Тема. Політика інформаційної безпеки у корпоративних системах

Розглянемо основні поняття захисту інформації та інформаційної безпеки комп'ютерних систем

Захист інформації- це діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається.

Об'єкт захисту- інформація або носій інформації або інформаційний процес, щодо яких необхідно забезпечувати захист відповідно до поставленої мети захисту інформації.

Мета захисту інформації- Це бажаний результат захисту інформації. Метою захисту інформації може бути запобігання шкоді власнику, власнику, користувачу інформації внаслідок можливого витоку інформації та/або несанкціонованого та ненавмисного впливу на інформацію.

Ефективність захисту інформації- ступінь відповідності результатів захисту поставленої мети.

Захист інформації від витоку- діяльність щодо запобігання неконтрольованому поширенню інформації, що захищається від її розголошення, несанкціонованого доступу до інформації, що захищається, і від отримання інформації, що захищається зловмисниками.

Захист інформації від несанкціонованого впливу- діяльність щодо запобігання впливу на інформацію, що захищається, з порушенням встановлених прав та/або правил на зміну інформації, що призводить до спотворення, знищення, копіювання, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

Захист інформації від ненавмисного впливу- діяльність щодо запобігання впливу на інформацію, що захищається, помилок користувача інформацією, збою технічних та програмних засобів інформаційних систем, а також природних явищ або інших ненацілених на зміну інформації впливів, пов'язаних з функціонуванням технічних засобів, систем або з діяльністю людей, що призводять до спотворення, знищення, копіювання, блокування доступу до інформації, а також втрати, знищення або збою функціонування носія інформації.

Захист інформації від розголошення- діяльність щодо запобігання несанкціонованому доведенню інформації, що захищається, до неконтрольованої кількості одержувачів інформації.

Захист інформації від несанкціонованого доступу(НСД) - діяльність із запобігання одержанню інформації, що захищається заінтересованим суб'єктом з порушенням встановлених правовими документами або власником, власником інформації прав або правил доступу до інформації, що захищається. Зацікавленим суб'єктом, який здійснює несанкціонований доступ до інформації, що захищається, може виступати держава, юридична особа, група фізичних осіб, у тому числі громадська організація, окрема фізична особа.

Система захисту інформації- сукупність органів та/або виконавців, використовувана ними техніка захисту інформації, а також об'єкти захисту, організовані та функціонуючі за правилами, встановленими відповідними

правовими, організаційно-розпорядчими та нормативними документами щодо захисту інформації.

Під інформаційною безпекою розуміють захищеність інформації від незаконного ознайомлення, перетворення та знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їхньої працездатності. Природа цих впливів може бути різноманітною. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних та програмних засобів, стихійні лиха (землетрус, ураган, пожежа тощо).

Сучасна автоматизована інформаційна система (ІВ) є складною системою, що складається з великої кількості компонентів різного ступеня автономності, які пов'язані між собою та обмінюються даними. Практично кожен компонент може зазнати зовнішнього впливу або вийти з ладу. Компоненти ІС можна розбити на такі групи:

• *апаратні засоби* -комп'ютери та їх складові (процесори, монітори, термінали, периферійні пристрої - дисководи, принтери, контролери, кабелі, лінії зв'язку) тощо;

• *програмне забезпечення*- набуті програми, вихідні, об'єктні, завантажувальні модулі; операційні системи та системні програми (компілятори, компонувальники та ін.), утиліти, діагностичні програми тощо;

• *дані*- зберігаються тимчасово та постійно, на магнітних носіях, друковані, архіви, системні журнали тощо;

• *персонал*- обслуговуючий персонал та користувачі.

Однією з особливостей забезпечення інформаційної безпеки в ІС є те, що таким абстрактним поняттям, як інформація, об'єкти та суб'єкти системи, ставляться у відповідність фізичні уявлення у комп'ютерному середовищі:

• *для подання інформації*- машинні носії інформації як зовнішніх пристроїв комп'ютерних систем (терміналів, друкуючих пристроїв, різних накопичувачів, ліній і каналів зв'язку), оперативної пам'яті, файлів, записів тощо;

• під об'єктами системи розуміють пасивні компоненти системи, що зберігають, приймають чи передають інформацію. Доступ до об'єкта означає доступ до інформації, що міститься в ньому;

• під суб'єктами системи розуміють активні компоненти системи, які можуть спричинити потоку інформації від об'єкта до суб'єкта чи зміни стану системи. Як суб'єктів можуть виступати користувачі, активні програми та процеси.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності та достовірності оброблюваних даних, а також доступності та цілісності інформаційних компонентів та ресурсів системи.

Перераховані вище базові властивості інформації потребують повнішого тлумачення.

Конфіденційність даних- це статус, наданий даними та визначальний необхідний ступінь їхнього захисту. До конфіденційних даних можна віднести, наприклад, такі: особисту інформацію користувачів; облікові записи (імена та паролі); дані про кредитні картки; дані про розробки та різні внутрішні документи; бухгалтерські відомості. Конфіденційна інформація має бути

відома лише допущеним і таким, що пройшли перевірку (авторизованим) суб'єктам системи (користувачам, процесам, програмам). Для інших суб'єктів системи ця інформація має бути невідомою.

Встановлення градацій важливості захисту інформації, що захищається (об'єкта захисту) називають категоруванням інформації, що захищається.

Під цілісністю інформації розуміється властивість інформації зберігати свою структуру та/або зміст у процесі передачі та зберігання. Цілісність інформації забезпечується у разі, якщо дані системі не відрізняються в семантичному відношенні від даних у вихідних документах, тобто. якщо не відбулося їх випадкового чи навмисного спотворення чи руйнування. Забезпечення цілісності даних є одним із складних завдань захисту інформації.

Достовірність інформації- властивість інформації, що виражається в суворій приналежності суб'єкту, який є її джерелом, або суб'єкту, від якого ця інформація прийнята.

*Юридична значимість інформації*означає, що документ, що є носієм інформації, має юридичну силу.

Доступність даних- робота користувача з даними можлива лише в тому випадку, якщо він має доступ до них.

Доступ до інформації- Отримання суб'єктом можливості ознайомлення з інформацією, у тому числі за допомогою технічних засобів. Суб'єкт доступу до інформації – учасник правовідносин в інформаційних процесах.

Оперативність доступу до інформації- це здатність інформації або деякого інформаційного ресурсу бути доступними для кінцевого користувача відповідно до його оперативних потреб.

Власник інформації- суб'єкт, який у повному обсязі реалізує повноваження володіння, користування, розпорядження інформацією відповідно до законодавчих актів.

Власник інформації- суб'єкт, який здійснює володіння та користування інформацією та реалізує повноваження розпорядження в межах прав, встановлених законом та/або власником інформації.

Користувач (споживач) інформації- суб'єкт, який користується інформацією, отриманою від її власника, власника або посередника відповідно до встановлених прав та правил доступу до інформації або з їх порушенням.

Право доступу до інформації- Сукупність правил доступу до інформації, встановлених правовими документами або власником, власником інформації.

Правило доступу до інформації- сукупність правил, що регламентують порядок та умови доступу суб'єкта до інформації та її носіїв.

Розрізняють санкціонований та несанкціонований доступ до інформації.

Санкціонований доступ до інформації -це доступ до інформації, яка не порушує встановлені правила розмежування доступу. Правила розмежування доступу є для регламентації права доступу до компонентів системи.

*Несанкціонований доступ*до інформації характеризується порушенням встановлених правил розмежування доступу. Особа чи процес, які здійснюють несанкціонований доступ до інформації, є порушниками правил розмежування доступу. Несанкціонований доступ є найпоширенішим видом комп'ютерних

порушень.

Відповідальним за захист комп'ютерної системи від несанкціонованого доступу до інформації є адміністратор захисту.

Доступність інформації передбачає також доступність компонента чи ресурсу комп'ютерної системи, тобто. властивість компонента чи ресурсу бути доступним законним суб'єктам системи. Ось зразковий перелік ресурсів, які мають бути доступні: принтери, сервери, робочі станції, дані користувачів, будь-які критичні дані, необхідні для роботи.

Цілісність ресурсу чи компонента системи- це властивість ресурсу чи компонента бути незмінними в семантичному сенсі при функціонуванні системи за умов випадкових чи навмисних спотворень чи руйнівних впливів.

З допуском до інформації та ресурсів системи пов'язана група таких важливих понять, як ідентифікація, автентифікація, авторизація.

З кожним суб'єктом системи (мережі) пов'язують деяку інформацію (число, рядок символів), що ідентифікує суб'єкт. Ця інформація є ідентифікатором суб'єкта системи (мережі). Суб'єкт, який має зареєстрований ідентифікатор, є законним (легітимним) суб'єктом. Ідентифікація суб'єкта - це процедура розпізнавання суб'єкта щодо його ідентифікатора. Ідентифікація виконується під час спроби суб'єкта увійти до системи (мережа).

Наступним кроком взаємодії системи із суб'єктом є автентифікація суб'єкта. Аутентифікація суб'єкта – це перевірка справжності суб'єкта з цим ідентифікатором. Процедура автентифікації встановлює, чи суб'єкт є саме тим, ким він себе оголосив.

Після ідентифікації та аутентифікації суб'єкта виконують процедуру авторизації.

Авторизація суб'єкта- це процедура надання законному суб'єкту, що успішно пройшов ідентифікацію та автентифікацію, відповідних повноважень та доступних ресурсів системи (мережі).

