Технически университет – София

ПГ по Компютърни Технологии и Системи - Правец

Упражнение - 1

СИСТЕМИ ЗА СИГУРНОСТ

Тема: Оценка и управление на риска на съвкупността от информационни системи на организация

Изготвил:

Доц. д-р Румен Трифонов

Въведение

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

Рискът е вероятността за настъпване в определен период от време на събитие, оказващо негативно въздействие върху ФИС или мрежа. Той е възможност (измерена количествено чрез вероятност) за реализация на заплаха, т.е. възможност да се използва уязвимостта на ФИС или мрежа, за да се компрометира в някаква степен нейната сигурност.

Най-често рискът се свързва с неопределеността и несигурността относно получаването на резултати от определени действия. С него се отчита възможността да се спечели или загуби при дадена съвкупност от събития. Измерването на степента на несигурност при извършването на човешките дейности е възприето да се нарича *оценка на риска.* В този смисъл основната цел на рационалното управление на информационната сигурност е да се минимизира риска при зададено желано равнище на разходите за това. От тук следва, че ефективната политика за информационна сигурност изисква предварително да се оценява и управлява рисковата компонента при вземане на управленски решения

Оценката на риска е процес на определяне на приоритетите в управлението на риска чрез оценяване и сравняване на нивото на риска спрямо предварително определени стандарти, целево (приемливо) ниво на риска или други критерии.

Управление на риска е процес на идентификация и контрол на опасностите с цел съхраняване и оптимално използване на ресурсите. В съвременната практика на управлението този процес се декомпозира на пет фази: идентификация на заплахите; оценка на заплахите и изчисляване на риска; създаване на система за управление на риска и вземане на решения; осигуряване управлението на риска; контрол и оценка.

Анализът на риска за сигурността на ФИС или мрежа е процес, при който се установяват заплахите и уязвимите места на ФИС или мрежата, вероятността за

осъществяване на заплахите при конкретните ресурси и работна среда и се оценяват последствията при тяхното реализиране. С него се цели:

1. определяне на необходимите мерки за сигурност;
2. ефективно комбиниране на видовете мерки за сигурност;
3. правилна оценка на остатъчния риск.

Анализът на риска се извършва периодично с оглед отчитането на:

1. новопоявили се уязвимости и/или заплахи към ФИС или мрежата;
2. промени в ресурсите на ФИС или мрежата и/или в нивото на класификация за сигурност на информацията.

За анализ на риска и определяне на адекватни мерки за противодействие се сформира екип от специалисти по физическа, персонална, документална, компютърна, комуникационна и криптографска сигурност и по защита от електромагнитни излъчвания. В този екип могат да се привличат и представители на проектантите. За сложни ФИС или мрежи при възможност се използват автоматизирани средства за оценка на риска.

Възможните резултати от анализа на всеки конкретен риск са:

1. елиминиране на риска - целта е цялостно елиминиране на реална или потенциална уязвимост на ФИС или мрежата чрез пълно прилагане на мерки за сигурност;
2. предотвратяване загубата на физически и информационни ресурси - целта е прилагане на мерки за предотвратяване на загубите, доколкото това е възможно, отчитайки, че някои рискове не могат да бъдат елиминирани поради технологични или други причини;
3. ограничаване загубата на физически и информационни ресурси - целта е прилагане на мерки за сигурност, ограничаващи загубите до приемливо ниво;
4. приемане на риска от загуба на физически и информационни ресурси - когато загубата не е голяма, вероятността за загуба е малка или цената на необходимите мерки за предотвратяване на загубите е много голяма.

Резултатите от анализа на риска се оформят във вид на Описание на специфичните заплахи, уязвимостите па ФИС или мрежата, режима за сигурност при експлоатация на системата, изискванията към физическата и техническата среда.

За условия на експлоатация на ФИС или мрежа, които не са свързани с конкретна глобална среда за сигурност (например мобилни, полеви и други условия), при анализа на риска се оценяват и рисковете, свързани с възможността за нерегламентиран достъп.

Започва се с избор на анализируемия обект. За неголеми организации може да се разглежда цялата информационна инфраструктура, но за крупни организации това може да се окаже необосновано скъпо и бавно. В тези случаи ще трябва да се анализират най-важните възли от мрежата. При анализа на риска са уязвими всички елементи от информационната система - от мрежовия кабел, който може да се прекъсне, до базата от данни, която може да бъде разрушена от неумелите действия на администратора. Много е важно да се избере разумна методология за оценка на риска. Целта на оценката е да получи отговор на два въпроса: Приемливи ли са съществуващите рискове и ако не, какви защитни средства е икономически изгодно да използваме? Това означава, че оценката е количествена. Управлението на риска е типична оптимизационна задача и съществуват достатъчно програмни средства, с които да се реши. Анализируеми обекти са: класифицираната информация, компонентите на информационната система, програмните ресурси, поддържащата инфраструктура, персоналът. Следва да се класифицират данните по нивото на сигурност, да се определят местата за съхранение и обработка, начините за достъп до тях. Важно е да се систематизират обектите, за да може да се направи оценка за последствията от нарушаване на защитата на информацията.

