МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

А. І. ПОВОРОЗНЮК, О. А. ПОВОРОЗНЮК

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчально-методичний посібник

Гриф Вченої ради НТУ «ХПІ»
протокол № 7 від 02.07.2021 р.

Харків
НТУ "ХПІ"
2021

УДК 004.056.5
ББК 32.81
П 42

Рецензенти: Г. Є. Філатова, д-р техн.. наук, проф., проф. каф. обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний інститут»
О. О. Можаєв, д-р техн. наук, проф., проф. каф. ІТ та кібербезпеки Харківського національного університету внутрішніх справ

Поворознюк О.А.
П42 Управління інформаційною безпекою: навчально-методичний посібник / А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.

Посібник дає системне уявлення про методи та засоби управління інформаційною безпекою в предметній галузі інформаційних технологій і забезпечує теоретичну та практичну підготовку для отримання студентами необхідних знань щодо принципів створення комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах.

Предметом дисципліни "Управління інформаційною безпекою" є вивчення методів створення комплексу заходів, спрямованих на розробку і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими актами та нормативними документами у сфері захисту інформації в інформаційно-телекомунікаційних системах різного призначення.

Призначено для бакалаврів спеціальності 125 “Кібербезпека”.

Іл. 23. Табл. 3. Бібліогр. 12 назв.

УДК 004.056.5
ББК 32.81

ЗМІСТ

ВСТУП

Нові ІТ активно впроваджуються в усі сфери народного господарства. Поява локальних і глобальних мереж передачі даних надало користувачам комп'ютерів нові можливості для оперативного обміну інформацією. Розвиток Internet привів до використання глобальних мереж передачі даних в повсякденному житті кожної людини. З розвитком і ускладненням засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від ступеня безпеки використовуваних їм ІТ.

Сучасні методи обробки, передачі та накопичення інформації сприяли появі погроз, пов'язаних з можливістю втрати, спотворення та розкриття даних, які адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку ІТ. Отже підготовка кваліфікований фахівців в цій галузі є вкрай необхідною.

Дисципліна «Управління інформаційною безпекою» є спеціальною дисципліною для бакалаврів спеціальності 125 «Кібербезпека». Вона забезпечує теоретичну та практичну підготовку для отримання студентами необхідних знань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно-телекомунікаційних системах (далі - ІТС).

Предметом дисципліни «Управління інформаційною безпекою» є вивчення методів створення комплексу заходів, спрямованих на розробку і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими актами та нормативними документами у сфері захисту інформації в інформаційно-телекомунікаційних системах різного призначення.

В даний час на кафедрі обчислювальної техніки і програмування НТУ «ХПІ» ведуться лекційні та практичні заняття з курсу «Управління інформаційною безпекою».

Структура і зміст посібника відповідає робочій програмі курсу і складається з чотирьох частин. Усі розділи містять контрольні питання, що можуть використовуватися як при самопідготовці, так і при контролі знань.

У першому розділі «Безпека інформації в ІТС. Концепція побудови захищеної ІТС» розглядаються основні положення інформаційної безпеки, приведені структура та складові комплексної системи захисту інформації. Визначено значення інформаційної безпеки як складової частини національної безпеки України.

Детально розглянуті такі питання, як: базові властивості інформації, ідентифікація, автентифікація, авторизація; приведені класифікація загроз інформаційної безпеки та класифікація автоматизованих систем. На концептуальному рівні визначена структура та складові комплексної системи захисту інформації.

У другому розділі «Етапи розробки та принципи створення КСЗІ» детально розглядаються всі стадії розробки комплексної системи захисту інформації, починаючи від обстеження ІТС, формування політики безпеки, розробки технічного завдання і закінчуючи державною експертизою та супроводом КСЗІ. Для кожного з цих етапів визначені послідовність дій під час розробки КСЗІ, методи та засоби захисту інформації, що використовуються на даному етапі, а також документальне оформлення та нормативні документи, яким воно повинно відповідати. Особлива увага приділяється розробці моделі загроз, моделі порушника та функціонального профілю захисту системи забезпечення безпеки інформації.

У третьому розділі «Методологія управління інформаційною безпекою» розглядаються питання аудиту КСЗІ та управління ризиками. У підрозділі «Управління інформаційною безпекою. Аудит КСЗІ» детально розглянуті методи, організація робіт та практичні кроки аудиту інформаційної безпеки, а також звітна документація аудиту. У підрозділі «Управління ризиками» приведені технології аналізу ризиків та методи вимірювання ризиків. Детально розглянуті два основних метода вимірювання ризику при якісних величинах: за двома та трьома факторами. Також розглядаються сучасні інструментальні засоби аналізу ризиків.

У четвертому розділі «Основні напрямки та методи забезпечення безпеки інформації» розглянуто питання забезпечення безпеки інформації на технічному та інструментальному рівні.

В підрозділі «Технічні засоби і методи захисту інформації» розглядаються технічні канали витоку інформації а також засоби їх виявлення. Особлива увага приділяється методам захисту інформації, які

розділяються на активні та пасивні. Розглянуті такі сучасні технічні засоби, як індикатори електромагнітного поля, скануючі радіоприймачі, аналізатори спектру, радіочастотоміри, металодетектори, а також багатофункціональні комплекти для виявлення каналів витоку інформації.

В підрозділі «Принципи криптографічного захисту інформації» розглянуті основні поняття криптографії, відмінності між симетричними та асиметричними криптографічними системами та ефективність захисту кожної з них. Також детально розглянуті питання генерації ключів та обміну ключами, а також формування електронного цифрового підпису.

В підрозділі «Антивірусний захист» розглянуті основні поняття антивірусного захисту, а саме: що таке вірус та його деструктивні можливості, класифікація комп'ютерних вірусів та принципи побудови антивірусних програм. Детально розглянуті такі поширені типи вірусів, як файлові та бутові віруси, мережеві «черв'яки», «троянський кінь».

В підрозділі «Захист операційних систем та програмного забезпечення» розглянуті основні аспекти створення захищеної операційної системи та прикладних програм. Приведені сучасні засоби захисту програм із запитом інформації, а також засоби активного та пасивного захисту програм.

В підрозділі «Безпечна взаємодія в комп’ютерних мережах» зазначені основні методи та засоби захисту інформації в комп’ютерних мережах. Розглядаються найбільш поширені засоби захисту мереж, а саме: сканери, аналізатори протоколів та міжмережеві екрани. Визначено, що більшість з цих засобів можуть використовуватись як для захисту інформації, так і зловмисниками для несанкціонованого доступу.

Розділ 1 та загальну редакцію виконав проф. Поворознюк А. І., розділи 2, 3, 4 та вступ – доц. Поворознюк О.А.

Автори висловлюють подяку рецензентам Г.Є. Філатовій та О О. Можаєву за цінні поради при підготовці даного видання.

Розділ 1. БЕЗПЕКА ІНФОРМАЦІЇ В ІТС. КОНЦЕПЦІЯ ПОБУДОВИ ЗАХИЩЕНОЇ ІТС

1.1. . Інформаційна безпека. Основні поняття та визначення

1.1.1. Складові частини національної безпеки України

Зміцнення та захист національного інформаційного простору України є складовою забезпечення її національної безпеки. Об'єктивно повноцінний інформаційний простір забезпечує суверенітет держави у виконанні нею внутрішніх і зовнішніх функцій. Тому наповнення національного інформаційного простору новітніми технологіями є нагальною потребою, важливою для дієвого захисту національних інтересів, а питання захисту інформації відіграють у цьому процесі головну роль.

На рис 1.1. - 1.3. приведені структура національної безпеки України та системи забезпечення інформаційної безпеки, що відображують роль інформаційної безпеки як невід'ємної складової частини національної безпеки України.

Рисунок 1.1. - Складові частини національної безпеки України

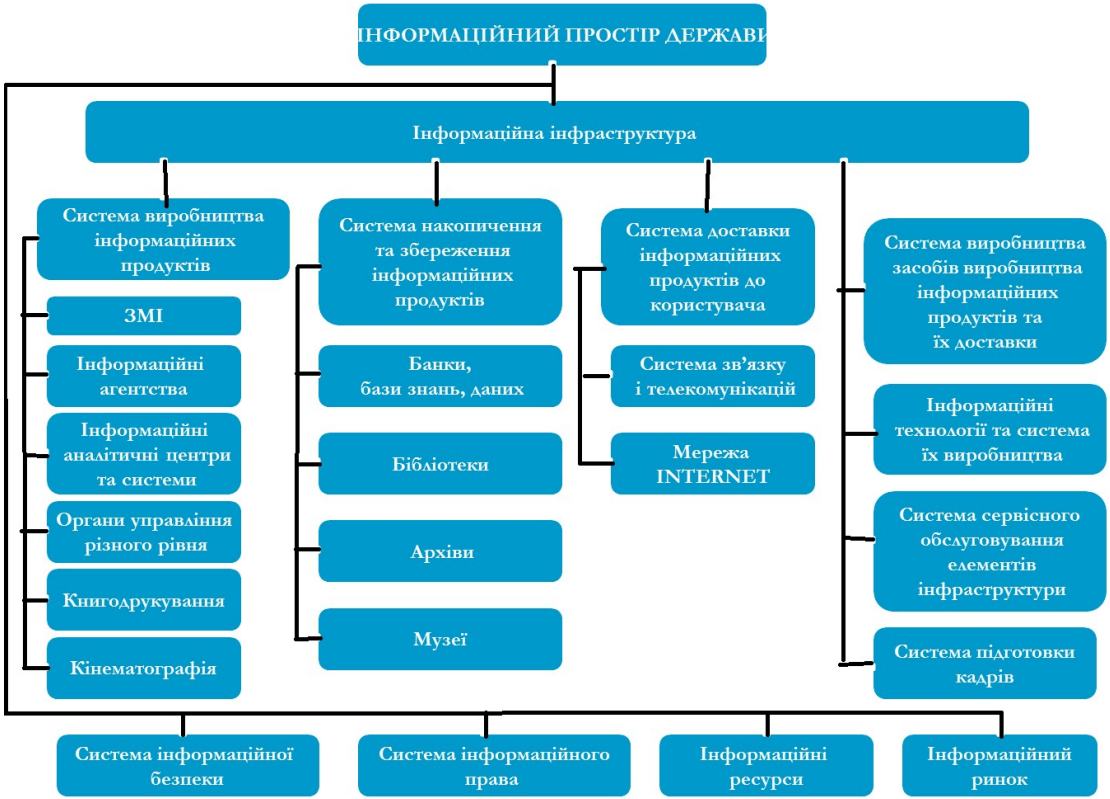

Рисунок 1.2. - Інформаційний простір держави

Рисунок 1.3. - Система забезпечення інформаційної безпеки України

1.1.2. Основні поняття та визначення курсу

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

Об'єкт захисту - інформація, 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 шкоди власнику або користувачеві інформації в результаті можливого витоку інформації і / або несанкціонованого і ненавмисного впливу на інформацію.

Ефективність захисту інформації - ступінь відповідності результатів захисту інформації поставленої мети.

Захист інформації від витоку - діяльність щодо запобігання неконтрольованого розповсюдження інформації, що захищається від її розголошення, несанкціонованого доступу (НСД) до інформації, що захищається і отримання інформації, що захищається зловмисниками.

Захист інформації від розголошення - діяльність щодо запобігання несанкціонованого доведення інформації що захищається до неконтрольованої кількості одержувачів інформації.

Захист інформації від несанкціонованого доступу - діяльність щодо запобігання отримання інформації, що захищається зацікавленим суб'єктом з порушенням встановлених правовими документами чи власником інформації прав або правил доступу до інформації, що захищається. Зацікавленим суб'єктом, що здійснює НСД до інформації, що захищається, може виступати держава, юридична особа, група фізичних осіб, в т. ч. громадська організація, окрема фізична особа.

Система захисту інформації - сукупність органів і / або виконавців, техніка захисту інформації, що використовується ними, а також об'єкти захисту, які організовані і функціонують за правилами, встановленими відповідними правовими, організаційно-розпорядчими та нормативними документами щодо захисту інформації.

Інформаційна безпека - захищеність інформації від незаконного ознайомлення, модифікації і знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їх працездатності. Природа цих впливів може бути найрізноманітнішою. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, і стихійні лиха (землетрус, ураган, пожежа) і т. п.

Сучасна автоматизована система (АС) обробки інформації являє собою складну систему, що складається з великої кількості компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними.

Практично кожен компонент може піддатися зовнішньому впливу або вийти з ладу.

Компоненти АС можна розбити на наступні групи:

- апаратні засоби - комп'ютери та їх складові частини (процесори, монітори, термінали, периферійні пристрої, дисководи, принтери, контролери, кабелі, лінії зв'язку і т. д.);

- програмне забезпечення - придбані програми, вихідні, об'єктні, завантажувальні модулі; ОС і системні програми (компілятори, компоновщики і ін.), утиліти, діагностичні програми і т. д .;

- дані - збережені тимчасово і постійно, на магнітних носіях, друковані, архіви, системні журнали і т. д .;

- персонал - обслуговуючий персонал і користувачі.

Особливість забезпечення інформаційної безпеки в АС - таким абстрактним поняттям, як інформація, об'єкти і суб'єкти системи, відповідають фізичні уявлення в комп'ютерному середовищі:

-для подання інформації - машинні носії інформації у вигляді зовнішніх пристроїв комп'ютерних систем (терміналів, друкуючих пристроїв, різних накопичувачів, ліній і каналів зв'язку), оперативної пам'яті, файлів, записів і т. д .;

-об'єктам системи - пасивні компоненти системи, що зберігають, приймають або передають інформацію. Доступ до об'єкту означає доступ до інформації, що міститься в ньому;

-суб'єктам системи - активні компоненти системи, які можуть стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи. В якості суб'єктів можуть виступати користувачі, активні програми і процеси.

1.1.3. Базові властивості інформації

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

Конфіденційність даних - статус, наданий даними, який визначає необхідний ступінь їх захисту. До конфіденційних даних належать: особисті дані користувачів; облікові записи (імена і паролі); дані про кредитні картки; дані про розробки і різноманітні внутрішні документи; бухгалтерські відомості.

Конфіденційна інформація повинна бути відома тільки допущеним і тим, які пройшли перевірку (авторизованим) суб'єктам системи (користувачам, процесам, програмам). Для інших суб'єктів системи ця інформація повинна бути невідомою.

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

Цілісність інформації - властивість інформації зберігати свою структуру і / або вміст в процесі передачі і зберігання. Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних у вихідних документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування. Забезпечення цілісності даних є однією з складних завдань захисту інформації.

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

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

Доступність даних. Робота користувача з даними можлива тільки в тому випадку, якщо він має до них доступ.

Доступ до інформації - отримання суб'єктом можливості ознайомлення з інформацією, в 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 оперативними потребами.

Власник (рос. собственник) інформації - суб'єкт, в повному обсязі реалізує повноваження володіння, користування, розпорядження інформацією відповідно до законодавчим актам.

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

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

Право доступу до інформації - сукупність правил доступу до інформації, встановлених правовими документами чи власником (собственником) або власником (владельцем) інформації.

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

Розрізняють санкціонований і несанкціонований доступ до інформації.

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

Несанкціонований доступ до інформації - порушення встановлених правил розмежування доступу. Особа або процес, які здійснюють несанкціонованого доступу до інформації, є порушниками правил розмежування доступу. НСД є найбільш поширеним видом комп'ютерних порушень.

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

Доступність інформації означає також доступність компонента або ресурсу комп'ютерної системи, тобто властивість компонента або ресурсу бути доступним для законних суб'єктів системи.

Перелік ресурсів, які можуть бути доступні: принтери, сервери, робочі станції, дані користувачів, будь-які критичні дані, необхідні для роботи.

Цілісність ресурсу або компонента системи - це властивість ресурсу або компонента бути незмінним в семантичному сенсі при функціонуванні системи в умовах випадкових або навмисних спотворень або руйнівних впливів.

1.1.4. Ідентифікація, автентифікація, авторизація

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

Вони потрібні для доступу до: соцмереж, електронній пошті, інтернет-магазинів, форумів, інтернет-банкінгу, платіжних систем.

Ці три терміни є елементами захисту інформації. Перша стадія - ідентифікація. На ній відбувається розпізнавання інформації про користувача, наприклад, логін і пароль. Друга стадія - автентифікація. Це процес перевірки інформації про користувача. Третя стадія - авторизація. Тут відбувається перевірка прав користувача і визначається можливість доступу.

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 (легальним) суб'єктом.