Під загрозою безпеці ІС розуміються можливі дії, здатні прямо чи опосередковано завдати шкоди її безпеці. Збитки безпеки мають на увазі порушення стану захищеності інформації, що міститься та обробляється в системі (мережі).

З поняттям небезпеки тісно пов'язане поняття вразливості комп'ютерної системи (мережі). Вразливість комп'ютерної системи - це властиве системі невдале властивість, що може призвести реалізації загрози.

Атака на комп'ютерну систему- це пошук та/або використання зловмисником тієї чи іншої уразливості системи. Іншими словами, атака – це реалізація загрози безпеці. Протидія загрозам безпеці є метою засобів захисту комп'ютерних систем та мереж.

Захищена система- це система із засобами захисту, які успішно та ефективно протистоять загрозам безпеці.

Спосіб захисту інформації- порядок та правила застосування певних принципів та засобів захисту інформації.

Засіб захисту інформації- технічний, програмний засіб, речовина та/або матеріал, призначені або використовувані для захисту інформації.

*Комплекс засобів захисту інформації (КСЗІ)*являє собою сукупність програмних та технічних засобів, що створюються та підтримуються для забезпечення інформаційної безпеки системи (мережі). КСЗІ створюється та підтримується відповідно до прийнятої в даній організації політики безпеки.

Техніка захисту інформації- засоби захисту інформації, засоби контролю ефективності захисту інформації, засоби та системи управління, призначені для забезпечення захисту інформації.

Корпоративні мережі (КС) відносяться до розподілених автоматизованих інформаційних систем, які здійснюють обробку інформації. Забезпечення безпеки КС передбачає організацію протидії будь-якому несанкціонованому вторгненню у процес функціонування КС, і навіть спробам модифікації, розкрадання, виведення з ладу чи руйнації її компонентів, тобто. захист усіх компонентів КС - апаратних засобів, програмного забезпечення, даних та персоналу. Конкретний підхід до проблеми забезпечення безпеки ґрунтується на розробленій для КС безпековій політиці.

Політика безпеки- це сукупність норм, правил та практичних рекомендацій, що регламентують роботу засобів захисту комп'ютерної системи від заданої множини загроз.

1.1. Аналіз загроз інформаційної безпеки

Розгляд можливих загроз інформаційної безпеки проводиться з метою визначення повного набору вимог до системи захисту. Зазвичай під загрозою (загалом сенсі) розуміють потенційно можливу подію (вплив, процес чи явище), що може призвести до заподіяння шкоди чиїмось інтересам. У подальшому розгляді під загрозою безпеці інформаційній системі розумітимемо можливість впливу на ІВ, яка прямо чи опосередковано може завдати шкоди її безпеці.

В даний час відомий досить широкий перелік загроз інформаційній безпеці ІВ, що містить сотні позицій. Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника є основою для аналізу ризику реалізації загроз та формулювання вимог до системи захисту ІВ. Крім виявлення можливих загроз, доцільно проведення аналізу цих загроз на основі їхньої класифікації за низкою ознак. Кожна з ознак класифікації відображає одну із узагальнених вимог до системи захисту. Загрози, що відповідають кожній ознакі класифікації, дозволяють деталізувати вимогу, що відображається цією ознакою.

Необхідність класифікації загроз інформаційної безпеки ІС обумовлена тим, що збережена та оброблювана інформація в сучасних ІС піддається впливу надзвичайно великої кількості факторів, внаслідок чого стає неможливим формалізувати завдання опису безлічі загроз. Тому для системи, що захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Класифікація можливих загроз інформаційній безпеці ІС може бути проведена за низкою базових ознак.

1. *За природою виникнення*розрізняють:

• *природні загрози,*викликані впливами на ІС об'єктивних фізичних

процесів чи стихійних природних явищ;

- *штучні погрози*безпеки ІВ, спричинені діяльністю людини.

2. *За рівнем навмисності прояви*розрізняють:

• *загрози, спричинені помилками чи недбалістю*персоналу, наприклад, некомпетентне використання засобів захисту, введення помилкових даних тощо;

- *загрози навмисної дії*, наприклад, дії зловмисників.

3. *За безпосереднім джерелом загроз.*Джерелами загроз можуть бути:

• *природне середовище*, наприклад стихійні лиха, магнітні бурі та ін;

• *людина*наприклад вербування шляхом підкупу персоналу, розголошення конфіденційних даних тощо;

• *санкціоновані програмно-апаратні засоби*наприклад видалення даних, відмова в роботі операційної системи;

• несанкціоновані програмно-апаратні засоби, наприклад, зараження комп'ютера вірусами з деструктивними функціями.

4. *За станом джерела загроз.*Джерело загроз може бути розташоване:

• *поза контрольованою зоною ІВ*, наприклад перехоплення даних, що передаються каналами зв'язку, перехоплення електромагнітних, акустичних та інших випромінювань пристроїв;

• *у межах контрольованої зони ІВ*наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації тощо;

- *безпосередньо в ІВ*наприклад некоректне використання ресурсів ІС.

5. *За рівнем залежності від активності ІВ.*Загрози проявляються:

• *незалежно від активності ІС*наприклад розкриття шифрів криптозахисту інформації;

• *тільки в процесі обробки даних*, наприклад загрози виконання та розповсюдження програмних вірусів.

6. *За ступенем впливу на ІВ*розрізняють:

• *пасивні загрози,*які при реалізації нічого не змінюють у структурі та змісті ІВ, наприклад, загроза копіювання секретних даних;

• *активні загрози*, які при впливі вносять зміни до структури та змісту ІС, наприклад впровадження «троянських коней» та вірусів.

7. *За етапами доступу користувачів або програм до ресурсів ІС*розрізняють:

• загрози, що виявляються на етапі доступу до ресурсів ІС, наприклад, загрози несанкціонованого доступу до ІВ;

• загрози, що виникають після дозволу доступу до ресурсів ІС, наприклад, загрози несанкціонованого або некоректного використання ресурсів ІВ.

8. *За способом доступу до ресурсів ІС*розрізняють:

• загрози з використанням стандартного шляху доступу до ресурсів ІС, наприклад, незаконне отримання паролів та інших реквізитів розмежування доступу з наступним маскуванням під зареєстрованого користувача;

• загрози з використанням прихованого нестандартного шляху доступу до ресурсів ІВ, наприклад, несанкціонований доступ до ресурсів ІВ шляхом використання недокументованих можливостей операційних систем (ОС).

9. *За поточним місцем розташування інформації, що зберігається та*

обробляється в ІВ, розрізняють:

• загрози доступу до інформації на зовнішніх пристроях, наприклад несанкціоноване копіювання секретної інформації з жорсткого диска;

• загрози доступу до інформації в оперативній пам'яті, наприклад, читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті з боку прикладних програм;

• загрози доступу до інформації, що циркулює в лініях зв'язку, наприклад, незаконне підключення до ліній зв'язку з подальшим введенням хибних повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої заміни законного користувача з подальшим введенням дезінформації та нав'язуванням хибних повідомлень;

• загрози доступу до інформації, що відображається на терміналі або друкується на принтері, наприклад запис інформації на приховану відеокамеру.

Як зазначалося, небезпечні на ИС поділяють на випадкові і навмисні. Аналіз досвіду проектування, виготовлення та експлуатації ІВ показує, що інформація піддається різним випадковим впливам на всіх етапах циклу життя та функціонування ІВ.

Причинами випадкових впливів під час експлуатації ІВ можуть бути:

- аварійні ситуації через стихійні лиха та відключення електроживлення;
- відмови та збої апаратури;
- помилки у програмному забезпеченні (ПЗ);
- помилки у роботі обслуговуючого персоналу та користувачів;
- перешкоди лініях зв'язку через впливів довкілля.

Помилки програмного забезпечення є поширеним видом комп'ютерних порушень. Програмне забезпечення серверів, робочих станцій, маршрутизаторів тощо. написано людьми, тому воно майже завжди містить помилки. Чим вище складність подібного ПЗ, тим більша ймовірність виявлення в ньому помилок та вразливостей. Більшість із них не становлять жодної небезпеки, деякі можуть призвести до серйозних наслідків, таких, як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів (використання комп'ютера як плацдарм для атаки тощо). Зазвичай такі помилки усуваються за допомогою пакетів оновлень, які регулярно випускаються виробником ПЗ. Своєчасне встановлення таких пакетів є необхідною умовою безпеки інформації.

Умисні загрози пов'язані з цілеспрямованими діями порушника. Як порушника можуть виступати службовець, відвідувач, конкурент, найманець і т.д. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом (хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися за всяку ціну тощо.

Виходячи з можливості виникнення найбільш небезпечної ситуації, обумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути лише на рівні розробника цієї системи;
- порушником може бути як стороння особа, і законний користувач

системи;

- порушнику відома інформація про принципи роботи системи;
- порушник вибере найслабшу ланку у захисті.

Зокрема, для банківських ІВ можна виділити такі навмисні загрози:

- несанкціонований доступ сторонніх осіб, які не належать до банківських службовців, та ознайомлення зі збереженою конфіденційною інформацією;
- ознайомлення банківських службовців з інформацією, до якої вони не повинні мати доступу;
- несанкціоноване копіювання програм та даних;
- крадіжка магнітних носіїв, що містять конфіденційну інформацію;
- крадіжка роздрукованих банківських документів;
- умисне знищення інформації;
- несанкціонована модифікація банківськими службовцями фінансових документів, звітності та баз даних;
- фальсифікація повідомлень, що передаються каналами зв'язку;
- відмова від авторства повідомлення, переданого каналами зв'язку;
- відмова від факту отримання інформації;
- нав'язування раніше переданого повідомлення;
- руйнування інформації, спричинене вірусними впливами;
- руйнування архівної банківської інформації, що зберігається на магнітних носіях;
- крадіжка обладнання.