Рискът се появява там, където има заплаха. Като правило наличието на една или друга заплаха е следствие на слабости в защитата на ФИС 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 ФИС 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 ФИС, организационна единица и персонал.

След това се прави оценка на риска. Най-простият метод е умножение на вероятността от осъществяване на заплаха и предполагаемите щети. 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. Ако по този показател новото средство се окаже икономически изгодно, може да бъде допуснато за по-нататъшно разглеждане.

Когато необходимите мерки са приети, трябва да се провери тяхната действеност, т.е. да се установи, че остатъчният риск е станал приемлив. След това се реализира процедурата по сертификация, според нашето законодателство. Ако не, ще се наложи да анализираме допуснатите грешки и да проведем повторен сеанс на управление на риска.

Рискът във фирмените информационни системи и мрежи е мярка за количествена оценка на възможността да се използват уязвимите им места, за да се реализира някаква заплаха, в резултата на което да им бъде нанесена вреда, във вид на компрометиране (в определена степен) на тяхната сигурност. Измерването на степента на тази несигурност се нарича *оценка на риска.*

Основната цел на рационалното управление на информационната сигурност и защитата на класифицираната информация в организационните единици е да се минимизира рискът при зададено желано равнище на разходите за това. Оттук следва, че ефективната политика за информационна сигурност и защита на класифицираната информация изисква предварително да се оценява и управлява рисковата компонента при вземане на решения.

Управление на риска във фирмените информационни системи и мрежи

Това е процес на идентификация и контрол на заплахите с цел съхраняване и оптимално използване на кадрите, ресурсите и процесите. В съвременната управленска практика този процес се декомпозира на пет фази: 1) идентификация на заплахите; 2) оценка на заплахите и изчисляване на риска; 3) създаване на система за управление на риска и вземане на решения; 4) осигуряване управлението на риска; 5) контрол и оценка.

Работата по управление на риска се състои в това да се оцени неговият размер, да се изготвят мерки за намаляването му и да се придобие увереност, че рискът е ограничен до приемливи размери.

Обикновено решенията, свързани с управлението на риска в ФИС или мрежи, се базират върху оценки, формирани върху навици. Ръководителите вземат решенията си въз основа на тяхната проницателност относно действието на основните фактори, придаващи уникалност на всяка ситуация. По време на изпълнение на основните си задължения те насочват своето внимание върху защитата на класифицирана информация, използвана в процеса на вземане на решения. По този начин се създават условия да се предвижда съществуването на заплахи, даже в области, където привидно такива не съществуват.

При провеждане на традиционна организационна дейност се срещат два вида риск: тактически и случаен. Тактическият риск *се* свързва със съществуване на заплахи при изпълнение на дадена организационна дейност. Този риск се отчита при различни сценарии на изпълнение на даден проект, в целия спектър от дейности.

Случайният риск включва риска, който съществува при всички операции, изключвайки тактическия. Тук се включва рискът и от действията на сродни организации, както и рискът, отнасящ се пряко до всички участници в дадената дейност, както и въздействието на дейността върху обкръжаващата среда.

Фазите 1 и 2 обхващат съдържанието на оценката на риска. В началото всеки член на организацията разпознава рисковете, които могат да бъдат срещнати при изпълнение на проекта. След това се определя въздействието на всяка отделна заплаха при изпълнение на проекта. Оценката на риска изисква всеки член на колектива да направи ситуационна оценка. Тя дава увереност в собствените на членовете на колектива и така се осигурява предприемане на своевременни, ефикасни мерки за противодействие.

Рискът се появява там, където има заплаха. Кратък преглед на най-разпространените заплахи показва, че те са много и не всички от тях имат отношение към компютърните системи и мрежи. Като правило, наличието на една или друга заплаха е следствие на слабости в защитата на информационната система, което се обяснява с отсъствието на някои програмно-технически средства за сигурност или с недостатъци в реализиращите ги защитни механизми. В примера с прегризания от мишки кабел заплахата идва не от съществуването на мишки, а от отсъствието или недостатъчната дебелина на защитната обвивка на кабела.

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 максимално пълен анализ. Целесъобразно е да се определят не само самите заплахи, но и източниците им. Това може да помогне при избора на допълнителни средства за защита.

