Шеста глава
СИГУРНОСТ НА КОМУНИКАЦИОННИТЕ МРЕЖИ

6.1.ВЪВЕДЕНИЕ В ПРОБЛЕМА ЗА СИГУРНОСТТА

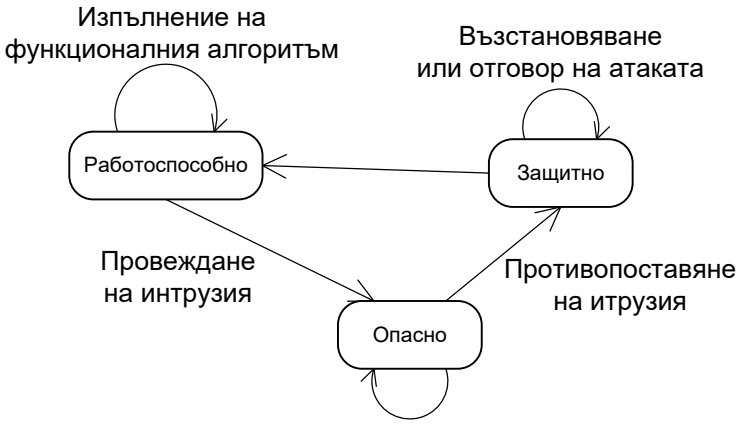
Всяка комуникационна мрежа може да се моделира от надеждностна гледна точка като сложна система с *недетерминирано поведение* след отказ. Недетерминираността на поведението й се определя от появата и натрупването на причини за откази в резултат на:

- случайни обективни неизправности;
- шумове и импулсни смущения;
- грешки в процеса на създаване на системата;
- интрузионни действия на субективни фактори.

Тази глава и следващата част на книгата е посветена на последния от тези фактори.

Неоторизираното умишлено проникване в комуникационна система и/или промяната на информация, както бе отбелязано в глава първа, се нарича **интрузия или атака.**

Интрузията може да доведе до големи материални загуби или загуба на човешки живот. В този аспект деградацията (промяната) на функционалното поведение на системата може да се определи като преминаване от **работоспособно** в **опасно състояние**. Но при активно противодействие и локализация на интрузията може да се говори за преминаване в защитно състояние (Фиг. 6.1), където атаката се отразява и се възстановява нейното работоспособно състояние.



Фиг. 6.1. Принципна схема на отразяване на атака

Защитата от интрузия е свързана с понятието „**политика на сигурност”**. **Политиката на сигурност** представлява *определяне и непрекъснато*

провеждане на стратегия за постигане и поддържане на зададено ***ниво на сигурност.*** За тази цел стратегията разполага с различни методи и средства за:

- детектиране на интрузията в момента на нейното възникване;
- противопоставяне на интрузията чрез изолиране и унищожаване;
- локализиране на източника на интрузионна активност;
- неутрализиране на източника на интрузионна активност.

Нивото на сигурност представлява *степента, в която системата трябва да е защитена* от интрузионни действия.

Стратегията по защита на информацията включва необходимостта от дефиниране на *правила* за:

- провеждане на планово архивиране, контрол на конфигурациите и контрол на преносната среда;
- прогнозиране на възможните случайни влияния и обективни опасности;
- методи и процедури за постигане на интегритет на данните.

Провеждането на успешна политика за постигане на определено ниво на сигурност е непрекъснат процес на *анализ, моделиране и синтез* на различни модели на интрузионно противодействие.

Нивото на сигурност на една информационна система или мрежа може да се определи единствено при отчитане на връзките на конкретната система с останалите системи, с които тя си взаимодейства (или имат аналогично на нейното действие). В този аспект може да се оцени адекватността на сигурността на конкретната система спрямо сигурността на обкръжението, в което тя работи.

6.2. ЕЛЕМЕНТИ НА СИГУРНОСТТА

Сигурността на комуникациите се свежда до осигуряване на защита срещу интрузия в:

- комуникационните ресурси на мрежата;
- информацията, която се намира в нея.