Найбільш поширеним та різноманітним видом комп'ютерних порушень є несанкціонований доступ. Суть НСД полягає у отриманні користувачем (порушником) доступу до об'єкта порушення правил розмежування доступу, встановлених відповідно до прийнятої у організації політикою безпеки. НСД використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, їх некоректній установці та налаштуванні. НСД може бути здійснений як штатними засобами ІВ, так і спеціально створеними апаратними та програмними засобами.

Перерахуємо основні канали несанкціонованого доступу, через які порушник може отримати доступ до компонентів ІС та здійснити розкрадання, модифікацію та/або руйнування інформації:

- штатні канали доступу до інформації (термінали користувачів, оператора, адміністратора системи; засоби відображення та документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;
- технологічні пульти керування;
- лінії зв'язку між апаратними засобами ІВ;
- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення та заземлення та ін.

З усієї різноманітності способів та прийомів несанкціонованого доступу зупинимося на наступних поширених та пов'язаних між собою порушеннях:

- перехоплення паролів;
- "маскарад";
- незаконне використання привілеїв

*Перехоплення паролів*здійснюється спеціально розробленими програмами.

При спробі законного користувача увійти в систему програма-перехоплювач імітує на екрані дисплея введення імені та пароля користувача, які одразу пересилаються власнику програми-перехоплювача, після чого на екран виводиться повідомлення про помилку та керування повертається операційній системі. Користувач припускає, що припустився помилки при введенні пароля. Він повторює введення та отримує доступ до системи. Власник програми-перехоплювача, який отримав ім'я та пароль законного користувача, може тепер використовувати їх у своїх цілях. Існують інші способи перехоплення паролів.

«Маскарад»- це виконання будь-яких дій одним користувачем від імені іншого користувача, який має відповідні повноваження. Метою маскараду є приписування будь-яких дій іншому користувачеві або присвоєння повноважень і привілеїв іншого користувача. Прикладами реалізації «маскараду» є:

• вхід у систему під ім'ям та паролем іншого користувача (цьому «маскараду» передує перехоплення пароля);

• надсилання повідомлень в мережі від імені іншого користувача.

«Маскарад» особливо небезпечний у банківських системах електронних платежів, де неправильна ідентифікація клієнта через «маскарад» зловмисника може призвести до великих збитків законного клієнта банку.

Незаконне використання привілеїв- більшість систем захисту встановлюють певні набори привілеїв виконання заданих функцій. Кожен користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад, за допомогою «маскараду» призводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або за наявності помилок у системі захисту, або через недбалість адміністратора при керуванні системою та призначенні привілеїв.

Шкідливі програми- до таких програм належать «комп'ютерні віруси», мережеві «хробаки», програма «троянський кінь». Особливо вразливі до цих програм робочі станції кінцевих користувачів. Дамо коротку характеристику цих поширених загроз безпеці ІС.

*"Троянський кінь"*є програмою, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи та деструктивних результатів. Аналогія такої програми з давньогрецьким «троянським конем» цілком виправдана, оскільки в обох випадках оболонка, що не викликає підозр, таїть серйозну загрозу. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, які мають зберігатися та захищатися від несанкціонованого доступу.

*Комп'ютерний вірус*є своєрідним явищем, що виник у процесі розвитку комп'ютерної та інформаційної техніки. Суть цього явища полягає в тому, що програми-віруси мають ряд властивостей, властивих живим організмам, - вони народжуються, розмножуються та вмирають. Термін "вірус" у застосуванні до комп'ютерів запропонував Фред Коен з Університету Південної Каліфорнії.

Історично перше визначення, дане Ф. Коен: «Комп'ютерний вірус - це програма, яка може заражати інші програми, модифікуючи їх за допомогою включення до них своєї, можливо, зміненої копії, причому остання зберігає здатність до подальшого розмножения». Комп'ютерні віруси завдають шкоди системі за рахунок швидкого розмноження та руйнування довкілля.

*Мережевий «хробак»*є різновидом програми-вірусу, яка поширюється глобальною мережею. Слід зазначити, що «троянські коні», комп'ютерні віруси та мережеві «хробаки» ставляться до вельми небезпечних загроз ІВ.

Особливістю сучасних шкідливих програм є їх орієнтація на конкретне прикладне програмне забезпечення, що стало стандартом de facto для більшості користувачів, насамперед це Microsoft Internet Explorer і Microsoft Outlook. Масове створення вірусів під продукти Microsoft пояснюється як низьким рівнем безпеки і надійності програм, важливу роль грає глобальне поширення цих продуктів. Автори шкідливого програмного забезпечення дедалі активніше починають досліджувати «дірки» у популярних системах управління базами даних (СУБД), що пов'язують ПЗ та корпоративні бізнес-додатки, побудовані на базі цих систем.

Шкідливі програми постійно еволюціонують, основною тенденцією їхнього розвитку є поліморфізм. Сьогодні вже досить складно провести кордон між вірусом, «хробаком» та «троянським конем», вони використовують практично одні й ті самі механізми, невелика різниця полягає лише у ступені цього використання. Пристрій шкідливого програмного забезпечення став сьогодні настільки уніфікованим, що, наприклад, відрізнити поштовий вірус від «хробака» з деструктивними функціями практично неможливо. Навіть у «троянських» програмах з'явилася функція реплікації (як один із засобів протидії антивірусним засобам), так що за бажання їх можна назвати вірусами (з механізмом поширення у вигляді маскування під прикладні програми).

Для захисту від шкідливих програм необхідно вжити ряд заходів:

- виключити несанкціонований доступ до виконуваних файлів;
- тестувати програмні засоби, що купуються;
- контролювати цілісність виконуваних файлів та системних областей;
- створити замкнуте середовище виконання програм.

Боротьба з вірусами, «хробаками» і «троянськими кіньми» ведеться за допомогою ефективного антивірусного програмного забезпечення, що працює на рівні користувача і на рівні мережі. У міру появи нових вірусів, «хробаків» та «троянських коней» потрібно встановлювати нові бази даних антивірусних засобів та додатків. Детальна класифікація та характеристика шкідливих програм наводиться в гол. 7, присвяченому захисту від шкідливих програм.

До непрограмних загроз належать спам, фішинг та фармінг. Поширеність цих загроз останнім часом значно зросла.

Спам, обсяг якого зараз перевищує 80% загального обсягу поштового трафіку, може створювати загрозу доступності інформації, блокуючи поштові сервери, або використовуватися для поширення шкідливого програмного забезпечення.

Фішинг (phishing)є відносно новим видом інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди належать крадіжки

паролів, номерів кредитних карток, банківських рахунків, PIN-кодів та іншої конфіденційної інформації, яка дає доступ до грошей користувача. Фішинг використовує не технічні недоліки програмного забезпечення, а легковірність користувачів Інтернету. Сам термін "phishing", співзвучний з "fishing" (рибний лов), розшифровується як "password harvesting fishing" - вивужування пароля. Справді, фішинг дуже схожий на риболовлю. Зловмисник закидає в Інтернет приманку та «виловлює» всіх «рибок» – користувачів Інтернету, які клюнуть на цю приманку.

Зловмисником створюється практично точна копія сайту обраного банку (електронної платіжної системи, аукціону тощо). Потім за допомогою спам-технології електронною поштою розсилається лист, складений таким чином, щоб бути максимально схожим на цей лист від обраного банку. При складанні листа використовуються логотипи банку, імена та прізвища реальних керівників банку. У такому листі зазвичай повідомляється про те, що через зміну програмного забезпечення в системі інтернет-банкінгу користувачеві необхідно підтвердити або змінити свої облікові дані. Як причини зміни даних можуть бути названі вихід з ладу ПЗ банку або напад хакерів. Наявність правдоподібної легенди, що спонукає користувача до необхідних дій, - неодмінна складова успіху шахраїв-фішерів. У всіх випадках ціль таких листів одна - змусити користувача натиснути на наведене посилання, а потім ввести свої конфіденційні дані (паролі, номери рахунків, PIN-коди) на хибному сайті банку (електронної платіжної системи, аукціону). Зайшовши на хибний сайт, користувач вводить у відповідні рядки свої конфіденційні дані, а далі аферисти отримують доступ у кращому випадку до його поштової скриньки, у гіршому – до електронного рахунку.

Технології фішерів удосконалюються, використовуються методи соціальної інженерії. Клієнта намагаються налякати, вигадати критичну причину для того, щоб він видав свої конфіденційні дані. Як правило, повідомлення містять погрози, наприклад, заблокувати рахунок у разі невиконання одержувачем вимог, викладених у повідомленні.

Нині шахраї часто використовують «троянські» програми. Завдання фішера в цьому випадку дуже спрощується - достатньо змусити користувача перебратися на фішерський сайт і «підчепити» програму, яка самостійно знайде на вінчестері жертви все, що потрібно. Нарівні з «троянськими» програмами почали використовувати і кейлоггери. На підставних сайтах на комп'ютери жертв завантажують шпигунські утиліти, які відстежують натискання клавіш. При використанні такого підходу не обов'язково знаходити виходи на клієнтів конкретного банку або компанії, а тому фішери почали підробляти і сайти «загального призначення», такі як стрічки новин та пошукові системи.

