УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА ”НАЦИОНАЛНА СИГУРНОСТ”

МАГИСТЪРСКА ПРОГРАМА

”ИНФОРМАЦИОННА СИГУРНОСТ”

МАГИСТЪРСКА ТЕЗА

на тема:

Защита на информацията в автоматизираните информационни системи

Дипломант:

Десислава Войкова

задочно обучение

Ф.№ 398-исмз

Научен ръководител:.....

(доц. Г. Петришки)

София

2017

Резюме

Войкова Д. Защита на информацията в автоматизираните информационни системи. Научен ръководител доц. Г. Петришки. София 2017 . Катедра „Национална сигурност“. Магистърска програма „Информационна сигурност“. УНИБИТ. 95 стр. Брой източници – 9, списък на фигурите в текста – 6, приложения – 0.

Целта на магистърската теза е да разгледа пътищата за предотвратяване и реагиране на различни заплахи за информацията и информационните системи, включително неразрешен достъп, разкриване, размножаване, изменение, присвояване, разрушаване, загубване, злоупотреба и отказ при ползване на информация. В магистърската теза се разглеждат някои възможни алтернативи за реализация на мерките в АИС, работещи с класифицирана информация, като следствие от оценката на ценността на информационните ресурси. Съдържа описание на възможните заплахи, злонамерени действия и мерките, които трябва се вземат за предотвратяването им.

Съдържание:

Увод:

Обемите от информация, с които съхраняват и управляват различните държавни и частни структури от всички сфери на отбраната и сигурността, икономиката и на административното обслужване на гражданите, постоянно се увеличават. Необходимостта от все по - обхватно и дълбоко интегриране на различните информационни масиви, през последните десетилетия доведе до изключително бурно развитие на различните информационни системи, които управляват, обменят и защитават данните, които постъпват постоянно в тях. Данните, които се намират в автоматизираните информационни системи са основна цел, както на различни лица и или групи от хакери, така и на различни бизнес или държавни структури, които ръководени от користни или други цели се стремят да ги придобият и дори да ги контролират явно или негласно.

Защитата на класифицираната информация се изразява в комплекс от мерки в областта на физическата, документалната, персоналната и компютърната сигурност. Не всички мерки са технически. В тези области е възможно да се прилагат различни мерки, които са описани по долу в настоящата работа.

Защитата на информацията е едновременно задължение на всяка една държава, която освен, че регламентира законодателно и технологично рамките, в които да се осъществява тази дейност, така и сфера за икономическа активност, която привлича все повече инвестиции – частни или държавни, а също така генерира големи обороти на финансови средства и източник на значителни печалби. Именно поради това заетите в

тази сфера, трябва да познават системата от принципи и възгледи за защита на информационните системи при създаване, съхраняване, обработка и разпространение на класифицирана информация. Едновременно с това, когато това са частни структури чиято цел е получаване на печалба, то задължително ще отчитат и пазарните принципи подобно на други отрасли от икономиката.

Съществуват две самостоятелни сфери на защитата на информацията от нерегламентиран достъп:

- на автоматизираните информационни системи (АИС);
- на компютърните системи и мрежи.

Разликата се състои в това, че компютърните системи и мрежи се произвеждат и доставят като градивни елементи за изграждане на информационни системи. Без програмни приложения компютърните системи и мрежи не съдържат потребителска информация и не са автоматизирани информационни системи.

Освен потребителска информация, при създаването на всяка АИС се формират нейните специфични характеристики, технология за обработка на информацията, права на потребителите и модели на заплахите. Това означава, че защитата на информацията в АИС от нерегламентиран достъп и защитата на АИС от несанкциониран достъп са еквивалентни и равнозначни понятия. При компютърните системи и мрежи защитата на информацията се свежда до защитата на процесите на създаване, съхраняване, обработка и разпространение на информация.

Глава I. Нерегламентиран достъп до класифицирана информация

Нерегламентиран достъп до информация може да се появи чрез преднамерена или непреднамерена човешка дейност. Това са неизправностите и отказите на техническите средства, наличието на грешки в програмното осигуряване, излъчването на паразитни електромагнитни или акустични излъчвания, природните бедствия, авариите и катастрофите. Всички те могат да доведат до нерегламентиран достъп във вид на нежелателно изтичане, модифициране или унищожаване на информация.

Нерегламентиран достъп до класифицирана информация е разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, които водят до нарушаване на защитата й, или до загубване на такава информация. За нерегламентиран достъп се счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до унищожаване от лице, което няма съответното разрешение или потвърждение за това.

1.1. Заплахи за автоматизираните информационни системи

Заплаха за АИС е всяка възможност за случаен или целенасочен нерегламентиран достъп до създаваната, обработваната, съхраняваната и пренасяната информация. Те са събития или действия,

поставящи в опасност даден обект и се появяват при наличие на уязвимост.

Уязвимост на АИС е слабост в системата от мерки за сигурност или в контрола за тяхното изпълнение, които могат да доведат до компрометиране или да улеснят компрометирането на сигурността. Уязвимостта може да бъде пропуск или да се дължи на недостатъчно ефективен надзор, недобра комплектуваност и устойчивост на работата, или на неефективна физическа защита. Уязвимостта може да бъде от техническо, програмно, технологично или процедурно естество. Наличието на уязвимост създава възможности за реализация на събития или действия, поставящи в опасност организацията (т.е. заплахи), в резултат на което могат да настъпят вреди.

Вреда в областта на АИС или мрежи е увреждане на интересите на техните потребители (или на интересите, които тя защитава), вредните последици от което не могат да бъдат елиминирани или смекчени само с последващи мерки. В зависимост от значимостта на интересите и сериозността на причинените вредни последици *вредите са непоправими или изключително големи, трудно поправими или големи и ограничени***.**

Непоправими или изключително големи вреди са тези, при които е настъпило (или би могло да настъпи) цялостно или частично разрушаване на АИС, или е извършено непоправимо посегателство върху интересите на свързаните с тях потребители.

Трудно поправими или големи вреди са тези, при които е оказано (или би могло да се окаже) значително негативно въздействие

върху АИС (или върху интересите на свързани с тях потребители), което не може да се компенсира без настъпване на вредни последици, или вредните последици могат да бъдат смекчени само със значителни последващи мерки.

Ограничени вреди са тези, при които е оказано (или би могло да се окаже) краткотрайно негативно въздействие върху АИС (или върху интересите на свързани с тях потребители), което може да се компенсира без настъпване на вредни последици, или вредните последици могат да бъдат смекчени с незначителни последващи мерки.

Заплаха за АИС могат да бъдат всички техни обекти (пасивни елементи, съдържащи или приемащи информация) и субекти (активни елементи - лице, процес или устройство, обменящи информация между обектите или внасящи изменения в състоянието на АИС). Тези заплахи могат да се класифицират на четири йерархично подредени нива, всяко от които включва стоящото под него, както следва:

1-во ниво: обхваща възможностите за водене на диалога в АИС, изпълнение на ограничено множество задачи (програми), реализиращи предвидени функции по обработка на информация.

2-ро ниво: обхваща възможностите за създаване и изпълнение на собствени програми с нови функции по обработка на информация.

3-то ниво: обхваща възможностите за управление функционирането на АИС, с които се въздейства върху базовото й програмно осигуряване и върху състава и конфигурацията на оборудването.

4-то ниво: обхваща възможностите на лицата, заети с проектиране, разработка, внедряване, експлоатация и ремонт на АИС, включително възможностите за включване на собствени програмни или технически средства с нови функции за обработка на информацията.

На всяко от нивата заплахата е със съответните компетенции (квалификация и ресурси), знае всичко за АИС и познава добре системата и средствата за нейната защита.

Познаването на възможните заплахи, както и на уязвимите места на АИС, които тези заплахи експлоатират, дава възможност да се подберат най - ефективите средства за защита. Трябва да се отбележи, че самото понятие заплаха в различни ситуации често се тълкува по различен начин. Например за подчертано открити организации може да не съществува понятието заплаха за конфиденциалността - цялата информация се явява общодостъпна. В много случаи обаче нерегламентираният достъп се оказва сериозна заплаха.

Много чести и доста опасни, от гледна точка на загубите, са грешките поради некомпетентност и невнимание на потребителите, операторите, системните администратори и други лица, обслужващи информационните системи. Понякога такива грешки се явяват като заплахи (неправилно въведени данни, грешка в програмата, която би могла да доведе до срив в системата), понякога създават слаби места, от които биха могли да се възползват определени сили. Пожарите и наводненията могат да се считат за нищожни, в сравнение с неграмотността и безотговорността. Най-радикалният начин за борбата с неволните грешки е

максималната автоматизация и строг контрол за правилността на извършените действия.

Съществени по размери на загубите са преднамерени действия на лица и организации с цел нерегламентиран достъп. В резултат на подобни незаконни действия ежедневно се нанасят значителни щети, като в повечето от разследваните случаи виновниците са щатни сътрудници на организациите, отлично запознати с режима на работа и мерките за защита. Това илюстрира обстоятелството, че вътрешните заплахи са не по-малко опасни от външните.

Особено опасни са действията на така наречени обидени служители - настоящи и бивши, които са ръководени от желание да нанесат вреда на организацията, като например:

- да повредят оборудването;
- да внедрят логическа бомба, която да разруши програми или данни;
- да въведат неверни данни;
- да променят данни и т.н.

Необходимо е да се следи при напускане на служители, запознати с порядките в организацията, правата им за достъп до информационните ресурси да бъдат анулирани или прекратени своевременно.

Заплахите, които идват от физическата среда, в която е разположена и работи една информационна система, се отличават с голямо разнообразие. На първо място трябва да бъдат посочени нарушенията на

инфраструктурата:

- аварии в електрозахранването;
- временна липса на връзка;
- пробив във водоснабдяването и пр.

Опитите за нерегламентиран достъп до конфиденциална информация са една от заплахите, но опасността е голяма тогава, когато това се върши от лица, свързани с чужди разузнавателни структури или терористични организации. Почти всеки Интернет сървър по няколко пъти на ден става обект на опити за проникване, но рядко тези опити се оказват успешни. Обикновено те се правят от лица, които имат големи познания в областта на компютърните и програмните технологии (така наречените *хакери)* и за които е предизвикателство проникването в добре защитени системи. Като цяло загубите, предизвикани от деятелността на хакерите, в сравнение с тези от други заплахи, не са големи.

По аналогичен начин стои и въпросът за заплахата от компютърни вируси. Вирусите са програми, притежаващи способността да се размножават в операционната среда на компютъра, създават копия със способност за по-нататъшно размножаване. Този процес може да доведе до затрудняване на трафика на данни в мрежата и до пълното й блокиране. Съвременната техническа литература, посветена на компютърни вируси, изобилства с екзотични наименования като червеи, логически бомби, троянски коне и пр., като същевременно се правят опити да бъдат класифицирани многобройните вируси, разпространени в мрежата. Някои видове вируси могат да нанесат големи щети, унищожавайки

информацията. Независимо от това, ако са открити навреме и ако е създадена съвременна защита в системата или мрежата, те могат да бъдат обезвредени. Съблюдаването на елементарни правила на комиютърна хигиена до голяма степен понижава риска от загуби.

В т. 4 от допълнителните разпоредби към Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи, в които се създава, обработва, съхранява и пренася класифицирана информация, е казано, че заплаха към АИС е възможност за ***случаен или целенасочен*** нерегламентиран достъп до класифицирана информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежата. Заплахи за информационните средства могат да бъдат:

- нарушаването на установения ред и организация за ползване на информационни услуги, включително нерегламентиран достъп, събиране и използване на класифицирана информация от бази данни и знания;
- използването на несертифицирани или забранени метода за създаване, събиране, обработка и потребление на информацията;
- разработването и разпространяването на продукти, нарушаващи нормалното функциониране на националните информационни системи, включително и на средствата и системите за защита на информацията;
- неправомерни въздействия върху системите за защита на информацията, включително използването на несертифицирани наши и

чужди информационни средства и технологии за защита на информацията или компрометирането на ключовете и средствата за криптографска защита;

- унищожаването, повреждането, радиоелектронното подаване или разрушаване на средства и системи за създаване, събиране, обработка и потребление на информация;
- внедряването на електронни устройства за прехващане на информация в технически средства за обработване, съхраняване и предаване на информация по свързочни канали, както и в служебни помещения на органите на държавната власт, местното самоуправление, учрежденията, организациите и предприятията, независимо от формата им на собственост;
- допускане на изтичането на информация по технически причини;
- унищожаването, повреждането, разрушаването или грабежа на средства за обработка или носители на информация;
- нарушаване на законовите ограничения за разпространяване на информацията.