Основните елементи, по отношение на които се защитава информацията са:

- конфиденциалност ;
- интегритет на данните;
- надеждност на информацията;
- автентификация на потребителите.

Някои от тези елементи като понятия с общо за настоящия курс значение, бяха разгледани в глава първа. Тук ще бъдат направени следните уточнения:

Интегритет на данните (Integrity) се разглежда като *процедура* за контрол на цялостност и непроменимост на информационен или комуникационен ресурс. Той се поддържа чрез дефиниране на *вътрешни* и *външни* зависимости между компонентите на обекта.

Вътрешните зависимости се постигат най-често чрез изчисляване на контролни суми върху бинарното съдържание на обекта.

Външните зависимости са свързани със създаване на връзки между съдържанието на два документа – например свързване на съдържанието на документ е текст и цифров подпис[1] на съставилия съдържанието.

Идентификацията се разглежда като *процес на еднозначно разпознаване на всяка функционална единица (обект), участваща в различните нива на комуникационен обмен или формиране на информационен ресурс*.

Автентификацията може да се раздели на три типа [39, 46, 50]:

1. В *първия тип* автентификация обектът се идентифицира с парола, код или и двете. Сигурността се базира на предположението, че единствено обектът, който подлежи на идентификация, притежава необходимите идентификационни признаци. По този начин са организирани компютърните пароли, кодовите брави, GSM мобилните апарати и др. Този тип автенитфикация може да се нарече "**Някои, които познавам**".

2. Във *втория тип* идентификация се предполага, че обектът притежава допълнително устройство (карта), което го идентифицира или е собственик на данни, необходими за последваща идентификационна процедура (ключ за криптиращ алгоритъм или цифров подпис). Този тип може да се обозначи като "**Някой, който има**".

3. *Третият тип* идентификация се базира на предположението, че обектът притежава специфични характеристики, които го правят уникален. На тази основа са разработени биометричните системи. Биометрията използва различни показатели на човешкото тяло, които уникално идентифицират всяка човешка личност. Този тип може да се нарече "**Някой който е**".

Идентификацията от третия тип може да бъде *пасивна* или *активна.*

Пасивната идентификация може да се базира върху сканиране на пръстови отпечатъци, сканиране на ирис, проба за ДНК.

Активната идентификация изисква наличие на уникална функционалност – например идентификация по пулс, по спектър на електромагнитно излъчване на сърцето, по глас и др.

Рискът, в разглеждания контекст, е вероятност за реализиране на успешна интрузионна дейност по отношение на застрашен информационен ресурс.

6.3 ОЦЕНКА НА РИСКА

По отношение на сигурността в сила е следното твърдение:

СИГУРНОСТТА НИКОГА НЕ МОЖЕ ДА БЪДЕ АБСОЛЮТНА.

Сигурността винаги е относителна. Тя зависи право пропорционално от усилията, влагани за поддържане на определено ниво на сигурност, адекватността му по отношение на потенциални интурзионни възможности,

[1] Цифровите подписи се разгледани в главата за криптиране.

влиянието на случайните фактори или наличието на грешки в етапа на синтезиране на определена система.

Щом не може да е абсолютна, то *каква информационна сигурност може да се постигне и как да се поддържа тя?*

Отговорът се крие в **адекватността** между *сигурност* и *вероятни заплахи*. В този аспект е необходимо да се оцени вероятността на възможните атаки срещу слабите места на системата и *да се балансира* стойността на защитата (вкл. изискванията на бизнеса) спрямо ценността на обектите, които защитава. Подробен метод за това е даден в [50].

Оценяването на мрежовата сигурност може да се свърже с оценката (финансовата стойност) на *евентуалните загуби*. С изключение на специални организации (военни, секретни, антитерористични, специални частни изследователски лаборатории), при които загубата на информация не може да се измери количествено, принципът на икономическия баланс е водещ.

От съществено значение при определяне на нивото на сигурността е необходимостта от оценка на възможните атаки по отношение на вероятните атаки. Оценката на вероятността за провеждане на успешна атака се нарича **оценка на риска**. Оценката на риска е от решаващо значение за успешното изграждане и провеждане на стратегията за постигане на определено ниво на информационна сигурност.