Успіху фішинг-афер сприяє низький рівень обізнаності користувачів щодо правил роботи компаній, від імені яких діють злочинці. Зокрема, близько 5% користувачів не знають простого факту: банки не розсилають листів із проханням підтвердити в онлайні номер своєї кредитної картки та її PIN-код.

З'явилося поєднане з фішингом поняття – фармінг.

Фармінг (Pharming) -це теж вид шахрайства, що ставить за мету отримати персональні дані користувачів, але не через пошту, а прямо через офіційні веб-сайти. Фармери замінюють на серверах DNS цифрові адреси легітимних веб-сайтів на підроблені адреси, в результаті чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства ще небезпечніший, оскільки помітити підробку практично неможливо.

За даними аналітиків (www.cnews.ru), збитки, завдані фішерами світової економіки, склали в 2004 році $44 млрд. За статистикою Symantec, у середині 2004 року фільтри компанії щотижня блокували до 9 млн листів із фішинговим контентом. До кінця року за той же період відсіювалося вже 33 млн.

Основним захистом від фішингу поки що залишаються спам-фільтри. На жаль, програмний інструментарій для захисту від фішингу має обмежену ефективність, оскільки зловмисники експлуатують в першу чергу не проломи в ПЗ, а людську психологію. Активно розробляються технічні засоби безпеки, насамперед плагіни для популярних браузерів. Суть захисту полягає у блокуванні сайтів, що потрапили до чорних списків шахрайських ресурсів. Наступним кроком можуть стати системи генерації одноразових паролів для інтернет-доступу до банківських рахунків та облікових записів у платіжних системах, повсюдне поширення додаткових рівнів захисту за рахунок комбінації введення пароля з використанням апаратного USB-ключа.

Прийнято вважати, що незалежно від конкретних видів загроз або їх проблемно-орієнтованої класифікації ІС задовольняє потреби осіб, які її експлуатують, якщо забезпечуються такі важливі властивості інформації та систем її обробки: конфіденційність, цілісність і доступність інформації.

Іншими словами, відповідно до існуючих підходів вважають, що інформаційна безпека ІС забезпечена у випадку, якщо для інформаційних ресурсів у системі підтримуються певні рівні, а саме:

- конфіденційності (неможливості несанкціонованого отримання будь-якої інформації);
- цілісності (неможливості несанкціонованої чи випадкової її модифікації);
- доступності (можливості за розумний час отримати потрібну інформацію).

Відповідно для автоматизованих інформаційних систем розглядають три основні види загроз:

- *загрози порушення конфіденційності,* спрямовані на розголошення конфіденційної чи секретної інформації. У разі реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. У термінах комп'ютерної безпеки загроза порушення конфіденційності має місце кожного разу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі або передається від однієї системи до іншої;
- *загрози порушення цілісності інформації,* що зберігається в комп'ютерній системі або передається по каналу зв'язку, спрямовані на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена навмисне зловмисником, а також в

результаті об'єктивних впливів з боку середовища, що оточує систему. Ця загроза є особливо актуальною для систем передачі інформації - комп'ютерних мереж та систем телекомунікацій. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція певної бази даних);

• *загрози порушення працездатності (відмова в обслуговуванні),* спрямовані створення таких ситуацій, коли певні навмисні дії або знижують працездатність ІВ, або блокують доступом до її ресурсам. Наприклад, якщо один користувач системи запитує доступ до деякої служби, а інший робить дії щодо блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним або тимчасовим.

Дані види загроз можна вважати первинними або безпосередніми, оскільки реалізація цих загроз веде до безпосереднього впливу на інформацію, що захищається.

p align="justify"> Для сучасних інформаційних технологій підсистеми захисту є невід'ємною частиною ІС обробки інформації. Атакуюча сторона повинна подолати цю підсистему захисту, щоб порушити, наприклад, конфіденційність ІС. Однак потрібно усвідомлювати, що не існує абсолютно стійкої системи захисту, питання лише в часі та засобах, що потрібні на її подолання. Виходячи з даних умов, розглянемо таку модель: захист інформаційної системи вважається подоланим, якщо в ході дослідження цієї системи визначено всі її вразливості.

Подолання захисту також є загрозою, тому для захищених систем можна розглядати четвертий вид загрози - загрозу розкриття параметрів ІВ, що включає підсистему захисту. На практиці будь-який захід передує етапу розвідки, в ході якого визначаються основні параметри системи, її характеристики тощо. Результатом цього етапу є уточнення поставленого завдання, а також вибір найоптимальнішого технічного засобу.

Загрозу розкриття параметрів ІВ можна вважати опосередкованою загрозою. Наслідки її реалізації не завдають будь-якої шкоди оброблюваної інформації, але дають можливість реалізувати первинні чи безпосередні загрози, перелічені вище.

При розгляді питань захисту ІВ доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється і захищається. Така градація доступу допоможе систематизувати як потенційні небезпеки, і заходи щодо їх нейтралізації і парірованію, тобто. допоможе систематизувати весь спектр методів забезпечення захисту, які стосуються інформаційної безпеки. Це такі рівні доступу:

- рівень носіїв інформації;
- рівень засобів взаємодії з носієм;
- рівень подання інформації;
- рівень змісту інформації.

Введення цих рівнів обумовлено такими міркуваннями.

По-перше, інформація для зручності маніпулювання найчастіше фіксується

на деякому матеріальному носії, яким може бути дискета чи щось подібне.

По-друге, якщо спосіб подання інформації такий, що вона не може бути безпосередньо сприйнята людиною, виникає необхідність у перетворювачах інформації у доступний для людини спосіб подання. Наприклад, читання інформації з дискети необхідний комп'ютер, обладнаний дисководом відповідного типу.

По-третє, як було зазначено, інформація може бути охарактеризована способом свого уявлення чи тим, що називається мовою в повсякденному сенсі. Мова символів, мова жестів тощо. - все це способи подання інформації.

По-четверте, людині має бути доступним зміст представленої інформації, її семантика.

До основних напрямів реалізації зловмисником інформаційних загроз належать:

- безпосереднє звернення до об'єктів доступу;
- створення програмних та технічних засобів, що виконують звернення до об'єктів доступу в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє реалізувати загрози інформаційній безпеці;
- впровадження в технічні засоби ІВ програмних чи технічних механізмів, що порушують передбачувану структуру та функції ІВ.

У табл.1.1 наведено основні методи реалізації загроз інформаційній безпеці.

Таблиця 1.1

Основні методи реалізації загроз інформаційній безпеці

Рівень доступу до	Методи реалізації загроз інформаційній безпеці			
	Загроза розкриття	Загроза порушення	Загроза порушення	Загроза відмови служб
Рівень носіїв	Визначення типу та	Викрадення (копіювання)	Знищення машинних	Виведення з ладу

Рівень засобів взаємодії з носієм	Отримання інформації про програмно-апаратне середовище. Отримання детальної інформації про функції, що виконуються ІС. Отримання даних про застосовувані системи захисту	Несанкціонований доступ до ресурсів ІС. Вчинення користувачем несанкціонованих дій. Несанкціоноване копіювання програмного забезпечення. Перехоплення даних, що передаються каналами зв'язку	Внесення користувачем несанкціонованих змін у програми та дані. Встановлення та використання нештатного програмного забезпечення. Зараження програмними вірусами	Прояв помилок проектування та розробки програмно-апаратних компонентів ІС. Обхід механізмів захисту ІВ

Для досягнення необхідного рівня інформаційної безпеки ІС необхідно забезпечити протидію різним технічним загрозам та мінімізувати можливий вплив людського чинника.

Розглянемо тенденції розвитку загроз інформаційних технологій (ІТ-загроз). У міру розвитку та ускладнення ІТ-інфраструктури автоматично зростає кількість потенційних ІТ-загроз та ризиків. Крім того, загрози виявляються дедалі витонченішими, оскільки хакери, спамери та інші зловмисники активно беруть на озброєння можливості, що відкриваються в міру розвитку інформаційних технологій.

Зростання небезпеки внутрішніх ІТ-загроз -Зазвичай найнебезпечнішими вважалися зовнішні небезпеки (насамперед віруси), захисту від яких приділялося особливу увагу. Проте поступово дедалі більше зростає небезпека внутрішніх ІТ-загроз. У 2007 році інсайдерські погрози вперше випередили вірусні, які раніше незмінно перебували в першому рядку рейтингу як за кількістю інцидентів, так і за обсягом збитків.

У звіті «Trends in IT Security Threats», підготовленому Computer Economics, на першій позиції фігурують погрози з боку інсайдерів (табл.1.2), що випереджають за сукупними збитками (фінансовими збитками та падінням репутації компанії) інші види загроз. Друге місце дісталося спаму - відбулося помітне зростання такого типу загроз. Загрози від шкідливих програм посідають третє місце в рейтингу, оскільки, як і раніше, є чимало організацій, де захист від подібних загроз поки що реалізований на недостатньому рівні.

На четвертому місці знаходиться неавторизований доступ із боку зовнішніх порушників, а на п'ятому – загроза фізичної втрати носія інформації.