Когато анализируем обект е не само класифицираната информация, а още компонентите на информационната система, програмните ресурси, поддържащата инфраструктура и персоналът, тогава трябва да се направи класификация на данните по ниво на секретност, като се определят местата за тяхното съхранение и обработка, начините за достъп до тях. Важно е да се систематизират обектите, за да може да се направи оценка на вредите от нарушаването на защитата на информацията.

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 размерът на щетите от тях е голям и т.н. Оценявайки заплахите, трябва да се изхожда не толкова от средностатистическите данни, но и да се отчитат специфичните особености на конкретната информационна система, организационна единица и персонал.

Следващата стъпка е оценката на риска. Може да се използва такъв прост метод като умножение на вероятността за осъществяване на заплаха и предполагаемите щети. Възможните варианти са нисък, среден и висок риск. По тази скала може да се оцени приемливостта на риска и съответно, ако някои рискове се окажат неприемливо високи, се реализират допълнителни мерки за защита.

Фазите 3, 4 и 5 са същността на управлението на риска. Чрез тях ръководителите намират баланса между провеждането на организационната дейност и взаимодействието с обкръжаващата среда, като се елиминира излишният риск. По време на извършване на тези дейности ръководителите постоянно оценяват възможните заплахи, както и ефективността на осъществявания контрол. По този начин се осигурява необходимата база за процеса на обучение на целия колектив.

За премахването на слабости, създаващи реална опасност, съществуват механизми, с голяма ефективност. Например, ако има голяма опасност от нерегламентиран достъп, може да се задължат потребителите да избират дълги

пароли, да задействат програма за генериране на пароли или да закупят интегрирана система за автентификация на основата на интелектуални карти.

Оценявайки стойността на защитните мерки, е необходимо да се отчитат не само средствата за закупуването на оборудването и програмите, но и разходите за внедряване, поддръжка, обучение и преквалификация на персонала. Ако по този показател новото средство се окаже икономически изгодно, може да бъде допуснато за по-нататъшно разглеждане.

Когато необходимите мерки са приети, трябва да се провери тяхната действеност, т.е. да се постигне убеденост, че остатъчният риск е станал приемлив. Ако това е така, може да започне процедурата по сертификация, според действащото законодателство. Ако не, се анализират допуснатите грешки и се провежда повторен сеанс на управление на риска.

Реализация на фазите

1. Идентификация на заплахите

През тази фаза се определят случайните рискове (реални или потенциални), които се срещат в работата на ФИС или мрежите. Случайни рискове могат да са нелоялната конкуренция или други незаконни действия. Случайните рискове присъстват при всички видове организационна дейност, такива като: производствен процес, реинженеринг, осигуряване, обучение и други. Традицион- но случайните рискове се разкриват в първите стъпки на вземане на решения: периоди за инвестиране, инвестиционни разходи, стратегии на организационно поведение, анализ на получените резултати. Ключова е способността ръководителите на фирмите да разкриват наличието на случайни рискове. Една от особеностите на съвременната среда е, че случайните рискове се генерират от непредвидени обстоятелства или човешки грешки, появяват се изненадващо и внезапно, като пораждат значителни заплахи. Факт е, че съществуващите методи за контрол трудно могат да предпазят от случайните заплахи в извънредно бързо променящите се ситуации. Това налага при управлението на риска да идентифицират случайните заплахи, пряко влияещи върху тактическия случаен риск.

При разработката на различни проекти за изграждане и експлоатация на система за защита на класифицираната информация ръководителите първоначално трябва да анализират *сложността на концепцията,* след това трябва да я реализират в проект и накрая - да стигнат до планове и задачи, като се съобразят с всички възможни развития. При някои проекти съществува много по-голям риск от другите, при което се отчита, че това е неотменимо състояние на реализацията. Ръководителите също така разкриват заплахите, свързвани със сложността на плановете, поради което те се декомпозират до най-ниски нива на действие, които са разбираеми и ясни.

През тази фаза ръководителите разглеждат потенциалните възможности на заплахите, като основният въпрос е: какво е най-вероятно да се случи, за да се компрометира информационната сигурност? Обикновено недооценяването на случайни и непредвидени рискове по време на изпълнение на проекта може да се срещне при: оценката на предимствата на информационните технологии от финансова и икономическа гледна точка; реалната оценка на потенциала на субектите на заплахите; намиране слабите места; точното определяне на направлението на развитие на атаките; и детайлното изучаване на ниските нива на организацията.

Изучаването на възможностите за атака на ФИС или мрежи играе важна роля по отношение на разкриване на заплахите, свързани с тактическия риск. Това е динамичен процес, в който постоянно се генерират данни за изготвяне на оценка на риска. Чрез него могат да се изяснят възможностите и ограниченията в средата, потенциалните заплахи, уязвимите места и основните действащите фактори.