Ідентифікація суб'єкта - це процедура розпізнавання суб'єкта за його ідентифікатором. Ідентифікація виконується при спробі суб'єкта увійти в систему (мережу). Наступним кроком взаємодії системи з суб'єктом є автентифікація суб'єкта.

Автентифікація суб'єкта - це перевірка сервером справжності суб'єкта з даним ідентифікатором. Процедура автентифікації встановлює, чи є суб'єкт

саме тим, ким він себе оголосив. Після ідентифікації і автентифікації суб'єкта виконують процедуру авторизації.

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

Рисунок 1.4. – Різниця між поняттями ідентифікація, автентифікація, авторизація

Методи автентифікації:
-Парольні
-Комбіновані
-Біометричні
-Інформація про користувача
-Дані користувача.
1)Парольні.

Найпоширеніший метод. Аутентифікація може проходити за одноразовими і багаторазовими паролями. Багаторазовий пароль задає користувач, а система зберігає його в базі даних. Він є однаковим для кожної сесії. До них відносяться PIN-коди, слова, цифри, графічні ключі. Одноразові паролі – різні для кожної сесії. Це може бути SMS з кодом.

2)Комбіновані

Цей метод говорить сам за себе. Аутентифікація відбувається з використанням декількох методів, наприклад, парольних і криптографічних сертифікатів. Він потребує спеціальний пристрій для зчитування інформації.

3)Біометричні

Це найдорожчий метод аутентифікації. Він запобігає витоку або крадіжці персональної інформації. Перевірка проходить за фізіологічними характеристиками користувача, наприклад, за відбитком пальця, сітківці ока, тембром голосу і навіть ДНК.

4)Інформація про користувача

Вона використовується для відновлення логіна або пароля і для двоетапної аутентифікації, щоб забезпечити безпеку. До цього методу відноситься номер телефону, дівоче прізвище матері, рік народження, дата реєстрації, кличка домашнього вихованця, місце проживання.

5)Дані користувача

Цей метод грунтується на геоданих про місцезнаходження користувача з використанням GPS, а також використовує інформацію про точки доступу бездротового зв'язку. Недолік полягає в тому, що за допомогою проксі-серверів можна підмінити дані.

Класифікація видів автентифікації

а)Залежно від кількості використовуваних методів

-Однофакторна. Використовується тільки один метод.

-Багатофакторна. Використовується кілька методів.

б)Залежно від політики безпеки систем і рівня довіри

-Одностороння. Користувач доводить право доступу до ресурсу його власнику.

-Взаємна. Перевіряється справжність прав доступу і користувача і власника сайту. Для цього використовують криптографічні способи.

1.2. Забезпечення безпеки.

1.2.1. Терміни та визначення

Під загрозою безпеки АС розуміються можливі дії, здатні прямо або побічно завдати шкоди її безпеці.

Під збитком безпеки мається на увазі порушення стану захищеності інформації, що міститься і обробляється в системі (мережі).

З поняттям загрози безпеки тісно пов'язане поняття уразливості комп'ютерної системи (мережі).

Уразливість комп'ютерної системи - це притаманна системі невдала властивість, яка може привести до реалізації загрози.

Атака на комп'ютерну систему - це пошук і / або використання

зловмисником тієї або іншої уразливості системи. Іншими словами, атака - це реалізація загрози безпеки.

Протидія загрозам безпеки є метою засобів захисту комп'ютерних систем і мереж.

Захищена система - це система із засобами захисту, які успішно і ефективно протистоять загрозам безпеки.

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

Засіб захисту - технічний, програмний засіб, речовина і / або матеріал, які призначені або використовуються для захисту інформації.

Комплекс засобів захисту (КЗЗ) - сукупність програмних і технічних засобів, що створюються і підтримуються для забезпечення інформаційної безпеки системи (мережі). КЗЗ створюється і підтримується відповідно до прийнятої в даній організації політики безпеки.

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

Забезпечення безпеки АС передбачає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування АС, а також спробам модифікації, розкрадання, виведення з ладу або руйнування її компонентів, тобто захист всіх компонентів АС - апаратних засобів, програмного забезпечення (ПО), даних і персоналу . Конкретний підхід до проблеми забезпечення безпеки заснований на розробленій для АС політиці безпеки.

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

1.2.2. Класифікація загроз інформаційної безпеки

Загроза (в загальному сенсі) - потенційно можлива подія (вплив, процес або явище), яке може привести до нанесення збитку чиїмось інтересам.

Загроза безпеки АС - будь-яка обставина або подія, яка прямо або побічно може завдати шкоди її безпеці, може бути причиною порушення політики безпеки інформації і / або нанесення шкоди АС.

Класифікація загроз

1) За природою виникнення:

-Природні загрози, викликані впливами на АС об'єктивних фізичних процесів або стихійних природних явищ;

-Штучні загрози безпеки АС, викликані діяльністю людини.

2) За ступенем навмисності прояви:

-Загрози, викликані помилками або халатністю персоналу, наприклад некомпетентне використання засобів захисту, введення помилкових даних і т.п.;

-Загрози навмисної дії, наприклад, дії зловмисників.

3)За безпосередім джерелом загроз:

-природне середовище, наприклад стихійні лиха, магнітні бурі та ін .;

-людина, наприклад вербування шляхом підкупу персоналу, розголошення конфіденційних даних і т. п .;

-санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі ОС;

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

4) За положенням джерела загроз:

-поза контрольованої зони АС, наприклад перехоплення даних, переданих по каналах зв'язку, перехоплення побічних електромагнітних, акустичних та інших випромінювань відпристроїв;

-в межах контрольованої зони АС, наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації і т. п .;

-безпосередньо в АС, наприклад некоректне використання ресурсів АС.

5) За ступенем залежності від активності АС:

-Незалежно від активності АС, наприклад, розшифрування шифрів криптозахисту інформації;

-Тільки в процесі обробки донних, наприклад, загрози виконання і розповсюдження програмних вірусів.

6) За ступенем впливу на АС:

-Пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті АС, наприклад загроза копіювання секретних даних;

-Активні загрози, які при впливі вносять зміни в структуру і зміст АС, наприклад впровадження троянських коней і вірусів.

7) За етапами доступу користувачів або програм до ресурсів АС:

-Загрози, які проявляються на етапі доступу до ресурсів АС, наприклад загрози несанкціонованого доступу в АС;

-Загрози, які проявляються після дозволу доступу до ресурсів АС, наприклад загрози несанкціонованого або некоректного використання ресурсів АС.

8) За способом доступу до ресурсів АС:

-Загрози, які здійснюються з використанням стандартного шляху доступу до ресурсів АС. Наприклад незаконне отримання паролів і інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;

-Загрози, які здійснюються з використанням прихованого нестандартного шляху доступу до ресурсом АС. Наприклад несанкціонований доступ до ресурсів АС шляхом використання недокументованих можливостей ОС.

9) За поточним місцем розташування інформації, що зберігається і обробляється в АС:

-Загрози доступу до інформації, що знаходиться на зовнішніх запам'ятовуючих пристроях, наприклад несанкціоноване копіювання секретної інформації з жорсткого диска;

-Загрози доступу до інформації, що знаходиться 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 помилкових повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим введенням дезінформації та нав'язуванням неправдивих повідомлень;

-Загрози доступу до інформації, яка відображається на терміналі або друкується але принтері, наприклад запис інформації, що відображається на приховану відеокамеру.

1.2.3. Структура та складові комплексної системи захисту інформації

Під комплексною системою захисту інформації (КСЗІ) розуміється сукупність організаційних та інженерних методів, апаратно-програмних засобів, які забезпечують захист інформації в автоматизованій системі (АС).

Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

Структура комплексної системи захисту інформації (КСЗІ) представлена на рис. 1.5.

До складу КСЗІ входять:

-Комплекс засобів захисту від НСД,

-Комплекс засобів блокування технічних каналів,

-Комплекс засобів криптографічного захисту,

-Фізична охорона об’єктів,

-Інженерно-технічні заходи,

-Служба захисту інформації.

Етапи розробки КСЗІ детально розглянуті в розділі 2.

Рисунок 1.5. - Структура комплексної системи захисту інформації (КСЗІ)

1.2.4. Класифікація автоматизованих систем

Мета введення класифікації АС і стандартних функціональних профілів захищеності - полегшення задачі співставлення вимог до КЗЗ обчислювальної системи АС з характеристиками АС.

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням АС.

Класифікація автоматизованих систем

1)Клас «1» — одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Істотні особливості:

-в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька;

-користувачі можуть мати різні повноваження (права) щодо доступу до інформації, яка обробляється.

Приклад - автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

2)Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Істотна відміна від попереднього класу - наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних ступенів обмеження доступу.

Приклад - ЛОМ.

3)Клас «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Істотна відміна від попереднього класу - необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад - глобальна мережа.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю (К), цілісністю (Ц) і доступністю (Д). В зв'язку з цим, в кожному класі АС х (х може бути 1, 2, або 3) виділяються такі підкласи, в яких підвищені вимоги до :

-підклас АС «х. К» — забезпечення конфіденційності оброблюваної інформації;

-підклас АС «х.Ц» — забезпечення цілісності оброблюваної інформації;

-підклас АС «х.Д» — забезпечення доступності оброблюваної інформації;

-підклас АС «х. КЦ» — забезпечення конфіденційності і цілісності оброблюваної інформації;

-підклас АС «х. КД» автоматизована система, в якій підвищені вимоги до забезпечення конфіденційності і доступності оброблюваної інформації;

-підклас АС «х. ЦД» — забезпечення цілісності і доступності оброблюваної інформації;

-підклас АС «х. КЦД» — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Контрольні питання

1. Обгрунтуйте значення інформаційної безпеки як складової частини національної безпеки України.

2. Назвіть складові системи забезпечення інформаційної безпеки України

3. Що є об'єктом та суб'єктом захисту інформації?

4. Назвіть компоненти автоматизованих систем (АС).

5. Назвіть та дайте визначення базовим властивостям інформації.

6. Що таке санкціонований та несанкціонований доступ до інформації?

7. У чому різниця між поняттями ідентифікація, автентифікація, авторизація?

8. Назвіть методи автентифікації.

9. Що таке політика безпеки інформації?

10. Приведіть класифікацію загроз.

11. Назвіть складові комплексної системи захисту інформації.

12. Приведіть класифікацію автоматизованих систем (класи та підкласи).

Розділ 2. ЕТАПИ РОЗРОБКИ ТА ПРИНЦИПИ СТВОРЕННЯ КСЗІ

Етапи розробки КСЗІ

1) Обстеження ІТС та підготовка базових даних для формування вимог до КСЗІ

2) Формування політики безпеки

3) Розробка ТЗ на створення КСЗІ

4) Розробка і реалізація проекту КСЗІ в ІТС

5) Введення КСЗІ в дію і оцінка захищеності інформації в ІТС

6) Попередні випробування

7) Дослідна експлуатація

8) Державна експертиза КСЗІ

9) Супровід КСЗІ

2.1. Обстеження ІТС та підготовка базових даних для формування вимог до КСЗІ

В ході першого етапу розробки КСЗІ виконується:

-аналіз нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

-визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів.

В ході етапу виконується обстеження середовищ функціонування ІТС.

ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІТС).

Метою обстеження є підготовка даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

2.1.1. Елементи обстеження ІТС

При обстеженні ІТС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);
- види і характеристики каналів зв'язку;
- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

2.1.2. Обстеження інформаційного середовища

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом.

Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

2.1.3. Обстеження фізичного середовища

При обстеженні фізичного середовища здійснюється аналіз взаємного

розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1.

Аналізу підлягають такі характеристики фізичного середовища:

-територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

-наявність охорони території та перепускний режим;

-наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

-режим доступу до компонентів фізичного середовища ІТС;

-вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

-наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;

-наявність та технічні характеристики систем заземлення;

-умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

-наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

2.1.4. Обстеження середовища користувачів

При обстеженні середовища користувачів здійснюється аналіз:

-функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

-повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

-повноважень користувачів щодо управління КСЗІ;

-наявності служби захисту інформації (СЗІ) в ІТС.

Оформлення результатів обстеження

Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС.

За результатами обстеження середовищ функціонування ІТС визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника.

Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

На цьому етапі:

-визначаються завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1 «Порядок проведення робіт»)

-здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

-визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації;

-здійснюється оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ (тактико-технічного завдання на створення КСЗІ.

2.1.5. Модель загроз

Загроза - будь-яка обставина або подія, яка може бути причиною порушення політики безпеки інформації та/або завдати шкоди АС.

Атака - спроба реалізації загрози.

Модель загроз - абстрактний формалізований чи неформалізований опис методів та способів реалізації загроз.

Основні принципи формування моделі загроз:

-Повнота аналізу загроз, адекватність моделі щодо реальних умов експлуатації АС

-Оцінка вірогідності реалізації загроз та розміру можливих збитків

-Врахування всіх існуючих загроз

-Формування окремих моделей загроз для досить незалежних компонентів АС

-Безперервний супровід моделі загроз (перегляд моделі загроз у зв'язку з модернізацією АС, зміною обладнання, складу користувачів, умов функціонування)

Загрози для інформації, що обробляється в ІТС, залежать від:

-Характеристик обчислювальної системи

-Фізичного середовища

-Персоналу

-Технологій обробки

-Оброблюваної інформації

Можливі способи реалізації загроз в АС:

-Технічні канали, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали.

-Канали спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації

-Несанкціонований доступ шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів

Основні види загроз, які можуть бути реалізовані стосовно АС:

-Зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

-Збої і відмови у роботі обладнання та технічних засобів АС;

-Наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

-Помилки персоналу (користувачів) АС під час експлуатації;

-Навмисні дії (спроби) потенційних порушників.

Класифікація загроз за результатами їхнього впливу на властивості КС:

-Порушення конфіденційності інформації - отримання користувачем чи процесом доступу до інформації в обхід політики розмежування доступу.

-Порушення цілісності інформації - повне або часткове знищення, зміна, нав'язування хибної інформації.

-Порушення доступності інформації - блокування доступу до інформації, неможливість пред'явити її користувачу в потрібному вигляді, повна або часткова втрата працездатності системи.

-Втрата спостережності чи керованості системою - порушення процедур аутентифікації користувачів, надання їм повноважень, здійснення контролю.

Загальна класифікація загроз представлена на рис. 2.1.

Рисунок 2.1. - Загальна класифікація загроз

Джерела загроз об'єктивної природи:

-Випадкові зміна умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту) природного характеру такі як: стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події;

-Випадкові зміна умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі як: аварія системи електропостачання, руйнування будівельних конструкцій приміщень, затоплення приміщень унаслідок аварії інженерних комунікацій холодного водопостачання, опалювання, пожежа або інші випадкові події;

-Випадкові збої і відмови в роботі оснащення і технічних засобів компонентів ІТС.

Джерела загроз суб'єктивної природи. Випадкові (ненавмисні):

-Наслідки помилок під час проектування і розробки компонентів ІТС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, даних та ін.);

-Помилки персоналу (користувачів) ІТС під час експлуатації оснащення і технічних засобів ІТС ;

Випадкові загрози суб’єктивної природи

Визначення: дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру, та призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.):

-Ненавмисне пошкодження носіїв інформації;

-Неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

Випадкові загрози суб’єктивної природи:

-Ненавмисне зараження ПЗ комп’ютерними вірусами;

-Невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

-Помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

-Будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

-Неправомірне впровадження і використання забороненого ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення);

-Наслідки некомпетентного застосування засобів захисту;

Джерела загроз суб'єктивної природи. Навмисні

-Навмисні зміни умов зовнішнього фізичного середовища техногенного характеру (аварії, пожежа або інші навмисні події);

-Навмисні зміни умов внутрішнього фізичного середовища такі як: аварія системи електропостачання, руйнування будівельних конструкцій, затоплення приміщень, пожежа або інші події;

-Навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів ІТС .

Джерела навмисних пасивних і активних можливих загроз:

-Внутрішні (нелояльні співробітники, користувачі системи)

-Зовнішні (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Навмисні загрози суб'єктивної природи

Визначення: загрози, що спрямовані на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів:

-Порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

-Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції);

-Порушення режимів функціонування АС (обладнання і ПЗ);

-Впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

-Використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

-Використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

-Крадіжки носіїв інформації, виробничих відходів (роздруків, записів);

-Несанкціоноване копіювання носіїв інформації;

-Читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

-Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

Неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

-Впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

-Інші.