Таблиця 1.2

Десятка найбільш небезпечних ІТ-загроз

Позиція у рейтингу	IT-загроза
1	Загроза інсайдерів
2	Спам
3	Загрози від шкідливих програм (комп'ютерні віруси, «хробаки», «троянці», spyware-модулі та adware-модулі)
4	Неавторизований доступ із боку зовнішніх порушників
5	Загроза фізичної втрати носія інформації
6	Електронне шахрайство
7	Pharming-атаки
8	Phishing-атаки
9	Електронний вандалізм та саботаж
10	DoS-атаки

Розширення спектру IT-загроз -сьогодні все більш серйозну загрозу для безпеки компаній становлять зростаюча мобільність користувачів (застосування ноутбуків за межами корпоративної мережі стало практично повсюдним) і сучасні користувальницькі IT-технології (безкоштовна пошта, ICQ, чати, блоги, Wi-Fi тощо), що все активніше проникають у корпоративну сферу.

Мобільні пристрої співробітників і IT-технології користувача (при всій своїй корисності) становлять для компаній величезну небезпеку. Мобільні пристрої разом із корпоративною інформацією, що перебуває на них, нерідко виявляються вкраденими або втраченими, причому конфіденційна інформація, що часто перебуває на них, ніяк не захищена. Крім того, мобільні пристрої та користувацькі технології надають безліч способів скопіювати конфіденційну інформацію, чим і користуються інсайдери.

Аналітики компанії Gartner назвали мобільні пристрої та користувальницькі IT-технології однією з найістотніших загроз корпоративній безпеці – і ті та інші дозволяють співробітникам абсолютно безконтрольно копіювати та поширювати конфіденційну інформацію та збільшують ймовірність отримати «вірус» або «троян». У зв'язку з цим компаніям слід організувати перегляд всього http-трафіку та peer-to-peer-трафіку, блокувати підозрілі пакети, контролювати використання мобільних носіїв, обмежувати та контролювати віддалений доступ (у тому числі бездротовий) тощо.

1.3. Способи забезпечення безпеки інформаційних систем

Існують два підходи до проблеми забезпечення безпеки інформаційних систем: фрагментарний та комплексний [11, 14].

*Фрагментарний підхід*спрямований на протидію чітко визначеним загрозам у заданих умовах. Як приклад реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми і т.п. Перевагою такого підходу є висока вибірковість до конкретної загрози. Істотним недоліком цього підходу є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні заходи захисту забезпечують захист конкретних об'єктів ІС лише від конкретної загрози. Навіть невелика видозміна загрози веде до втрати ефективності захисту.

*Комплексний підхід*орієнтований створення захищеного середовища обробки інформації в ІВ, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки ІВ, що є безперечною перевагою комплексного підходу. До недоліків цього підходу належать: обмеження на свободу дій користувачів ІВ, чутливість до помилок встановлення та налаштування засобів захисту, складність управління.

Комплексний підхід застосовують для захисту (корпоративних інформаційних систем (КІС) великих організацій або невеликих ІС, що виконують відповідальні завдання або обробляють особливо важливу інформацію. Порушення безпеки інформації в КІС великих організацій може завдати величезних матеріальних збитків як самим організаціям, так і їхнім клієнтам). організації змушені приділяти особливу увагу гарантіям безпеки та

реалізовувати комплексний захист.Комплексного підходу дотримуються більшість державних та великих комерційних підприємств та установ, що відбилося в різних стандартах.

Комплексний підхід до проблеми забезпечення безпеки ґрунтується на розробленій для конкретної ІС безпеці. Політика безпеки регламентує ефективну роботу засобів захисту ІС. Вона охоплює всі особливості процесу обробки інформації, визначаючи поведінку системи у різних ситуаціях. Надійна система безпеки мережі не може бути створена без ефективної політики безпеки мережі.

Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати такі заходи:

- законодавчо-нормативного (закони, стандарти, нормативні акти тощо);
- адміністративно-організаційного (дії загального характеру, що вживаються керівництвом організації, та конкретні заходи безпеки, що мають справу з людьми);
- програмно-технічного (конкретні технічні заходи).

*Заходи законодавчо*нормативного рівня дуже важливі для забезпечення інформаційної безпеки. До цього рівня можна віднести весь комплекс заходів, спрямованих на створення та підтримку у суспільстві та на підприємстві негативного ставлення до порушень та порушників інформаційної безпеки.

Заходи адміністративно-організаційного рівня -адміністрація організації повинна усвідомлювати необхідність підтримки режиму безпеки та виділення з цією метою відповідних ресурсів. Основою заходів захисту адміністративно-організаційного рівня є безпекова політика та комплекс організаційних заходів. Під політикою безпеки розуміється сукупність документованих управлінських рішень, вкладених у захист інформації та асоційованих із нею ресурсів організації.

До комплексу організаційних заходів належать такі заходи безпеки:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

Для підтримки режиму інформаційної безпеки особливо важливими є заходи програмнотехнічного рівня, оскільки основна загроза комп'ютерним системам виходить від них самих: збої обладнання, помилки програмного забезпечення, помилки користувачів та адміністраторів тощо.

Заходи та засоби програмно-технічного рівня -в рамках сучасних інформаційних систем мають бути доступні принаймні такі засоби та механізми безпеки:

- засоби криптографії;
- механізми ідентифікації та аутентифікації;
- засоби контролю доступу до робочих місць;
- засоби виявлення та запобігання атак;
- засоби захисту від шкідливих програм;

- засоби протоколювання та аудиту;
- засоби централізованого керування захистом інформації.

Необхідність застосування стандартів- інформаційні системи компаній майже завжди побудовані на основі програмних та апаратних продуктів різних виробників, оскільки немає жодної компанії-розробника, яка б надала споживачеві повний перелік коштів для побудови сучасної ІС. Щоб забезпечити в різнорідній ІВ надійний захист інформації, потрібні фахівці високої кваліфікації, які відповідатимуть за безпеку кожного компонента ІВ: правильно їх налаштовувати, постійно відстежувати зміни, що відбуваються, контролювати роботу користувачів.

Очевидно, що чим різноманітніша інформаційна система, тим складніше забезпечити її безпеку. Достаток у корпоративних мережах та системах різноманітних засобів захисту, а також зростаючий попит на доступ до корпоративних даних з боку співробітників, партнерів та замовників призводять до створення складного середовища захисту, тяжкого для управління.

Більшість гетерогенних середовищ важливо забезпечити узгоджену взаємодію Космосу з продуктами інших виробників. Інтероперабельність продуктів захисту є важливою вимогою більшості корпоративних інформаційних систем. Тому цілком очевидна потреба у застосуванні єдиного набору стандартів постачальниками засобів захисту, компаніями - системними інтеграторами та організаціями, які виступають як замовники систем безпеки для своїх корпоративних мереж та систем.

Стандарти утворюють понятійний базис, на якому будуються всі роботи із забезпечення інформаційної безпеки, та визначають критерії, яким має керуватися безпекою. Стандарти є необхідною базою, що забезпечує сумісність продуктів різних виробників, що є надзвичайно важливим при створенні систем мережевої безпеки в гетерогенних середовищах. Міжнародні та вітчизняні стандарти інформаційної безпеки розглядаються в гол. 12.

Комплексний підхід до вирішення проблеми забезпечення безпеки, раціональне поєднання законодавчих, адміністративно-організаційних та програмно-технічних заходів та обов'язкове дотримання промислових, національних та міжнародних стандартів є тим фундаментом, на якому будується вся система захисту корпоративних інформаційних систем.

Політика інформаційної безпеки

Під політикою безпеки організації розуміють сукупність управлінських рішень, вкладених у захист інформації та асоційованих із нею ресурсів. Взагалі політика безпеки визначається використовуваним комп'ютерним середовищем і відбиває специфічні потреби організації.

Зазвичай корпоративна інформаційна система є складним комплексом різноманітного апаратного та програмного забезпечення: комп'ютерів, операційних систем, мережевих засобів, СУБД, різноманітних додатків. Всі ці

компоненти зазвичай мають власні засоби захисту, які потрібно узгодити між собою. Тому дуже важлива ефективна безпекова політика як узгоджена платформа щодо забезпечення безпеки корпоративної системи. У міру зростання комп'ютерної системи та інтеграції її в глобальну мережу необхідно забезпечити відсутність у системі слабких місць, оскільки всі зусилля захисту інформації можуть бути знецінені лише однією помилкою.

Можна побудувати політику безпеки, яка встановлюватиме, хто має доступ до конкретних активів та додатків, які ролі та обов'язки матимуть конкретні особи, а також передбачити процедури безпеки, які чітко наказують, як мають виконуватися конкретні завдання безпеки. Індивідуальні особливості роботи співробітника можуть вимагати доступу до інформації, яка має бути доступна іншим працівникам. Наприклад, менеджер з персоналу може мати доступ до приватної інформації будь-якого співробітника, тоді як фахівець із звітності може мати доступ лише до фінансових даних цих співробітників. А рядовий співробітник матиме доступ лише до власної персональної інформації.

Політика безпеки визначає позицію організації щодо раціонального використання комп'ютерів та мережі, а також процедури щодо запобігання та реагування на інциденти безпеки. У великій корпоративній системі можна застосовувати широкий діапазон різних політик - від бізнес-політик до специфічних правил доступу до наборів даних. Ці політики повністю визначаються конкретними потребами організації.

2.1. Основні поняття політики безпеки

Політика безпеки визначає стратегію управління в галузі інформаційної безпеки, а також ту міру уваги та кількість ресурсів, яку вважає за доцільне виділити керівництво.