Успехът на провеждането на организационната дейност зависи от състоянието на *средата* и вътрешния климат, като тези два фактора обуславят различните типове случайни рискове. Когато субектът на заплахата използва като свое предимство средата, то рискът е подчертано тактически. Средата и климатът в организацията могат да породят ситуации, в които рискът доминира. От тази гледна точка изпълнението на плановете зависи от това, доколко дълго дадена организация може да съществува в тази среда и климат. В този контекст,

най-важните аспекти на средата, които трябва да бъдат изяснени, са действията на субектите на заплахите, наличието и състоянието на информационните хранилища, количество на получаваната на входа на организацията информация, състоянието на информационната среда и достигането на критични нива в нея, особености на достъпа. Разпознаването на заплахите, свързани с *климата в организацията,* налага да се оценят: състоянието на персонала, организационните комуникации, моралът, служебните взаимоотношения, организационните ценности и култура. Тези фактори влияят по много различни начини на вътрешното състояние на организацията и на информационните *процеси в нея.*

Персоналът на организацията може да бъде източник на заплахи. За тяхната оценка трябва да се вземе под внимание нивото на подготовка, вътрешното взаимодействие между хората, ниво на поддръжка на екипировката и техниката, състояние на духа, физическото и емоционалното здраве на хората. Заплахите в тази сфери могат да доведат до компрометиране на информационната сигурност, даже при условие че всички условия за труд са създадени. Провалът може да бъде предизвикан от: недобро физическо и емоционално здраве на персонала, неадекватни санитарни условия, лошо обслужване и слабо логистично планиране. Провалът може да е следствие още от: лоша вътрешна комуникация, недобро взаимодействие и координация, неефективно управление; краткотрайността на задачите (т.е. поява на смут сред персонала поради отслабване на мотивацията), текучество на ръководителите, недостиг на опит, липса на осведоменост за ситуацията, липса на необходимите умения в ръководството на организацията.

Съществена част от заплахите за компрометиране на информационната сигурност са свързани с *дефицита на време* за планиране, подготовка и изпълнение. Ръководителите рутинно прилагат съотношението -- 1/3 за планиране, спрямо 2/3 за подготовка и изпълнение - с цел да дадат максимум време на подчинените за работа. При провал на проекта поради дефицит на време, обикновено се съкращава субординацията.

2. Оценка на заплахите

През тази фаза се завършва оценката на риска. Тук се преценява вероятността рискът да се срещне при всички нива или строго детерминирани нива, във вид на един или повече случайни инцидента, които могат да бъдат предизвикани от различни заплахи. Инцидентите имат вероятностен характер и се дефинират на базата на разумни очаквания да се случат. Крайният резултат е оценка на риска за всяка отделна заплаха и оценка на общия риск за ФИС или мрежи, съществуващ поради наличие на заплахи, които не могат да бъдат елиминирани. Ръководителите трябва да оценят риска по отношение на всеки отделен елемент на ФИС или мрежа, както и да оценят въздействието им върху обкръжаващата среда. Традиционно това се извършва на три нива.

На първо ниво ръководителите на организационните единици и техните служители по сигурността оценяват всяка заплаха за бъдещ инцидент с ФИС или мрежа, имащ вероятностен характер. Вероятностният характер предполага, че различни нива на заплаха могат да възникнат по време на работа с ФИС или мрежата. Показаната долу таблица дава концентриран израз на пет степени на такава вероятност (таблица 6).

Таблица 6. Оценка на заплахите

ЧЕСТО СЕ СЛУЧВА ИЛИ ПОСТОЯННО	
Единичен проблем	Случва се много често при персонала на фирмата.
Верига от проблеми	Постоянно се случват по време на изпълнение на проекта.
На отделен член на колектива	Очаква се да му се случи много често по време на изпълнение на проекта.
На всички членове на колектива	Постоянно се случва по време на изпълнение на проекта .
ЧЕСТО СЕ СЛУЧВА ИЛИ МНОГОКРАТНО	
Единичен проблем	Случва се няколко пъти при персонала на фирмата.
Верига от проблеми	Случва се на равни интервали, с постоянна честота.
На отделен член на колектива	Случва се няколко пъти по време на изпълнение на проекта.
На всички членове на колектива	Случва се средно често по време на изпълнение на проекта.
СЛУЧВА СЕ СПОРАДИЧНО ИЛИ ОТ ВРЕМЕ НА ВРЕМЕ	
Единичен проблем	Случва се от време на време на персонала на фирмата.
Верига от проблеми	Случва се няколко пъти в фирмата.
На отделен член на колектива	Случва се няколко пъти – не много често.
На всички членове на колектива	Случва се спорадично, от време на време.
РЯДКО СЕ СЛУЧВА, НО МОЖЕ ДА СЕ ПОЯВИ ПО ВСЯКО ВРЕМЕ	
Единичен проблем	Възможно е да се случи по време на кариерата, но не е задължително.
Верига от проблеми	Случва се под формата на изолирани инциденти.
На отделен член на колектива	Случва се под формата на изолирани случаи, но не се очаква по време на изпълнение на проекта.
На всички членове на колектива	Случва се рядко под формата на изолирани инциденти.
МАЛКО ВЕРОЯТНО, НО НЕ Е НЕВЪЗМОЖНО ДА СЕ ПОЯВИ	
Единичен проблем	Не е възможно да се случи – допуска се, че няма да се случи.
Верига от проблеми	Случва се много рядко – инцидентно.
На отделен член на колектива	Не е възможно да се случи, допуска се, че няма да се случи в изпълнение на проекта.
На всички членове на колектива	Случва се много рядко, но не е невъзможно.