Для кожної з загроз необхідно визначити:

1)на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями):

К-порушення конфіденційності,

Ц-цілісності,

Д-доступності інформації,

КС - спостережності та керованості АС;

2)джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

3)можливі способи здійснення загроз.

2.1.6. Модель порушника

Порушник – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи.

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін.

Модель порушника повинна визначати:

-можливу мету порушника та її градацію за ступенями небезпечності для АС;

-категорії осіб, з числа яких може бути порушник

-припущення про кваліфікацію порушника;

-припущення про характер його дій.

Мета порушника:

-отримання необхідної інформації;

-отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

-нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Категорія осіб, до якої може належати порушник

1. **внутрішні порушники** (з числа співробітників, користувачів системи):
    1. користувачі,
    2. інженерний склад,
    3. співробітники відділів, що супроводжують ПЗ,
    4. технічний персонал, що обслуговує будинок,
    5. співробітники служби безпеки,
    6. керівники.
2. **зовнішні порушники** (сторонні особи або будь-які особи, що

знаходяться за межами контрольованої зони).

Мотиви порушень

-Безвідповідальність

-Самоствердження

-Користь

-Професійний обов'язок

Класифікація порушників за рівнем можливостей

-перший рівень визначає можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

-другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

-третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

-четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Класифікація порушників за рівнем знань (рівні 1-найнижчий 4-найвищий):

1-володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

2- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

3-володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

4-володіють інформацією про функції та механізм дії засобів захисту.

Класифікація порушників за використовуваними методами та способами:

- використовують виключно агентурні методи одержання відомостей;

- використовують пасивні технічні засоби перехоплення інформаційних сигналів;

- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Класифікація порушників за часом дії:

-до впровадження АС або її окремих компонентів;

- під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.);

- під час функціонування АС (або компонентів системи);

- як у процесі функціонування АС, так і під час призупинки компонентів системи.

Класифікація порушників за місцем здійснення дії:

-без одержання доступу на контрольовану територію організації (АС);

- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

- з одержанням доступу до робочих місць кінцевих користувачів АС;

- з одержанням доступу до місць накопичення і зберігання інформації;

- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

2.1.7. Типові атаки на інформаційній ресурс.

Класифікація запропонована Пітером Меллом (Peter Mell):

-Віддалене проникнення (remote penetration). Атаки, які дозволяють реалізувати віддалене керування комп'ютером через мережу.

-Локальне проникнення (local penetration). Атака, що приводить до отримання несанкціонованого доступу до вузла, на якому вона ініційована.

- Віддалена відмова в обслуговуванні (remote denial of service). Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер через мережу (в тому числі через Інтернет).

- Локальна відмова в бслуговуванні (local denial of service). Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер, на якому вони ініційовані. Приклади атак цього типу: аплет, що перезавантажує процесор (наприклад, відкриттям великої кількості вікон великого розміру), що приводить до неможливості обробки запитів інших програм.

- Сканування мережі (network scanning). Аналіз топології мережі і активних сервісів, що доступні для атаки. Атака може здійснюватись за допомогою службового програмного забезпечення.

- Злом паролів (password cracking). Для цього використовуються програмні засоби, що підбирають паролі користувачів. В залежності від надійності системи зберігання паролів, можуть використовуватись методи зламу або підбору пароля за словником.

- Використання сканерів вразливостей (vulnerability scanning). Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Вони в першу чергу призначені служити

діагностичним інструментом системних адміністраторів, але можуть бути використані і як зброя для розвідки й атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus.

- Аналіз протоколів (sniffing) - прослуховування трафіку). Пасивна атака, яка спрямована на розкриття конфіденційних даних, зокрема, ідентифікаторів і паролів доступу.

- Підміна об’єкта (spoofing) - атаки, що спрямовані на введення в оману протоколів пошуку в мережі. Типові приклади: несправжній DNS-сервер, підміна IP-адреси джерела (IPspoofing), несправжній ARP-запит (ARPspoofing).

2.1.8. Методи несанкціонованого доступу (НСД).

НСД - найбільш поширений і різноманітний вид комп'ютерних порушень.

Основні канали НСД, через які порушник може отримати доступ до компонентів АС і здійснити розкрадання, модіфікацію і / або руйнування інформації:

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

Типи НСД:

З усього розмаїття способів і прийомів НСД зупинимося на наступних поширених і пов'язаних між собою порушень:

- перехоплення паролів;
- «маскарад»;
- незаконне використання привілеїв.

Перехоплення паролів

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 відразу пересилаються власнику програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається ОС.

Користувач думає, що припустився помилки при введенні пароля. Він повторює введення і отримує доступ до системи. Власник програми-

перехоплювача, який отримав ім'я і пароль законного користувача, може тепер використовувати їх у своїх цілях. Існують і інші способи перехоплення паролів.

«Маскарад»

«Маскарад» - це виконання будь-яких дій одним користувачем від імені іншого користувача, що володіє відповідними повноваженнями. Метою «маскараду» є приписування будь-яких дій іншому користувачеві або привласнення повноважень і привілеїв іншого користувача. Прикладами реалізації «маскараду» є:

- вхід в систему під ім'ям і паролем іншого користувача (цьому «маскараду» передує перехоплення пароля);
- передача повідомлень в мережі від імені іншого користувача.

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

Незаконне використання привілеїв.

Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій.

Кожен користувач отримує свій набір привілеїв: звичайні користувачі - мінімальний, адміністратори - максимальний.

Несанкціонований захват привілеїв, наприклад за допомогою «маскараду», призводить до можливості виконання порушником певних дій в обхід системи захисту.

Незаконний захват привілеїв можливий або при наявності помилок в системі захисту, або через недбалість адміністратора при управлінні системою і призначення привілеїв.

2.1.9. Аналіз ризиків та оцінка величини можливих збитків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС.

Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

1. Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі.

Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об’єкти захисту).

Для цього використовуються відомості, одержані в результаті

обстеження середовищ функціонування АС.

2. Ідентифікація загроз з об'єктами захисту

Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) АС.

Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АС.

У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригується модель загроз.

3. Оцінка ризиків

Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу.

Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій).

Оцінку слід робити за припущення, що кожна подія має найгірший закон розподілу, а також за умови відсутності заходів захисту інформації.

На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками.

У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку:

- експертним методом, на підставі досвіду експлуатації подібних систем
- шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози.

Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

4. Оцінка величини можливих збитків

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз.

Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози.

Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків.

Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

Вибір варіанту побудови КСЗІ

В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ.

Основний критерій – витрати на розробку, впровадження та експлуатацію КСЗІ не повинні перевищувати величину можливих збитків.

2.2. Формування політики безпеки (ПБ)

Під політикою безпеки інформації в Системі розуміється набір законів, нормативних документів, вимог, правил, обмежень, інструкцій, рекомендацій, що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених загроз.

Політика безпеки розробляється для окремого компонента Системи, послуги захисту і Системи в цілому.

2.2.1. Принципи розробки ПБ в ІТС

Політика безпеки інформації в Системі є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи і положення.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Зміст політики безпеки Системи визначається:

-технологією обробки інформації,

-моделями порушників і загроз,

-особливостями обчислювальної системи, фізичного середовища й інших факторів.

Політика безпеки повинна передбачати використання всіх можливих заходів захисту: правових і морально-етичних норм, організаційних (адміністративних) мір, фізичних, технічних (апаратних і програмних) способів і засобів захисту інформації, а також визначати правила і порядок їхнього застосування в Системі.

Політика безпеки повинна базуватися на принципах системності, комплексності, безперервності захисту, достатності механізмів і заходів

захисту і їхньої адекватності загрозам, гнучкості керування системою захисту, простоти і зручності її використання, відкритості алгоритмів і механізмів захисту.

Політика безпеки повинна доказово давати гарантії того, що:

- у Системі (у кожній окремій складовій частині, у кожній функціональній задачі і т.п..) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- у будь-якому середовищі функціонування Системи забезпечується оцінка і перевірка захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (щодо суб'єктів Системи), звітність (реєстрація, аудит) для всіх критичних з погляду безпеки ресурсів, до яких здійснюється доступ;
- персонал і користувачі забезпечені досить повним комплектом документації щодо порядку забезпечення захисту інформації;
- усі критичні з погляду безпеки інформації технології (функції) Системи мають відповідні плани забезпечення безупинної роботи і її поновлення у випадку виникнення непередбачених ситуацій.

2.2.2. Об’єкти захисту

Об’єктами захисту є:

- відомості (незалежно від виду їхнього представлення), віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в АС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;
- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;
- обладнання АС та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки.
- технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку та буферизації для утворення твердих копій, накопичувачі інформації;
- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- користувачі (персонал) АС, власникі інформації та АС, а також їхні права.

Забезпечення безпеки інформації в АС досягається:

- організацією та впровадженням системи допуску співробітників

(користувачів) до роботи з інформацією, яка потребує захисту;

- організацією обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв;
- організацією і координацією робіт з захисту інформації, яка обробляється та передається засобами АС;
- здійсненням контролю за забезпеченням захисту інформації, яка обробляється засобами АС, та за збереженням конфіденційних документів (носіїв).

2.2.3. Етапи розробка політики безпеки

На етапі розробки політики безпеки інформації розробник КСЗІ проводить:

-детальне вивчення об'єкта, на якому створюється КСЗІ,

-уточнює моделі загроз, потенційного порушника,

-готуються альтернативні варіанти концепції створення КСЗІ і планів їх реалізації, здійснює вибір найбільш оптимального варіанту.

На етапі розробки політики безпеки інформації здійснюється:

- вибір основних рішень з протидії всім суттєвим загрозам;
- формування загальних вимог, правил, обмежень, рекомендацій, які регламентують:
- використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації;
- діяльність користувачів всіх категорій;
- документальне оформлення політики безпеки інформації.

До основних розділів політики ІБ належить опис:

-об'єктів ОС;

-основних загроз інформації;

-принципів управління доступом користувачів до інформації (довірене або адміністративне);

-правил розмежування інформаційних потоків;

-правил маркування носіїв інформації;

-основних атрибутів доступу користувачів, процесів, пасивних об'єктів;

-правил розмежування доступу користувачів і процесів до пасивних об'єктів;

-правила адміністрування КЗЗ та реєстрації дії користувачів.

2.2.4. Методологія розробки політики безпеки

Методологія містить наступні роботи:

1. розробка концепції безпеки інформації в Системі;

2. аналіз ризиків – був розглянутий в ЛК 4;
3. визначення вимог до методів і засобів захисту;
4. вибір основних рішень по забезпеченню безпеки інформації;
5. організація виконання відбудовних робіт і забезпечення безупинного функціонування Системи;
6. документальне оформлення політики безпеки.

1.Концепція безпеки

Концепція безпеки інформації в АС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної АС і виконується на підставі аналізу наступних чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями АС;
- загроз, яким зазнають впливу ресурси АС, що підлягають захисту.

За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в АС:

-мета і пріоритети, яких необхідно дотримуватись в АС під час забезпечення безпеки інформації;

-загальні напрями діяльності, необхідні для досягнення цієї мети;

-аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;

-відповідальність посадових осіб та інших суб'єктів взаємовідносин в АС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Визначення вимог до заходів, методів та засобів захисту

3. Визначення вимог до заходів, методів та засобів захисту

Вихідними даними є:

- завдання і функції АС;
- результати аналізу середовищ функціонування АС;
- модель загроз, модель порушників;
- результати аналізу ризиків.

На підставі цих даних визначаються компоненти АС (наприклад, окрема ЛВС, спеціалізований АРМ, Internet-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в АС.

Для кожного компонента та (або) АС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99). Визначені вимоги складають

профіль захищеності інформації в АС (компоненті).

Для кожного компонента та (або) АС в цілому визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

4. Вибір основних рішень з забезпечення безпеки інформації

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

1. правовому;
2. організаційному;
3. технічному.

а) Правовий рівень

На правовому рівні повинні бути вироблені підходи щодо:

- системи нормативно-правового забезпечення робіт з захисту інформації в АС (організації);

- підтримки керівництвом організації заходів з забезпечення безпеки інформації, виконання правових та (або) договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ;

- процедур доведення до персоналу і користувачів АС основних положень політики безпеки, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

- системи контролю за своєчасністю, ефективністю і повнотою реалізації в АС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

б) Організаційний рівень

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

-застосування режимних заходів на об’єктах АС;

-забезпечення фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;

-організації проведення обстеження середовищ функціонування АС;

-порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;

-виконання робіт з модернізації АС (окремих компонентів);

-регламентації доступу сторонніх користувачів до ресурсів АС;

-регламентації доступу власних користувачів і персоналу до ресурсів АС;

-здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки,

попередження появи вірусів та ін.);

-реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до АС, використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого ПЗ та ін.).

Правила розмежування доступу (ПРД)

ПРД - є найбільш суттєвим елементом політики безпеки.

Загальні ПРД можуть бути наступними (в АС визначено такі ролі – адміністратор безпеки АС, адміністратор, користувач):

-кожне робоче місце повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

-для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів АС, керування механізмами захисту здійснюється адміністратором безпеки АС;

-для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ – користувачі, адміністратор, в АС - адміністратор безпеки АС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

-за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки АС. Такі роботи виконуються за його дозволом;

-кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки АС.

-видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

-користувачі проходять процедуру автентифікації для отримання доступу до ресурсів АС;

-атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;

-процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування та ін.), авторизовані і здійснюються під контролем адміністратора безпеки АС;

- усі користувачі повинні знати "Інструкцію користувача" (пройти

відповідний курс навчання, скласти іспит);

- адміністратор безпеки АС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

в) Технічний рівень

На технічному рівні повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації.

Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

-інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти АС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

-реєстрація санкціонованих користувачів АС, авторизація користувачів в системі;

-керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

-виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

-перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в АС;

-забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

-резервне копіювання критичних даних, супроводження архівів даних і ПЗ;

-відновлення роботи АС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

-захист ПЗ, окремих компонентів і АС в цілому від внесення несанкціонованих доповнень і змін;

-забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

5. Організація проведення відновлювальних робіт і забезпечення неперервного функціонування АС

Повинно бути планування і порядок виконання відновлювальних робіт після збоїв, аварій, інших надзвичайних ситуацій з метою забезпечення неперервного функціонування АС в захищеному режимі. Під час планування цих робіт враховуються наступні питання:

-виявлення критичних з точки зору безпеки процесів у роботі АС;

-визначення можливого негативного впливу надзвичайних ситуацій на роботу АС;

-визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

-підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення робіт

План повинен описувати дії щодо улагодження інцидента, дії щодо резервування, дії щодо відновлення. Він включає в себе:

-опис типових надзвичайних ситуацій, які потенційно найбільш можливі в АС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

-опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;

-опис процедур тимчасового переводу АС або окремих її компонентів на аварійний режим роботи;

-опис процедур поновлення нормальної виробничої діяльності АС або окремих її компонентів;

-порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

План підлягає перегляду у разі виникнення істотних змін в АС. Такими змінами можуть бути:

-встановлення нового обладнання або модернізація існуючого, включення до складу АС нових компонентів;

-встановлення нових систем життєзабезпечення АС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);

-проведення будівельно-ремонтних робіт;

-організаційні зміни у структурі АС, виробничих процесах, процедурах обслуговування АС;

-зміни у технології обробки інформації;

-зміни у програмному забезпеченні;

-будь-які зміни у складі і функціях КСЗІ.

6. Документальне оформлення політики безпеки

Результати робіт оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в АС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні розділи:

-загальний, у якому визначається відношення керівництва АС (організації) до проблеми безпеки інформації;

-організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад

з точки зору безпеки інформації, організація навчання та перепідго-товки персоналу, порядок реагування на порушення режиму безпеки та ін.);

-класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в АС, та необхідний рівень їхнього захисту;

-розділ, у якому визначаються ПРД до інформації;

-розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

-розділ, у якому висвітлюються питання фізичного захисту;

-розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

-розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

-розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування АС;

-юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

2.3. Концепція інформаційної безпеки компанії

Концепція інформаційної безпеки Компанії – сукупність офіційних поглядів керівництва Компанії на цілі, завдання, основні принципи та основні напрямки забезпечення безпеки інформації.

Мета – визначення принципових засад втілення корпоративної політики інформаційної безпеки в усі сфери життєдіяльності компанії

Структура концепції:

- Концептуальні положення інформаційної безпеки Компанії
- Мета, завдання та основні принципи забезпечення безпеки інформації Компанії
- Стратегія, основні напрямки та загальні методи забезпечення безпеки інформації
- Організаційна структура системи забезпечення безпеки інформації
- Засоби забезпечення безпеки інформації Компанії
- Основні положення корпоративної політики інформаційної безпеки Компанії
- Очікувані результати реалізації концепції.