Източниците на заплахи биват външни и вътрешни. За класифицираната информация ***външни*** могат да се явят:

- враждебни действия на чуждестранни организации, групи от хора и отделни личности от политически, икономически и разузнавателни структури, които целят нерегламентиран достъп до класифицирана информация;

- дейността на международни терористични организации, целяща проникване в информационните системи на държавни, военни и други структури, които имат отношение към сигурността на държавата;
- дейността на космически, въздушни, морски, наземни и други технически разузнавателни средства на чужди държави, събиращи класифицирана информация.

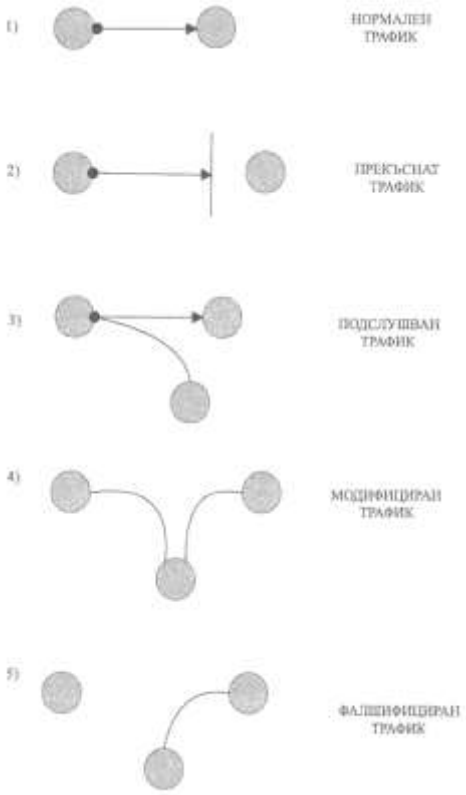
Към ***вътрешните*** заплахи могат да се отнесат:

- враждебни действия на отделни личности в самите организации, които работят е класифицирана информация;
- пропуски в нормативната база, регламентираща тези отношения, както и неефективното прилагане на закона;
- некомпетентността на служителите;
- недобрата координация между държавните органи за прилагането на Закона за класифицирана информация, както и структурните реформи, извършвани в организационните единици;
- изостаналост по отношение на техническите и информационните ресурси от водещите тенденции в света;
- използване на несертифицирани в съответствие с изискванията на закона мрежи и системи за работа е класифицирана информация;
- недостатъчно финансиране на мероприятията по организацията на защита на класифицираната информация;
- предизвиканите от човешка дейност технически аварии, както и природните бедствия в организациите и пр.

1.2. Модел на заплахите за сигурността на АИС или мрежи

Представени са пет различни варианта на модела на заплахата, като са дефинирани четири категории атаки срещу автоматизираните информационни системи или мрежи (фиг. 1).

Различните обекти се разглеждат абстрактно, т.е. самостоятелни работни станции, обменящи данни или комуникационни средства, управляващи поток от данни и обменящи служебна информация за пътищата за предаване на данните.



Фиг. 1. Варианти на модела на заплахите в автоматизираните информационни системи

Вариантите на модела са, както следва:

1. Трафикът протича нормално, без да има наличие на външно вмешателство или нерегламентирано подслушване.

2. Налице е прекъсване на нормалния трафик - едно от ценните (жизнените) качества на системата е разрушено или е невъзможно използването му. Прекъсването може да бъде причинено от най-различни неща, например проникване в глобалната среда за сигурност, довело до прекратяване на нормалния трафик.

3. Регистрирано е подслушване на трафика или пресрещане (прихващане) - едно неоторизирано действие дава достъп до системата. Подслушването може да се осъществява отдалечено, като чрез подходяща апаратура се прихваща излъчваният сигнал, моделира се и се превежда в удобен четящ вид. Подслушване може да се реализира и при непосредствен достъп до комуникационната система, било то до кабели, компютри, комутатори, сървъри и маршрутизатори; има модифициране на трафика. При този вариант, един път прихванал трафика, третото лице подправя трафика и го изпраща на крайния му потребител.

4. Изфабрикуван (подменен) е оригиналният трафик. При него има симулиране на трафик, като се подменят данните от изпращача, по този начин крайният потребител губи реална представа за истинския автор на получения от него трафик. Прихващането е пасивна атака, когато няма намеса в комуникационните канали. Единственото нещо, което се осъществява, е постоянно наблюдение на преминаващата информация,

докато прекъсването, модифицирането и изфабрикуването са активни атаки, тъй като там се регистрира намеса от трети лица.

1.3. Типове атаки

Най-често използваните атаки срещу автоматизираните информационни системи и мрежи могат да се обобщят в седем категории:

- Кражба на пароли - методи за получаване на други потребителски пароли.
- Социален инженеринг - придобиване на информация, до която нямате достъп.
- Грешки и черни врати (bugs and backdoors) - получаване (използване) на преимущества посредством използване на системни грешки;
- Възможностите за автентикация - използване на дефектите (противоречивост и непълнота) на механизмите за автентикация.
- Грешки (провали) в някои протоколи - протоколи с грешки в проектирането и реализацията.
- Изтичане на информация - използване на системи като системата за подписване (finger) или системата за именуване (DNS) за информация, необходима на администратора или необходима за функционирането на мрежата, но която може да се използва за мрежови атаки.
- Отказ от обслужване - опити за лишаване на потребителите от услугите на тяхната компютърна система.

1.4. Категоризация в зависимост от резултатите

Тази категоризация е съставена в зависимост от постигнатите резултати от атаката.

- ***Разрушение.*** При него има логическо разрушаване на комуникационните канали (например VPN) и физическо разрушаване като прекъсване на кабели.
- ***Изтичане.*** Пробив или уязвимост в системата, довела до изтичане на информация.
- ***Отказ (блокировка).*** Вследствие на атаката се е получило блокиране на системата, което за известно време (в зависимост от предприетите политики това може да намали или увеличи времето за реакция) прави системата неизползваема.

1.5. Емпиричен списък

Емпиричната класификация на заплахите позволява да се дефинират осем категории. Основното преимущество на тази класификация е, че съществуват атаки, които логически не могат да попаднат в точно една от трите изброени по - горе групи и които се обхващат от тази класификация.

- Външна кражба на информация.
- Външна злоупотреба с/на ресурсите.
- Представяне (преструване) - записване и използване на мрежовия трафик.
- Вредителски програми (инсталиране на злонамерени програми).

• Повторение на автентификацията или авторизацията (разбиване на пароли).

• Злоупотреба с авторизацията (фалшифициране на записи).

• Злоупотреба с бездействие (лошо администриране).

• Индиректна злоупотреба (използвайки други системи за създаване на зловредни програми).

Потенциални канали, през които може да изтече информация от АИС или мрежи, и мероприятия за тяхното отстраняване и ограничаване са показани в таблицата по - долу (фиг.2).

Обекти и субекти на АИС или мрежи	Потенциални заплахи за информационната сигурност	Препоръчителни мероприятия за защита
Защитени помещения	Защитени помещения: 1. Радиопредаватели; 2. Изтичане на информация по технически канали (акустичен, Виброакустичен, акусто-електрически, паразитни електромагнитни излъчвания, Визуално-оптичен).	1. Проверка на помещенията за излъчватели; 2. Проверка на помещенията за съответствие на изискванията на действащите стандарти; 3. Сертификация на помещенията.
Система за електрозахранване и заземяване	1. Изтичане на информация по електрозахранващите вериги и по линиите за заземяване; 2. Изгаряне от строя на компютърната техника под въздействие на електромагнитни излъчвания.	1. Монтаж на трансформаторни подстанции в контролираната зона; 2. Монтаж на заземяващия контур в границите на зоната на сигурност; 3. Поставяне на филтри на входовете на основното електрозахранване.
Кабелна система и пасивно оборудване на мрежата за пренос на данни	1. Паразитни електромагнитни излъчвания; 2. Информационни излъчвания по паралелни кабелни линии на техническите средства за свързка; 3. Несанкционирано включване към кабелните магистрали и техните възли.	1. Проверка за паразитни електромагнитни излъчвания в границите на зоната на сигурност; 2. Екраниране на магистралните линии; 3. Затваряне на кабелните системи в защитни обвивки; 4. Физическа защита на техническите помещения и ограничаване на достъпа към съединителните възли; 5. Линейно зашумяване на линиите за предаване на данни. Използване на оптически кабели.

Активно мрежово оборудване на мрежата за пренос на данни	1. Паразитни електромагнитни излъчвания; 2. Несанкционирано включване към портовете на оборудването; 3. Прехващане на трафик; 4. Изключване на захранването; 5. Откази или неизправности на оборудването.	1. Въвеждане на инструкция за експлоатация; 2. Разполагане в екранирани приборни стойки и шкафове; 3. Физическа защита на помещенията и ограничаване на достъпа до оборудването; 4. Проверка и защита на програмното осигуряване на работните станции и сървъри от несанкционирана промяна; 5. Използване на непрекъсваемо токозахранване; 6. Резервиране на оборудването и ремонтните комплекти.
Компютри (сървъри и работни станции)	1. Паразитни електромагнитни излъчвания; 2. Достъп до информацията чрез използване на несертифицирано програмно осигуряване; 3. Изключване на електрозахранването; 4. Несанкциониран достъп към сървърите и работното място на администратора по сигурността; 5. Откази или неизправности на оборудването.	1. Въвеждане на инструкция за експлоатация; 2. Използване на сертифицирани програмно-технически средства за защита от нерегламентиран достъп; 3. Използване на непрекъсваемо токозахранване; 4. Физическа защита на помещенията и ограничаване на достъпа до оборудването; 5. Резервиране на оборудването и ремонтните комплекти; 6. Зашумяване на помещенията срещу подслушване.
Системно програмно осигуряване	1. Нарушаване на целостта на програмното осигуряване чрез използване на нерегистрирано програмно осигуряване; 2. Грешки на администратора; 3. Грешки на потребителя.	1. Използване на сертифицирани програмно-технически средства за защита от нерегламентиран достъп; 2. Използване на защита от вируси; 3. Резервно копиране на информацията; 4. Контрол от администратора по сигурността; 5. Обучение на потребителите.
Приложно програмно осигуряване	1. Нарушаване на целостта на програмното осигуряване чрез използване на нерегистрирано програмно осигуряване;	1. Използване на сертифицирани програмно-технически средства за защита от нерегламентиран достъп;

Приложно програмно осигуряване	2. Грешки на администратора; 3. Грешки на потребителя.	2. Използване на защита от вируси; 3. Резервно копиране на информацията; 4. Контрол от администратора по безопасността; 5. Обучение на потребителите.
Данни	Несанкциониран достъп до данните (кражба, унищожаване, изменение)	1. Използване на сертифицирани програмно-технически средства за защита от нерегламентиран достъп; 2. Използване на защита от вируси; 3. Резервно копиране на информацията; 4. Контрол от администратора по безопасността; 5. Обучение на потребителите.
Персонал	1. Кражба на преносими носители; 2. Кражба на отпечатани на книжен носител документи; 3. Несанкциониран достъп до информацията в АВС; 4. Непреднамерени грешки на потребителя; 5. Грешки на администрирането; 6. Компрометиране на паролите и достъпа към софтуерните ключове и шифри;	1. Отчет и съхранение на сменяемите носители; 2. Премахване на сменяемите и преносими информационни носители; 3. Отчет и съхранение на книжните копия; 4. Поставяне на печатащите устройства в охраняеми помещения; 5. Използване на сертифицирани програмно - технически средства за защита от нерегламентиран достъп; 6. Обучение на потребителите. 7. Разработка и внедряване на нормативни документи и инструкции; 8. Разделяне функциите на администрирането и контрола между системните администратори и администраторите по сигурността; 9. Организация и поддържане на система за генериране на пароли; 10. Организация на скрит контрол върху работата на персонала.

Фиг. 2. Заплахи и мероприятия за защита

Анализ на атаките

При наличие на атака трябва обстойно да се анализират уязвимите точки, довели до тази атака. За пълния анализ на атаките е целесъобразно всяка една от тях да се разглежда (класифицира) в следната последователност: хакери (атакуващи); средства, използвани при атаката; достъп до автоматизираната информационни структура; постигнати резултати при атаката; цели на атаката.

Класификацията на атакуващите компютърните мрежи и системи е във вида: хакери - за предизвикателството и статуса на получили достъп; шпиони; терористи; корпоративни нарушители; професионални престъпници; вандали.

1.6. Атакуващи и тяхната първична мотивация

1.6.1. Достъп

Основното свързващо звено между атакуващите и техните цели е неоторизираният достъп или неоторизираното използване на ресурсите в автоматизираната информационна структура или мрежа. Неоторизираният достъп или използване е свързано също с процесите или с файловете и данните, предавани по мрежата чрез процесите. Неоторизираният достъп и използване са един от начините (пътища) за атака. Не трябва да се пренебрегва и фактът, че са възможни и атаки при злоупотреба с правата за достъп. Не по-малко от 80% от проникванията в системите са от напълно оторизирани потребители, които са злоупотребили с правата си за достъп. Това е потенциално и един от най-големите проблеми при защита на автоматизираните информационни

системи или мрежи.