На второ ниво се анализира сериозността на потенциалните заплахи. Тя се изразява във степента, в която може да се компрометира информационната сигурност от: (а) от персонала, (б) хардуера и софтуера, (в) външни субекти.

Сериозността на заплахите се определя чрез взаимното сравнение между тях и на- личната информация за сходни такива. Показаната в таблицата схема дава представа за четири степени на сериозност от заплахите (таблица 7).

1. Катастрофални – пълна загуба на възможности за приключване на проекта. Случаи на смърт или перманентна нетрудоспособност на персонала. Загуба на екипировка. Непредвидени материални загуби.
2. Критични – внезапна загуба на възможността за завършване на проекта. Перманентна неспособност в рамките на 3 месеца. Голяма загуба на екипировка и несигурност. Неочаквани съпътстващи загуби.
3. Частични – загуба на възможности. Загуба на част от екипировката, техника или поле за действие. Нараняване или заболяване на персонала в рамките на 3 месеца.
4. Незначителни – малко или незначително въздействие върху възможността за завършване на проекта. Малки загуби в рамките на фирмата.

Таблица 7. Степени на заплаха на заплахите

На трето ниво ръководителите на организационните единици и техните щабове елиминират неопределеността относно заплахите от инциденти, оценяват нивата на риск за всяка отделна заплаха, както и цялостния риск за ФИС или мрежата. Оценяването на риска започва с тестване на резултатите от предните нива, които дават вероятността да се сбъднат прогнозите и ефектът от инцидентите. Тук решенията зависят повече от натрупания опит и интуитивния анализ. Неопределеността се проявява по отношение на оценката на вероятността и сериозността на заплахите. Неопределеността е резултат от непълнотата, неточността, противоречивостта и непредвидимостта на ситуациите. При изпълнение на служебните си задължения при стратегическа обстановка ръководителите, притежаващи ресурси от находчивост и изобретателност, са принудени да се съобразяват с реалностите на ситуацията, които често пъти, в значителна степен ги задължават да действат при увеличаващ се риск от грешки или неуспех.

Поради това, че обстановката се променя много бързо, проявата на излишна енергичност води до нарастване рисковете за ФИС или мрежата.'

По-долу, в таблицата, е дадена стандартната матрица, която често се използва за оценка на степента на риск (таблица 8).

Много големият риск е при голяма вероятност за компрометиране на информационната сигурност, когато заплахите се реализират. Средният риск е вероятност за компрометиране поради намалени способности да се реагира адекватно на потенциалните заплахи. Ниският риск е при голяма вероятност за малки загуби.

Таблица 8. Матрица за оценка на риска

Степен на риск / Степени на сериозност	ВЕРОЯТНОСТИ РЕАЛИЗАЦИЯ НА СЪБИТИЕ				
	Много вероятно	Вероятно	Средно	Рядко	Невероятно
	A	B	C	Д	E
Катастрофална	Много голям	Много голям	Много голям	Много голям	Много голям
Критични	Много голям	Много голям	Голям	Среден	Малък
Частичен	Голям	Среден	Среден	Малък	Малък
Незначителен	Среден	Малък	Малък	Малък	Малък

3. Изграждане на система за контрол на риска

През тази фаза се изграждат контролните механизми и се създава системата за вземане на решения, свързани с риска в ФИС или мрежа. След оценка на всяка заплаха, ръководителите разработват една или повече системи за контрол, които да елиминират самите заплахи или намалят риска за

инциденти. Тези системи могат условно да се класифицират като образователни, физически, и превантивни. Образователните системи се базират на предаване на знания и формиране на умения за контрол посредством индивидуален и колективен тренировъчен процес, който превръща изискванията за сигурност и надеждност в стандартни процедури.