2.3.1. Структура концепції інформаційної безпеки компанії

Структура концепції інформаційної безпеки компанії представлена на рис. 2.2. – 2.7.

Рисунок 2.2. - Концептуальна модель інформаційної безпеки Компанії

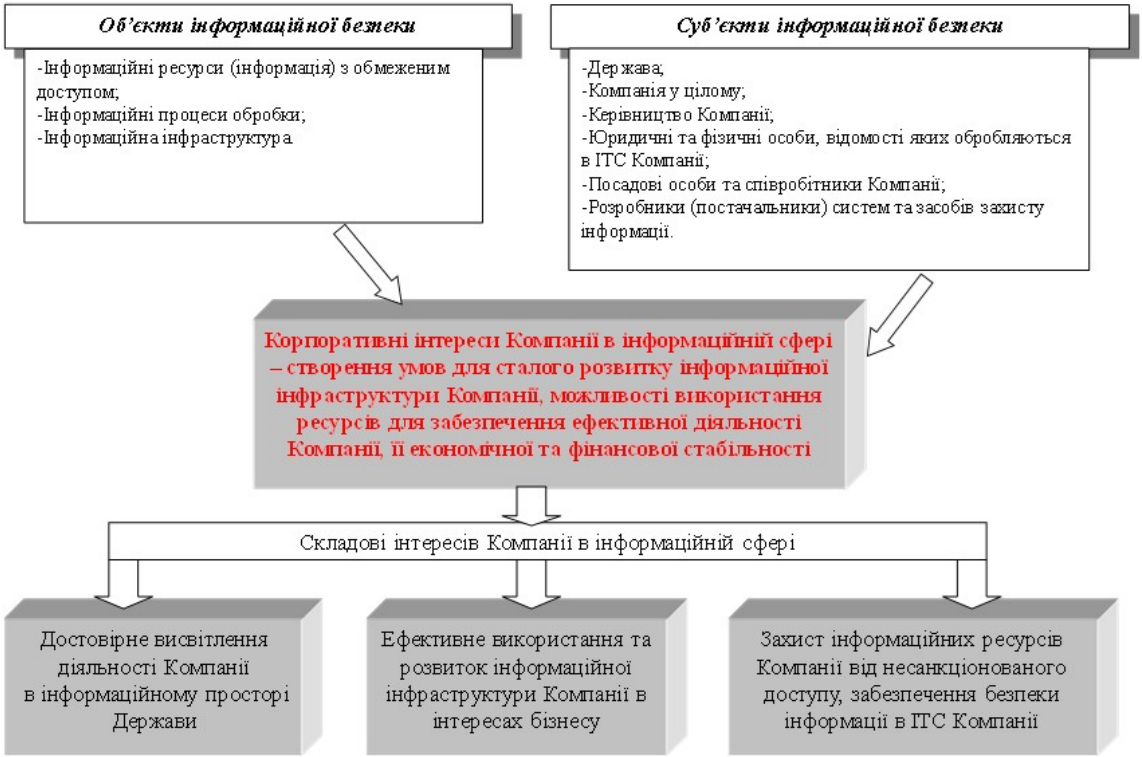

Рисунок 2.3. - Складові корпоративних інтересів

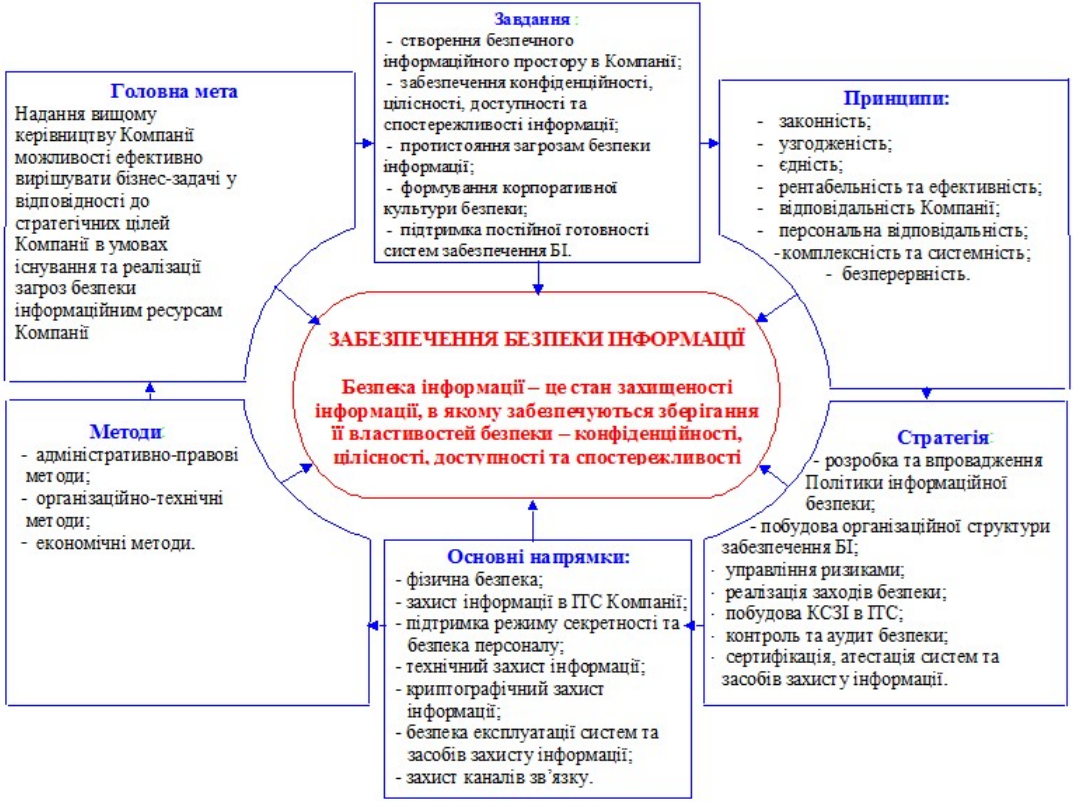

Рисунок 2.4. - Мета та завдання забезпечення безпеки інформації

Рисунок 2.5. - Система забезпечення безпеки інформації

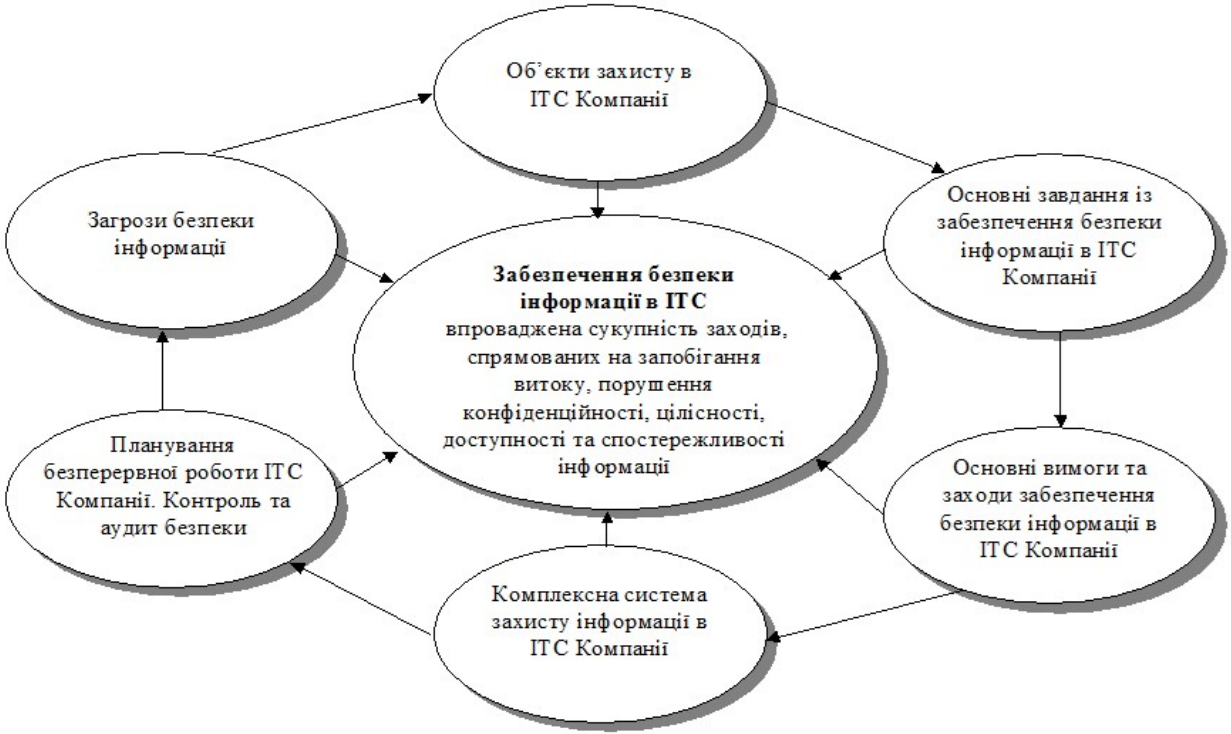

Рисунок 2.6. - Загальна модель забезпечення безпеки інформації в ІТС Компанії

Рисунок 2.7. - Комплексна система захисту інформації (принципи побудови, вимоги, функціональні підсистеми, послуги)

2.3.2. Структура критеріїв захищеності інформації0

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

- вимоги до функцій захисту (послуг безпеки);
- вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг (згідно з НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99).

Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз.

Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Рівні починаються з першого (1) і зростають до значення *n*, де *n* - унікальне для кожного виду послуг.

Структура критеріїв захищеності інформації представлена на рис. 2.8.

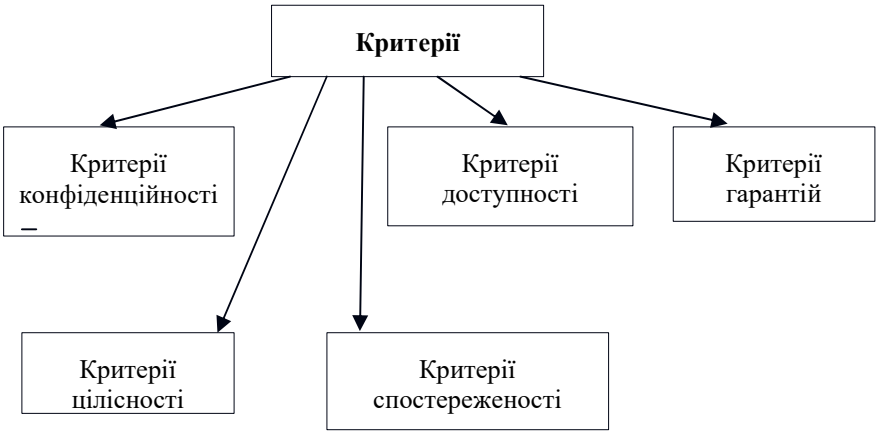

Рисунок 2.8. - Структура критеріїв захищеності інформації

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів:

-Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

-Цілісність. Загрози, що відносяться до несанкціонованої модифікації

інформації, становлять загрози цілісності.

-Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

-Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, розглядаються критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

В цих критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними.

Ієрархія рівнів гарантій відображає поступово наростаючу міру впевненості в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми їх реалізації є коректними і можуть забезпечити очікуваний споживачем рівень захищеності.

1)Критерії конфіденційності представлені на рис. 2.9.

Довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену (створеному користувачем), до інших користувачів. Рівні послуги:

КД-1. Мінімальна довірча конфіденційність

КД-2. Базова довірча конфіденційність

КД-3. Повна довірча конфіденційність

КД-4. Абсолютна довірча конфіденційність

Адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління:

КА-1. Мінімальна адміністративна конфіденційність

КА-2. Базова адміністративна конфіденційність

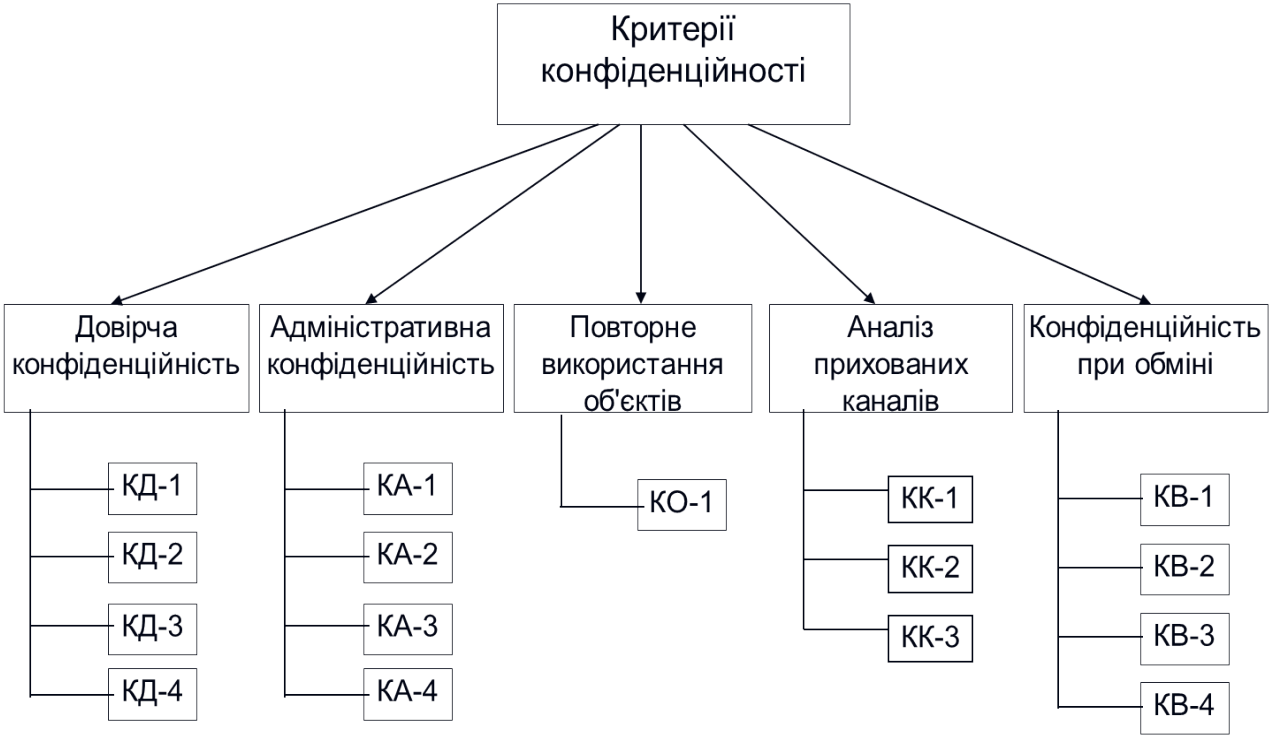

Рисунок 2.9. - Критерії конфіденційності

КА-3. Повна адміністративна конфіденційність

КА-4. Абсолютна адміністративна конфіденційність

Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Рівень - КО-1.

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги:

КК-1. Виявлення прихованих каналів

КК-2. Контроль прихованих каналів

КК-3. Перекриття прихованих каналів .

Конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги:

КВ-1. Мінімальна конфіденційність при обміні

КВ-2. Базова конфіденційність при обміні

КВ-3. Повна конфіденційність при обміні

КВ-4. Абсолютна конфіденційність при обміні

2)Критерії цілісності представлені на рис. 2.10.

Довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні послуги:

ЦД-1. Мінімальна довірча цілісність

ЦД-2. Базова довірча цілісність

ЦД-3. Повна довірча цілісність

ЦД-4. Абсолютна довірча цілісність

Адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні послуги:

ЦА-1. Мінімальна адміністративна цілісність

ЦА-2. Базова адміністративна цілісність

ЦА-3. Повна адміністративна цілісність

ЦА-4. Абсолютна адміністративна цілісність

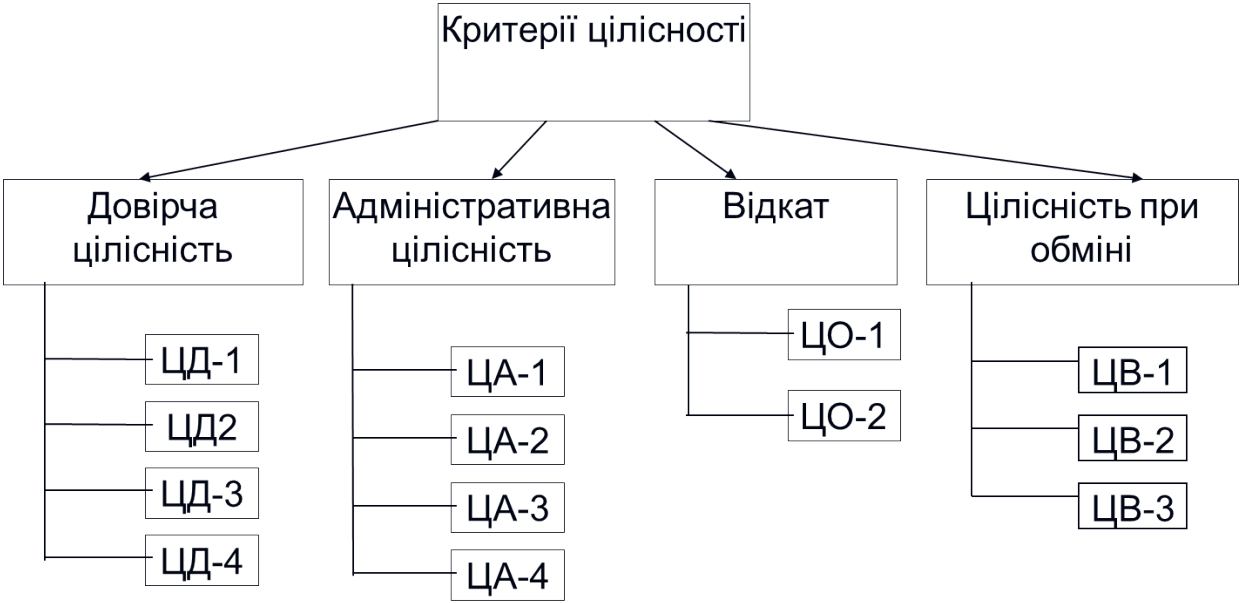

Рисунок 2.10. - Критерії цілісності

Відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

ЦО-1. Обмежений відкат - певний набір (множина) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦО-2. Повний відкат - всі операції, виконані над захищеним об'єктом за певний проміжок часу

Цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні послуги:

ЦВ-1: Мінімальна цілісність при обміні

ЦВ-2: Базова цілісність при обміні

ЦВ-3: Повна цілісність при обміні

3)Критерії доступності представлені на рис. 2.11.

Використання ресурсів. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні послуги:

ДР-1. Квоти

ДР-2. Недопущення захоплення ресурсів

ДР-3. Пріоритетність використання ресурсів

Стійкість до відмов. Ця послуга гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови:

ДС-1. Стійкість при обмежених відмовах

ДС-2. Стійкість з погіршенням характеристик обслуговування

ДС-3. Стійкість без погіршення характеристик обслуговування

Гаряча заміна. Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні послуги:

ДЗ-1. Модернізація. Модернізація КС не повинна призводити до необхідності проводити інсталяцію КС.

ДЗ-2. Обмежена гаряча заміна. Можливість заміни компонента без переривання обслуговування

ДЗ-3. Гаряча заміна будь-якого компонента

Відновлення після збоїв. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

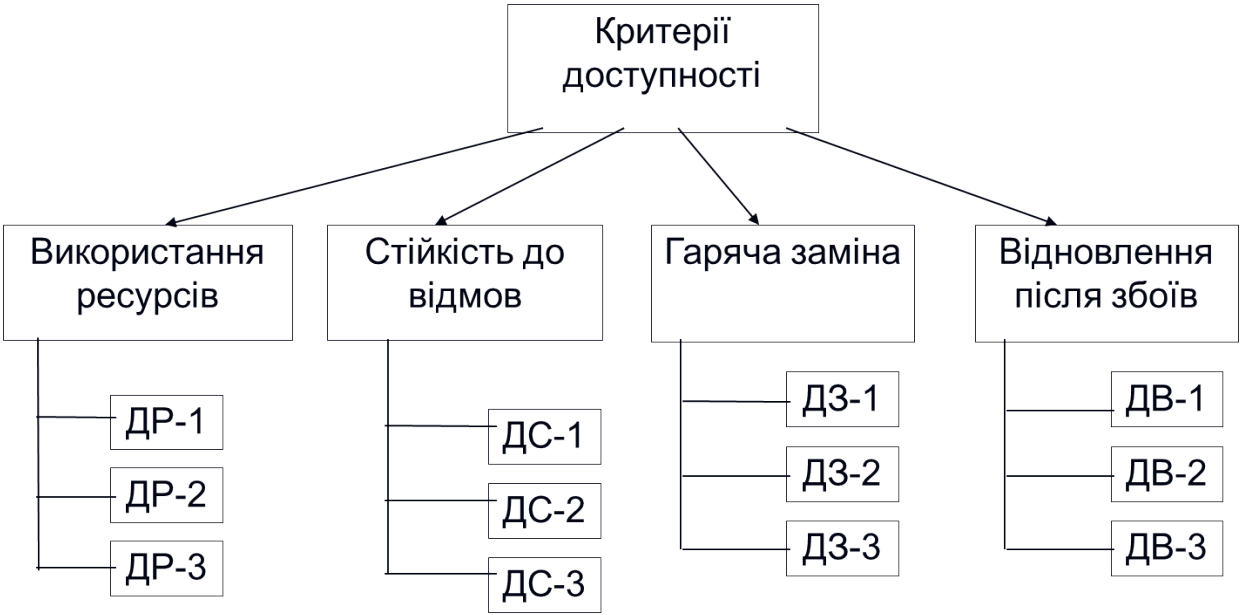

Рисунок 2.11. - Критерії доступності

ДВ-1. Ручне відновлення

ДВ-2. Автоматизоване відновлення

ДВ-3. Вибіркове відновлення

4)Критерії спостереженості представлені на рис. 2.12-2.13.

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НР-1. Зовнішній аналіз

НР-2. Захищений журнал

НР-3. Сигналізація про небезпеку

НР-4. Детальна реєстрація

НР-5. Аналіз в реальному часі

Достовірний канал Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ та виконувати захищений обмін. Рівні послуги:

НК-1. Однонаправлений достовірний канал

НК-2. Двонаправлений достовірний канал

Цілісність комплексу засобів захисту. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НЦ-1. КЗЗ з контролем цілісності

НЦ-2. КЗЗ з гарантованою цілісністю

НЦ-3. КЗЗ з функціями диспетчера доступу

Ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НИ-1. Зовнішня ідентифікація і автентифікація

НИ-2. Одиночна ідентифікація і автентифікація

НИ-3. Множинна ідентифікація і автентифікація

Розподіл обов'язків. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НО-1. Виділення адміністратора

НО-2. Розподіл обов'язків адміністраторів

НО-3. Розподіл обов'язків на підставі привілеїв

Самотестування. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні послуги:

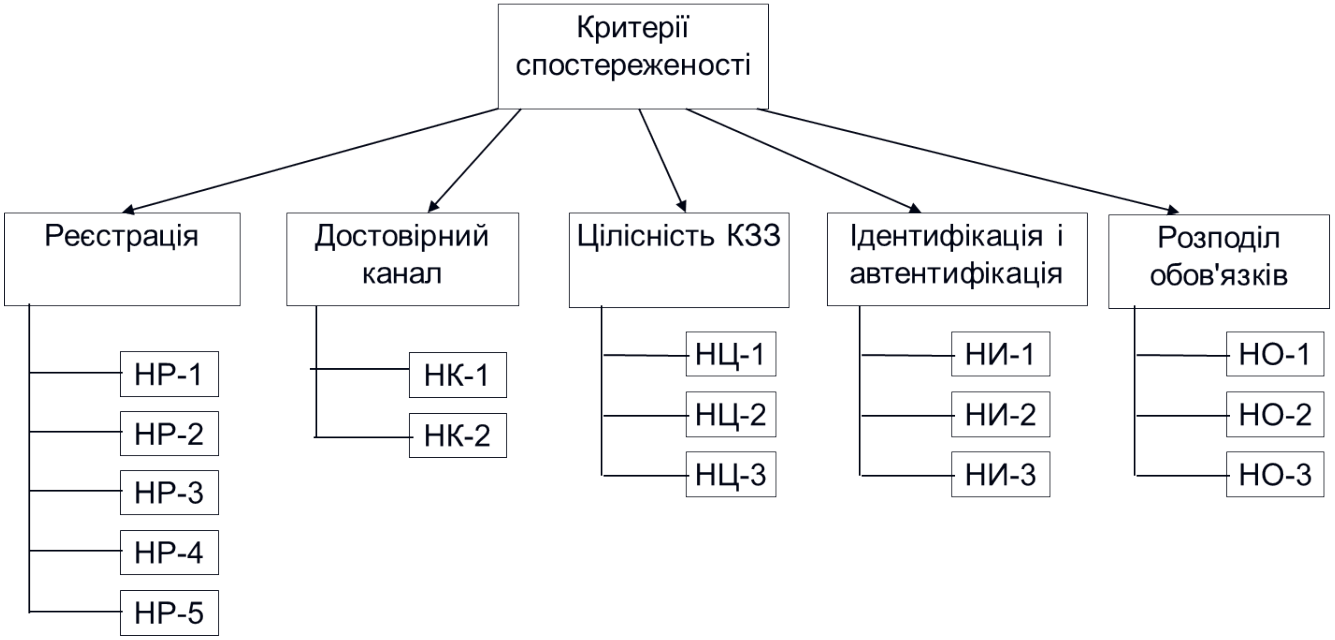

Рисунок 2.12. - Критерії спостереженості (частина 1)

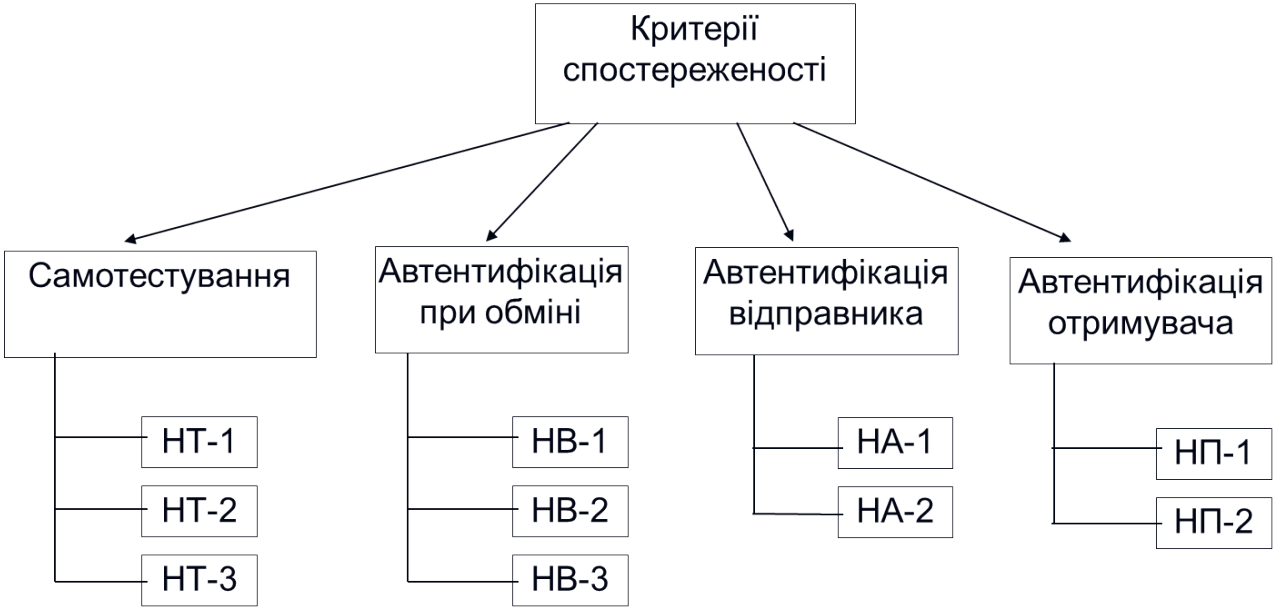

Рисунок 2.13. - Критерії спостереженості (частина 2)

НТ-1. Самотестування за запитом

НТ-2. Самотестування при старті

НТ-3. Самотестування в реальному часі

Ідентифікація і автентифікація при обміні. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні послуги:

НВ-1: Автентифікація вузла

НВ-2: Автентифікація джерела даних

НВ-3: Автентифікація з підтвердженням

Автентифікація відправника. Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НА-1: Базова автентифікація відправника

НА-2: Автентифікація відправника з підтвердженням

Автентифікація отримувача. Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НП-1: Базова автентифікація отримувача

НП-2: Автентифікація отримувача з підтвердженням

5)Критерії гарантій представлені на рис. 2.14.

Критерії гарантій включають вимоги до:

- архітектури КЗЗ,
- середовища розробки,
- послідовності розробки,
- середовища функціонування,
- документації і випробувань КЗЗ.

В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Більшість з вимог критеріїв гарантій являють собою конкретизацію вимог щодо створення КЗЗ КС стандартів серії ДСТУ ISO 9000 і для їх викладення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95).

Рисунок 2.14. - Критерії гарантій

2.4. Вимоги до КСЗІ. Розробка функціонального профілю захищеності

Вимоги до КСЗІ в формалізованому виді задаються в вигляді функціонального профілю захищеності.

Функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти необхідні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих функціональних послуг (див. п. 2.3.2.), що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються до КЗСІ.

2.4.1. Функціональний профіль захищеності. Семантика профілю.

Опис профілю складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки.

$$I=\{U1, U2, \ldots, Un\}$$

Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад:

2.К.4 - функціональний профіль номер чотири, що визначає вимоги до АС класу 2 (локальна мережа), призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності (К).

3.ЦД.1 - функціональний профіль номер один, що визначає вимоги до АС класу 3 (розподілена система), призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення цілісності (Ц) та доступності (Д) оброблюваної інформації.

Приклад профілю:

3.КЦ.1 = { КД-2, ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1 } -

функціональний профіль №1, для АС класу 3 (розподілена система), з основними вимогами по забезпеченню конфіденційності (К) та цілісності (Ц), повинен забезпечувати наступний перелік рівнів послуг:

КД-2. Базова довірча конфіденційність

ЦД-1. Мінімальна довірча цілісність

НР-2. Захищений журнал

НИ-2. Одиночна ідентифікація і автентифікація користувачів

НК-1. Однонаправлений достовірний канал

НО-1. Виділення адміністратора

НЦ-1. КЗЗ з контролем цілісност

2.4.2. Стандартні профілі та рекомендації щодо їх використання

В розд. НД ТЗІ 2.5-005-99 наведені стандартні профілі захищеності для різних класів АС, що описують вимоги до КЗЗ ОС, які входять до складу цих АС. Наведені профілі відповідають тим видам КС, потреба в яких найактуальніша.

До всіх профілів включені послуги спостереженості, оскільки, з одного боку, реалізація багатьох з них є необхідною умовою для реалізації інших послуг, а з іншого, - спостереженість та керованість важливі для будь-якої системи, що реалізує будь-які функції захисту інформації.

Рекомендації щодо вибору профілю захищеності залежно від призначення АС:

а)АС автоматизації діяльності органів державної влади.

В них часто обробляється інформація з обмеженим доступом, тому у першу чергу пред'являються вимоги щодо забезпечення конфіденційності оброблюваної інформації, персональної відповідальності користувачів за дотримання режиму секретності.

Рекомендується використовувати профілі х.К.х. Якщо існують додаткові вимоги, то рекомендується використовувати профілі х.КЦ.х., хКД.х., х.КЦД.х.

б)АС автоматизації банківської діяльності

Основні загрози для банківської інформації:

- це в першу чергу загрози шахрайства (підробка, відмова від авторства, відмова від одержання) і порушення технології роботи;

- в другу - порушення доступності і конфіденційності.

Крім того, вимоги істотно залежать від того, чи здійснюється обробка в реальному часі або відкладена обробка. Необхідно врахувати, що банківські АС, як правило, відносяться до класу 3, тобто є розподіленими.

В зазначених АС рекомендується використовувати КЗЗ, що реалізують профілі 3. КЦД.х.

в)АС керування технологічними процесами

Основними загрозами для інформації оброблюваної в АС керування технологічними процесами є загрози порушення доступності АС і технології обробки інформації. В зв'язку з цим до КЗЗ ОС, що входять до складу таких АС, в першу чергу пред'являються вимоги до забезпечення доступності і адміністративного керування доступом щодо інформації з боку об'єктів-процесів.

В зазначених АС рекомендується використовувати КЗЗ, які реалізують профілі 1.ЦД.х., 2.ЦД.х.