1.6.2. Уязвимост

Най-често атакуващите използват компютърната и мрежовата уязвимост. Уязвимостта може да се използва, както следва:

- Чрез софтуерни/хардуерни грешки (bug). Типичен пример са Unix системите, които са в основата на Internet (Intranet) и които имат много проблеми, в sendmail програмата, която често се използва, за получаване на неоторизиран достъп до Host компютъра.
- Използвайки грешките, възникнали при проектирането на системите. Internet sendmail е типичен пример за това.
- Грешките, възникнали при конфигурирането на системите. Грешките при конфигурирането на системи включват такива проблеми за сигурността като системни правомощия с добре известни пароли, разрешение по подразбиране за използване на нови файлове.
- И други.

УЯЗВИМОСТ	ДОСТЪП	РЕЗУЛТАТ
Уязвимост при разработването	Неоторизиран достъп до информация.	Разрушаване или разкриване на информация (достъп до информационни масиви или отделни файлове).
Уязвимост при проектирането	Неоторизирано използване на ресурси.	Кражба на услуги (кражба на данни, предаване или неправомерно използване на услуги).
Уязвимост при конфигурацията	Неправомерно използване на системни правомощия.	Отказ на услуги (блокиране на процеси) или разрушаване на системата.

Фиг. 3. Организация на връзката „уязвимост – достъпност – резултат“

1.6.3. Резултати

Между придобиването на достъп и целите на атакуващите са резултатите от атаката. В тази точка от последователността на една атака атакуващият получава достъп до желаните процеси, файлове и данни. В този момент той е свободен да използва този достъп за чувствителните файлове, да забрани услуги, да получи информация или да използва услуги (таблица 3).

1.6.4. Средства

Средствата за атака могат да се разделят в следните категории:

- Потребителски команди - въвеждани от командната линия или посредством потребителски графичен интерфейс.
- Скриптове или програми - стартирани от атакуващия и използващи уязвимостта на системите.
- Анонимни агенти - инсталират се програми или фрагменти от тях, които работят впоследствие независимо от потребителя и използват уязвимостта на системата.
- Средства за разработване - софтуерни пакети, съдържащи скриптове, програми или анонимни агенти.
- Разпределени средства - средствата за атака се разпределят върху различни компютри.
- Извличане на данни - когато се подслушва електромагнитното излъчване от компютърните системи и мрежи чрез устройства, външни за мрежите.

По време на експлоатацията на автоматизираните информационни системи и мрежите се крият най - големите опасности за тяхната сигурност. Неволните грешки на системния администратор и на потребителите могат да доведат до повреди на апаратурата, разрушаване на програмите и данните, в най - добрия случай се допускат слабости, които повишават рисковете от заплахи. Скъпите мерки за сигурност губят своя смисъл, ако са недобре документирани, в конфликт с други програмни продукти, а паролите на системния администратор не се сменят от момента на монтирането. Именно за това, за осигуряване на по - добра защита на информацията в автоматизираните информационни системи и мрежи е необходима ежедневна дейност по поддръжката.

Поддръжката на потребителите, например, се състои в консултиране и оказване на помощ при разрешаването на различни проблеми. Важно е в потока от въпроси на потребителите да се доловят проблеми, свързани с информационната сигурност.

Глава II. Политика за защита на класифицираната информация в информационните системи

2.1. Условия и изисквания за сигурност на информационните системи

Политиката за защита на класифицираната информация в автоматизираните информационни системи и мрежи е съвкупност от споделени идеи и разбирания на ръководителите на организацията, благодарение на които се вземат решения и се реализира организационното поведение. Тя е ръководство (наставление) за вземане на решения, което се разработва на високите йерархични равнища в организацията, има относително постоянен характер и служи като ориентир за всички управленски нива.

На най - високото управленско ниво се вземат решения какви да са целите и общите намерения на организацията и нейната философия (кредо, идеология). Там се определят приоритетите и задачите. Едновременно се определят и разпределят ресурсите за тяхното постигане и принципите на изразходването им във времето.

Провеждане на организационни политика за защита на класифицираната информация е ефективно управление на сигурността на автоматизираните информационни системи и мрежи в рамките на трите базови императива - ресурси, оперативни способности и ключови процеси.

Защитата на класифицирана информация в автоматизираните информационни системи и мрежи касае всяка автоматизирана система за

обработка на информация и управление (АСОИУ), всеки компютър и всички компютърни мрежи, използвани и/или администрирани от дадена организационна единица, в които се създава, обработва, съхранява и пренася класифицирана информация.

Достъп до класифицирана информация в АИС или мрежи се предоставя само на лица, получили разрешение за достъп, при спазване на принципа „необходимост да се знае", освен ако този закон предвижда друго. Спазването на *принципа „необходимост да се знае"* се състои в:

- ограничаване достъпа само до определена класифицирана информация;
- ограничаване достъпа само за лица, чиито служебни задължения налагат това;
- ограничаване достъпа само за лица, на които са възложени конкретни задачи, налагащи такъв достъп.

Освен принципа „необходимост да се знае", контекстно приложение намират принципите:

- осигуряване на еднаква защита на класифицираната информация независимо къде и от кого се съхранява;
- предоставяне на достъп до класифицирана информация след извършено проучване за надеждност на лицето, което ще ползва достъпа;
- отчетност - цялостна регламентация на документалната сигурност на класифицирана информация;

- да се знае само колкото е необходимо за изпълнение на преките служебни задължения;
- непрекъснато проследяване движението на класифицирана информация;
- съхранение на толкова класифицирана информация, колкото е необходимо за изпълнение на преките служебни задължения.

Сигурността на автоматизираните информационни системи (АИС) или мрежи е система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежи. Тя включва прилагане на балансирана система от мерки за сигурност, осигуряващи изпълнението на Задължителни общи условия за сигурност на АИС или мрежи.

Задължителните общи условия за сигурност на АИС или мрежи обхващат компютърната, комуникационната, криптографската, физическата и персоналната сигурност, сигурността на самата информация на всякакъв електронен носител, както и защитата от паразитни електромагнитни излъчвания, определени в наредба, приета от Министерския съвет по предложение на министъра на вътрешните работи. Тези условия включват (фиг. 4)

Фиг. 4. Задължителни общи условия за сигурност на АИС или мрежи

1. органите по сигурността на АИС или мрежи;

2. условията и реда за извършване на комплексна оценка на сигурността и издаване на сертификати за АИС или мрежи, наричани по-нататък акредитиране;

3. задължителните общи изисквания за сигурност на АИС или мрежи в областта на (фиг. 5):

а) физическата сигурност;

б) персоналната сигурност;

в) документалната сигурност;

г) комуникационната сигурност;

д) криптографската сигурност;

е) защитата от паразитни електромагнитни излъчвания;

ж) компютърната сигурност.

За всяка АИС или мрежа, в която се създава, обработва, съхранява и пренася класифицирана информация, се изготвят Специфични изисквания за сигурност (СИС). Те се определят от ръководителя на организационната единица по предложение на служителя по сигурността на информацията. Тези изисквания подлежат на утвърждаване от дирекция Защита на средствата за връзка на Министерството на вътрешните работи. Всички последващи промени в тях се утвърждават от дирекция Защита на средствата за връзка на Министерството на вътрешните работи.

Фиг. 5. Задължителни общи изисквания за сигурност на АИС или мрежи

Специфичните изисквания за сигурност на АИС или мрежи се формулират по време на най-ранния стадий от проектирането на системата и се детайлизират и развиват в процеса на разработване и изпълнение на проекта. Степента на детайлизация зависи от сложността на системата или мрежата, от режима на сигурност, в който се експлоатира, и от нивото на класификация на обработваната информация. В своя завършен вид СИС определят как се постига, управлява и контролира сигурността на АИС или мрежата.

В отделните етапи на разработка и експлоатация на АИС или мрежата СИС изпълняват различни функции:

1. в етапа на **планиране** СИС представляват **Схематично описание на глобалната и локалната среда за сигурност**, в които ще се експлоатира системата, с постепенна детайлизация на изискванията за сигурност;

2. в етапа на **разработка или доставка** се детайлизират техническите аспекти на СИС, което спомага за правилната спецификация на системата или мрежата;

3. преди комплексната оценка СИС са в завършен вид и са основа за формулиране на **Процедурите за сигурност;**

4. в етапа на **експлоатация** СИС определят границите на отговорност на ОРЕ и на останалия състав, действащ в локалната и глобалната среда за сигурност;

5. в етапа на прекратяване на експлоатацията СИС се ползват за определяне на **действията, които трябва да се предприемат**

с цел запазване сигурността на информацията.

Специфичните изисквания за сигурност в завършен вид съдържат:

1. подробно описание на АИС или мрежата по отношение на:

• формата на представяне и нивото на класификация на информацията;

• групите потребители според нивото на достъп и начина на взаимодействие със системата;

• физическата среда за работа;

• функционалните елементи, включително архитектура, интерфейси и външни връзки;

2. описание на специфичните заплахи, уязвимостите на АИС или мрежата, режима за сигурност при експлоатация на системата, изискванията към физическата и техническата среда;

3. описание на глобалната, локалната и електронната среда за сигурност на АИС или мрежата;

4. подробно описание на мерките за сигурност относно:

а) управлението на достъпа, включително физическия, и определяне автентичността на потребителите;

б) отчетността на действията на отделните потребители и възможностите за проверка на валидността на тези действия;

в) предотвратяване на възможността за нерегламентиран достъп до информация, включително при повторно използване обектите на системата;

г) съхраняване интегритета на информацията;

д) осигуряване достъпност на информацията;

е) пренасянето на информацията;

ж) други специфични рискове;

5. управление на сигурността, включително при прилагане на разработените процедури по сигурността, конфигурационния контрол, поддръжката, разработването на документи по сигурността, обучението, случаите, в които се налага допълнително акредитиране;

6. описание на мерките за сигурност при критични ситуации;

7. описание на мерките за сигурност при прекратяване на експлоатацията на АИС или мрежата.

При необходимост от по-детайлно разработване на отделните аспекти на сигурността ОАС може да изисква допълнителни СИС за тези аспекти.

Преди въвеждане в експлоатация на АИС или мрежи дирекция Защита на средствата за връзка на Министерството на вътрешните работи извършва комплексна оценка на сигурността им съгласно изискванията на ППЗЗКИ и издава сертификат по образец. Ръководителят на организационната единица, в която се използват АИС или мрежи за обработка на класифицирана информация, по предложение

на служителя по сигурността на информацията назначава или възлага на назначени служители от административното звено по сигурността и охраната функции по контрола за спазване на изискванията за сигурност на тези системи или мрежи.

Не се допуска създаване, обработване, съхраняване и пренасяне на класифицирана информация в АИС или мрежи без наличието на издаден сертификат за тези АИС или мрежи. Не се допуска включването на АИС или мрежи, предназначени за създаване, обработка, съхраняване и пренасяне на класифицирана информация към публични мрежи като Интернет и други подобни електронни комуникационни мрежи.

2.2. Управленски мерки за защита на класифицираната информация във АИС и мрежи

Главната цел на мерките, предприети на управленско ниво, е да се сформира програма за работа в организационната единица по отношение на информационната сигурност, да се осигури изпълнението, като се отделят необходимите ресурси и се осъществява последващ контрол. Основа на тази програма е политиката за сигурност, която отразява подхода на организационната единица към защитата на своите информационни масиви.

Политиката за информационната сигурност и защита на класифицираната информация е съвкупност от закони, принципи, правила и норми на поведение, определящи методите и средствата за вземане на решения за защитата на класифицирана информация в процесите на

нейното създаване, обработка, съх- ракние, ползване и обмен, в границите на дадената система. В частност, правилата определят кога потребителят може да работи с определени данни. Колкото по - надеждна е дадена информационна система, толкова по - дисциплинираща разнообразна е политиката за сигурност. В зависимост от формулираната политика се избират конкретните методи и средства за гарантиране на сигурността й.

Политиката за информационната сигурност и защита на класифицираната информация е активен компонент на защитата, включващ в себе си резултатите от анализа на възможните заплахи, сценарии за реализацията им, оценката на риска и избор на методи и средства за противодействие. Тя поддържа интересите на субектите на автоматизираните информационни системи и мрежи и допринася за постигане на техните цели.

Политиката за информационна сигурност и защита на класифицираната информация не е самоцелна или рефлексивна проява по отношение на някакви заплахи. Тя включва система (комплекс) от знания и технологии за рационално използване на информационните инфраструктури и ресурси със стратегическа цел - защита на жизненоважните интереси на личността, обществото и държавата от заплахи в информационното пространство. На стратегическо равнище тези интереси включват:

- опазване на националния суверенитет в националното информационно пространство;
- създаване на благоприятни условия за материално,

духовно и интелектуално процъфтяване на нацията;

- развитие на националния научен и образователен потенциал и разцвет на националната култура.

