогнозируема, практически случайна траектория. При това в тези радари от ново поколение се използва много добре отработен алгоритъм за идентификация на птици, за което военните трябва да са благодарни на орнитолозите, чиято „птича математика" сега се използва за военни цели. Ключова за тези радари с активна фазирана антенна решетка (АФАР) е технологията на многолъчеви методи за идентификация с натрупване на информация за увеличава-

---

[17] *Target Signature (от англ. – обозначение на целта) – характерна сигнатура на целта, изобразена от техниката за откриване и идентификация. AAP-06 NATO Glossary of Terms and Definitions, 2014.*

не на възможностите за откриване на апарата по доплеровата съставна на сигнала.

Този тип радари са в състояние да анализират сигнатурата и кинематиката на БЛА, а за по-точна пеленгация и идентификация на целите работят заедно с оптико-електронни станции. В този случай ефективно се използват и данните от уникалното радиоизлъчване на БЛА, което се фиксира от системите за радиотехническо разузнаване (РТР). След като апаратът започне да излъчва, БЛА сам се демаскира и се открива от системите за радиотехническо разузнаване, а след това координатите му се предават и в системата за ПВО.

Тук обаче нещата също търпят развитие. При безпилотните апарати с РЛС на борда се използват LPI сигнали (*Low Probability of Intercept* – „с ниска вероятност за откриване"), които е сложно да бъдат отличени от шум, ако, разбира се, детекторът не „знае" ключа. Същото е положението и с техните системи за комуникация, които използват шумоподобни сигнали, тясно насочени антени, или изобщо лазерно излъчване.

Физическото унищожаване на тези типове средства може да се осъществи с помощта на ракета, снаряд или лазерен лъч. Информационно подавяне с помощта на системи за радиоелектронна борба със стандартни, добре отработени способи, а така също с помощта на най-нови електронни технологии в кибератаките може да се използва за всички БЛА, без изключение. Въпреки това изборът на средства за физическо унищожаване не е толкова лесна задача, тъй като трябва да се отчита критерият *стойност – ефективност*. Малките и леки БЛА могат да бъдат свалени с помощта на стрелково оръжие, а за унищожаване на тежки безпилотни апарати е необходимо използването на зенитноракетни системи.

Както вече бе споменато, големите тактически БЛА имат сравнително голяма радиолокационна сигнатура, достатъчна за захват от зенитна ракета. За по-малките апарати обаче, поради тяхната ниска стойност, в някои случаи не си струва да се изразходва дори относително евтина, изстрелвана от рамо ракета, въпреки че лишаването на противника от събраната информация може да спаси не един човешки живот.

За борба с „ято“ малоразмерни БЛА се изисква нещо по-евтино и ефективно. Отговор в това направление могат да дадат артилерийските зенитни установки. Армиите на редица страни разполагат с по-стари образци зенитноартилерийско въоръжение и това в условия на ограничени военни разходи може да е ключ към тяхното завръщане. От друга страна, вероятността за пряко попадение с обикновен снаряд в такава малоразмерна цел е изключително малка. Ако обаче обикновено зенитно оръдие използва снаряди със специална бойна част, всичко става значително по-просто.

Появата на боеприпаси с все по-интелигентни взриватели и зададено въздействие позволява да се надграждат способности за борба със самолети и БЛА в съществуващите системи на въоръжение. Това са т.нар. телескопични боеприпаси *Cased Telescoped Cannon and Ammunition (CTCA)* или боеприпаси, известни като *AA-AB (Anti-Air Air Burst* – въздушно взривяване срещу въздушни цели) за борба с въздушни цели. Тези боеприпаси освен срещу малоразмерни БЛА са ефективни и срещу хеликоптери, самолети, балистични ракети и дори неуправляеми ракети, артилерийски снаряди и мини или високоскоростни противорадиолокационни ракети. На пътя на летателния апарат всеки снаряд след взривяване образува облак от 150 до 860 волфрамови топчета с тегло от 0,6 до 3,3 грама.