Політика безпеки будується з урахуванням аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли проведено аналіз ризиків та визначено стратегію захисту, складається програма, реалізація якої має забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю за виконанням програми тощо.

Для того щоб познайомитися з основними поняттями політик безпеки, розглянемо як конкретний приклад гіпотетичну ІС, що належить певній організації, та асоційовану з нею політику безпеки.

Політика безпеки організації повинна мати структуру короткого документа високорівневої політики, який легко розуміється, який підтримується рядом більш конкретних документів спеціалізованих політик і процедур безпеки.

Високорівнева безпекова політика повинна періодично переглядатися, щоб гарантувати, що вона враховує поточні потреби організації. Цей документ складають так, щоб політика була відносно незалежною від конкретних технологій. У такому разі цей документ політики не потрібно змінювати надто часто. Політика безпеки зазвичай оформляється у вигляді документа, що включає такі розділи, як опис проблеми, сфера застосування, позиція організації, розподіл ролей та обов'язків, санкції та ін.

Опис проблеми -інформація, що циркулює у межах ІВ, є критично важливою. ІС дозволяє користувачам спільно використовувати програми та дані, що збільшує загрозу безпеці. Тому кожен з комп'ютерів, що входять до ІС, потребує більш сильного захисту. Ці підвищені заходи безпеки є темою даного документа. Документ має такі цілі - продемонструвати співробітникам організації важливість захисту мережевого середовища, описати їх роль у

забезпечення безпеки, а також розподілити конкретні обов'язки захисту інформації, що циркулює в ІС.

Галузь застосування -у сферу дії цієї політики потрапляють усі апаратні, програмні та інформаційні ресурси, що входять до ІС підприємства. Політика орієнтована також на людей, які працюють з ІС, у тому числі на користувачів, субпідрядників та постачальників.

Позиція організації -метою організації є забезпечення цілісності, доступності та конфіденційності даних, а також їх повноти та актуальності. Більше приватними цілями є:

- забезпечення рівня безпеки, що відповідає нормативним документам;
- дотримання економічної доцільності у виборі захисних заходів (витрати на захист не повинні перевищувати передбачувану шкоду від порушення інформаційної безпеки);
- забезпечення безпеки у кожній функціональній області ІВ;
- забезпечення підзвітності всіх дій користувачів з інформацією та ресурсами;
- забезпечення аналізу реєстраційної інформації;
- надання користувачам достатньої інформації для свідомої підтримки режиму безпеки;
- вироблення планів відновлення після аварій та інших критичних ситуацій для всіх функціональних областей з метою забезпечення безперервності роботи ІС;
- забезпечення відповідності з наявними законами та загальноорганізаційною політикою безпеки.

Розподіл ролей та обов'язків-за реалізацію сформульованих вище цілей відповідають відповідні посадові особи та користувачі ІС. Керівники підрозділів відповідають за доведення положень політики безпеки до користувачів та контакти з ними. Адміністратори ІС забезпечують безперервне функціонування ІВ та відповідають за реалізацію технічних заходів, необхідних для проведення політики безпеки. Адміністратори сервісів відповідають за конкретні сервіси і, зокрема, за те, щоб захист був побудований відповідно до загальної політики безпеки. Користувачі зобов'язані працювати з ІС відповідно до політики безпеки, підкорятися розпорядженням осіб, які відповідають за окремі аспекти безпеки, повідомляти керівництво про всі підозрілі ситуації.

Нижче наведено докладніші відомості про ролі та обов'язки посадових осіб та користувачів ІС.

Санкції -порушення політики безпеки може піддати ІС та циркулюючу в ній інформацію неприпустимому ризику. Випадки порушення безпеки з боку персоналу повинні оперативно розглядатися керівництвом для вжиття дисциплінарних заходів до звільнення.

Додаткова інформація -конкретним групам виконавців можуть знадобитися якісь додаткові документи, зокрема документи спеціалізованих політик та процедур безпеки, а також інші керівні вказівки. Необхідність у додаткових документах політик безпеки значною мірою залежить від розмірів та складності організації. Для досить великої організації можуть знадобитися

на додаток до базової політики спеціалізовані політики безпеки. Організації меншого розміру потребують лише деякого підмножини спеціалізованих політик. Багато цих документів підтримки можуть бути досить короткими - обсягом в одну-дві сторінки.

З практичної точки зору політики безпеки можна розділити на три рівні: верхній, середній та нижній [1, 14].

Верхній рівеньБезпека визначає рішення, що стосуються організації в цілому. Ці рішення мають дуже загальний характері і виходять, зазвичай, від керівництва організації.

Такі рішення можуть включати такі елементи:

• формулювання цілей, які переслідує організація у сфері інформаційної безпеки, визначення загальних напрямів у досягненні цих цілей;

• формування або перегляд комплексної програми забезпечення інформаційної безпеки; визначення відповідальних осіб за просування програми;

• забезпечення матеріальної бази для дотримання законів та правил;

• формулювання управлінських рішень з питань реалізації програми безпеки, які мають розглядатися лише на рівні організації загалом.

*Політика безпеки верхнього рівня*формулює цілі організації в галузі інформаційної безпеки у термінах цілісності, доступності та конфіденційності. На верхній рівень виноситься управління ресурсами безпеки та координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, які забезпечують або контролюють безпековий режим.

Політика верхнього рівня має справу з трьома аспектами законослухняності та виконавчої дисципліни. По-перше, організація повинна дотримуватись існуючих законів. По-друге, слід контролювати дії осіб, відповідальних за вироблення програми безпеки. По-третє, необхідно забезпечити виконавську дисципліну персоналу за допомогою системи заохочень та покарань.

Середній рівень Безпека визначає вирішення питань, що стосуються окремих аспектів інформаційної безпеки, але важливих для різних систем, що експлуатуються організацією. Прикладами таких питань є ставлення до доступу в Інтернет (проблема поєднання свободи отримання інформації із захистом від зовнішніх загроз), використання домашніх комп'ютерів тощо.

*Політика безпеки середнього рівня*має визначати для кожного аспекту інформаційної безпеки такі моменти:

• *опис аспекту* -позиція організації може бути сформульована у досить загальному вигляді як набір цілей, які має організація в даному аспекті;

• *галузь застосування* -слід специфікувати, де, коли, як, стосовно кого і чого застосовується ця політика безпеки;

• *ролі та обов'язки* -документ повинен містити інформацію про посадових осіб, які відповідають за проведення безпекової політики;

• *санкції* -політика має містити загальний опис заборонених дій та покарань за них;

• *точки контакту*- повинно бути відомо, куди слід звертатися за роз'ясненнями, допомогою та додатковою інформацією. Зазвичай "точкою

контакту" служить посадова особа.

нижній рівеньполітики безпеки належить до конкретних послуг. Ця політика включає два аспекти - цілі та правила їх досягнення, тому її важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, політика, що розглядається, повинна бути більш детальною.

Наведемо кілька прикладів питань, на які слід дати відповідь при дотриманні політики безпеки нижнього рівня:

- Хто має право доступу до об'єктів, які підтримує сервіс?
- За яких умов можна читати та модифікувати дані?
- Як організовано віддалений доступ до сервісу?

У випадку цілі повинні пов'язувати між собою об'єкти сервісу і осмислені дії з ними.

З цілей виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим чіткіше і формально вони викладені, тим простіше підтримати виконання програмно-технічними заходами. Зазвичай формально задаються права доступу до об'єктів.

Стисло сформулюємо обов'язки кожної категорії персоналу.

*Керівники підрозділів*відповідають за доведення положень безпекової політики до користувачів.

*Адміністратори ІС*забезпечують безперервне функціонування ІВ та відповідають за реалізацію технічних заходів, необхідних для здійснення політики безпеки.

*Адміністратори сервісів*відповідають за конкретні сервіси і, зокрема, за те, щоб захист був побудований відповідно до загальної політики безпеки.

*Користувачі*зобов'язані працювати з ІС відповідно до політики безпеки, підпорядковуватися розпорядженням осіб, які відповідають за окремі аспекти безпеки, повідомляти керівництво про всі підозрілі ситуації.

Головною метою заходів, що вживаються на управлінському рівні, є формування програми робіт у галузі інформаційної безпеки та забезпечення її виконання шляхом виділення необхідних ресурсів та здійснення регулярного контролю стану справ. Основою цієї програми є багаторівнева безпекова політика, що відображає комплексний підхід організації до захисту своїх ресурсів та інформаційних активів.

2.2. Структура політики безпеки організації

Для більшості організацій політика безпеки є абсолютно необхідною. Політика безпеки визначає ставлення організації до забезпечення безпеки та необхідні дії організації щодо захисту своїх ресурсів та активів. На основі політики безпеки встановлюються необхідні засоби та процедури безпеки, а також визначаються ролі та відповідальність співробітників організації у забезпеченні безпеки.

Зазвичай політика безпеки організації включає такі компоненти:

- базову безпекову політику;
- процедури безпеки;

- спеціалізовані безпекові політики (рис.2.1).

Основні положення безпекової організації описуються в наступних документах:

- огляд політики безпеки;

• опис базової безпекової політики;
• посібник з архітектури безпеки.

*Рис.2.1.*Структура політики безпеки організації

Головним компонентом політики безпеки організації є базова безпекова політика.

2.2.1. Базова політика безпеки

*Базова політика безпеки*встановлює, як організація обробляє інформацію, хто може отримати доступ до неї і як це можна зробити. В описі базової політики безпеки визначаються дозволені та заборонені дії, а також вказуються необхідні засоби управління в рамках архітектури безпеки, що реалізується. З базовою безпековою політикою узгоджуються спеціалізовані політики та процедури безпеки.