Оценката на риска може да се извърши на следните стъпки[2]:

1. Идентифициране и определяне на *приоритетите* на отделните информационни ресурси (обекти) за дадената компания.
2. Идентифициране на възможните *заплахи* по отношение на всеки един от информационните ресурси.
3. Идентифициране на възможните *атаки* и вероятността за тяхното провеждане.
4. Идентифициране на целевото ниво на информационна сигурност и стратегиите за неговото постигане.
5. Анализ на стойността на предприетата стратегия за постигане на определеното ниво на информационна сигурност и ефекта върху целия бизнес процес.
6. Анализ на процедурите за постигане на определеното ниво на информационна сигурност.

За да се определи приоритета на отделните информационни ресурси и да се гарантира възможността за анализ на ефекта от определена процедура за реализиране на система за сигурност, е необходимо да се отговори на следните въпроси:

1. *Какво е необходимо да се защити?*
2. *Защо е необходимо да се защити?*
3. *Каква е неговата стойност?*
4. *Какви са възможните заплахи срещу него?*

[2] Подробно описание на техниките за оценяване може да се намери в [30,36,44,45,46,49]

5. *Какъв е риска?*
6. *Какви са евентуалните последици при реализиране на успешна интрузионна дейност?*
7. *Какви са възможните сценарии за провеждането на интрузия?*

Отговорът на всеки от тези въпроси трябва да се обвърже с финансовата стойност на съответния информационен ресурс, която се определя като се отчита пряката стойност на ресурса и финансова загуба, предизвикана от спад на доверие в конкретната система или мрежа.

Планирането на защитата на всяка система или мрежа се извършва на две нива:

- *Стратегическо*, което описва *целта* на защитата, *принципите* чрез които се организира и *формалните методи* за верификация;
- *Тактическо,* което описва с какви конкретни средства да се постигат стратегическите задачи.

Планирането на сигурността се извършва въз основа на **модела на сигурността**.

6.4. МОДЕЛИ И СТРАТЕГИИ ЗА ПОСТИГАНЕ НА СИГУРНОСТ

6.4.1 Модели

Най-често се използват **три модела**, описващи мрежовата сигурност[3]:

1. *Сигурност чрез неизвестност.*
2. *Сигурност по периметъра.*
3. *Сигурност в дълбочина.*

Сигурност чрез неизвестност. Използването на този модел се базира върху допускането, че ако един ресурс е неизвестен (скрит) то той не може да бъде обект на атака. При скриване на една информационна мрежа в друга и ползването й само от определен кръг потребители, вероятността за атака срещу нея е относително малка. Слабата страна на този модел е, че един път, след като определен информационен ресурс се открие, атаките срещу него най-вероятно ще бъдат проведени с висока вероятност за успех.

Сигурност по периметъра. В този модел информационната сигурност се постига посредством изолиране на информационните ресурси в самостоятелна, защитена среда. За целта се използват специализирани рутери (маршрутизатори), т.н. защитни стени, разделящи комуникационните мрежи на *доверени* и *общи*. При прилагането на периметрова защита се очаква вероятните интрудери, намиращи се от външната страна на мрежата, да бъдат спирани в съответните гранични защитни устройства. Недостатъчци на този модел са:

- невъзможността за постигане на ниво на информационна сигурност по отношение на възможна *интрузия "отвътре";*
- при евентуален *пробив* на дадена периферна защитна система е невъзможна защитата на охранявания информационен ресурс.

[3] Детайлно описание може да с намери в [39,44,46,50].

Защита в дълбочина. Най-сигурният и ясен модел е реализирането на защита в различните нива (информационно и преносно) за дадена система или мрежа. В този аспект всяка система (мрежа) се разделя на поднива (отделни обекти) и всеки обект трябва да бъде защитен отделно. При евентуален пробив защитата в дълбочина гарантира възможност за локализиране на интрузията в определена област при запазване на работоспособността на останалите системни модули (обекти, компоненти).