Друга особеност на снаряда е интелигентният, програмируем по време взривател, който осигурява взривяване на боеприпаса в точката на среща с целта. Взривателят на всеки снаряд се програмира автоматично по данни на доплеровия радар от мултисензорния следящ блок и системата за управление на артилерийската установка в момента на напускане на дулния срез на оръдието, като се отчита началната скорост на снаряда, която е различна за всеки. Броят на снарядите, изстрелвани по една цел, е около 24, но може да се променя в зависимост от типа и параметрите на полета на целта.

Както вече беше споменато, БЛА може да бъдат открити и от станциите за радиотехническо разузнаване, които откриват и пеленговат каналите за управление и предаване на информацията на БЛА от малкия клас (за големите и средни класове безпилотни апарати, този тип комплекси работят като средство за ПВО). Станцията за РТР

пеленгова целта, предава целеуказване на РЛС по пеленга на целта, след което по тази информация се включва оптико-електронна система за получаване на точни координати на целта. След уточняване на координатите в района се изпраща БЛА прехващач за унищожаване на целта. Тези системи откриват БЛА по информационната съставяща от работата на навигационната система GPS. Даже в случай на „затваряне“ на общодостъпния сигнал на GPS, БЛА може да бъде открит, тъй като е наличен самият сигнал.

Друга иновация в електронната война е насоченото въздействие върху целта с мощно свръх високочестотно (СВЧ) излъчване. СВЧ ударът е в състояние да изгори всяко радиоелектронно оборудване, да повреди компютъра, да унищожи паметта, софтуера и по този начин да превърне безпилотния апарат просто в „парче желязо“.

Интересен способ за унищожаване на БЛА бе демонстриран по време на конфликта в Украйна. Твърди се, че с помощта на мотоделтапланер, леко стрелково оръжие и информация за местоположението с голям успех може да бъдат унищожавани леки БЛА.

Ако зенитноракетните или зенитноартилерийските установки се окажат неподходящи, прекалено скъпи или неефективни против БЛА, оръжията с насочена енергия могат да бъдат още един вариант за борба с БЛА.

Сред преимуществата на лазерните системи може да се отбележат следните: теоретично за тях е необходима „къса“ логистична верига, доколкото те не се нуждаят от презареждане и могат да работят толкова дълго, колкото им се подава енергия; възможност за смесено използване на бойни лазери с традиционни противовъздушни системи. В този случай лазерите помагат на зенитноракетните комплекси (ЗРК) да унищожават БЛА с инфрачервена сигнатура извън техните бойни възможности. При това те се използват за „подгряване“ на малки БЛА с много ниска топлинна сигнатура до такова ниво, че да може да ги захване и унищожи ракета с инфрачервено насочване.

Разработват се и активни кинетични системи, които с помощта на лазерна установка с висока мощност *HPLW (high-power laser weapon)*, осъществяват прехват и унищожаване на неуправляеми ракети, артилерийски снаряди, мини и БЛА.

Следва да се отбележи, че всички по-горе разгледани методи за противодействие на БЛА, неуправляеми ракети, артилерийски снаряди и мини включват използването на съществуващите системи и оръжия. По този начин унищожаването на вражески апарат с различна вероятност е възможно и при сегашното развитие на оръжията и военната техника. Увеличаване на вероятността за изпълнение на тези задачи ще зависи от характеристиките на новите системи и БЛА, на които те ще противодействат. Очевидно е, че и сега съществуват средствата за противодействие на безпилотни летателни апарати и RAM заплахи, които могат да бъдат използвани при изграждане на ПВО на военно летище. Очаква се в бъдеще те да се усъвършенстват и привеждат в съответствие с тенденциите в развитието на заплахите от въздуха.

# ЗАКЛЮЧЕНИЕ

Бъдещето развитие на въздушния транспорт предполага прилагането на нов стратегически подход по отношение на гарантирането на сигурността. Изправени пред предизвикателствата на XXI век, залагайки в основите строги и устойчиви принципи, стабилността на сигурността трябва да се гарантира чрез правила и норми, които да бъдат превърнати в твърди оперативни действия. Очевидно е, че за осигуряване на сигурност и защита на гражданско летище е необходимо изпълнението на целия комплекс от мерки, правила и стандарти за сигурност. При това е необходимо да се отчитат уникалните характеристики на всяко отделно летище. За осъществяване на пълноценни сигурност и защита летищните служби за сигурност трябва постоянно да се развиват и прилагат допълнителни мерки, като се използват най-нови технологии и световният опит в това направление.