Оперативната цел на тази политика е да се подобри защитеността на класифицираната информация в рамките на държания суверенитет, при спазване на конституционното право на всеки субект да търси, получава и разпространява информация. Осъществяването на това право може да се ограничава дотолкова, доколкото не може да бъде насочено срещу правата и доброто име на други граждани, както и срещу националната сигурност, обществения ред, народното здраве и морал.

По своята същност, провеждането на политика за информационна сигурност и защита на класифицираната информация е държавна дейност, произтичаща от възприетия общополитически курс, осигуряващ най -благоприятни условия за развитие на обществото, държавата, личността и гарантиращ националните интереси в информационното пространство чрез установяване на оптимално съотношение между структурните елементи на сигурността. За да ре-ализират политиката за информационна сигурност, субектите на изпълнителната, законодателната и съдебната функция на държавна власт все повече се нуждаят от ефективни информационни инфраструктури, подпомагащи вземането на управленски решения. В тези инфраструктури има множество уязвими места, които могат да бъдат атакувани и разрушени от специфични сили с голяма информационна мощ.

В началото на XXI век тази заплаха се превърна в една от най - сериозните за националната сигурност на страната. Ускореното внедряване на информационни технологии ще води до все по - засилваща се зависимост на отделната личност, обществото и държавата от тях. Това ще разширява възможностите за употреба на информационни средства за насилие, т.е. ще засилва инфраструктурната уязвимост на обществото. Тази уязвимост разкрива нови възможности за постигане на крайни политически цели.

Това става чрез нанасяне на неприемлив ущърб в информационното пространство, което доскоро не се считаше за област със стратегически рискове и заплахи.

Увеличаването на значението на информационната компонента на сигурността налага да се разработи ефективна политика за акумулиране и използване на информационна мощ с цел отразяване на заплахите в информационното пространство.

От практическа гледна точка политиката за информационната сигурност и защита на класифицираната информация може да се раздели на три нива.

Към политиката за информационна сигурност и защита на класифицираната информация на високо (стратегическо) ниво може да се отнесат решения, които имат отношение към цялата организация. Те се вземат от ръководството на организацията и са с по-общ характер, като например:

- Решение да се проектира или преразгледа комплексна

програма за защита на информацията.

- Да се формулират целите, които преследва организацията в областта на защитата на класифицираната информация.
- Да се осигури база за спазване на законите и наредбите.
- Да се систематизират управленските решения по въпросите за реализация на програмите за защита, които са валидни за цялата организация.

Целите на организацията в областта на информационната сигурност на това първо ниво се формулират с термините конфиденциалност, достъпност и интегритет. Към това ниво на управление се отнасят защитата на ресурсите и координацията при използването на тези ресурси, обособяване на специален персонал за защита на критично важни системи, поддържане на контактите с други организации и пр.

Политиката за сигурност от това ниво има връзка с три аспекта на законосъобразност и изпълнителска дисциплина. Първо, организационната единица е длъжна да спазва съществуващите закони. Второ, трябва да контролира действията на лицата, които отговарят за изработване на програмите за сигурност. И накрая, необходимо е да се осигури определена степен на отговорност на персонала.

Политиката за информационна сигурност и защита на класифицираната информация на средно (оперативно) ниво касае въпроси, които имат отношение към отделни аспекти на защитата на информацията. Пример за такива въпроси е достъпът до Интернет (как да се съчетае правото да получаваш информация със защитата от външни

заплахи), използване от потребителите на неофициално програмно осигуряване и т.н. Политиката за сигурност на това ниво има отношение към изброените по-долу теми:

- **Описание на аспекта.** Под описание на аспекта се разбира описанието на заданието за конкретните изисквания към мрежата, с каква информация ще се работи, с какви ресурси се разполага, на какви изисквания за защита трябва да отговори системата и т.н.
- Обхвата и нивото на сигурността на мрежата зависи от конкретната работна среда. Например за мрежа, съхраняваща данните на важно държавно учреждение, трябва да има по-висока степен на защита, отколкото мрежа, обединяваща компютрите на една малка фирма. Въпреки това, мрежовата сигурност изисква изчерпателен набор от правила и политики за сигурност, съставен така, че нищо да не бъде оставено на случайността.
- **Сфера на използване.** Отговаря на въпросите къде, кога, как, по отношение на кого и какво се приема дадената политика за сигурност.
- **Позиция на организацията по дадения аспект.** Към тази тема могат да се отнесат целите на организацията по отношение на защитата на класифицираната информация. Най - добрите политики за сигурност на данните използват превантивния подход. Чрез предотвратяване на възможността за неоторизиран достъп данните ще останат защитени.
- **Права и задължения на лицата, отговарящи за**

провеждането на политиката за сигурност. Тези права и задължения се определят със Закона за защита на класифицирана информация и съпътстващите го поднормативни документи. Политиките определят насоките и правилата, които могат да бъдат от полза на администраторите и потребителите при възникване на непредвидени ситуации в мрежата. Например, ако трябва да се проверяват дискети от друг компютър, е необходимо да се опишат процедурите за проверка. Ако не трябва да се използват неофициални програмни продукти, е необходимо да се знае кой отговаря за изпълнението за това правило и т.н. Най - общо групите хора, които имат отношение към сигурността на информацията в една система или мрежа, са: ръководителите, системни инженери, системни администратори, системни организатори и потребители. Техните права и задължения могат накратко да се опишат, както следва:

- Ръководителят трябва да държи в полезрението си въпросите по защитата на информацията; да контролира действията на подчинените си по този въпрос; да отчита рисковете и заплахите; да информира администраторите за всяка промяна на статуса на работниците - смяна па длъжност, уволнение и пр.
- Администраторът на мрежата трябва ежедневно да следи и анализира информацията, отнасяща се за мрежата като цяло; да информира ръководството за ефективността на съществуващата политика за сигурност, както и за опити да бъде нарушена защитата; периодически да извършва проверки за надеждността на защитата на локалната мрежа и т.н.

- Потребителите, от своя страна, трябва да се запознаят и спазват законовите разпоредби и вътрешноведомствените правила на политиката за сигурност, да използват достъпни защитни механизми за осигуряване на конфиденциалността на своята лична информация, да знаят слабостите, които се използват за нерегламентиран достъп и проникване в системата, да следят за такива опити и своевременно да информират компетентните лица и пр.
- **Законосъобразност.** Политиката за сигурност на една организация трябва да съдържа общо описание на забранените действия и наказанията за тях. Случаите на нарушения от страна на персонала трябва да се разглеждат от ръководството и да се предприемат наказателни мерки, включително и уволнение.
- При определяне на политиката за сигурност, трябва да се знае към кого може да се обръщаме за разяснение, помощ и допълнителна информация.

Политиката за сигурност на най - ниско (тактическо) ниво касае конкретното програмно осигуряване. За разлика от предишните две нива тя е доста по - детайлна. Ето няколко примера на въпроси, па които трябва да се отговори при определяне на политиката за сигурност на това ниво:

- При какви условия могат да се четат и изменят данните в информационната система?
- Кой има право на достъп до обектите, поддържащи програмното осигуряване?

Формулирането на целите на политиката па най-ниското ниво може да се основава на съображенията за конфиденциалност, достъпност и цялостност, но тези цели трябва да бъдат конкретно формулирани.

От целите произтичат правила за защита на информацията, описващи кой, при какви условия и какво може да върнш. Колкото са по - детайлни правилата, толкова по - лесно е да се изпълняват програмно-техническите изисквания. От друга страна много строгите правила може да пречат на работата на потребителите. Затова ръководството трябва да намери разумен компромис, при който за приемлива цена може да се осигури приемливо ниво на защита, без да се ограничават служителите.

2.3. Сигурност на АИС и мрежи

2.3.1 Колективни действия

За да е ефективна системата за информационна сигурност, са необходими общи усилия, включващи участието, разбирането и подкрепата на всички служители, които работят с информация и информационни системи. Поради необходимостта от работа в екип, изложената по-долу политика изяснява отговорностите на всички служители и действията, които те трябва да предприемат, за да окажат помощ при защитата на информацията и информационните системи на организацията. В настоящата тема се описват пътищата за предотвратяваше и реагиране на различни заплахи за информацията и информационните системи, включително неразрешен достъп, разкриване, размножаване, изменение, присвояване, разрушаване, загубване, злоупотреба и отказ при ползване на информация.

Обхванат персонал

Всички служители на организацията, без значение от техния статус (ръководители, специалисти, консултанти, външни експерти и т.н.), трябва да са запознати, да са съгласни и да изпълняват политиката за информационна сигурност, изложена по-долу. Служителите, които многократно или преднамерено нарушават тези и други положения за информационна сигурност, подлежат на дисциплинарни действия, включително и уволнение.

Обхванати системи

Описаната по-долу политика касае всяка автоматизирана система за обработка на информация и управление (АСОИУ), всеки компютър и всички компютърни мрежи, използвани и/или администрирани от организацията, в които се създава, обработва, съхранява и пренася класифицирана информация. Както беше възприето по-горе, наричаме тези системи: **АИС или мрежи,** в съответствие с публикуваните държавни нормативни документи.

Автоматизирана информационна система (АИС) е съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяване на функции по създаването, съхраняването, обработването, ползването и обмена на класифицирана информация в границите на системата. Границите на системата се определят от органа работещ по сигурността (ОРЕ). Автоматизираната информационна система може да бъде изградена и на основата на една или

повече отделни работни станции, несвързани в мрежа, които са в отговорността на ОРЕ.

Автоматизирана информационна мрежа (или само **мрежа)** е съвкупност от технически и програмни средства, методи и ако е необходимо, персонал и процедури, организирани за осъществяване обмен на данни (информация) между две или повече АИС или в рамките на една АИС.

Изложената политика важи за всички платформи (операционни системи), за компютърни системи от всякакъв вид (от персонални компютри до големи изчислителни машини) и всички приложни системи (независимо дали са собствена разработка или поръчка на външен изпълнител), в които се събира, съхранява, обработва и разпространява класифицирана информация. Тя обхваща само такива компютри и/или мрежи. Както беше отбелязано по - горе, съгласно българското законодателство класифицирана информация е „информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация“.

Глобална среда за сигурност на АИС или мрежата е средата, в която **е** разположена АИС или мрежата и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на служителя по сигурността на информацията на организационната единица и са извън контрола на ОРЕ.

Локална среда за сигурност на АИС или мрежата е средата, в която е разположена АИС или мрежата и в която са приложени

мерки за физическа, персонална и документална сигурност, които са в отговорността на Органа по развитие и експлоатация на АИС или мрежи (ОРЕ).

Обект на АИС или мрежа (или само обект) е пасивен елемент на АИС или мрежата, който съдържа или приема информация. **Субект на АИС или мрежа** (или само субект) е активен елемент на АИС или мрежата (лице, процес или устройство), който осъществява обмен на информация между обектите или изменение в състоянието на системата или мрежата.

Създаване, обработване, съхраняване или предоставяне на класифицирана информация е създаването, маркирането, регистрирането, съхраняването, ползването, предоставянето, трансформирането и разсекретяването на класифицирана информация.

2.3.2. Организационни мерки за защита на класифицираната информация в АИС и/или мрежи

Тези мерки са ориентирани към хората. Именно хората формират режима на защита и те се оказват главната заплаха, затова човешкият фактор заслужава първостепенно внимание. Заедно с това към тези мерки се отнася и организацията на физическата защита и документалната сигурност.

Контролът на доверието към персонала започва с приемането на служителя на работа и дори преди това - при съставянето на длъжностната характеристика. Още на този етап е необходимо да се привлече специалист по защита на информацията, който да определи

компютърните привилегии за тази длъжност. Съществуват два принципа, които трябва да се вземат под внимание:

Принцип на разделение на отговорностите. Този принцип е задължителен от гледна точка на ЗЗКИ, т.е. за една информационна ценност отговаря един потребител. Ролите и отговорностите се разпределят така, че един човек да не може да наруши критически важен за организационната единица процес.

Принцип на минимизация на привилегиите. Той предписва как да се дават на потребителите само тези права на достъп, които са им необходими за изпълнение на служебните задължения.

В нашата нормативна база подробно и категорично са определени критериите за издаване на разрешение на лице за работа с класифицирана информация, като кандидатите се проверяват щателно от съответните служби за сигурност, извършват се проверки и/или беседи, за да не се допусне назначаване на лица, извършили престъпления, душевно болни или ненадеждни от гледна точка на опазване на тайната. Процедурата е дълга и зависи от нивото на класификация на информацията за достъп, до която кандидатства лицето.

Когато кандидатът е одобрен, той трябва да премине обучение, да бъде запознат с нормативната база и да му бъде проведен изпит по защита на класифицираната информация. Законът изисква тези процедури да са извършени преди встъпването в длъжност и преди да бъде включен в списъка с входящи имена, пароли и допуски. След този момент започва неговото администриране, протоколиране и анализ на действията

му като потребител. Когато един потребител напусне организацията, особено в случаите на конфликт между сътрудника и организацията, е необходимо да се действа максимално оперативно. Възможно е и физическо ограничаване на достъпа до работното място.