6.4.2 Стратегии

Сигурността на компютърните комуникации се основава на съчетаването на **три базови стратегии** (Фиг.6.1):

- *стратегия на превантивни действия* (Prevention);
- *стратегия детектиране на интрузия* (Detection);
- *стратегия за ответна адекватна реакция* (Response);

Фиг. 6.2 Стратегии за постигане на сигурност

Стратегията за превантивни действия е в основата на сигурността. Гарантирането на определено ниво на сигурност е свързано с предварително предприети (превантивни) мерки за количествено и качествено оценяване на вариантите за евентуална успешна интрузионна активност. Схемите за организиране на сигурността се базират на следния принцип:
По-лесно е да се организират превантивните мероприятия, гарантиращи сигурността, отколкото да се открие интурзия и да се предприемат ефикасни мерки срещу нея.

Стратегия за детектиране на интрузия. Детектирането на интрузия е процедура по откриване на потенциален проблем в използването на методите и средствата за гарантиране на сигурността. От основно значение в случая е откриването на интрузионната дейност да е веднага с нейното възникване.

Стратегия за ответна реакция. Ответната реакция е набор от действия свързани с анализ и ограничаване или цялостно ликвидиране на последиците от детектирана интрузионна активност, локализиране на източника на интрузионна дейност и отнемане на възможност за повторна интрузионна активност.

6.4.3 Заплахи и уязвимости

Стратегиите за постигане на сигурност задължително включват в себе си определянето на възможните *заплахи* (Threats) и *уязвимост* (Vulnerabilities) на системите (вж. гл. първа).

Заплахата е възможността за намаляване на надеждността на мрежата, интегритета на данните в нея или фунцкионирането на мрежовите устройства. Тя може да е продукт на откази, нарушение на операциите или природни събития. Заплахите, това са видовете атаки или откази които могат да се случат в процеса на експлоатация на една система.

Уязвимостта свойство на всяка мрежа и неизбежно се изявява. Тя е резултат от грешки в проектирането, начина на конфигуриране и управлението на мрежата по време на експлоатация или използването на софтуер, който влияе негативно на мрежовите функции.

Уязвимостта се дължи на един от следните три фактора:

1. **Неправилен дизайн** (грешка в стратегията на перфектност). Софтуерните и хардуерните системи се основават на правила, които могат да се използват с цел реализиране на интрузия. Повечето комерсиални системи се реализират в бизнес условия, без към тях да се предявени особено високи изисквания по отношение на сигурността. Това е резултат от конкуренцията между фирмите, която се изразява в непрекъснато добавяне на нови функции и възможности. В процеса на това състезание не е възможно да се обърне достатъчно внимание на доказването на сигурност. Най-често това се оставя в последващи версии (updates), които се предоставят на потребителите от сайтовете на фирмите.

2. Лоша конфигурация, се нарича такава конфигурация на средство (хадруерно или софтуерно) за постигане на сигурност, която позволява неговото заобикаляне или неутрализиране. Системи и мрежи с лоша конфигурация стават обект на успешни атаки. Лошата конфигурация може да се дължи на:

- програми с възможни слаби места по отношение на сигурността в реализацията си;
- липса на опит на екипа, поддържащ системата;
- неправилно конфигуриране на нова услуга при правилна стара конфигурация.

3. Лош мениджмънт. Лошият мениджмънт се изразява в липса на политика по архивиране, неправилно или ненавременно провеждане на одити по сигурността, липса на документация с резултати от проверки и описание на мерките за отстраняване на регистрираните нередности.

Един от основните източници на уязвимост е **физическата**. Осигуряването на **физическа защита** на информационния ресурс е първата дейност, когато се цели постигането на определено ниво на сигурност. Всички информационни ресурси и средствата за тяхното съхраняване и архивиране трябва да се намират в помещения със специален режим на достъп, който осигурява постигане на определено ниво на сигурност.