Физически, системите за информационна сигурност се реализират под формата на защити, звукови сигнализации и предупредителни надписи за съществуваща заплаха. В отделни случаи се назначава надзиращ персонал, който отговаря за локализиране на заплахите. Превантивните системи осигуряват вземане на решения, предотвратяващи заплахите.

Основен елемент на системите за контрол на информационната сигурност са критериите за вземане на решения. Те трябва да са: (а) *подходящи,* т.е. трябва да премахват риска или да го намаляват до приемливи нива; (б) *осъществими,* т.е. колективът трябва да има възможност да приложи контрола; (в) *приемливи,* т.е. ползата от прилагането на контрола трябва да оправдае стойността на ресурсите и времето; (г) *приложими,* при наличие на съответен персонал, екипировка, снабдяване и всичко необходимо по прилагането; (д) *стандартни,* т.е. ясни, практични и конкретни; *разбираеми* и *адекватни* на приложението.

Оценката на приемливостта на критериите за контрол е субективна. Ръководителите трябва да са достатъчно компетентни за техния избор и прилагане.

От своя страна индивидуалните членове на колектива трябва да са достатъчно дисциплинирани, за да ги прилагат. На практика, трябва да се приложи съответната организация и техника, контролираща или елиминираща заплахите. Това става чрез: избор на действия, при които се избягват грешките и конфликтите; ограничаване броя на хората с достъп до необходимия минимум; проверка на персонала за допускане до работа с ФИС или мрежа; осигуряване на устройства за контрол на достъпа; осигуряване на предупредителни знаци и сигнали; осигуряване график на достъпа до ФИС или мрежа; защита на комуникационните връзки. Основният въпрос тук е - кой, какво, къде, кога, и колко трябва да бъде контролиран.

Отговорните ръководители разкриват и въвеждат контрол, като едновременно отчитат т.н. *остатъчен риск* за всяка заплаха или цялостния остатъчен риск на ФИС или мрежа. Остатъчният риск е този, който остава след действието на контрола и се идентифицира като заплаха. Тоест рискът е реален само след като не е уловен от контрола. След контрола на риска, остатъчният такъв се идентифицира и класифицира, а заплахите от него се оценяват по методите за оценка на втората фаза, описана по-горе. Този процес е итеративен и продължава, докато остатъчният риск се оцени като приемлив (едно подходящо ниско ниво) и не може в бъдеще да бъде намален. Цялостният остатъчен риск на ФИС или мрежа трябва да бъде определен, след като са открити повече от една заплахи. Остатъчният риск за всяка една от заплахите може да бъде на различно ниво, зависещо от оценката или от сериозността на евентуалния инцидент. Цялостният остатъчен риск трябва да се определи на базата на инцидент, определящ най-голямото ниво на остатъчния риск. Ако една заплаха има висок риск, то цялостният остатъчен риск на ФИС или мрежа е висок.

Ключов елемент на определянето и детерминирането на риска е вземането на решение за него, в случай че той е оправдан. Ръководителят трябва да сравни и балансира риска и очакванията за ФИС или мрежа, да прецени дали контролът е ефикасен и приемлив и дали да приеме остатъчния риск. Ако сметне, че нивото е твърде високо, той взема решение да въведе допълнителен или алтернативен контрол, като съответно модифицира или промени плановете на действие. Ръководителите могат да използват матрицата за оценка на риска, за да определят доколко рискът може да се делегира на подчинените. Така може да се създаде субординация, която забранява свободата на действие там, където рискът застрашава ФИС или мрежата.

4. Прилагане на контрола

По време на обсъждането на защитата на класифицираната информация ръководителите и техните служители по сигурността трябва да се уверят, че контролът се трансформира в прости и ясни правила и заповеди на всички нива. Прилагането на контрола включва координация и комуникация с ръководителите на колективите, подчинените им и изпълнителите на проекта. Ръководителите

прилагат мерките по контрола, които се свеждат до: провеждане на обучение на персонала; ориентиране на временно-заместващия персонал; инсталиране и разполагане на ефективни комуникационни връзки; съпровождане на информационните продукти и услуги в процеса на тяхното производство.

5. Оценка на резултатите

По време на изграждането на ФИС или мрежа ръководителите трябва да се убедят, че подчинените структури са наясно как да прилагат контрола на риска. Ръководителите трябва да следят ситуациите, като постоянно се убеждават, че контролът не се пренебрегва. Така се придобива поглед за нуждаещите се от подобряване области и постоянно се оценява ефективността на работата на подчинените звена. Ръководителите контролират изпълнението посредством стандартни процедури и техники, които могат да включват: проверки на място, инспекции, ситуационни доклади, кратки изложения на досегашното развитие, вътрешни проверки, както и близко наблюдение. Чрез тях ръководителите се убеждават, че действията им са ефективни и че вярно предвиждат, идентифицират и оценяват новите заплахи. Лидерите постоянно оценяват различните фактори, които могат да се превърнат в потенциални заплахи. При развитие на обстановката ръководителите променят контрола с цел да се поддържа рискът на приемливи нива. За да е успешно внедряването и експлоатацията на ФИС или мрежа, ръководителите трябва да се убедени, че контролът съответства на промените в ситуациите и заплахите.