Понякога обслужването и администрирането на компоненти от АИС и/или мрежи се поема от външни организации. Това може да създаде допълнителни слабости в защитата, които е необходимо да се компенсират със засилен контрол на достъпа или с обучение на собствени служители. Проблемът за обучението на персонала е един от основните, що се отнася до защитата на информацията. Ако служителят не е запознат с политиката за сигурност, той не може да се стреми към постигането на формираните цели. Ако не знае мерките за сигурност, не може да ги съблюдава. Напротив, ако знае, че неговите действия се контролират, е възможно да се въздържи от нарушение. Обучението трябва да се провежда регулярно и всеки път по различен начин, иначе ще се превърне във формалност и ще загуби своята ефективност.

Организиране поддържането на работоспособност. През време на експлоатацията на АИС и/или мрежите се крият най - големите опасности за нейната сигурност. Неволните грешки на системния администратор и на потребителите могат да доведат до повреди на апаратурата, разрушаване на програмите и данните, в най - добрият случай се допускат слабости, които повишават рисковете от заплахи. Скъпите мерки за сигурност губят своя смисъл, ако са недобре документирани, в конфликт с други програмни продукти, а паролите на системния

администратор не се сменят от момента на инсталация, т.е. за осигуряване на по - добра защита на информацията в АИС и мрежите е необходима ежедневна дейност по поддръжката.

Поддръжката на потребителите например се състои в консултиране и оказване на помощ при разрешаването на различни проблеми. Важно е в потока от въпроси на потребителите да се доловят проблеми, свързани с информационната сигурност. Практически полезно е администраторите да записват въпросите на потребителите, за да могат да извлекат най-често възникващите проблеми и да направят бележки със съвети за най -разпространените.

Поддръжката на програмното осигуряване е съществен елемент от осигуряването на цялостност на информацията. Ако потребителите имат право сами да си инсталират програмни средства, това крие опасност от заразяване с вируси. Големи опасности крие и включването към интернет. В ЗЗКИ категорично се забранява свързването с глобални мрежи на АИС и/или мрежи, в които се създава, съхранява, обработва и пренася класифицирана информация. Въпреки това трябва да се контролират самоволните действия на потребителите по програмните ресурси и да се осъществява контрол и за нерегламентирани промени в програмите и правата за достъп до тях. От практиката е доказано, че колкото е по -автоматизиран е един процес, толкова по - малко вероятни са грешките, така че може да се твърди, че автоматизацията е стълб на сигурността.

За възстановяване на програмите и данните след аварии е задължително да се архивира. И тук е добре процесът да се автоматизира, а копията да се съхраняват на безопасно място, защитено от пожари и други заплахи.

2.4. Органи, работещи по информационната сигурност

Те са показани по - долу на фиг. 6.

Ръководителят на организационната единица ръководи, организира и контролира дейността по защита на класифицираната информация. Той е отговорен за създаването, установяването и поддръжката на политиката (стратегията) за защита на класифицирана информация и в частност, за внедряването на стандартите, ръководствата и процедурите, касаещи цялата организация.

Ръководителят на организационната единица назначава **служител по сигурността на информацията** след получаване на разрешение за достъп на това лице до класифицирана информация, издадено от ДКСИ. По изключение, в зависимост от нивото и обема на класифицираната информация, ръководителят на организационната единица може да изпълнява функциите на служител по сигурността на информацията, ако отговаря на описаните в закона изисквания. Служителят по сигурността на информацията е пряко подчинен на ръководители на организационната единица.

Фиг. 6. Органи, работещи по информационната сигурност

В изпълнение на функциите си по ЗЗКИ Държавната комисия по сигурността на информацията (ДКСИ), службите за сигурност и службите за обществен ред, както и съответните организационни единици създават, обработват, поддържат и съхраняват информационни фондове.

В съответствие с дадените от законодателя пълномощия:

Държавната комисия по сигурността на информацията (ДКСИ) осъществява общ контрол:

1. по защита на класифицираната информация, съхранявана, обработвана и пренасяна в АИС или мрежи;

2. на процеса по акредитиране на АИС или мрежи. Орган по акредитиране на сигурността на АИС или мрежи (ОАС) е Дирекция Защита на средствата за връзка (ДЗСВ) на ДАНС.

Ръководителят на организационната единица, в която се експлоатират или се предвижда изграждането на АИС или мрежи за обработка на класифицирана информация, по предложение на служителя по сигурността на информацията назначава в административното звено по сигурността служител по сигурността на АИС или мрежи или възлага на назначени служители от същото звено неговите функции.

Служителят по сигурността на АИС или мрежи е отговорен за установяването на политиката за сигурност на АИС или мрежи в организационната единица. Той определя изискванията за сигурност към АИС или мрежи, произтичащи от общата политика за сигурност на организационната единица, координира изготвянето на специфичните изисквания за сигурност на АИС или мрежи, процедурите за сигурност и на изработените на тяхна основа експлоатационни документи по сигурността, координира обучението по сигурността на АИС или мрежи, осъществява контрол за спазване на изискванията за сигурност, разследва обстоятелствата, свързани с компрометиране на сигурността, и докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОАС.

Органът по развитие и експлоатация на АИС и мрежи в организационната единица:

- участва в определянето на политиката за сигурност на АИС или мрежи в организационната единица;
- изготвя документите по сигурността на АИС или мрежата;

- осигурява изпълнението на изискванията за акредитиране на АИС или мрежи и прави заявки за допълнително акредитиране на АИС или мрежата, когато това е необходимо;
- участва в определянето на мерките за сигурност и границите на отговорност при осъществяване на връзки с други АИС или мрежи;
- прави предложение за възлагане функции на администратор по сигурността на АИС или мрежата и осигурява подготовката му;
- организира и провежда обучение по сигурността в АИС или мрежи на служителите в ОРЕ и на потребителите на АИС или мрежата;
- прилага одобрените мерки за сигурност в АИС или мрежата;
- прави преглед на свързаната със сигурността документация периодично или при предложени промени в техническото или програмното осигуряване, връзките с други АИС или мрежи, режима за сигурност, нивото на класификация на информацията или при други дейности, които могат да повлияят на сигурността на АИС или мрежата, като за резултатите информира служителя по сигурността на АИС или мрежи;
- участва заедно със служителя по сигурността на АИС или мрежи в установяването на обстоятелствата, свързани с компрометиране сигурността на АИС или мрежи.

Със заповед на ръководителя на организационната единица по предложение на ОРЕ, съгласувано със служителя по сигурността на информацията, се възлагат функции на **администратор по сигурността на АИС или мрежата.** Той е от състава на ОРЕ или от друго звено в организационната единица, имаща отношение към АИС или мрежата. При необходимост могат да се определят повече от един администратор по сигурността, отговарящи за обособени части, като един от тях се определя за администратор по сигурността на цялата АИС или мрежа. Задълженията на администратора по сигурността на АИС или мрежата и на администратора на АИС или мрежата трябва да са ясно разграничени.

Администраторът по сигурността на АИС или мрежата трябва да има разрешение за достъп до най - високото ниво на класифицирана информация в АИС или мрежата. Когато автоматизираната мрежа обхваща няколко организационни единици, всяка от тях определя администратор по сигурността за нейната част от мрежата.

Администраторът по сигурността на АИС или мрежата: -

- участва в изготвянето и актуализирането на процедурите по сигурността на АИС или мрежата;
- изготвя експлоатационни документи по сигурността на АИС или мрежата за обслужващия персонал и потребителите на базата на утвърдените процедури за сигурност;
- изпълнява възложените му процедури за сигурност в АИС или мрежата:
- периодично информира обслужващия персонал и

потребителите по въпросите на сигурността на АИС или мрежата;

- осигурява на потребителите достъп до ресурсите на АИС или мрежата в съответствие с предоставените им права;
- осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в АИС или мрежата, като:

а) следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на АИС или мрежата;

б) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в АИС или мрежата;

в) следи за правилното функциониране на механизмите за сигурност:

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата и при констатиране или при съмнения за компрометиране на сигурността докладва на ОРЕ и на служителя по сигурността на АИС или мрежи;

д) осигурява резервиране и съхраняване на одитните записи в определените срокове;

- участва заедно със служителя по сигурността на АИС или мрежи и с ОРЕ в установяването на обстоятелствата, свързани с компрометиране на сигурността на АИС или мрежата;
- изпълнява функциите на администратор по криптографска защита на информацията, ако в АИС или мрежата се

прилагат криптографски методи и средства.

Потребител на АИС или мрежата е лице, което:

- има издадено разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която има право да работи в АИС или мрежата;
- което е преминало обучение в областта на сигурността на АИС или мрежа;
- на което са предоставени права за достъп до ресурсите на АИС или мрежа.

Потребителите в АИС или мрежа изпълняват задълженията, посочени в експлоатационните документи по сигурността на АИС или мрежа. Те изпълняват указанията на администратора по сигурността на АИС или мрежа, свързани със сигурността на системата или мрежата и уведомяват администратора по сигурността за всички случаи или съмнения за компрометиране сигурността на АИС или мрежата.

2.5. Класифицирана информация

Както беше отбелязано по - горе, **класифицирана информация** по смисъла на българското законодателство е „информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация". Държавните субекти формулират **Списък на категориите информация, подлежащи на класификация като държавна тайна.**

Държавна тайна е информацията, определена в този списък. Нерегламентираният достъп до нея би създал опасност за или би увредил

интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

Служебна тайна е информацията, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правнозащитен интерес. Информацията, подлежаща на класификация като служебна тайна, се определя със закон. Съответно, ръководителят на организационната единица обявява със заповед списъка на категориите информация, подлежащи на класификация като служебна тайна.

Ръководителят на съответната организационна единица в рамките на закона обявява списък на категориите информация за сферата на дейност на организационната единица. Редът и начинът за обявяване на списъка се определят в правилника за прилагане на ЗЗКИ.

Чуждестранна класифицирана информация е класифицираната информация, предоставена от друга държава или международна организация по силата на международен договор, по който Република България е страна.

Класифициране на информацията е дейност, при която се установява;

1. попада ли конкретната информация в списъка на категориите информация съгласно приложение № 1 към чл. 25 на ЗЗКИ или в списъка по чл. 26, ал. 3 на ЗЗКИ;

2. налице ли е заплаха или опасност от увреждане или увреждане на интересите по т. 1 в съответната степен, определена съгласно чл. 28, ал. 2 и чл. 26, ал. 1 във връзка с § 1, т. 15 от допълнителните разпоредби на ЗЗКИ;

3. дали нерегламентираният достъп до нея би създал опасност за интересите по т. 1. 4, налице ли са обществените интереси, подлежащи на защита съгласно чл. 25 и 26 във връзка с § 1, т. 13 и 14 от допълнителните разпоредби на ЗЗКИ. Информацията се класифицира според собственото й съдържание, а не според класификацията на информацията, на която се базира, или на информацията, за която се отнася.

2.6. Нива на класификация за сигурност на информацията

Нивата на класификация за сигурност на информацията и техният гриф за сигурност са: ***„Строго секретно“; „Секретно“; „Поверително“; „За служебно ползване“.***

Информацията, класифицирана като държавна тайна, се маркира с **гриф за сигурност:**

„Строго секретно“ - в случаите, когато нерегламентиран достъп би застрашил в изключително висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл ла създаде опасност от възникване на непоправими или изключително големи вреди, или да причини такива

вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

„Секретно“ - в случаите, когато нерегламентиран достъп би застрашил във висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от зъзникване на трудно поправими или големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституциошю установения ред.

„Поверително“ - в случаите, когато нерегламентиран достъп би застрашил суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

„За служебно ползване“ - информацията, класифицирана като служебна тайна.

С цел осигуряване на допълнителна защита, когато това се налага от характера на информацията или когато е предвидено в международни договори, по които Република България е страна, ДКСИ по предложение на министъра на вътрешните работи, министъра на отбраната или директорите на службите за сигурност може да определи с решение:

- допълнителни маркировки на материали и документи с по-високо ниво на класификация от „Строго секретно“;
- специален ред за създаване, ползване, размножаване, предоставяне и съхраняване на тези материали и документи;
- кръга на лицата с право на достъп до тези материали и документи.

Приравняването на нивата на класификация за сигурност на получаваната чуждестранна класифицирана информация или на предоставяната от Република България на друга държава или международна организация такава информация в изпълнение на влязъл в сила международен договор за Република България и за съответната чужда държава или международна организация се осъществява в съответствие с разпоредбите на договора.