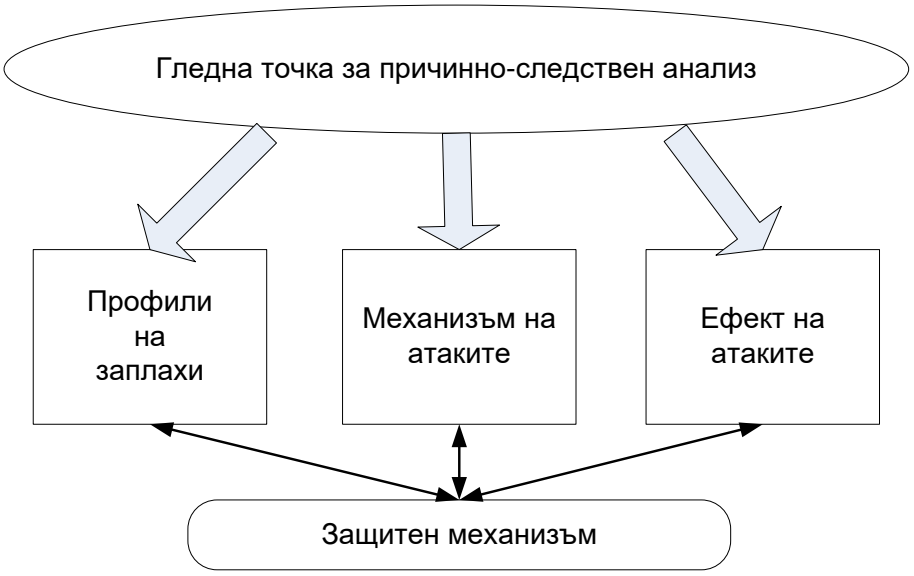
Друг източник на уязвимост е **откритият комуникационен канал**. В съвременния свят все по-често секретната информация се пренася по незащитените канали на комерсиалните комуникационни мрежи. От комуникационната линия данните мога да бъдат копирани или променяни, посредством директно или индиректно подслушване, пробив в съответното комуникационно устройство или прихващане на информацията на ниво файл.

Основен източник на уязвимост е **човешкият фактор**. Статистиката сочи, че най-много загуби на информация се дължат на неправилна манипулация с информационни ресурси или средства за работа с тях от некомпетентни лица. Едва след това в класацията попадат "хакерите". По-голямата част от успешно провежданите атаки, водещи до големи загуби са извършвани с помощта на лица, служители на съответните компании. Човешкият фактор е ключов по отношение на информационната сигурност и по-принцип е **най-слабата част** в политиката на сигурност на която и да е фирма или организация.

6.4.4 Анализ на влиянието на заплахите

За да се анализира **влиянието на заплахите** върху работата на системата могат да се приложат различни модели.

Един от тях се нарича **причинно-следствен модел**. Основната предпоставка на този модел е, че всичко което се случва има определена причина, механизъм на реализация и постигнат ефект. На Фиг. 6.3 е дадена графичната интерпретация на този модел.



Фиг. 6.3 Модел на причинно-следствен анализ

Анализът на заплахите се провежда от експерти. Те формират гледната точка, която впоследствие рефлектира в политиката на сигурност. Въз основа на тази гледна точка се изграждат *профилите за заплаха*, които отразяват всички последователности от събития, нарушаващи работоспособността на системата. Гедната точка отразява и разбирането на това, как евентуално би се провела една атака и какъв ефект би имала. След дефинирането на възможните ефекти от атаките се определят и защитните механизми.

Съществува рсиак от използване на експертна оценка, тъй като определянето на профилите на заплахите и механизмите на атаките може да бъде сгрешено. Но досега липсва формален модел за оценка и твърде вероятно няма да може да се създаде такъв[4].

В процеса на провеждане на причинно-следствен анализ е възможно да се използват следните подходи:

Анализ на индикациите и предупрежденията е друг модел на анализ на зплахите. Индикациите и предупрежденията са различни системни събития или събития в информационната среда на сигурността (форуми, електронна поща, дискусии, книги), които сигнализират за възможна поява на слабост и възможност за атака в даден клас интузионен обект. На базата на анализ на предупрежденията може да се прогнозират евентуалните методи за атака и на тяхна основа да се изгради определена стратегия за защита. Целта на анализа е да се създаде *метрика*, с която да се оцени възможността за реализация на атака, използваща вероятната слабост, описана в конкретното предупреждение. На базата на създадената метрика за индикация на възможна атака се разработват и сензори за детектиране на атаката и алгоритми за противодействие.