Ръководителите трябва да поддържат висока степен на дисциплина на персонала, като се стремят да предотвратяват появата на *самоувереност и самодоволство,* които се пораждат в резултат на множество успехи. Ръководителите трябва да се убедят, че персоналът не се осланя само на собствената си бдителност, придобита след дълги и постоянно повтарящи се тренировки. Трябва да се отчитат непрекъснато променящите се роли, активност и влошаване на придобитите умения на персонала. Аналогично трябва да сс наблюдава еволюцията на риска в рамките на продължителен период, когато се проявяват т.н. *дълготрайни заплахи.*

С течение на времето ръководителите и персоналът могат да преценят доколко процесът по управлението на риска е бил ефективен. Те трябва: да се убедят, че успехът им ще бъде продължен, като: разпространят придобитите умения; оценят прецизността на оценката на вероятността и сериозността на заплахите; определят дали нивото на остатъчния риск при всяка загшаха е ефикасно оценено; оценят ефективността на контрола и дали той намалява или премахва риска, включително на местата, които до този момент са били ефективни.

Ръководителите и персоналът определят защо в някои случаи контролът е неефективен и какво трябва да се направи, в случай че заплахата се породи отново. Контролът може да бъде променен по начин, който традиционно се прилага или изпълнява или така, че да бъде изцяло ефективен. Периодично трябва да се обновяват методите за работа, като се определят системните проблеми, които спъват ефективността на ФИС или мрежата. Процесът на управление на риска е непрекъснат и постоянен. Той трябва постоянно да се усъвършенства. Това е неотменна част от процеса на вземане на решения. Той изисква добра оценка и интуитивен анализ, които градят чувство на увереност у ръководителите и са знак за тяхната опитност.

Инструментариум и евентуални неуспехи

В съществуващата литература има много примери на инструменти за управление на риска, които подпомагат ръководителите при оценка на заплахите, изграждането на контрол и вземане на решения за контрол на ФИС или мрежи. Инструментариумът трябва да бъде съобразен с отделните ситуации. Трябва да се има предвид, че отделният човек трябва да се обучава и тренира по единни стандарти и че персоналът трябва да действа независимо от степента на истинската или възприетата сложност на заплахите. На базата на това убеждение се разработват стандартите за намаляване на риска в рутинните процедури. Провалите се появяват, когато инструментариумът за управлението на риска се използва без адаптация към околната среда и действащите в нея фактори. Стандартният *оценъчен документ* (т.н. *контролен лист)* е един от най-масово из-

ползваните инструменти за анализ на риска и разгръщане на контрола в случаите, където рутинните задачи са основни. Чрез него се получава решение от вида *„ДА или НЕ“,* което е базирано на предвижданията за първоначалния риск и не дава възможност да се разкрие ефективността на контрола.

Неуспехите в реализацията на проектите започват, когато оценката на риска не е с необходимата точност, а видът на заплахите и нивото на остатъчния риск са неизвестни. Тогава ръководителят може да вземе неверни и неточни решения. Ако при оценката на риска се възприеме схващане, че ФИС или мрежа са без рискове, то ръководителят няма да бъде информиран за новопоявяващи- те се рискове, което може да застраши или даже да компрометира информационната сигурност в организацията. Процесът по управление на риска има основно предназначение да осигури реален контрол, без излишен остатъчен риск.

Сигурност на жизнения цикъл на системата

Жизненият цикъл на ФИС или мрежи е формален процес на тяхното създаване, следващ определени правила, процедури и стандарти, изборът на които зависи от размера на организацията, образованието и опита на създателите, наличните средства и прилаганите техники. Фазите на жизнения цикъл са показани в таблицата по-долу (таблица 9).

Фаза	Цел	Средства
Анализ на съществуващата система.	Установяване на недостатъците.	Интервю и анкетиране на потребителите Запознаване с процедурите; Събиране на документи – форми, отчети и др.; Наблюдение на операциите.
Дефиниране на изисквания към нова система.	Избор на алтернативен модел – данни, програми, компютърна техника.	Прототип, който се оценява от потребителите.
Проектиране на нова система.	1. Изготвяне на проект; 2. Установяване на среда за функциониране и контрол.	Диаграми на потоците от данни; Блокови схеми на алгоритми; Таблици; CASE софтуер.
Създаване на нова система.	1. Създаване на софтуер; 2. Инсталиране на хардуер; 3. Обучение на потребителите; 4. Тестване на системата.	Програмни системи и езици Компютри и интерфейсни устройства; Инструкции за работа.
Приложение на новата система.	1. Изготвяне на документация; 2. Изготвяне на процедури за използване.	Директно приложение; Паралелно приложение; Постепенно приложение; Пилотно приложение.
Поддържане и оценка на новата система	Установяване на съответствие с изискванията.	Анализ на недостатъците и ефективността на поддържане и развитие.