Бързото внедряване на високотехнологичните постижения в сектора за сигурност и промяната на схващането за тяхното използване в съвременни условия и мрежова среда подсказват необходимостта от прилагането на гъвкави подходи за генериране на способности на системата за сигурност на летище, за да участва тя в превенцията и разрешаването на възникнали нежелани ситуации.

## ИЗТОЧНИЦИ

1. Документ 30. Част II. Сигурност. Европейска конференция за гражданска авиация. 13-о изд., май 2010.

2. Закон за гражданското въздухоплаване. – В: Държавен вестник, 1972, № 94.

3. Национална програма за сигурност в гражданското въздухоплаване. 5-о изд., 2013.

4. Регламент (ЕО) № 300/2008 г. на Европейския парламент и на Съвета на европейския съюз от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване.

5. Регламент (ЕО) № 185/2010 г. на Комисията от 4 март 2010 г. за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването.

6. Ръководство по сигурност за защита на гражданската авиация от актове на незаконна намеса (Документ 8973). Международна организация за гражданска авиация. 7-о издание. Т. III, IV, 2010.

7. AAP-06 NATO Glossary of Terms and Definitions, 2014.

8. FTA Office of Research Demonstration and Innovation, FTA Office of Program Management. Transit Security Design Considerations. Global Security,. Homepage. November, 2004. http://www.globalsecurity.org/

**Димитър Караджинов**
**Росен Димитров**

**ЗАЩИТА НА ЛЕТИЩЕ**

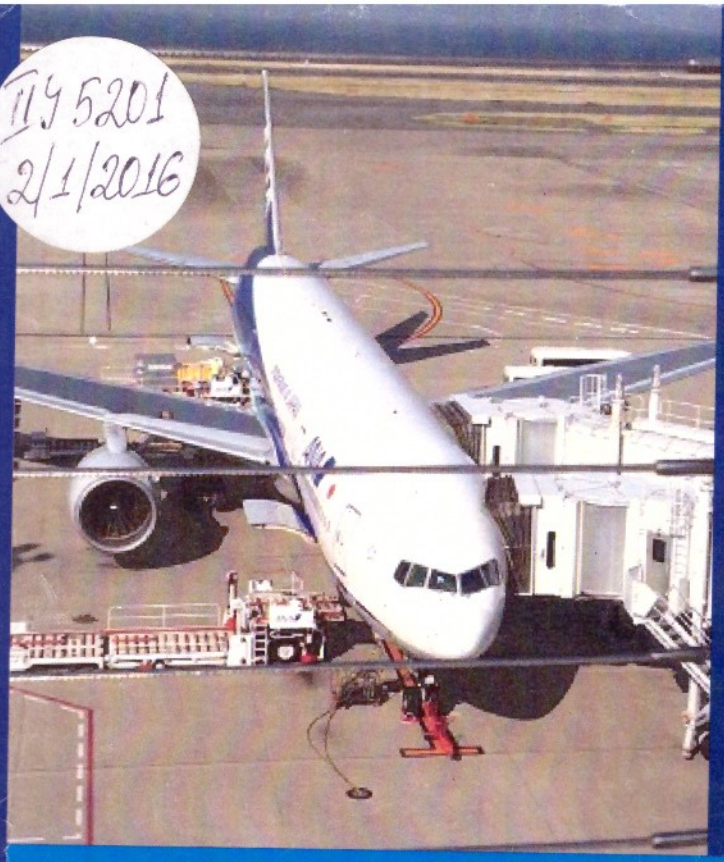
Българска
Първо издание

Редактор *Денка Колева*

Формат 70/100/16

Печат – Военна академия „Г. С. Раковски“

ISBN 978-954-9348-76-7



Димитър Караджинов

Росен Димитров

# ЗАЩИТА НА ЛЕТИЩЕ