Анализ на покритието има за цел да изследва множество от възможни атаки, насочени към една система, и множество от възможни реализуеми защити за нея. Целта на този тип анализ е да се определи цената на всяка атака и цената на съответната защита. Получените цени се съпоставят с цената на атакувания обект с цел балансиране (оптимизиране) на съотношението: цена на вид защита/ цена на съхраняваните данни/ налични финансови ресурси. Оптимизацията се извършва при начални условия, приемащи определени параметри за комплексната мощност на интрузионния източник

Целта на анализа на покритието е да се определи до каква степен системите за противопоставяне на интрузия:

- притежават сензори за разпознаване на изследвания клас от атаки;
- могат да анализират правилно промяната в системните файлове (log-files)
- притежават механизъм за ограничаване на контрола на достъпа;
- могат да управляват процес на филтриране на входящия трафик;
- са резервирани и имат необходимия коефициент на готовност;
- имат изготвен график за одит, спазва ли се графика и как се изпълняват препоръките на одита;

[4] Поне такова е мнението на авторите към датата на издаване на тази книга.

- как се документира дейността по определяне и изпълнение на политиката на сигурност;

Резултатът от такъв анализ е свързан с определяне на това, дали множеството от предвидени защитни мерки покрива множеството от атаки и дали съществува процедура, която реално гарантира функционалността (функцията на готовност) на системата за сигурност.

6.5 СТАНДАРТИ ЗА СИГУРНОСТ

Стандартизирането на сигурността е процес на създаване на обективни показатели за оценка на проектираната и провеждана политика на сигурност. Оценяването на дадена политика на сигурност е свързана с провеждането на тестове и верификационни процедури за оценка на защитата, която тя предлага. Тестовете и верификационните процедури имат за цел оценяването на конкретен **критерий на сигурността.**

Критерият на сигурност представлява *формална дефиниция на свойство, което трябва да притежава оценяваният обект*. В нея се включва и количествена стойност на критерия, в случаите в които това е възможно.

Основният проблем за създаването на формален аналитичен модел е сложността на моделиране на проведените атаки. Всяка атака е последователност от събития, между които съществува причинно-следствена връзка. Тя изисква дефинирането на многопараметрични зависимости, които са сложни за решаване. Затова за част от оценките вместо решение, базирано на строг аналитичен модел, се търси експертно решение, основаващо се на резултати от тестове.

Критериите за оценяване на сигурност се развиват паралелно в Европа и Съединените щати. През 1980 г. представители на Англия, Германия, Франция и др. създават стандарта ITSEC, а през 1983 година Департментът по сигурност на САЩ публикува стандарта Trusted Computer Security Evaluation Criteria (“Оранжевата книга”). С цел уеднаквяване на изискванията през 1999 година се създава стандарта COMMON CRITERIA. Неговата версия 2.0. е стандартизирана от ISO като стандарт ISO IS 15408.

COMMON CRITERIA предлага оценяването на сигурността на комуникационните и информационните системи да става по нива (*Таблица 6.1*). Нивата са седем и се наричат **Evaluation Assurance Level (EAL).**

Таблица 6.1

Код на ниво	*Описание на нивото*
EAL 1	Тестване на функции и елементи
EAL 2	Тестване на структури
EAL 3	Тестване и оценка качеството на тестовете
EAL 4	Тестване на методиката за дизайн, тестове и ревизии
EAL 5	Оценяване на сигурността с полуформални методи
EAL 6	Полуформална верификация на политиката на сигурност

EAL 7	Формална верификация на методите за постигане на политика на сигурност и методите за тестване

По подразбиране всяка система, която не е минала през верификационна процедура, притежава ниво EAL0. То означава, че тя не е защитена.