г)Довідково-пошукові системи

Основними загрозами для довідково-пошукових систем масового обслуговування є порушення їх доступності. В зв'язку з цим до КЗЗ ОС, що входять до складу таких систем, в першу чергу пред'являються вимоги щодо забезпечення доступності.

В зазначених АС рекомендується використовувати КЗЗ, які реалізують профілі х.Д.х., х.ЦД.х.

2.5. Служба захисту інформації, структура та функції.

Метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в АС та здійснення контролю за її функціонуванням.

На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проектування, розроблення і модернізації КСЗІ, а також з

експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

СЗІ є штатним підрозділом організації безпосередньо підпорядкованим керівнику організації (або його заступнику)

Або:

СЗІ є структурною одиницею служби безпеки організації.

Структура СЗІ, її склад і чисельність визначається фактичними потребами АС для виконання вимог політики безпеки інформації та затверджується керівництвом організації.

Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань з захисту інформації в АС.

Основні обов'язки СЗІ:

-організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в АС;

-вчасно і в повному обсязі доводити до користувачів і персоналу АС інформацію про зміни в галузі захисту інформації, які їх стосуються;

-перевіряти відповідність прийнятих в АС (організації) правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

-здійснювати контрольні перевірки стану захищеності інформації в АС;

-негайно повідомляти керівництво АС (організації) про виявлені атаки та викритих порушників;

-інші обов'язки.

Функції служби захисту інформації:

1)Функції під час створення комплексної системи захисту інформації:

-визначення об'єктів захисту в АС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації,

-розробка та коригування моделі загроз і моделі захисту інформації в АС, політики безпеки інформації в АС;

-визначення і формування вимог до КСЗІ;

-організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах з створення КСЗІ;

-організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

-участь у розробці нормативних документів, чинних у межах організації і АС, які встановлюють правила доступу користувачів до ресурсів АС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

2)Функції під час експлуатації комплексної системи захисту інформації:

Основною функцією є організація процесу керування КСЗІ, зокрема:

-забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

-організація керування доступом до ресурсів АС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

-спостереження (реєстрація і аудит подій в АС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

-негайне втручання в процес роботи АС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

-контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації

-контроль за забезпеченням охорони і порядку зберігання носіїв інформації, які містять відомості, що підлягають захисту.

3)Функції з організації навчання персоналу з питань забезпечення захисту інформації:

-розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу АС;

-розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в організації (АС), необхідний рівень її захищеності та ін.;

-участь в організації і проведенні навчання користувачів і персоналу АС правилам забезпечення захисту інформації;

-роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

-взаємодія з державними органами, учбовими закладами, іншими організаціями з питань навчання та підвищення кваліфікації;

-участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та ін.

Штат СЗІ

Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту (вищу, середню спеціальну, спеціальні курси підвищення кваліфікації у галузі ТЗІ) та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації.

Функціональні обов’язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом АС (організації).

В залежності від обсягів і особливостей завдань СЗІ до її складу можуть входити спеціалісти (групи спеціалістів, підрозділи та ін.) різного фаху:

-спеціалісти з питань захисту інформації від витоку технічними каналами;

-спеціалісти з питань захисту каналів зв’язку і комутаційного

обладнання, налагодження і керування активним мережевим обладнанням;

-спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;

-спеціалісти з питань захищених технологій обробки інформації.

За посадами співробітники СЗІ поділяються на такі категорії (за рівнем ієрархії):

-керівник СЗІ;

-адміністратори захисту АРМ (безпеки баз даних, безпеки системи тощо);

-спеціалісти служби захисту.

З метою забезпечення конфіденційності робіт, які виконуються співробітниками СЗІ, при прийомі на роботу (звільненні з роботи) вони дають письмові зобов'язання щодо нерозголошення відомостей, що становлять службову, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

СЗІ здійснює свою роботу у відповідності з планами робіт. До планів включаться наступні основні заходи:

-разові (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);

-постійно виконувані (заходи, що потребують виконання неперервно або дискретно у випадковий чи заданий час);

-періодично виконувані (з заданим інтервалом часу);

-виконувані за необхідності (заходи, що потребують виконання під час здійснення або виникнення певних змін в АС чи зовнішньому середовищі).

Основними видами планів робіт СЗІ можуть бути:

-календарний план робіт (щодо реалізації заходів з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань);

-план заходів з оперативного реагування на непередбачені ситуації (в тому числі надзвичайні та аварійні) та поновлення функціонування АС;

-поточний план робіт (на місяць, квартал, рік);

-перспективний план розвитку та удосконалення діяльності СЗІ з питань захисту інформації (до 5 років);

-план заходів з забезпечення безпеки інформації під час виконання окремих важливих робіт, при проведенні нарад, укладенні договорів, угод тощо

Взаємодія СЗІ з іншими підрозділами організації та зовнішніми організаціями

Заходи з захисту інформації в АС повинні бути узгоджені СЗІ з заходами охоронної та режимно-секретної діяльності інших підрозділів організації.

СЗІ взаємодіє з:

-режимно-секретним відділом організації;

-службою безпеки, охорони та пожарної безпеки організації;

-адміністрацією АС та іншими підрозділами організації, виробнича діяльність яких пов'язана з захистом інформації або її автоматизованою обробкою;

-зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;

-підрозділами служб безпеки іноземних фірм – партнерів;

-іншими суб'єктами діяльності у сфері захисту інформації, зокрема координує свою діяльність з аудиторською службою під час проведення аудиторських перевірок.

2.6. Розробка технічного завдання (ТЗ) на створення КСЗІ.

Для виконання будь якого проекту (в тому числі в галузі ІТ-технологій) необхідна розробка проектної документації.

Першим і визначальним документом є технічне завдання (ТЗ) на розробку – своєрідний договір між Замовником та Виконавцем, в якому прописані вимоги Замовника щодо характеристик розробленої продукції, методи їх контролю, терміни та етапи розробки (календарний план), фінансування, та ін.

В навчальних проектах (бакалаврський та магістерський дипломний проекти) обов'язковим елементом є ТЗ.

Основними нормативними документами, які використовуються при розробці ТЗ на створення КСЗІ є:

-НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

-НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

-НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від не санкціонованого доступу.

Розробка ТЗ

ТЗ на створення КСЗІ в ІТС є організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої АС.

ТЗ на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІТС.

Для експертної організації ТЗ на КСЗІ є документом, що визначає основні критерії відповідності КСЗІ вимогам Замовника і загрозам, що діють у середовищі експлуатації.

Перелік основних робіт етапу формування ТЗ такий:

-класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій), технології обробки, персоналу і користувачів, території і приміщень і ін.);

-опис інформаційних потоків АС, інтерфейсів між користувачем і АС;

-визначення переліку загроз і можливих каналів витоку інформації;

-експертна оцінка очікуваних втрат у разі здійснення загроз;

-визначення послуг безпеки, які треба реалізувати;

-обгрунтування необхідності проведення спецперевірок і спецдосліджень основних технічних засобів (ОТЗ) та додатнових технічних засобів (ДТЗ);

-визначення вимог до організаційних, фізичних та інших заходів захисту;

-прийняття остаточного рішення про склад КСЗІ.

Основними розділами документа ‘‘ТЗ на створення КСЗІ’’ є:

1. загальні відомості;
2. мета і призначення КСЗІ;
3. загальна характеристика автоматизованої системи та умов її функціонування;
4. вимоги до КСЗІ;
5. вимоги до складу проектної та експлуатаційної документації;
6. етапи виконання робіт;
7. порядок внесення змін і доповнень до ТЗ;
8. порядок проведення випробувань КСЗІ.

1. Загальні відомості

В підрозділі зазначають:

-повне найменування КСЗІ та її умовне позначення;

шифр теми і реквізити договору;

-найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;

-перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;

-планові терміни початку і закінчення роботи із створення КСЗІ;

-відомості про джерела і порядок фінансування робіт;

-порядок оформлення і подання замовнику результатів робіт

2. Мета і призначення КСЗІ

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування.

Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

3. Загальна характеристика автоматизованої системи та умов її функціонування

Зазначаються такі моменти, які впливають на безпеку інформації та на загальні вимоги до СЗІ:

-загальну структурну схему і склад ОС АС;

-технічні характеристики каналів зв'язку;

-характеристики інформації, що обробляється (категорії інформації, гриф секретності і т.д.);

характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);

-характеристики фізичного середовища (наявність категорованих приміщень, територіальне розміщення, захищеність від засобів технічної розвідки і т.п.);

4. Вимоги до КСЗІ

а)Вимоги до КСЗІ в АС в частині захисту від несанкціонованого доступу (НСД):

-Повинні бути зазначені вимоги обох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій.

-Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати.

-Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту АС.

б)Вимоги до КСЗІ в АС в частині захисту від витоку інформації технічними каналами:

-Загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання.

-Вимоги до розмірів зони безпеки інформації.

-Необхідні величини показників захищеності:

■ -відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті;

■ -відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті;

■ -величина нерівномірності струму, який споживається по мережі електроживлення;

■ -коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

-Вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності :

■ -системо- і схемотехнічних методів (екранування, фільтри)

■ -оптимального розміщення обєктів та ін.

5. Вимоги до складу проектної та експлуатаційної документації

Склад обов'язкової проектної і експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій).

Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

6. Етапи виконання робіт

Процес створення КСЗІ доцільно поділяти на три основні етапи:

- попередній,
- проектування і розробка КСЗІ,
- проведення випробувань і передача в експлуатацію КСЗІ.

Кожний з етапів допускається поділяти на окремі підетапи.

7. Порядок внесення змін і доповнень до ТЗ

Зміни затвердженого ТЗ на створення КСЗІ в АС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в АС складається з вступної частини і змінюваних підрозділів. У вступній частині зазначається причина випуску доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються

8. Порядок проведення випробувань КСЗІ.

Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє "Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в АС", яка затверджується в установленому порядку.

Терміни подання проекту Програми, його розгляду і затвердження погоджуються з Замовником.

Для проведення випробувань Замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

2.7. Розробка проекту КСЗІ (ескізний, технічний, робочий проект)

Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект. Дозволяється вилучати етап "Ескізний проект КСЗІ", а також поєднувати етапи "Технічний проект КСЗІ" і "Робочий проект КСЗІ" в один етап "Техноробочий проект КСЗІ".

Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ.

Технічний проект КСЗІ

Виконується розробка:

-загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ;

-рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту;

-рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

Виконується розробка, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

Готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ.

Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розробку відповідних засобів.

Робочий проект КСЗІ

На цьому етапі здійснюється розробка, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

Робоча документація містить детальні рішення щодо:

- реалізації технічного проекту КСЗІ,

-забезпечення управління КСЗІ і взаємодії її компонентів,

-документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

- проводиться розробка засобів захисту інформації, або адаптація готової продукції до умов функціонування КСЗІ.

До складу робочої документації на комплекси технічного захисту інформації від витоку технічними каналами повинні входити:

Схеми розміщення обєктів ІТС, кабельного обладнання, мереж живлення та систем заземлення,

При цьому враховуються умови їх розміщення і мінімально допустимі відстані між цими засобами та додаткових засобів (засоби зв'язку, системи та засоби кондиціювання, сигналізації, електроосвітлення, радіомовлення, часофікації тощо), що знаходяться у приміщенні, де розташоване обладнання ІТС, та у суміжних приміщеннях.

До складу робочої документації на програмне забезпечення КСЗІ повинні входити:

- описи процедур інсталяції та ініціалізації комплексу,
- налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС,
- контролю за діями користувачів,
- формування та актуалізації баз даних захисту,
-контроль цілісності програмного забезпечення та баз даних захисту.

Експлуатаційна документація включає:

- опис порядку функціонування КСЗІ
-настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами,
- порядку супроводження КСЗІ впродовж життєвого циклу ІТС.

2.8. Введення КСЗІ в дію і оцінка захищеності інформації в ІТС

Введення в дію КСЗІ здійснюється за наступним планом:

-Етап підготовки
-Пусконалагоджувальні роботи
-Попередні випробування.

2.8.1. Введення в дію КСЗІ. Етап підготовки

На етапі підготовки виконуються:

-роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС. Здійснюється створення СЗІ, якщо цього не було зроблено на попередніх етапах.

-навчання користувачів ІТС всіх категорій основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

-забезпечується отримання продукції (засобів захисту інформації,

матеріалів, обладнання та ін.) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідних сертифікату або експертного висновку.

- при проведенні будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ в ІТС. Будівельні роботи здійснюються силами організації-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво.

- після завершення будівельних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника будівельних робіт, проектної та будівельно-монтажної організацій. За результатами роботи комісії складається за довільною формою акт приймання робіт з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.

-проводяться пусконалагоджувальні роботи.

2.8.2. Пусконалагоджувальні роботи

В ході пусконалагоджувальних робіт здійснюється:

-монтаж обладнання і атестація комплексу технічного захисту інформації від витоку технічними каналами;

-встановлення і налагодження КЗЗ;

-перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІТС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на здійснення відповідного виду робіт.

За результатами робіт складається акт, де зазначаються: категорії приміщень, де розташоване обладнання ІТС, межі контрольованих зон для приміщень, перелік ОТЗ, ДТЗ і комунікацій, що знаходяться у цих приміщеннях, оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та нормативних документів, визначених на 4 етапі, пропозиції щодо застосування додаткових заходів захисту. Акт затверджується керівником організації - власника ІТС.

Оцінка повноти та якості

Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу технічного захисту

інформації від витоку технічними каналами, за результатами якої надається документ– “Акт атестації комплексу технічного захисту інформації”.

Перевірка працездатності КЗЗ

Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту КЗЗ.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об’єктів КС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані.

2.8.3. Попередні випробування

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС.

Результати попередніх випробувань оформлюються “Протоколом випробувань”, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

2.9. Дослідна експлуатація.

Під час дослідної експлуатації КСЗІ:

-відпрацьовуються технології оброблення інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

-співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

-здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ; коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

2.10. Державна експертиза КСЗІ

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Приймальні випробування ІТС проводяться при функціонуючій в її складі КСЗІ.

Суб'єкти експертизи:

-Замовники: юридичні та фізичні особи - власники КСЗІ ;

-Організатори: підприємства, установи та організації, які проводять експертизу;

-Експерти: фізичні особи, які на постійній або професійній основі виконують експертні роботи

-Державні органи, які проводять експертизу у сфері свого управління;

-Адміністрація Держспецзв’язку.

Об'єкти експертизи:

-КСЗІ, які є невід'ємною складовою інформаційно-телекомунікаційної системи (ІТС);

-Технічні та програмні засоби, які реалізують функції технічного захисту інформації (ТЗІ);

-Організаційно-технічні рішення на розгортання типових складових компонентів КСЗІ в ІТС (ОТР КСЗІ).

Методи проведення експертизи

Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам нормативних документів із ТЗІ, та проводиться шляхом експертних випробувань або шляхом аналізу декларації.

1)Експертиза шляхом експертних випробувань:

- засобів технічного захисту інформації:
- Організаційно-технічних рішень КСЗІ
- КСЗІ (у більшості випадків)

2)Експертиза (тільки КСЗІ) шляхом аналізу декларації проводиться у випадках:

-ІТС є одномашинним однокористувачевим комплексом, але число користувачів в різні моменти часу може бути декілька з різними ступенями доступу

-засоби захисту інформації від НСД, засоби антивірусного захисту мають чинний на момент подання декларації позитивний експертний висновок;

-комплекс захисту інформації від витоку технічними каналами засвідчено актом атестації.

Експертиза може бути первинною, додатковою та контрольною.

-Первинна експертиза є основним видом експертизи.

-Додаткова експертиза проводиться якщо відкрилися нові наукові та науково-технічні обставини, а також у зв'язку із закінченням строку дії документів, що засвідчують результати експертизи.

-Контрольна експертиза проводиться іншим Організатором з ініціативи Замовника у разі наявності у нього обґрунтованих претензій до первинної чи додаткової експертизи або з ініціативи Адміністрації Держспецзв'язку для перевірки висновку первинної чи додаткової експертизи.

Порядок проведення експертизи

1)Між Замовником і Організатором укладається договір на проведення експертизи, в якому вказані:

-Витрати, пов'язані з проведенням експертизи.

-Строк проведення експертизи

-Кількість і персональний склад експертів (визначається Організатором).

2)Замовник надає Організатору комплект технічної документації, необхідної для проведення експертних випробувань.