Ръководителят на съответната организационна единица обявява със заповед списъка на категориите информация, подлежащи на класификация като служебна тайна. Ръководител на държавен орган, управляващ правата на собственост на държавата в организационни единици - търговски дружества с повече от 51 на сто държавно участие, обявява със заповед общия списък на категориите класифицирана информация, съставляваща служебна тайна за отрасъла, подотрасъла или търговската дейност. Този списък съдържа само категории информация, създавана, обработвана и съхранявана в организационната единица, определени като тайна в специални закони.

Ръководителят на организационната единица определя със заповед списък на длъжностите или задачите, за които се изисква достъп до класифицирана информация, представляваща служебна тайна. Той изпраща копие на този списък в ДКСИ.

2.7. Маркиране, съхраняване и защита на информацията

Ръководителите на организационните единици организират обучението на подчинените им служители за условията и реда за маркиране на информацията (поставянето, промяната и заличаването на грифовете за сигурност) под методическото ръководство на ДКСИ. Редът и начинът за маркиране, съхраняване и защита на класифицирана информация се определят с Правилника за прилагане на ЗЗКИ.

Политиката за информационната сигурност и защита на класифицираната информация е съвкупност от закони, принципи, правила и норми на поведение, определящи методите и средствата за вземане на решения за защитата на класифицирана информация в процесите на нейното създаване, обработка, съхранение, ползване и обмен, в границите на дадената система. В частност, правилата определят кога потребителят може да работи с определени данни. Колкото по - надеждна е дадена информационна система, толкова по-дисциплинираща разнообразна е политиката за сигурност. В зависимост от формулираната политика се избират конкретните методи и средства за гарантиране на сигурността й.

Политиката за информационната сигурност и защита на класифицираната информация е активен компонент на защитата, включващ в себе си резултатите от анализа на възможните заплахи,

сценарии за реализацията им, оценката на риска и избор на методи и средства за противодействие. Тя поддържа интересите на субектите на автоматизираните информационни системи и мрежи и допринася за постигане на техните цели.

Политиката за информационна сигурност и защита на класифицираната информация не е самоцелна или рефлексивна проява по отношение на някакви заплахи. Тя включва система (комплекс) от знания и технологии за рационално използване на информационните инфраструктури и ресурси със стратегическа цел - защита на жизненоважните интереси на личността, обществото и държавата от заплахи в информационното пространство.

Глава III. Автоматизирани информационни системи за класифицирана информация

3.1. Автоматизирани информационни системи за класифицирана информация

Автоматизираните информационни системи са съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяването на функции по създаването, обработването, съхраняването, ползването и обмена на класифицирана информация в границите на дадена система.Тя може да бъде изградена и върху основата на една или повече отделни работни станции, който не са свързани в мрежа.

Мрежата това е съвкупност от технически и програмни средства, методи и ако е необходимо персонал и процедури, организирани за осъществяване на обмен на данни между две или повече АИС или в рамките на една АИС. Компютърните мрежи се разделят на две главни категории:

1. равноправни;
2. базирани на сървър.

При равноправната мрежа всичките компютри са равнопоставени. Мрежата няма конкретен администратор, а потребителите сами определят какви ресурси да поделят в мрежата. Системата за сигурност се състои в задаване на парола за всеки ресурс, като например

поделена директория или устройство. В равноправната мрежа всеки потребител настройва сам своята система за сигурност, поради което централизирания контрол е труден. За това, ако сигурността е важен фактор, се изгражда мрежа базирана на сървър. При тези мрежи, има компютър, работещ само като сървър, без да се използва като работна станция. С нарастването на размера на трафика на мрежите се появява нуждата от повече от един сървър. Разпределението на задачите между няколко сървъра позволява мрежата да работи по - ефективно. Сървърите на големите мрежи трябва да бъдат специализирани, за да задоволяват нуждите на потребителя.

Основното предимство на мрежите със сървър е че използването на данните може да се администрира и контролира централно. Сигурността може да се управлява от един администратор, който установява правилата за защита и ги прилага към всеки потребител от мрежата.

Комуникационната система е съвкупност от взаимосвързани комуникационни средства, криптографски средства и среда на разпространение на сигнала, предоставящи комуникационен ресурс на АИС или мрежа. Използваните технически и програмни средства за създаването на АИС, както и потребителската и системната информация в тях, са ресурсите на тази АИС. Мрежовите ресурси могат да се разделят на:

1. физически ресурси – оперативната памет, процесорът, входно изходните устройства и др.;

2. информационни ресурси – това са програмните продукти и данните, който се съхраняват и се обработват от физическите устройства.

Ресурсите на мрежите се използват за представяне на пакет от системни и потребителски услуги като:

1. Обмен на данни от различен тип;

2. Обмен на електронна поща в мрежата;

3. Търсене на услуги и ресурси по мрежата;

4. Комуникации между клиенти на мрежата;

5. Администриране, контрол, управление, защита и развитие на мрежата.

В съвременното технологично развитие използването на АИС е невъзможно без създаването на база данни. Базата данни представлява съвкупност от данни, организирани за общо ползване в рамките на различни изчислителни процеси. За тяхното създаване, поддържане и експлоатация се използват специални системи, наречени системи за управление на база данни чиито основни функции са:

1. Транслиране на схемата на база данни;

2. Създаване и верифициране на база данни;

3. Изпълняване на запитвания към база данни;

4. Актуализиране на данните в база данни;

5. Копиране и възстановяване на база данни.

6. Защитаване на база данни чрез управление на достъпа и криптографиране.

Създаването, обработването и съхраняването на класифицирана информация, както и използването на база данни с класифициран характер в АИС или мрежи не се различават по своята организация и методите си на работа от всички останали мрежи. Единствената разлика е в необходимостта от сериозно гарантиране на сигурността им и защитата от заплахи от нерегламентиран достъп.

Имаме две самостоятелни сфери на защита на информацията от нерегламентиран достъп:

1. На автоматизираните информационни системи.
2. На компютърните системи и мрежи.

Основните направления, в който преднамерената и непреднамерената човешка дейност могат да доведат до нерегламентиран достъп са:

1. Неизправностите и отказите на техническите средства;

2. Наличието на грешки в програмното осигуряване;

3. Излъчването на паразитни електромагнитни или акустични излъчвания;

4. Природните бедствия;

5. Авариите и катастрофите.

Всички те могат да доведат до нерегламентиран достъп във вид на нежелателно изтичане, модифициране или унищожаване на информация.

Нерегламентиран достъп до класифицирана информация е всяко:

1. разгласяване;
3. злоупотреба;
4. промяна;
5. увреждане;
6. предоставяне;
7. унищожаване на класифицирана информация.

Както и всякакви други действия, водещи до нарушаване на защитата и или до загубване на такава информация.

3.2. Нормативна база

При АИС или мрежи предназначени за създаване, обработка, съхраняване и пренасяне на класифицирана информация не се допуска тяхното включване към публични мрежи като Интернет и други подобни електронни комуникационни мрежи (ЗЗКИ чл. 94). Класифицираната информация в сертифицираните АИС и мрежи се маркират със съответното ниво на класификация за сигурност и се отчитат по реда на наредба приета от Министерски съвет по предложение на министъра на вътрешните работи. При изход на документи, съдържащи класифицирана информация трябва те да имат поставен гриф за сигурност и се завежда в регистратурата. Запис на документи се извършва само върху заведени на отчет носители в регистратурата и ако имат съответното или по-високо ниво на класификация (ППЗККИ). С наредбата за задължителни общи условия за сигурност на АИС се разглеждат: органите по тяхната сигурност, акредитирането им и видовете сигурност.

Общият контрол по защита на класифицирана информация в АИС или мрежа, и контрола по процеса на тяхното акредитиране се извършва от Държавната комисия по сигурността на информацията.

Самият орган по акредитиране е дирекция „Защита на средствата за връзка“ (ДЗСВ) на ДАНС. Функциите на този орган са :

- да дават препоръки и указания по сигурността на АИС или мрежи.
- да препоръчва стандарти и средства, който могат да се използват в АИС или мрежи за защита на класифицирана информация.
- утвърждава документите по сигурността на АИС или мрежи.
- извършват комплексна оценка на тяхната сигурност.
- издава сертификати за сигурност на АИС или мрежи.
- определят условията, при който следва да се извърши допълнително и ново акредитиране на АИС или мрежи.
- координира и контролира дейността по защита от паразитни електромагнитни излъчвания на техническите средства, обработващи, съхраняващи и пренасящи класифицирана информация.
- провежда обучението на служители по сигурността на АИС или мрежи.
- води регистър на сертифицираните АИС или мрежи.

Ръководителят на организационната единица, в която се експлоатират или се предвижда изграждането на АИС или мрежа за обработка на класифицирана информация, по предложение на служителя

по сигурността на информацията назначава в административното звено по сигурността служител по сигурността на АИС или мрежи или възлага на служители от същото звено.Той трябва да има разрешение за достъп до най - високото ниво на класифицирана информация в организацията. Неговите функции са:

- той е отговорен за установяването на политиката за сигурност на АИС или мрежи в организационната единица.
- определя изискванията за сигурност към АИС или мрежи, произтичащи от общата политика за сигурност на организационната единица.
- координира изготвянето на специфичните изисквания за сигурност на АИС или мрежи, процедурите за сигурност и изработените на тяхна основа експлоатационни документи по сигурността.
- координира обучението по сигурността на АИС или мрежи.
- осъществява контрол за спазването на тези изисквания.
- разследва обстоятелствата, свързани с компрометиране на сигурността в АИС или мрежи, и докладва за резултатите на служителя по сигурността на информацията в организационната единица, а той уведомява Органа по акредитиране (ДЗСВ –ДАНС).

Следващият орган по сигурността на АИС или мрежи е Органа по развитие и експлоатация на АИС или мрежи. Неговите функции са:

- да участва в определянето на политиката за сигурност на

АИС или мрежи в организационната единица.

- да изготвя документите по сигурността на АИС или мрежата.
- осигурява изпълнението на изискванията за акредитиране на АИС или мрежа и прави заявки за допълнително акредитиране на АИС и мрежа, когато това е необходимо.
- да участва в определянето на мерките за сигурност и границите на отговорност при осъществяване на връзки с други АИС или мрежи.
- прави предложение за възлагане функции за администратор по сигурността на АИС или мрежата и осигурява подготовката му.
- организира и провежда обучението по сигурността на АИС или мрежа на служителите в органа по развитие и експлоатация и на потребителите на АИС или мрежи.
- прилага одобрените мерки за сигурност .
- прави периодичен преглед на свързаната със сигурността документация или при предложени промени в техническото или програмното осигуряване, връзките с други АИС или мрежи, режима за сигурност, нивото на класификация на информацията или при други дейности, който могат да повлияят на сигурността на АИС или мрежата, като за резултатите уведомява служителя по сигурността на АИС или мрежа.
- участва заедно с служителя по сигурността на АИС или

мрежи в установяване на обстоятелствата, свързани с компрометиране на сигурността на АИС и мрежи.

В една организационна единица не може да има повече от един такъв орган, а в органите на държавната власт и местно самоуправление, в който са обособени повече от една организационна единица, може да бъде създаден един орган за няколко или за всички организационни единици. Със заповед на ръководителя на организационната единица по предложение на органа по развитие и експлоатация съгласувано със служителя по сигурността на информацията се възлагат функции на администратор по сигурността на АИС или мрежи. При необходимост може да се определят повече от един администратор, като всеки отговаря за обособени нейни части, като един от тях се определя за администратор по сигурността на цялата АИС или мрежа. Неговите задължения трябва да са ясно разграничени от задълженията на администратора на мрежата.Той трябва да е с най - високата степен на достъп до класифицирана информация в АИС или мрежата. Функциите на администратора по сигурността на АИС или мрежата са:

- да участва в изготвянето и актуализирането на процедурите по сигурността на АИС или мрежата.
- изготвя експлоатационни документи по сигурността на АИС или мрежата за обслужващият персонал и потребителите на базата на утвърдените процедури за сигурност.
- изпълнява възложените му процедури за сигурност на АИС или мрежи.

• периодично информира обслужващият персонал и потребителите по въпросите на сигурността на АИС или мрежи.

• осигурява на потребителите достъп до ресурсите на АИС или мрежите в съответствие с предоставените им права.

• осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в АИС или мрежата, като:

1. следи за спазването на мерките и процедурите за сигурност в зоните за сигурност в АИС или мрежата;

2. следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в АИС или мрежата;

3. следи за правилното функциониране на механизмите за сигурност;

4. управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата и при констатиране или при съмнения за компрометиране на сигурността докладва на органа по развитие и експлоатация;

5. осигурява резервиране и съхраняване на одитните записи в определените срокове.

• участва заедно със служителя по сигурността на АИС или мрежи и с органа по развитие и експлоатация в установяването на обстоятелствата, свързани с компрометиране на сигурността на АИС или мрежата.

• изпълнява функциите на администратор по криптографска защита на информацията, ако в АИС или мрежата се прилагат криптографски методи и средства.