Низхідний підхід, що реалізується базовою політикою безпеки, дає можливість поступово та послідовно виконувати роботу зі створення системи безпеки, не намагаючись одразу виконати її цілком. Базова політика дозволяє у будь-який час ознайомитися з політикою безпеки у повному обсязі та з'ясувати поточний стан безпеки в організації.

*Огляд політики безпеки*розкриває мету політики безпеки, описує структуру політики безпеки, докладно викладає, хто і за що відповідає, встановлює процедури та передбачувані часові рамки для внесення змін. Залежно від масштабу організації, політика безпеки може містити більше або менше розділів.

*Посібник з архітектури безпеки*описує реалізацію механізмів безпеки у компонентах архітектури, які у мережі організації.

Як зазначалося вище, структура та склад політики безпеки залежить від розміру та цілей компанії. Зазвичай, базова політика безпеки організації підтримується набором спеціалізованих політик та процедур безпеки.

2.2.2. Спеціалізовані політики безпеки

Потенційно існують десятки спеціалізованих політик, які можуть застосовуватись більшістю організацій середнього та великого розміру. Деякі політики призначаються кожної організації, інші політики специфічні певних комп'ютерних оточень.

З урахуванням особливостей застосування спеціалізовані політики безпеки можна поділити на дві групи:

- політики, що зачіпають значну кількість користувачів;
- політики, пов'язані з конкретними технічними галузями.

До спеціалізованих політик, що зачіпають значну кількість користувачів, належать:

- політика допустимого використання;
- політика віддаленого доступу до ресурсів мережі;
- політика захисту;
- політика захисту паролів та ін.

До спеціалізованих політик, пов'язаних з конкретними технічними областями, належать:

- політика конфігурації міжмережевих екранів;
- політика з шифрування та управління криптоключами;
- політика безпеки віртуальних захищених мереж VPN;
- політика з обладнання бездротової мережі та ін.

Розглянемо докладніше деякі із ключових спеціалізованих політик.

Політика припустимого використання.Базова безпекова політика зазвичай пов'язана з рядом політик допустимого використання. Метою політики допустимого використання є встановлення стандартних норм безпечного використання комп'ютерного обладнання та сервісів у компанії, а також відповідних заходів безпеки працівників з метою захисту корпоративних ресурсів та власної інформації. Неправильне використання комп'ютерного обладнання та сервісів наражає компанію на ризики, включаючи вірусні атаки, компрометацію мережевих систем та сервісів. Конкретний тип та кількість політик допустимого використання залежать від результатів аналізу вимог бізнесу, оцінки ризиків та корпоративної культури в організації.

Політика допустимого використання застосовується до співробітників, консультантів, тимчасових службовців та інших працівників у компанії, включаючи співробітників сторонніх організацій. Політика допустимого використання призначається переважно кінцевих користувачів. Ця політика вказує користувачам, які дії дозволено, а які заборонені.

Політика допустимого використання має встановити:

• відповідальність користувачів за захист будь-якої інформації, яка використовується та/або зберігається їх комп'ютерами;

• чи можуть користувачі читати і копіювати файли, які є їх власними, але доступні їм;

• рівень допустимого використання для електронної пошти та Web-доступу.

Існує багато видів політики припустимого використання. Зокрема, можуть бути політики допустимого використання комп'ютерів, передачі, комунікацій електронної пошти, портативних персональних комп'ютерів, Web-доступу та інших.

Для освітніх та державних установ політика допустимого використання, по суті, є просто обов'язковою. Без зафіксованої у відповідному документі політики допустимого використання штатні співробітники управління та підтримки мережі не мають формальних підстав для прийняття санкцій до свого чи стороннього співробітника, який припустився грубого порушення правил безпечної роботи на комп'ютері чи мережі.

Для політики допустимого використання немає спеціального формату. У цій політиці має бути вказано ім'я сервісу, системи або підсистеми (наприклад, політика використання комп'ютера, електронної пошти, компактних комп'ютерів та паролів) та описано у найчіткіших термінах дозволену та заборонену поведінку. У цій політиці мають бути також докладно описані наслідки порушення її правил та санкції, що накладаються на порушника.

Розробка політики допустимого використання виконується кваліфікованими спеціалістами з відповідного сервісу, системи чи підсистеми під контролем комісії (команди), якій доручено розробку політики безпеки організації.

Політика віддаленого доступу.Метою політики віддаленого доступу є встановлення стандартних норм безпечного віддаленого з'єднання будь-якого хоста з мережею компанії. Ці стандартні норми покликані мінімізувати збитки компанії через можливе неавторизоване використання ресурсів компанії. До таких збитків відносяться втрата інтелектуальної власності компанії, втрата

конфіденційних даних, спотворення іміджу компанії, пошкодження критичних внутрішніх систем компанії тощо.

Ця політика стосується всіх співробітників, постачальників та агентів компанії під час використання ними для віддаленого з'єднання з мережею компанії комп'ютерів або робочих станцій, які є власністю компанії або перебувають у власній власності.

Політика віддаленого доступу:

• намічає та визначає допустимі методи віддаленого з'єднання з внутрішньою мережею;

• істотна у великій організації, де мережі територіально розподілені та простягаються до будинків;

• повинна охоплювати наскільки можна всі поширені методи віддаленого доступу до внутрішніх ресурсів.

Політика віддаленого доступу має визначити:

• які методи дозволяються для віддаленого доступу;

• обмеження на дані, до яких можна отримати віддалений доступ;

• хто може мати віддалений доступ.

Захищений віддалений доступ має бути строго контрольованим. Процедура контролю, що застосовується, повинна гарантувати, що доступ до належної інформації або сервісів отримають лише люди, що пройшли перевірку. Співробітник компанії не повинен передавати свій логін та пароль ніколи і нікому, включаючи членів своєї сім'ї. Керування віддаленим доступом не повинно бути настільки складним, щоб це призводило до помилок.

Контроль доступу доцільно виконувати за допомогою одноразової парольної автентифікації або відкритими/секретними ключами (див. гл. 3 і 4).

Співробітники компанії з правами віддаленого доступу повинні забезпечити, щоб персональний комп'ютер або робоча станція, що належать їм або компанії, які віддалено приєднані до корпоративної мережі компанії, не були пов'язані в цей же час з будь-якою іншою мережею, за винятком персональних мереж, що знаходяться під повним контролем користувача.

Співробітники компанії з правами віддаленого доступу до корпоративної мережі компанії повинні забезпечити, щоб їхнє з'єднання віддаленого доступу мало такі ж характеристики безпеки, як звичайне локальне з'єднання з компанією.

Всі хости, які підключені до внутрішніх мереж компанії за допомогою технологій віддаленого доступу, повинні використовувати найсучасніше антивірусне забезпечення, ця вимога стосується і персональних комп'ютерів компанії.

Будь-який співробітник компанії, викритий у порушенні цієї політики, може бути підданий дисциплінарному стягненню до звільнення з роботи.

2.2.3. Процедури безпеки

Процедури безпеки важливі не менше, ніж політики. Процедури безпеки є необхідним та важливим доповненням до політик безпеки. Політики безпеки лише описують, що має бути захищено та які основні правила захисту. Процедури безпеки визначають, як захистити ресурси та механізми виконання політики, тобто. як реалізовувати безпекові політики.

Фактично, процедури безпеки є покрокові інструкції до виконання оперативних завдань. Часто процедура є інструментом, з допомогою якого політика перетворюється на реальну дію. Наприклад, політика паролів формулює правила конструювання паролів, правила про те, як захистити пароль і як часто замінювати паролі. Процедура керування паролями описує процес створення нових паролів, розподілу їх, а також процес гарантованої зміни паролів на критичних пристроях.

Процедури безпеки детально визначають дії, які потрібно вжити під час реагування на конкретні події. Процедури безпеки забезпечують швидке реагування у критичній ситуації. Процедури допомагають усунути проблему єдиної точки відмови у роботі, якщо, наприклад, під час кризи працівник несподівано залишає робоче місце або виявляється недоступним.

Багато процедур, пов'язаних з безпекою, повинні бути стандартними засобами будь-якого підрозділу. Як приклади можна вказати процедури для резервного копіювання та позасистемного зберігання захищених копій, а також процедури для виведення користувача з активного стану та/або архівування логіну та пароля користувача, які застосовуються відразу, як тільки даний користувач звільняється з організації.

Розглянемо кілька важливих процедур безпеки, які потрібні майже кожній організації.

Процедура реагування на події.Ця процедура є необхідним засобом безпеки більшості організацій. Організація особливо вразлива, коли виявляється вторгнення в її мережу або коли вона стикається зі стихійним лихом. Неважко уявити, що станеться у наступні хвилини та години, якщо інтелектуальна власність компанії становить мільйони чи мільярди доларів.

Процедуру реагування на події іноді називають процедурою обробки подій чи процедурою реагування на інциденти. Практично неможливо вказати на всі події порушень безпеки, але потрібно прагнути охопити основні типи

порушень, які можуть статися.

Деякі приклади подій порушень безпеки: сканування портів мережі, атака типу відмова у обслуговуванні, компрометація хоста, несанкціонований доступ та інших.