Ниво **EAL 1** включва оценяване на функциите, отговарящи за сигурността в дадена система. Функциите се оценяват на базата на техните спецификации (гл. първа). В оценката се включват и резултати от тестването им, проведено от независима тестваща организация. Функциите са минималните градивни единици на една система, затова може да се възприеме виждането, че EAL 1 е процедура за *доказване на сигурност на ниво елементи.*

Ниво **EAL 2** включва оценяване на сигурността на структурната реализация на системата. Структурното оценяване на сигурността включва отново тестване на функции. В случая се включва и оценката на влиянието на всяка функция (елемент) върху работоспособността на останалите функции. Ниво **EAL 2** може да се възприеме, като *доказване на сигурност на подсистеми.*

Ниво **EAL 3** включва независима оценка на тестовете на производителя по отношение на цялата система. Оценява се стратегията (модела) за провеждане на тестове, избрания от производителя на системата метод за тестване, начина за неговото провеждане, начина за обработване на резултатите.

Ниво **EAL 4** включва оценяване на оценка на начина на проектиране на отделните модули, начина на тяхното тестване и организацията на одита[5] по време на експлоатационния режим. За да се постигне това ниво, се извършва независимо тестване на сигурността от трети лица, като те определят какви са възможните заплахи за системата.

Ниво **EAL 5** изисква оценяването на системите да се реализира с полуформални методи. За всяка подсистема или функция се изработва математически модел[6] и се проверява устойчивостта на модела при различни атаки. Тестват се спецификациите за разработване на системата на ниво модули и подсистеми. Тестват се и методите за дизайн на отделните елементи и подсистеми. Оценява се дизайна на цялата система. Целта на това оценяване е да се провери дали проектирането на системата е реализирано на модули или не. Модулната реализация показва че е използван обектно - ориентиран подход[7] при изграждане на сигурността.

EAL 6 включва провеждане на тестови и верификационни процедури, които са свързани с изработване на аналитични модели на изследваните обекти и доказването на тяхната сигурност по няколко различни метода. Целта е всеки метод да анализира изследвания обект от специфична гледна точка по

[5] Периодично тестване на определено устройство, провеждане на профилактика и контрол за времето и начина за отстраняване на недостатъците, констатирани в предходни проверки.

[6] В рамките на възможното моделиране

[7] Към датата на издаване на книгата този подход се счита за най-правилен.

отношение на сигурността. Така в края на процедурата се получава комплексна оценка за сигурността.

EAL 7 включва пълна формализация на процедурата по тестване и верифициране. За целта се създава формален модел на самата процедура по верификация и се тества първо той. Това тестване се извършва с цел да се констатира дали самия модел за провеждане на верификацията пропуска да следи за определени заплахи или уязвимости. След като се докаже коректността на метода за провеждане на сертифициране, започва сертифицирането на цялата система. Системата се сертифицира по елементи, подсистеми и като цяло. На всяка стъпка в процеса на сертифициране се извършва аналогична процедура на предходната – верификация на метода за сертифициране на конкретен обект с последваща верификация и тестване на самия обект.

ЗАДАЧИ ЗА САМОСТОЯТЕЛНА РАБОТА

1. Каква е разликата между конфиденциалност и интегритет на данните?
2. Може ли интегритетът на данните да се използва за автентификация?
3. Каква е разликата между заплаха и уязвимост?
4. Опишете заплахите по отношение на един хост (най-добре личния ви компютър).
5. Анализът на покритието как влияе на политиката на сигурност?
6. Каква е разликата между анализ на покритието и анализ на индикациите и предупрежденията?
7. Кое състояние на даден хост бихте определили като опасно и кое като защитно? Аргументирайте отговора си.
8. Каква е разликата между EAL 7 и EAL 6?
9. Как бихте постигнали „сигурност чрез неизвестност” по отношение на комуникацията между две крайни системи?
10. Как бихте защитили компютъра си, чрез „сигурност в дълбочина”?
11. Предложете пример за сигурност по периметъра. Обяснете го.