Таблица 9. Фази на жизнения цикъл на АИС или мрежи

Функционални области на приложение на Автоматизирани ИС или мрежи в организациите могат да се класифицират, както следва: *финанси и счетоводство* (регистриране на финансови операции, сметки, фактури, отчети, прогнози, материална отчетност и т.п.); *производство* (функционални операции); *маркетинг и продажби* (реклами, изложения, поръчки, продажби); *управление на персонала* (списъчен състав, присъствия, отпуски, атестации); *научни изследвания* (изследване, създаване и тестване на нови или подобрени продукти и услуги); контрол на изпълнението на решенията; обработка на кореспонденцията; поддръжка на обучението и тренинга на личния състав; управление на материално-техническото снабдяване и т.н.

Тези приложения се управляват на три нива: *тактическо управление* (ниско ниво) - контрол и управление на ежедневни операции според ясно дефинирани и рутинни процедури; *оперативно управление* (средно ниво) - планиране, контрол и управление на дългосрочни дейности в определена област; *стратегическо управление* (високо ниво) - управление на основните функционални области (стратегическо планиране, разпределение на ресурсите, определяне на политиката на организацията). В процеса на управление на внедряване и развитие на АИС или мрежи възникват множество въпроси, отговорите на които не винаги са известни на експертите. Понякога техните решения са остарели, не- актуални и насочени по-скоро към технологичната, отколкото към глобалната организационна перспектива.

В същото време надделява схващането, че в днешно време тези системи или мрежи са важен стратегически ресурс с голямо значение за всяка организация. Това налага внедряването на АИС или мрежи да се управлява далновидно, през целия жизнен цикъл, като стриктно се следи за гарантирането на информационната сигурност и защитата на класифицираната информация в тях.

Жизненият цикъл на АИС или мрежа се разделя на следните етапи:

Стартиране. На този етап се оформя разбирането за това, че е необходимо да се придобие нов (или значително да се модернизира съществуващ) продукт. Изготвят се задания с характеристики и функции, които

трябва да притежава продуктът. Оценяват се финансовите и други ограничения. На всеки един от етапите се отчита фактът, че в системата или мрежата ще се обработва класифицирана информация. Необходимо е да се направи оценка на критичността на самата система, от която оценка зависи степента на внимание, което службата за сигурност на организационната единица трябва да отдели на системата, през следващите етапи от жизнения й цикъл.

Покупка. Това е най-трудният етап. Трябва окончателно да се формулират изискванията към средствата за защита на новата система, към фирмата, която ще монтира системата, към квалификацията на персонала и пр. Всички тези сведения се оформят в спецификация, където влиза документацията, сервизното обслужване, обучението на персонала и др. Особено внимание трябва да се обърне на въпроса за съвместимостта на новата система с наличните конфигурации. Трябва да се отбележи, че нерядко средствата за защита се явяват незадължителни компоненти на търговските продукти и е необходимо да се проследи съответните пунктове да не са отпаднали от сертификацията.

Монтаж. Това е етапът, в който новата система се установява, конфигурира, тества и въвежда 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 има свойството да отслабва. Потребителите не държат ревностно да изпълняват инструкциите, администраторите с по-малка бдителност анализират регистрираната информация. Ту един, ту друг потребител получава допълнителни привилегии. На пръв поглед нищо не се изменя, но на практика защитата на информацията намалява. За борба с ефекта на бавните изменения трябва да се прибегне до периодични проверки на сигурността на системата за защита.

Извеждане от експлоатация. В нашият случай, говорейки за АИС и мрежи, в които се обработва класифицирана информация, при извеждане на системата от експлоатация трябва да се унищожават физически апаратните компоненти, носители на такава информация.

Задачи за изпълнение

1) Направете фаза „идентификация на заплахите“ от управлението на риска на информационните системи на организация.

2) Направете фаза „оценка на заплахите и изчисляване на риска“ от управлението на риска на информационните системи на организация.

3) Направете фаза „създаване на система за управление на риска и вземане на решения“ от управлението на риска на информационните системи на организация.

4) Направете фаза „осигуряване управлението на риска“ от управлението на риска на информационните системи на организация.

5) Направете фаза „контрол и оценка“ от управлението на риска на информационните системи на организация.