Потребител в АИС или мрежа е лице:

• което има издадено разрешение за достъп до най-високо ниво за класификация за сигурност на информацията, с която има право да работи в АИС или мрежата.

• което е преминало обучение в областта на сигурността на АИС или мрежи.

• на което са предоставени права за достъп до ресурсите на АИС или мрежа.

Сигурността на АИС или мрежа, в която се създава, обработва, съхранява или пренася класифицирана информация, включва прилагане на балансирана система от мерки за сигурност.

3.3. Изисквания за сигурност на АИС с класифицирана информация

Физическата сигурност – сигурността на АИС или мрежи зависи от обкръжението, в което работят, следователно е необходимо да се предприемат мерки за защита на сградите и прилежащите територии, инфраструктурата и самите компютри. Мерките за физическо управление на достъпа позволяват да се контролира и при необходимост да се ограничават влизането и излизането на служители и посетители. Може да се контролира цялата сграда на организацията, както и отделни помещения

(зони за сигурност) - например тези в който са разположени комуникационната апаратура и сървърите. Средствата за физическа охрана са: охрана, прегради, видео наблюдение, обемни детектори и други. Важното е да се отделят компютрите от потока посетители или в краен случай да се направи така, че от прозорците и вратите да не се наблюдават екраните на мониторите и принтерите. При голяма централизирана система, в която много от данните са поверителни сървърите трябва да са физически обезопасени от случайно или умишлено повреждане. Най - простото решение е той да се заключи в отделна стая, до която достъпа да е ограничен. Така ще се гарантира сигурността му. Опасността от пожари е твърде голяма, а щетите после също, така че противопожарната защита е съществена част от физическата защита. Необходимо е в помещенията където има компютри да има противопожарна сигнализация и автоматични средства за пожарогасене.

Към поддържащата инфраструктура могат да се отнесат системите за електроснабдяване, водоснабдяване, топлоснабдяване, средствата за комуникация. Към тях трябва да има същите изисквания за достъпност и цялост, както и към информационните системи. За осигуряване на цялост е необходимо да се защити оборудването от кражби и повреди. Нерегламентираният достъп до данните може да се осъществи по различни начини: наблюдаване на екрана на монитора, четене на пакети, предавани по локалната мрежа, анализ на излъчваните електромагнитни вълни и други. Някой от способите за прихващане на данни са доста лесни, борбата с тях е трудна и скъпа. Физическата защита се базира на здравият разум,

който показва правилните решения. Зоните в който са разположени ресурсите на АИС или мрежа, където се създава, обработва, съхранява или пренася класифицирана информация или в който е възможен достъп до такава информация, се определят като зони за сигурност. Тези зони се защитават със съответните за най-високо ниво на класификация на информацията мерки, способи и средства за физическа сигурност, с цел да не се допуска нерегламентиран достъп. В рамките на зоните за сигурност се определят места за:

- компютърно и комуникационно оборудване.
- въвеждане и извеждане на документи във и от системата.
- център за управление на АИС или мрежа.
- работа с криптографски средства и ключове.
- библиотеки за компютърни носители на класифицирана информация и др.

Документална сигурност – тя е неизменна част от сигурността на класифицираната информация в АИС или мрежи. Всички документи, съдържащи класифицирана информация, който се създават, обработват, съхраняват и пренасят в АИС или мрежи, се идентифицират, маркират и контролират по подходящи начини. Маркировката на документите трябва да осигурява винаги еднозначна информация за нивото на класификация при работа с тях. Начините за идентифициране, маркиране и контролиране се определят в документите по сигурността на АИС или мрежа.

Извеждането на документи, съдържащи класифицирана информация, от сертифицирани АИС или мрежи се извършва в зоните за сигурност в съответствие с изискванията на Правилника за прилагане на закона за класифицирана информация. При създаване на документи, съдържащи класифицирана информация, от сертифицирани АИС или мрежи се спазват следните правила:

- отпечатаните документи трябва да имат поставен гриф за сигурност и се завеждат в регистратурата.
- запис на документи се извършва само върху заведени на отчет носители в регистратурата и ако имат съответното или по-високо ниво на класификация.

Материалните носители за многократен запис на класифицирана информация се водят на отчет в отделен регистър и се маркират с гриф за сигурност. Този гриф и регистрационния номер се поставят преди първоначалното използване на носителите за многократен запис. Върху тях се забранява записването на класифицирана информация с ниво на класификация, по - високо от обозначеното върху носителят. Документи, съдържащи класифицирана информация, се пренасят от една АИС или мрежа към друга, само ако получателя е АИС или мрежа, сертифицирана за ниво на класификация на информация, което е същото или по - високо от нивото на класификация на пренасяните документи. Информацията и материалите, които вече не се използват за осигуряване на достъп до ресурсите на АИС или мрежата се унищожават в съответствие с правилата в експлоатационната документация по

сигурността и по начин, който не допуска възстановяване на информацията.

Персонална сигурност - потребителите на АИС или мрежата трябва да имат разрешение за достъп до най - високото ниво за достъп на класификация за сигурност на информацията, с която имат право да работят в АИС или мрежата. А също така това условие важи и за системният персонал, както и лицата който участват в проектирането и изграждането на системата за сигурност на АИС или мрежата. Системният персонал и потребителите на АИС или мрежата преминават обучение по сигурността на АИС или мрежа. Тяхното обучение се провежда от Органа по развитие и експлоатация за различните категории служители. При успешно завършено обучение те се допускат до работа в АИС или мрежата. Правомощията на персонала се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на АИС или мрежата.

Компютърна сигурност – тя представлява система от мерки за сигурност, прилагани с цел да се осигуряват конфиденциалност, интегритет и достъпност на класифицираната информация в АИС или мрежа. Тези мерки за сигурност се реализират чрез възможностите на техническите и програмните средства на компютърните системи и на специализирани средства. Минималните изисквания за компютърна сигурност на АИС или мрежа включват:

- еднозначна идентификация и автентикация на потребителя, които трябва да предхождат всички останали негови

действия в АИС или мрежата.

- контрол на достъпа по преценка – осигуряване на достъпа до обектите на АИС или мрежата чрез предоставяне на правила за достъп въз основа на идентификацията на потребителя или неговата принадлежност към потребителска група. Правата за достъп се предоставят само от упълномощени потребители или от администратора по сигурността на АИС или мрежа. Механизмите за контрол трябва да осигуряват възможност за разделяне на потребителите и за достъп до информацията според принципа „необходимо е да се знае”.
- непрекъснат запис на събития, свързани със сигурността на АИС или мрежа (одитни записи). Записват се всички действия, свързани с контрола на достъпа, включително неуспешни опити за достъп, създаване или разрушаване на обекти или действия на оторизирани субекти, влияещи върху сигурността на информационната система.
- възможност за изучаване на одитните записи и установяване на свързаните със сигурността действия на отделните субекти на АИС или мрежа.
- обработка на обекти на АИС или мрежа така, че при следващото им разпределяне към субект на АИС или мрежа той не може да установи предишното им съдържание или да получи права за достъп на използвалите ги преди това субекти.
- защита от вредни програмни средства.

За осигуряване на минималните изисквания за сигурност се реализират програмни и технически механизми, спрямо които трябва да се

осъществява конфигурационен контрол и които трябва да са защитени от нерегламентиран достъп.

Комуникационна сигурност – представлява система от мерки за сигурност, прилагани с цел защита на класифицираната информация от нерегламентиран достъп при нейното пренасяне по комуникационни системи. Тази система включва защита с криптографски методи и средства, защита от излъчвания и защита при пренасяне на информацията. Комуникационните системи за пренос на класифицирана информация трябва да осигуряват механизми за:

- надеждна и защитена идентификация и автентикация на изпращача и на получателя на информацията, които да се извършат преди началото на преноса на информацията.
- осигуряване на конфиденциалност, интегритет и достъпност на пренасяната информация.
- потвърждаването на получаването на информацията.

Класифицирана информация се пренася по комуникационни системи извън зоните за сигурност на АИС или мрежи, когато е защитена с криптографски средства. АИС или мрежи, в който се създава, обработва, съхранява и пренася класифицирана информация с ниво на класификация „Поверително„ и по - висока степен, трябва да са осигурени срещу паразитни електромагнитни излъчвания, които могат да доведат до нерегламентиран достъп до защитената информация. Мерките за защита от електромагнитни излъчвания съответстват на най - високото ниво на класификация на информацията в АИС или мрежа.

Криптографията е едно от най мощните средства за защита на целостта и конфиденциалността на информацията. В много отношения тя заема централно място сред програмно - техническите регулатори на сигурността, като основен, а понякога и единствен начин за защита. Например при преносимите компютри само криптографията гарантира сигурността на информацията, даже в случай на кражба. Имаме два начина за криптиране на данните - софтуерен и хардуерен. При софтуерния криптирането на данните се извършва със специална помощна програма. Данните, изпратени по мрежата са разбъркани по някакъв алгоритъм. Така дори някой да се закачи към кабела и да открадне данни, тяхното разчитане е изключително сложно и практически трудно осъществимо. Когато данните стигнат до получателя, помощната програма декодира криптираните данни и ги превръща отново в разбираема информация. Модерните методи за криптиране автоматизират и двата процеса - криптиране и декриптиране. При хардуерните системи за криптиране се използва специална електронна апаратура.
Много важна част от една компютърна мрежа са кабелите. Всеки кабел действа като антена и излъчва в ефира сигнал, който е с много малка сила. Това обаче е напълно достатъчно сигнала да бъде уловен с подходящо електронно устройство за подслушване. Информацията може да бъде откраднатa и директно от самият кабел с помощта на съответно оборудване. Затова до кабелите, по който се предава поверителна информация, достъп трябва да имат само оторизирани лица. Това може да

се осъществи при подходящо планиране, като кабелите се прекарат по добре защитени трасета.

За подобряване на сигурността на компютърната мрежа е много важно какви кабели ще се използват. Относително най - сигурни са кабелите с оптични нишки. При тях информацията се пренася под формата на модулирани светлинни импулси.Това е относително безопасен начин, тъй като по кабела не се пренасят електрически импулси, които могат да бъдат регистрирани, за да се откраднат данни, което е възможно при всички видове медни кабели.

3.4. Програмно-технически мерки за защита на класифицираната информация в АИС и/или мрежи

Основната част от загубите се нанасят от действията на легалните потребители, по отношение на които управленските и организационните мерки не дават решаващ ефект. Главните врагове са некомпетентността и неточността на персонала при изпълнение на служебните задължения, опитите за нерегламентиран достъп до системите и само програмно-техническите мерки са в състояние да им противостоят.

Биват програмни и програмно - технически. Към **програмните методи** могат се отнесат: идентификация и автентификация; управление на достъпа; протоколиране и одит; защита от вируси.

Идентификация и автентификация. Идентификацията позволява на субекта да назове себе си (да съобщи името си). Посредством

автентификацията втората страна се убеждава, че субектът е действително онзи, за когото се представя. В качеството на синоним на термина автентификация понякога се използва термина "проверка на идентичност". Субектът може да потвърди своята идентичност, като демонстрира едно от следните качества: нещо, което той знае (парола, личен идентификационен номер, криптографски ключ и пр.); нещо, което притежава (лична карта или друго устройство с аналогично предназначение); нещо, което е част от самия него (глас, отпечатъци от пръсти, роговица и др.).

Надеждната идентификация и автентификация е затруднена по ред причини. *Първо*, компютърната система се основава на информация във вида, в който е била получена. *Второ*, почти всички автентификационни същности могат да се узнаят, откраднат или подправят. *Трето*, има противоречие между надеждната автентификация и удобството на потребителя. И *четвърто,* колкото по - надеждно е едно средство за защита, толкова е по - скъпо. Най - често разпространеното средство за автентификация са паролите. Системата сравнява въведените и по - рано зададени от потребителя пароли и в случай на съвпадение идентичност а на потребителя се счита за доказана. Друго средство, което постепенно набира популярност, са секретните криптографски ключове. Главното достойнство на паролната автентификация е простотата и привичността. При правилно използване паролите могат да осигурят приемливо за много организации ниво на защита. Надеждността на паролата се основава на способността да се помни и пази в тайна. За да се запомня лесно, паролата често се прави елементарна (името на близък,

название на коли и отбори и т.н.), което, разбира се, е грешно, защото не е трудно да се отгатне. Паролите могат да бъдат разбрани по много начини: могат да бъдат видени, чрез използване на специални прибори, често се съобщават на колеги, да бъдат разшифровани чрез програмни средства, да бъдат прихванати по електронен път и др.

На практика единственият изход е използването на криптографията за криптиране на паролите. Приложими са следните мерки за повишаване на надеждността: налагане на технически ограничения - паролите да не са кратки, да съдържат букви, цифри и други знаци; управление на сроковете на действие на паролите, тяхната периодична смяна; ограничаване на достъпа до файла с паролите; ограничаване броя на несполучливите опити за вход в системата; обучение на потребителите; използване на програмни генератори на пароли.