3)Організатор за результатами аналізу наданих документів формує:

- програму і методику проведення експертизи об'єкта,

-здійснює відбір зразків засобів ТЗІ та складає перелік необхідного програмно-технічного забезпечення для проведення випробувань.

4)Програма проведення експертизи погоджується із Замовником та уповноваженим структурним підрозділом Адміністрації Держспецзв'язку,.

5)Результати роботи оформлюються у вигляді протоколу виконання робіт, який затверджується Організатором.

6)У разі виявлення невідповідності об'єкта експертизи вимогам Організатор може запропонувати Замовнику виконати доопрацювання.

Результати експертизи

За результатами проведених робіт Організатор складає:

-Експертний висновок та в разі позитивних результатів експертної оцінки - атестат відповідності КСЗІ;

-Експертний висновок для засобу ТЗІ;

-Експертний висновок для ОТР КСЗІ.

Зазначені документи засвідчуються Організатором і разом з протоколами виконання робіт подаються до Адміністрації Держспецзв'язку.

Строки дії

Строк дії вище названих документів визначаються Організатором з урахуванням вимог:

-для атестата відповідності КСЗІ АС класу 1 - безстроковий;

-для атестата відповідності КСЗІ АС класів 2, 3 - до 5 років;

-для Експертного висновку на засіб ТЗІ - до 3 років;

-для Експертного висновку на ОТР КСЗІ - до 5 років.

2.11. Супровід КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Контрольні питання

1. Назвіть етапи розробки КСЗІ
2. Які середовища функціонування ІТС обстежуються під час першого етапу розробки КСЗІ?
3. Що таке модель загроз? Назвіть основні принципи формування моделі загроз.
4. Які існують джерела загроз об'єктивної та суб'єктивної природи?
5. Що таке модель порушника? Які характеристики потенційного порушника вона повинна визначати?
6. Які типові атаки на інформаційній ресурс були визначені Пітером Меллом?
7. Що таке «маскарад» з точки зору інформаційної безпеки?
8. Назвіть методи несанкціонованого доступу (НСД).
9. Яких принципів розробки політики безпеки в ІТС необхідно дотримуватись?
10. Назвіть основні розділи політики безпеки.

11. На яких трьох рівнях розглядається забезпечення безпеки інформації?

12. Назвіть декілька правил розмежування доступу.

13. Визначте основні положення концептуальної моделі інформаційної безпеки компанії.

14. Приведіть структуру критеріїв захищеності інформації згідно з НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99.

15. Що таке функціональний профіль захищеності?

16. Приведіть основну формулу функціонального профілю.

17. Які рекомендації щодо вибору профілю захищеності залежно від призначення АС наведені в НД ТЗІ 2.5-005-99?

18. Назвіть основні обов'язки та функції служби захисту інформації.

19. Назвіть основні розділи технічного завдання (ТЗ) на створення КСЗІ.

20. Чим відрізняються ескізний проект, технічний проект та робочий проект КСЗІ?

21. Назвіть етапи введення в дію КСЗІ.

22. Які методи проведення державної експертизи існують?

Розділ 3. МЕТОДОЛОГІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1. Управління інформаційною безпекою. Аудит КСЗІ

Система управління інформаційною безпекою (СУІБ)- це не тільки програмно-апаратні засоби КСЗІ (розглянуті раніше), а комплекс заходів, спрямованих на забезпечення режиму інформаційної безпеки на всіх стадіях життєвого циклу інформаційної системи (проектування, впровадження, експлуатація).

3.1.1. Концептуальна модель системи безпеки компанії. Управління ризиками

Концептуальна модель системи безпеки компанії представлена на рис. 3.1.

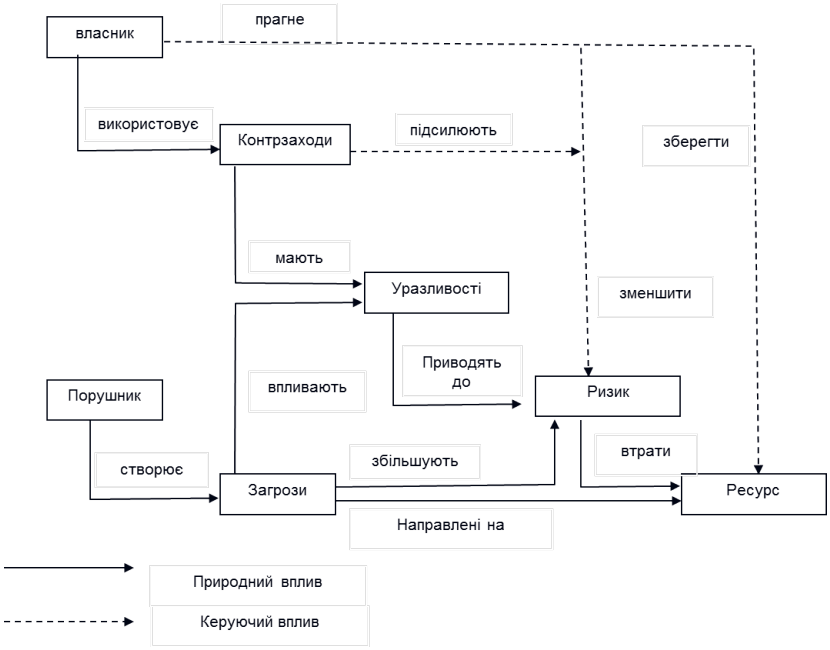

Рисунок 3.1. - Концептуальна модель системи безпеки компанії

Ризик - це фактор, що відображає можливий збиток організації в результаті реалізації загрози інформаційної безпеки (ІБ) - ймовірні фінансові втрати (прямі або непрямі).

Ризик залежить від:

- показників цінності ресурсів (апаратні - файлові сервери, робочі станції, мости, маршрутизатори і т.п.), програмні, дані);
- ймовірності нанесення збитку ресурсів (ймовірності реалізації загроз для ресурсів);
- уразливості системи захисту (ступінь легкості, з якою уразливості можуть бути використані при виникненні загроз);
- існуючих або запланованих засобів забезпечення ІБ.

Для аналізу ризиків застосовують методи:

1)Базовий аналіз ризиків - аналіз ризиків, що проводиться відповідно до вимог Базового мінімально-необхідного рівня захищеності. При цьому зазвичай не враховують цінність ресурсів і не оцінюють ефективність контрзаходів. Застосовуються у випадках, коли до інформаційної системи не пред'являється підвищених вимог в області ІБ.

2) Повний аналіз ризиків - аналіз ризиків для інформаційних систем, що пред'являють підвищені вимоги в області ІБ. Включає в себе визначення цінності інформаційних ресурсів, оцінки загроз і вразливостей, вибір адекватних контрзаходів, оцінку їх ефективності.

Для того щоб сформулювати підвищені вимоги до режиму ІБ, необхідно:

- Визначити цінність ресурсів;
- Доповнити стандартний набір загроз списком загроз, актуальних для досліджуваної інформаційної системи;
- Оцінити ймовірність загроз;
- Визначити вразливість ресурсів.

Управління ризиками полягає у визначенні комплексу необхідних контрзаходів відповідно до виконаного аналізу ризиків.

Контрзаходи можуть зменшити рівні ризиків різними способами:

- Усуненням вразливостей або зменшенням їх величини;
- Зменшенням імовірності здійснення загроз безпеки;
- Зменшенням величини можливого збитку;
- Виявлення атак і інших порушень безпеки;
- Відновленням ресурсів КІС, яким було завдано збитків.

3.1.2. Аудит інформаційної безпеки. Організація робіт.

Аудит інформаційної безпеки корпоративної системи Internet / Intranet - системний процес одержання об'єктивних якісних і кількісних оцінок про

поточний стан інформаційної безпеки компанії відповідно до визначених критеріїв та показників безпеки.

Аудит дає відповідь на питання: «Як оцінити рівень безпеки корпоративної інформаціонной системи нашого підприємства для управління ним в цілому і визначення перспектив його розвитку?».

Вважається, що результати якісно виконаного аудиту інформаційної безпеки компанії дозволяє побудувати оптимальну по ефективності і витратам корпоративну систему захисту, адекватну її поточним завданням і цілям бізнесу.

Аудити бувають:

-внутрішній – виконується співробітниками компанії-власника (деколи називають аудит, що проводиться першою стороною)

- зовнішній, який в свою чергу ділиться на:

а)Виконується постачальником (аудит, що проводиться другою стороною)

б)Виконується аудиторською компанією з метою видачі сертифіката безпеки (аудит, що проводиться третьою стороною).

В результаті проведення аудиту вирішуються задачі:

1. забезпечити (при необхідності підвищити) інформаційну безпеку підприємства;
2. знизити потенційні втрати підприємства шляхом підвищення стійкості функціонування корпоративної мережі;
3. захистити конфіденційну інформацію, передану по відкритих каналах зв'язку;
4. захистити інформацію від навмисного спотворення (руйнування), несанкціонованого копіювання, доступу або використання;
5. забезпечити контроль дій користувачів в корпоративній мережі підприємства;
6. своєчасно оцінити і переоцінити інформаційні ризики бізнес-діяльності компанії;
7. виробити оптимальні плани розвитку і управління підприємством.

Організація проведення робіт з аудиту

Починається з офіційних вступних зборів. На зборах до співробітників, що займаються питаннями безпеки, керівництва середнього і верхньої ланки доводяться наступні питання:

-план проведення аудиту, в якому описано, що і коли планується перевіряти;

-пояснюються методи оцінки ризиків, які передбачається використовувати в процесі перевірки;

-пояснюється процедура визначення невідповідностей, їх кваліфікація і дії щодо їх усунення;

-роз'яснюються причини, за якими за результатами перевірки можуть бути зроблені зауваження, і можлива реакція на них;

-перераховуються керівні документи аудитора і компанії та правила доступу до них;

-з'ясовуються можливі труднощі, які можуть виникнути в процесі роботи - відсутність провідних фахівців і т.д .;

-обговорюється організація роботи з конфіденційною інформацією компанії, необхідними для проведення аудиту, включаючи звіт про проведення аудиту та зауваження про невідповідності.

План проведення аудиту містить розділи:

- коротка характеристика робіт;
- вступ;
- розподіл обов'язків;
- вимоги інформаційної безпеки;
- формалізація оцінок рівня безпеки компанії;
- план-графік робіт (практичні кроки аудиту та терміни їх виконання);
- підтримка і супровід;
- звітні документи;
- додатки.

3.1.3. Практичні кроки аудиту інформаційної безпеки.

Аудит інформаційної безпеки повинен виконувати наступні дії:

1)Комплексний аналіз ІС підприємства і підсистеми інформаційної безпеки на методологічному, організаційно-управлінському, технологічному і технічному рівнях:

-Комплексна оцінка відповідності типових вимог міжнародних стандартів ISO, ДССЗЗІ, Спеціальних вимог Замовника системі інформаційної безпеки підприємства.

-Оцінка ризиків на основі якісних і кількісних оцінок.

-Інструментальні дослідження елементів інфраструктури комп'ютерної мережі і корпоративної інформаційної системи на наявність вразливостей, захищеності точок доступу компанії в Internet.

2)Розробка комплексних рекомендацій по методологічному, організаційно-управлінського, технологічного, загальнотехнічного і програмно-апаратного забезпечення режиму інформаційної безпеки підприємства.

3)Організаційно-технологічний аналіз ІС підприємства.

- Оцінка відповідності типових вимог керівних документів СТЗ інформації системи інформаційної безпеки підприємства в області організаційно-технологічних норм.

- Аналіз документообігу підприємства категорії ІЗОД вимогам підприємства щодо забезпечення конфіденційності інформації.

4)Експертиза рішень і проектів створення КСЗІ на відповідність вимогам щодо забезпечення інформаційної безпеки експертно-документальним методом.

5)Розробка технічного проекту модернізації засобів захисту КІС, встановлених у Замовника за результатами проведеного комплексного аналітичного дослідження корпоративної мережі.

6) Підготовка підприємства до атестації на відповідність вимогам ДСТСЗІ, міжнародних стандартів ISO 15408, ISO 17799, стандарту ISO 9001.

7)Підвищення кваліфікації та перепідготовка фахівців.

- Тренінги в області організаційно-правової складової захисту інформації.

- Навчання основам економічної безпеки.

- Тренінги в області технології захисту інформації.

- Тренінги по застосуванню технічних засобів захисту інформації.

-Навчання діям при спробі злому інформаційних систем.

- Навчання та тренінги з відновлення працездатності системи після порушення штатного режиму її функціонування також по відновленню даними програм з резервних копій.

8)Супровід системи інформаційної безпеки після проведеного комплексного аналізу або аналізу елементів системи ІБ підприємства.

9)Щорічна переоцінка стану ІБ.

Питання заключних зборів:

-підтвердження заявлених перед перевіркою обсягу перевірок і рамок аудиту;

-короткий виклад знайдених невідповідностей і узгоджених змін;

-ознайомлення присутніх із зауваженнями і пропозиціями щодо їх усунення;

-загальні зауваження по ходу аудиту та коментарі до звіту;

-оприлюднення висновків: позитивний висновок, відмова в сертифікації або продовження аудиту;

-підтвердження взятих зобов'язань щодо збереження конфіденційності відомостей, отриманих в ході аудиту.

Офіційний звіт включає:

-ступінь відповідності комп'ютерної інформаційної системи, яка перевіряється, стандартам і власним вимогам компанії в області інформаційної безпеки згідно з планом проведення аудиту;

- детальне посилання на основні документи замовника: політика безпеки, опис процедур забезпечення інформаційної безпеки та ін.;

- загальні зауваження за висновками проведення аудиту;

- кількість і категорії отриманих невідповідностей і зауважень;
- необхідність додаткових дій з аудиту (якщо така є) і їх загальний план;
- список співробітників, які брали участь в тестуванні.

3.1.4. Нормативні документи та звітна документація аудиту.

Стандарти управління інформаційною безпекою

-Першим стандартом є Британський стандарт BS 7799 «Практичні правила управління інформаційною безпекою» випущений в 1995 р. переглянутий в 2002 р. і став міжнародни стандартом ISO 17799

-Німецький стандарт BSI (1998 р.)

-Стандарт США NIST 800-30 – докладно розглядає питання управління інформаційними ризиками.

-Стандарт NASA «Безпека інформаційних технологій».

Розробники міжнародних стандартів

ISO (Міжнародна Організація по Стандартизації) і IEC (Міжнародна Електротехнічна Комісія) формують спеціалізовану систему всесвітньої стандартизації через технічні комітети, створені в окремих областях технічної діяльності.

Сімейство Міжнародних Стандартів на Системи Управління Інформаційною Безпекою 27000 розробляється комітетом ISO/IEC JTC 1 / SC 27 «Інформаційна безпека, кібербезпека і захист конфіденційності».

Для цього сімейства стандартів використовується послідовна схема нумерації, починаючи з 27000 і далі.

На Україні відповідно Міжнародним Стандартам діють Державні стандарти України (ДСТУ)

Всі стандарти переглядаються кожні 5 років.

-ISO/IEC 27000: 2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary (Визначення та основні принципи). Випущений в липні 2009 р.

-ISO/IEC 27001: 2005 / BS 7799-2: 2005 Information technology. Security techniques. Information security management systems. Requirements Інформаційні технології (Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги). Випущений в жовтні 2005 р.

-ISO/IEC 27002: 2005, BS 7799-1: 2005, BS ISO / IEC 17799: 2005 Information technology. Security techniques. Code of practice for information security management (Інформаційні технології. Методи забезпечення безпеки.). Випущений в червні 2005 р.

-ISO / IEC 27003: 2010 Information Technology - Security Techniques - Information Security Management Systems Implementation Guidance (Керівництво по впровадженню системи управління інформаційною

безпекою). Випущений в січні 2010 р.

-ISO/IEC 27004: 2009 Information technology. Security techniques. Information security management. Measurement (Вимірювання ефективності системи управління інформаційною безпекою. Випущений в січні 2010 р .

-ISO/IEC 27005: 2008 Information technology. Security techniques. Information security risk management (Управління ризиками інформаційної безпеки). Випущений в червні 2008 р .

-ISO/IEC 27006: 2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems (Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою). Випущений в березні 2007 р.

3.2. Управління ризиками.

Керування ризиком - процес прийняття рішень і здійснення заходів, спрямованих на забезпечення мінімально можливого (припустимого) ризику.