Ця процедура визначає:

- обов'язки членів команди реагування;
- яку інформацію реєструвати та простежувати;
- як обробляти дослідження відхилень від норми та атаки вторгнення;
- кого повідомляти і коли;
- хто може випускати у світ інформацію та яка процедура випуску інформації;
- як має виконуватися наступний аналіз і хто в цьому братиме участь.

До команди реагування можуть бути включені посадові особи компанії, менеджер маркетингу (для зв'язку з пресою), системний та мережевий адміністратори та представник відповідних правоохоронних органів. Процедура повинна зазначити, коли і в якому порядку вони викликаються.

Процедура керування конфігурацією.Процедура управління конфігурацією зазвичай визначається корпоративному рівні чи рівні підрозділи. Ця процедура має визначити процес документування та запиту змін конфігурації на всіх рівнях прийняття рішень. У принципі, має існувати центральна група, яка розглядає всі запити зміни конфігурації та приймає необхідні рішення.

Процедура керування конфігурацією визначає:

- хто має повноваження виконати зміни конфігурації апаратного та програмного забезпечення;
- як тестується та встановлюється нове апаратне та програмне забезпечення;
- як документуються зміни в апаратному та програмному забезпеченні;

• хто має бути поінформований, коли трапляються зміни в апаратному та програмному забезпеченні.

Процес управління конфігурацією важливий з кількох причин:

• документує зроблені зміни та забезпечує можливість аудиту;

• документує можливу просту систему;

• дає спосіб координувати зміни так, щоб одна зміна не завадила іншій зміні.

2.3. Розробка політики безпеки організації

Розробка політики безпеки є ключовим етапом побудови захищеної інформаційної системи чи мережі. Слід зазначити, що складання безпекової політики чи політик є лише початком здійснення спільної програми забезпечення безпеки організації. Детальна програма безпеки необхідна для створення ефективної системи безпеки організації на основі розробленої політики безпеки.

Основними етапами програми забезпечення безпеки є такі:

• визначення цінності технологічних та інформаційних активів організації;

• оцінка ризиків цих активів (спочатку шляхом ідентифікації погроз, для яких кожен актив є цільовим об'єктом, а потім оцінкою ймовірності того, що ці погрози будуть реалізовані на практиці);

• встановлення рівня безпеки, визначального захисту кожного активу, тобто. заходів безпеки, які вважатимуться рентабельними застосування;

• формування на базі попередніх етапів безпекової політики організації;

• залучення необхідних фінансових ресурсів для реалізації політики безпеки, придбання та встановлення необхідних засобів безпеки;

• проведення роз'яснювальних заходів та навчання персоналу для підтримки співробітниками та керівництвом необхідних заходів безпеки;

• регулярний контроль покрокової реалізації плану безпеки з метою виявлення поточних проблем, урахування зміни зовнішнього оточення та внесення необхідних змін до складу персоналу.

Досвід показав, що загалом організації отримують суттєву вигоду від добре розробленої методології рішення зазначених вище завдань.

Першими кроками з розробки політики безпеки є такі:

• створення команди із розробки політики;

• прийняття рішення про сферу дії та цілі політики;

• прийняття рішення про особливості політики, що розробляється;

• визначення особи або органу для роботи як офіційного інтерпретатора політики.

До всіх політик безпеки, що розробляються, доцільно застосовувати уніфікований процес проектування з однаковими вимогами до політиків.

Одним із перших кроків є створення команди з розробки політики безпеки організації. Іноді цю команду називають групою, комісією чи комітетом. Команда створюється керівництвом організації, яке має усвідомлювати важливість інформаційної безпеки та повністю реалізувати свою позитивну роль у успішній розробці, прийнятті та впровадженні цієї політики.

До складу команди слід включати кваліфікованих фахівців, які добре знаються на вимогах бізнесу, інформаційних технологіях та безпеці, юриста та

члена керівництва, який зможе проводити в життя цю безпекову політику.До роботи цієї команди повинні бути залучені адміністратори безпеки та системні адміністратори, представник від спільноти користувачів.

Розмір команди з розробки політики залежить від масштабу та сфери дії політики. Великомасштабні політики можуть вимагати команди з 5 - 10 осіб, тоді як політики невеликого масштабу можуть вимагати лише однієї чи двох осіб.

Як тільки створено таку команду, її першим кроком є аналіз вимог бізнесу. Члени команди з різними позиціями та поглядами повинні проаналізувати вимоги бізнесу до використання комп'ютерних та мережевих сервісів. Коли думки деяких членів цієї команди не збігаються, зіткнення їхніх інтересів та перетину різних галузей знання під час обговорення вимог бізнесу дозволяють отримати більш повну та об'єктивну картину, ніж при звичайному опитуванні людей, які працюють у галузі маркетингу, продажу чи розробки [1].

На цьому етапі аналізуються та вирішуються питання на кшталт: Які комп'ютерні та мережеві сервіси потрібні для бізнесу, і як ці вимоги можуть бути задоволені за умови забезпечення безпеки? Скільки співробітників залежать від доступу до Інтернету, використання e-mail та доступності інтранет-сервісів? Чи залежать комп'ютерні та мережеві послуги від віддаленого доступу до внутрішньої мережі? Чи є вимоги щодо доступу до Web? Чи потрібні клієнтам дані тих

нічної підтримки через Інтернет? При аналізі кожного сервісу слід обов'язково запитувати, чи є вимога бізнесу цей сервис. Це – найважливіше питання.

Після аналізу та систематизації вимог бізнесу команда з розробки політики безпеки переходить до аналізу та оцінки ризиків. Використання інформаційних систем та мереж пов'язане з певною сукупністю ризиків.

*Аналіз ризиків*є найважливішим етапом формування безпекової політики (рис.2.2).

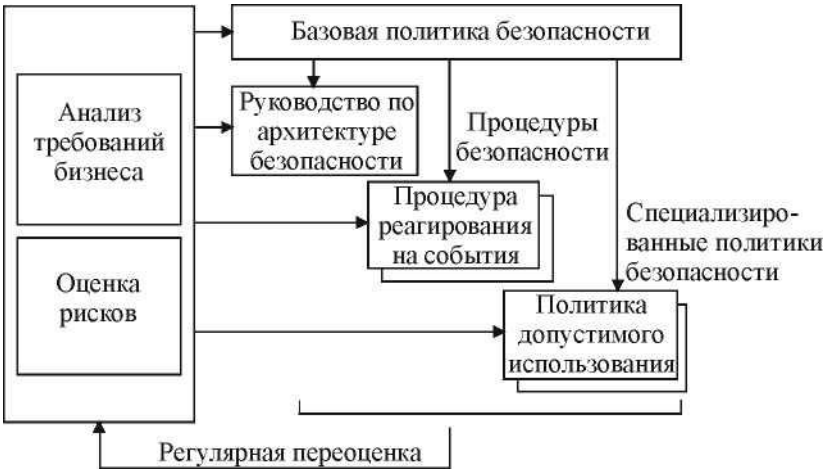

*Рис.2.2.*Схема розробки політики безпеки

Іноді цей етап називають також аналізом уразливостей чи оцінкою загроз. Хоча ці терміни мають дещо різняться тлумачення, кінцеві результати подібні.

На етапі аналізу ризиків здійснюються такі действия:

- ідентифікація та оцінка вартості технологічних та інформаційних активів;
- аналіз тих загроз, для яких цей актив є цільовим об'єктом;
- оцінка ймовірності того, що загроза буде реалізована на практиці;
- оцінка ризиків цих активів.

Оцінка ризику виявляє як найцінніші, і найуразливіші активи, вона дозволяє точно встановити, які проблеми потрібно звернути особливу увагу. Звіт про оцінку ризиків є цінним інструментом для формування політики мережевої безпеки.

Після оцінки ризиків активів можна переходити до рівня безпеки, визначального захист кожного активу, тобто. заходів безпеки, які вважатимуться рентабельними застосування.

У принципі, вартість захисту конкретного активу має перевищувати вартості самого активу. Необхідно скласти докладний перелік усіх активів, який включає такі матеріальні об'єкти, як сервери та робочі станції, та такі нематеріальні об'єкти, як дані та програмне забезпечення. Повинні бути ідентифіковані директорії, які містять конфіденційні файли або цільові файли. Після ідентифікації цих активів має бути визначено вартість заміни кожного активу з метою призначення пріоритетів у переліку активів.

Для контролю ефективності діяльності в галузі безпеки та для врахування змін обстановки необхідна регулярна переоцінка ризиків.

Після проведення описаної вище роботи можна переходити до

безпосереднього складання безпекової політики. У політиці безпеки організації повинні бути визначені стандарти, правила та процеси безпеки, що використовуються.

*Стандарти*вказують, яким критеріям має керуватися безпекою. Правила докладно описують принципи та методи управління безпекою. Процеси повинні здійснювати точну реалізацію правил відповідно до прийнятих стандартів.

Крім того, політика безпеки повинна визначити значущі для безпеки ролі та вказати на відповідальність цих ролей. Ролі встановлюються під час формулювання процесів безпеки.

*Посібник з архітектури безпеки*детально визначає контрзаходи проти загроз, розкритих в оцінці ризиків. Цей посібник описує компоненти архітектури безпеки ІВ, рекомендує конкретні продукти безпеки та дає інструкції, як розгорнути та керувати ними. Зокрема, цей посібник може містити рекомендації, де слід поставити міжмережеві екрани, коли використовувати шифрування, де розмістити Web-сервери і як організувати управління комунікаціями з бізнес-партнерами та замовниками. Посібник з архітектури безпеки визначає також гарантії безпеки, аудит та засоби