Както е известно, едно от най - мощните средства в ръцете на злонамерени лица е изменението на програмата за автентификация, при което паролата не само се проверява, но и се запомня за последващ нерегламентиран достъп.

Устройствата за контрол, базирани на биометрични характеристики, са скъпи и сложни, затова се използват само в специфични организации с високи изисквания за сигурност. Администрирането на идентификацията и автентификацията е много важна и трудна задача. Необходимо е постоянно да се поддържа конфиденциалност, цялостност и достъпност. Най - лесният начин за това е като се централизира процесът на администриране, което позволява да се

реализира концепцията за единен вход. Веднъж преминал проверката за идентичност, потребителят има достъп до всички ресурси на мрежата (в пределите на неговите правомощия).

Управление на достъпа. Средствата за управление на достъпа позволяват да се характеризират и контролират действия, които субектите (потребители и процеси) могат да изпълняват над обектите (информации и други ресурси). Тук става дума за логическо управление на достъпа, което се реализира с програмни средства.

Пример: Нека имаме съвкупност от субекти и набор от обекти. Задачата на логическото управление на достъпа се състои в това за всеки субект и обект да се определи списък от допустими операции и да се контролира установеният ред. Контролът за правата на достъп се създава от различни компоненти на програмната среда: операционна система, допълнителни средства за сигурност, управление на база от данни, посредническо - програмно осигуряване и т.н. При вземане на решение за предоставяне на достъп обикновено се анализира следната информация: идентификатор на субекта (потребителя), мрежови адрес на компютър и др.; атрибути на субекта - белега за сигурност, групата на потребителя; място на действието; време на действието; вътрешни ограничения на програмата.

Голяма част от операционните системи и системите за управление на бази от данни реализират произволно управление на достъпа. Основното му достойнство е гъвкавостта. Всеки субект може независимо да задава права за достъп, което е особено лесно, ако се

използва списък за управление на достъп. Този подход има редица недостатъци. Децентрализацията на управлението на достъпа води до това, че надеждни трябва да бъдат много потребители, а не само системните оператори и администратори. Разсеяността и некомпетентността на притежателя на класифицирана информация може да доведе до откриването й от всички потребители.

Следва да се подчертае важността на управлението на достъпа, което трябва да бъде заложено в съществуващата политика за сигурност, а също и квалифицираното системно администриране.

Протоколиране и одит. Под протоколиране се разбира информация за събития, които се случват в информационната система на организацията. Във всеки програмен продукт има набор от възможни събития, но в най-честия случай могат да се подразделят на вътрешни (предизвикани от действията на самия продукт), външни (предизвикани от действия на други продукти) и клиентски (предизвикани от действията на потребителите и администраторите).

Одит - това е анализ на събраната информация, провеждан оперативно, в реално време или периодично. Целите на протоколирането и одита са:

- осигуряване на отчетността на потребителите и администраторите;
- възможност за реконструкция на последователността на събитията;

- регистриране на опитите за нарушение на информационната сигурност;
- предоставяне на информация за проявленията и анализа на проблемите.

Протоколирането трябва да се ръководи от здрав разум: какви събития да се регистрират и с каква степен на детайлизация? Необходимо е да се обърне внимание на постигането на целите, от една страна, а от друга разходите за ресурси да не са над разумните граници. Твърде детайлното протоколиране не само снижава производителността, но и затруднява одита.

Друга особеност на протоколирането и одита е зависимостта от други средства за сигурност. Идентификацията и автентификацията са отправна точка за отчетността за потребителите. Осигуряването на отчетност е важно като средство за предупреждение. Ако потребителите знаят, че техните действия са фиксирани, те ще се въздържат от незаконни операции. Очевидно е, че ако се подозира един потребител в опити за нерегламентиран достъп, могат да се регистрират неговите действия особено детайлно, стигайки до всяко натискане на клавиш. Това само по себе си защитава цялостта на информацията.

Реконструкцията на последователността на събитията позволява да се открият слабостите на защитата на системата, да се намери виновникът, да се оцени мащабът на причинената вреда и да се върне към нормална работа. Анализът на проблемите може да помогне да се подобри такъв параметър на защитата като достъпност. Протоколирането и одитът

могат да се превърнат в безсмислена формалност, но могат да бъдат и ефективен инструмент за поддържане режима на информационна сигурност.

Защита от вируси. За защита от вируси се използват специални антивирусни програми. По принцип е невъзможно да се създаде програма, защитаваща от всички възможни вируси. Антивирусните програми правят следното: предотвратяват активирането на вирусите, премахват ги; възстановяват до известна степен причинените от вирусите щети; държат вирусите под контрол след тяхното активиране.

Един от най - добрите начини за предпазване от вируси е предотвратяването на нерегламентиран достъп. За целта администраторът трябва да вземе всички предпазни мерки. Политиката за въвеждане на антивирусна защита на клиентските компютри и мрежовите сървъри е част от политиката за сигурност.

Екраниране. В известен смисъл всеки ресурс се пази от защитна стена. В тази стена има врати, през които потребителите могат да преминат, за да ползват ресурса. Някои врати позволяват на потребителя да прави повече неща с ресурса, отколкото други. Администраторът определя кои потребители през кои врати могат да минават. Някои врати позволяват пълен достъп или пълен контрол над ресурса, докато други предоставят достъп например само за четене. Всеки отделен ресурс или файл съдържа в себе си списък с потребителите или групите и асоциираните с тях позволения (врати).

Използване на терминали. Терминалите (или компютри без дискове) нямат флопи- и хард дискове. От гледна точка на сигурността тези компютри са идеални, защото потребителят не може да свали файлове и да ги вземе със себе си. Те не се нуждаят от диск за първоначално зареждане, могат да комуникират със сървъра и да влизат в системата благодарение на специален чип за първоначално зареждане, инсталиран на мрежовата адаптерна карта. При включването на такъв компютър, чипът изпраща съобщение на сървъра, че желае да зареди. Сървърът отговаря, сваляйки зареждащ софтуер в RAM паметта на този компютър, и автоматично показва на екрана прозореца за влизане в системата като част от процеса на зареждане. След като потребителят влезе, компютърът е свързан към мрежата.

Използване на непрекъсваемо електрозахранване. В случай на бедствие, предизвикано от проблеми в електрозахранването, необходимото време за възстановяване на данните от архива може да доведе до сериозно намаляване на продуктивността. Има начин за подсигуряване срещу загуба на данни чрез използване на непрекъсваемо електрозахранване (UPS). Стандартните UPS устройства осигуряват два критично важни компонента за мрежата: източник за захранване на сървъра за определено време; безопасно изключване на системата.

При прекъсване на електрозахранването UPS системата предупреждава потребителите да прекратят работата по текущите задачи. След това изчаква определено време, зададено предварително, и изключва системата.

Рискът се появява там, където има заплаха. Като правило наличието на една или друга заплаха е следствие на слабости в защитата на АИС и/или мрежите, което се обяснява с отсъствието на някои програмно - технически средства за сигурност или в недостатъци в реализиращите ги защитни механизми. При определянето на заплахите за класифицираната информация в АИС и/или мрежите също се прави идентификация. Анализируемите видове заплахи следва да се избират на базата на здравия разум (като оставим настрана например заплахата от земетресение и други природни бедствия), но в рамките на избраните видове трябва да се направи пълно разглеждане. Важно е да се определят не само заплахите, но и източниците на тяхното възникване - това може да помогне при избора на допълнителни средства за защита. След идентификацията на заплахите е необходимо да се оцени вероятността за осъществяването им. Може да се използва тристепенна скала: ниска, средна и висока вероятност. Освен вероятността за осъществяване, важен е и потенциалният размер на щетите (също висок, среден и нисък). Например пожари се случват рядко, но размера на щетите от тях е голям и т.н. Оценявайки заплахите, трябва да се изхожда не толкова от средностатистическите данни, а от специфичните особености на конкретната АИС, организационна единица и персонал. За премахването и изглаждането на слабости, създаващи реална опасност,

съществуват механизми, отличаващи се с голяма степен на ефективност. Например, ако има голяма опасност от нерегламентирано проникване в системата, може да се задължат потребителите да избират дълги пароли, да задействат програма за генериране на пароли или да се закупи интегрирана система за автентификация. За да се оценят като стойност защитните мерки, е нужно да се отчитат не само средствата, които ще са необходими за закупуване на оборудване и програми, но и разходите за внедряване, поддръжка, обучение и преквалификация на персонала.

Заключение:

Дейностите на една организация, работеща с класифицирана информация, са изложени на много рискове, още повече когато тази информация се разпространява по АИС и/или мрежи.

Могат да се изброят и много други управленски, организационни, програмни и програмно - технически мерки за защита на класифицираната информация в АИС и/или мрежи, още повече че практиката по този проблем е все още минимална. Малко са сертифицираните системи и мрежи у нас, все още няма утвърдени процедури по прилагането на ЗЗКИ и съпътстващите го наредби. В хода на работата в организационните единици възникват въпроси и предложения, които предстои да бъдат прилагани и решавани. От практическа гледна точка могат да се дадат следните препоръки:

- Необходима е по - добра координация (особено в големи организационни единици) между отделите „Човешки ресурси” и администраторите на АИС и/или мрежи. Така те ще бъдат уведомявани своевременно за новоназначени, преместени и напуснали служители, за даване и респективно отнемане на права за достъп до класифицирана информация в съответните организации.
- Администраторите на мрежата следва да следят за новостите в организационно и техническо отношение за защита на класифицираната информация и да информират за тях ръководството и потребителите. Потребителите, освен обучение във връзка с прилагането

на ЗЗКИ и поднормативните актове, биха могли да преминат и обучение по отношение защитата на сигурността на персоналните си компютри и данните, които създават, обработват и съхраняват в тях. Това обучение може да се замени с ръководство на потребителя, където да бъдат описани най - честите проблеми при работата с програмните продукти в съответната организационна единица, да бъдат посочени разрешения на тези проблеми, както и методи за защита на персоналната информация на всеки потребител с достъп до класифицирана информация.

- По-добро отчитане на особеностите в жизнения цикъл на системата, който включва:

- *Задание*, т.е оформя се разбирането за това, че е необходимо да се придобие нов или значително да се модернизира съществуващият продукт; изпълняват се задания какви характеристики и какви функции трябва да притежава; оценяват се финансовите и други ограничения, като задължително се отчита, че ще се обработва класифицирана информация. Прави се оценка на критичността на самата система, от която зависи степента на внимание, което службата за сигурност на организационната единица трябва да отдели на системата през следващите етапи от жизнения й цикъл.

- *Закупуване* - най-трудният етап, защото е необходимо да се формулират изискванията към средствата за защита на новата система, към фирмата, която ще разработва и инсталира системата, към квалификацията на персонала и пр. Всички тези сведения се оформят в спецификацията, където влизат документацията, сервизното обслужване,

обучението на персонала и др. Особено внимание трябва да се обърне на въпроса за съвместимостта на новата система с наличните конфигурации, нерядко средствата за защита са незадължителни компоненти на търговските продукти и е необходимо да се проследят внимателно дали съответните пунктове не са отпаднали.

- *Инсталиране* - период от време за установяване, конфигуриране, тестване и въвеждане в експлоатация.
- *Експлоатация* - това е най-дългият и сложен процес. Най-голяма заплаха за информацията има през този етап. Ако сигурността на една система не се поддържа, тя отслабва. Потребителите не държат ревностно да изпълняват инструкциите, администраторите с по - малка бдителност анализират регистрационната информация. Ту един, ту друг потребител получава допълнителни привилегии. На пръв поглед нищо не се изменя, но на практика се нарушава защитата на информацията. За борба с ефекта на бавните изменения трябва да се прибегне до периодични проверки на сигурността на системата за защита.
- *Извеждане от експлоатация* - за АИС и/или мрежи, в които се обработва класифицирана информация, при извеждане на системата от експлоатация трябва да се унищожават физически апаратните компоненти, носители на такава информация.

Използвана литература:

1. Доктрина за комуникационните и информационни системи на БА, 2001, приета от Съвета по отбрана, Протокол № 4/04.03.1999.
2. Закон за защита на личните данни, ДВ, бр. 1/2002.
3. Закон за защита на класифицираната информация, ДВ, бр. 45/2002.
4. Концепция за информационна стратегия на МО, приета от Съвета по отбрана, Протокол № 6/20.04.1999.
5. Концепция за информационна дейност на МВР, ДВ, бр. 38/30.04.2001.
6. Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи/мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, ПМС № 99/10.05.2003, ДВ, бр. 46/2003.
7. Наредба за криптографска сигурност на класифицираната информация, ДВ, бр. 102/21.11.2003.
8. Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация
9. Правилник за прилагане на Закона за защита на класифицираната информация, ПМС № 276/02.12.2002, ДВ, бр.115/10.12.2002.