Механізм управління ризиками - це сукупність інструментів, методів, форм та засобів взаємодії суб'єктів управління ризиками з метою розроблення та реалізації управлінських рішень, спрямованих на попередження настання ризиків, зменшення і подолання наслідків їх впливу

Аналіз ризиків визначає цінність інформаційних активів, ідентифікує загрози і вразливості, які існують (або можуть існувати), ідентифікує існуючі засоби контролю і їх вплив на ризики, визначає потенційні наслідки і, нарешті, ранжирує ризики відповідно до пріоритетів.

3.2.1. Технології аналізу ризиків.

Оцінка ризиків складається з наступних заходів:

-Ідентифікацію ризиків;

-Оцінювання ризиків;

-Обробка ризиків (вибір контрзаходів).

1)Ідентифікація ризиків

Ідентифікація ризиків повинні збирати вхідні дані для їх кількісної оцінки і включає:

- ідентифікація ресурсів - обєктів ІС, що мають цінність для компанії і потребують захисту;

-ідентифікація загроз і вразливостей;

- ідентифікація існуючих методів контролю ризиків та контрзасобів;

- ідентифікація наслідків - втрати конфіденційності, цілісності та доступності, що приводить до втрати ефективності, фінінсових втрат, втрати бізнесу, збиток, нанесений репутації і т.д.

2)Оцінювання ризиків

При оцінюванні ризиків рекомендується розглядати такі аспекти:

- шкали та критерії, за якими можна вимірювати ризики;
- оцінку ймовірностей подій;
- технології вимірювання ризиків.

Шкала для отримання експертної оцінки, наприклад, має три значення:

- малоцінний інформаційний ресурс: від нього не залежать критично важливі завдання і він може бути відновлений з невеликими витратами часу і грошей;
- ресурс середньої цінності: від нього залежить ряд важливих завдань, але в разі втрати він може бути відновлений за час, що не перевищує критично допустимий, але вартість відновлення - висока;
- цінний ресурс: від нього залежать критично важливі завдання, в разі втрати час відновлення перевищує критично допустимий або вартість надзвичайно висока

Ризики можна оцінювати за об'єктивними або суб'єктивними критеріями.

Прикладом об'єктивного критерію є ймовірність виходу з ладу будь-якого обладнання, наприклад ПК, за певний проміжок часу.

Приклад суб'єктивного критерію - оцінка власником інформаційного ресурсу ризику виходу з ладу ПК.

В останньому випадку зазвичай розробляється якісна шкала з декількома градаціями, наприклад:

- низький ризик - джерело загрози (порушник) має низький рівень мотивації, або існують надзвичайно ефективні методи зменшення уразливості;
- середній ризик - порушник має високий рівень мотивації, проте використовуються ефективні методи зменшення уразливості;
- високий ризик - (порушник) має дуже високий рівень мотивації, а методи зменшення уразливості малоефективні.

3.2.2. Методи вимірювання ризиків

Сьогодні існує ряд підходів до вимірювання ризиків. Найбільш поширені - оцінку ризиків **за двома** і **за трьома** факторами.

У найпростішому випадку проводиться оцінка двох факторів: ймовірність події і тяжкість можливих наслідків. Загальна ідея виражена формулою:

$$\text{РИЗИК} = \text{Р}_{\text{події}} \times \text{ЦІНА ВТРАТИ}. \quad (1)$$

де Рподії – ймовірність події

Якщо змінні є кількісними величинами, то ризик - це оцінка математичного очікування втрат.

Коли змінні - якісні величини (найбільш часто зустрічається ситуація), то в явному вигляді цю формулу застосовувати не слід (якісні величини неможливо перемножати).

3.2.2. Вимірювання ризику при якісних величинах (за двома факторами)

Спочатку повинні бути визначені шкали. Приклад суб'єктивної шкали ймовірностей подій:

- A - подія практично ніколи не відбувається;
- B - подія трапляється рідко;
- C - ймовірність події за розглянутий проміжок часу - близько 0,5;
- D - швидше за все, подія відбудеться;
- E - подія майже обов'язково станеться.

Крім того, встановлюється суб'єктивна шкала серйозності подій:

- N (Negligible) - впливом можна знехтувати;
- Mi (Minor) - незначне подія: витрати на ліквідацію наслідків невеликі, вплив на інформаційну технологію незначний;
- Mo (Moderate) - подія з помірними результатами: ліквідація наслідків не пов'язана з великими витратами, вплив на інформаційну технологію невелике і не зачіпає критично важливі завдання;
- S (Serious) - подія з серйозними наслідками: ліквідація наслідків пов'язана зі значними витратами, вплив на інформаційні технології відчутно, впливає на виконання критично важливих завдань;
- C (Critical) - подія призводить до неможливості вирішення критично важливих завдань.

Для оцінки ризиків встановлюється шкала з трьох значень:

- низький ризик;
- середній ризик;
- високий ризик.

Визначення ризику в залежності від двох факторів виконується згідно таблиці 3.1. Знаючи значення ймовірності та серйозності подій, по таблиці (на пересіченні відповідного рядка та стовпця) визначається рівень ризику.

Таблиця 3.1. - Визначення ризику в залежності від двох факторів

Шкала	Серйозність подій				
Ймовірність подій	Negligible	Minor	Moderate	Serious	Critical
A	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
B	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
C	Низький ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
D	Середній ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
E	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

3.2.4. Визначення ризику по трьом факторам

У методиках, розрахованих на більш високі вимоги, ніж базовий рівень, використовується модель оцінки ризику з трьома факторами: загроза, вразливість, ціна втрати.

В формулі (1) деталізується

$$Р\text{події} = Р\text{загрози} \times Р\text{вразливості},$$

і одержуємо:

$$\text{РИЗИК} = Р\text{загрози х } Р\text{вразливості} \times \text{ЦІНА ВТРАТИ}. \qquad (2)$$

Цей вираз є математичною формулою для кількісних шкал, або є основою табличних методів, якщо хоча б одна з шкал - якісна.

Шкала ризику

Наприклад, показник ризику вимірюється по 8-бальній шкалі наступним чином:

1 - ризик практично відсутній. Теоретично можливі ситуації, при яких подія настає, але на практиці це трапляється рідко, а потенційний збиток порівняно невеликий;

2 - ризик дуже малий. Подібні події траплялися досить рідко, крім того, негативні наслідки порівняно невеликі;

...

8 - ризик дуже великий. Подія, швидше за все, наступить, і наслідки

будуть надзвичайно важкими.

Матриця може бути побудована так, як при аналізі 2-х факторів (див. табл. 3.1.).

Шкала ймовірностей

При реальних розрахунках можливе використання різних суб'єктивних шкал ймовірностей загроз та вразливостей:

- 5-ти рівнева шкала (див. п. 3.2.3.)
- трьох-рівнева шкала:
  - низький рівень;
  - середній рівень;
  - високий рівень.

Використаємо трьох-рівневу шкалу Рзагрози та Рвразливості.

Визначення ризику по трьом факторам виконується згідно таблиці 3.2. Знаючи значення ймовірності (рівнів) загроз та вразливостей вибирається відповідний стовпець таблиці і на пересіченні відповідного рядка - Ступінь серйозності події - визначається рівень ризику.

Таблиця 3.2. - Визначення ризику по трьом факторам

Шкала	Рівень загрози								
	Низький (Н)			Середній (С)			Високий (В)		
	Рівні вразливостей			Рівні вразливостей			Рівні вразливостей		
Ступінь серйозності події	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Технологія оцінки загроз і вразливостей

Для оцінки загроз та вразливостей застосовуються різні методи, в основі яких лежать:

-експертні оцінки (необхідно виконати вимоги щодо їх кваліфікації);

-статистичні дані - накопичення даних про події, які мали місце, аналіз і класифікація їх причин, виявлення чинників, від яких вони залежать (недолік – необхідно зібрати досить великий матеріал про події в цій галузі, що не завжди можливо зробити;

-врахування факторів, що впливають на рівні загроз і вразливостей (найбільш поширений в даний час підхід).

Метод врахування факторів, що впливають на рівні загроз і вразливостей

Метод дозволяє абстрагуватися від малоістотних технічних деталей, взяти до уваги не тільки програмно-технічні, а й інші аспекти. Суть методу:

-Для кожного типу ризику (окремо для загрози і вразливості) є стандартний набір непрямих факторів, які впливають на рівні загроз і вразливостей;

-Для кожного непрямого фактору є набір питань і кілька фіксованих варіантів відповідей, які «коштують» певну кількість балів.

-Даються відповіді на питання;

-Шляхом підсумовування балів визначається оцінка загрози і вразливості даного класу

До недоліків відноситься те, що непрямі чинники і їх вага залежать від сфери діяльності організації, тому методика завжди вимагає підстроювання під конкретний об'єкт.

При цьому доказ повноти обраних непрямих чинників і правильності їх вагових коефіцієнтів - задача мало формалізована і складна, яка на практиці вирішується експертними методами (перевірка відповідності отриманих за методикою результатів очікуваним для тестових ситуацій).

Подібні методики, як правило, розробляються для організацій певного профілю (відомств), апробуються і потім використовуються в якості відомчого стандарту. Таким шляхом пішли і творці CRAMM (див. далі), випустивши близько десятка версій методу для різних відомств (міністерство закордонних справ, збройні сили і т.д.).

3.2.5. Інструментальні засоби аналізу ризиків

Інструментальні засоби аналізу ризиків дозволяють автоматизувати роботу спеціалістів в області захисту інформації, які здійснюють оцінку або переоцінку інформаційних ризиків підприємства.

Спеціалізоване ПЗ, що реалізує методики аналізу ризиків, може бути на ринку або бути власністю організації і не продаватися.

Спеціалізоване ПЗ, умовно ділиться на дві групи: ПЗ базового рівня і ПЗ повного аналізу ризиків.

ПЗ базового рівня

ПЗ, що відповідають стандарту ISO 17799:

а)довідкові та методичні матеріали:

-політика інформаційної безпеки (Information Security Police);

-гіпертекстові довідники з питань захисту інформації (Sos -Interactive "Online" Security Policies And Support);

-керівництва для співробітників служб безпеки (Security Professionals

Guide).

б)ПЗ аналізу ризиків та аудиту:

- Cobra – (виробник C & A Systems Security Ltd) дозволяє представити вимоги стандарту у вигляді тематичних «питань» по окремим аспектам діяльності організації і автоматично формується звіт;

- RA Software Tool містить модулі:

- .....Керівництво з оцінки та управління ризиками;
- .....Оцінка готовності компанії до аудиту;
- .....Керівництво по вибору системи захисту та ін.

ПЗ повного аналізу ризиків

Такі методи є інструментаріями для:

- побудови моделі інформаційної системи (ІС) з позиції інформаційної безпеки (ІБ);
- оцінки цінності ресурсів;
- складання списку загроз і оцінки їх ймовірностей;
- вибору контрзаходів і аналізу їх ефективності;
- аналізу варіантів побудови захисту;
- документування (генерації звітів).

Один з найбільш відомих продуктів - CRAMM.

Метод CRAMM

CRAMM (CCTA Risk Analysis and Managment Method) розробник - Центральне агентство з комп'ютерів і телекомунікацій (CCTA) Великобританії.

Концепція, покладена в основу методу включає ідентифікацію та обчислення рівнів (заходів) ризиків на основі оцінок, присвоєних ресурсів, загроз і вразливостей ресурсів.

Контроль ризиків полягає в ідентифікації та виборі контрзаходів, завдяки яким вдається знизити ризики до прийнятного рівня.

Формальний метод, заснований на цій концепції, дозволяє переконатися, що захист охоплює всю систему і є впевненість в тому, що:

- всі можливі ризики ідентифіковані;
- вразливості ресурсів ідентифіковані та їх рівні оцінені;
- загрози ідентифіковані та їх рівні оцінені;
- контрзаходи ефективні;
- витрати, пов'язані з ІБ, виправдані.

Переваги:

-використання технології оцінки загроз і вразливостей за непрямими факторами з можливістю верифікації результатів;

-зручна система моделювання інформаційної системи з позиції безпеки;

-великій базі даних по контрзаходів. Метод – найбільш «потужний» і найбільш трудомісткий, він дозволяє детально оцінити ризики і різні варіанти

контрзаходів.

Недоліки з позиції вітчизняного споживача:

-складність русифікації

-великий обсяг вихідних документів (сотні сторінок), тому аудитор змушений на основі отриманих документів сам писати звіт для замовника.

Етапи роботи CRAMM:

-Ініціалізація (Initiation) - проводиться формалізований опис ІС, її основних функцій, категорій користувачів;

-Ідентифікація та оцінка ресурсів (Identification and Valuation of Assets) – опис та визначення цінності ресурсів системи.

-Оцінювання загроз і вразливостей (Threat and Vulnerability Assessment) - не обов'язковий, якщо замовника задовольнить базовий рівень безпеки.

-Аналіз ризиків (Risk Analysis) – виконується оцінка ризиків або на основі зроблених оцінок загроз і вразливостей (повний аналіз), або по спрощеним методикам для базового рівня безпеки.

-Управління ризиками (Risk Management) - пошук адекватних контрзаходів, які найкращим чином задовольняють вимогам замовника.

ПЗ компанії MethodWare

Компанія MethodWare випускає ПЗ:

-ПЗ аналізу та управління ризиками Operational Risk Builder і Risk Advisor;

-ПЗ управління життєвим циклом інформаційної технології відповідно до відкритого стандарту в області інформаційних технологій CobiT Advisor 3rd Edition (Audit) і CobiT 3rd Edition Management Advisor. В інструкціях CobiT істотне місце приділяється аналізу та управління ризиками;

-ПЗ для автоматизації побудови різноманітних опитувальних листів Questionnaire Builder.

ПЗ Risk Advisor

В ПЗ реалізована методика, що дозволяє задати модель інформаційної системи, ідентифікувати ризики, загрози, втрати в результаті інцидентів. Сильною стороною даного методу є можливість подання різнопланових взаємозв'язків, адекватного врахування багатьох факторів ризику і істотно менша трудомісткість в порівнянні з CRAMM.

Основні етапи роботи:

-опис контексту;

-опис ризиків;

-опис загроз;

-оцінка втрат;

-аналіз управляючих дій;

-пропозиція контрзаходів і плану дій.

Експертна система «АванГард»

«АванГард» - комплексна експертна система управління інформаційною безпекою. Розробник - Інститут системного аналізу РАН (РФ).

Типовий пакет включає два програмних комплекса - «Авангард-Аналіз» і «Авангард-Контроль». Кожен з цих комплексів базується на своїй методиці оцінки ризиків.

Методика оцінки ризиків комплексу «Авангард-Аналіз» відноситься до ризиків можливих порушень безпеки оцінюваної системи;

Методика комплексу «Авангард-Контроль» присвячена ризикам, що є результатом невиконання вимог забезпечення безпеки оцінюваної системи і її компонентів.

Контрольні питання

1. Дайте визначення аудиту інформаційної безпеки.
2. Які бувають види аудиту?
3. Назвіть практичні кроки аудиту безпеки.
4. Які міжнародні стандарти управління інформаційною безпекою використовуються в нашій країні?
5. Які технології аналізу ризиків існують?
6. Назвіть основні методи вимірювання ризиків.
7. В чому різниця між вимірюванням ризику за двома та трьома факторами?
8. Приведіть основну формулу оцінки ризику.
9. Назвіть найпоширеніші інструментальні засоби аналізу ризиків.

Розділ 4. ОСНОВНІ НАПРЯМКИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

4.1. Технічні засоби і методи захисту інформації.

4.1.1. Технічні канали витоку інформації.

Під технічним каналом витоку інформації розуміють сукупність об'єкта розвідки, технічного засоба розвідки і фізичного середовища, в якому поширюється інформаційний сигнал.

Найбільший інтерес з точки зору створення каналів небажаного витоку інформації представляють технічні засоби прийому, обробки та передачі інформації в ІС (ТЗПІ) та допоміжні технічні засоби (ДТЗ) (телефонний, гучномовний звязок, пожежна та охоронна сигналізація, радіо- та телетрансляція, контрольно-вимірювальна апаратура, електропобутові прилади і т.д., а також самі приміщення), які мають вихід за межі контрольованої зони, тобто зони з пропускною системою.

Класифікація технічних каналів витоку інформації

1. технічні канали витоку інформації, яка обробляється ТЗПІ
2. технічні канали витоку інформації при передачі її по каналам зв'язку
3. технічні канали витоку мовної інформації
4. технічні канали витоку видової інформації (зображеня)

Розглянемо їх детальніше.

1) Технічні канали витоку інформації, яка обробляється ТЗПІ

-Електромагнітні випромінювання елементів ТЗПІ;

-Електричні:

- наведення електромагнітних випромінювань елементів ТЗПІ на сторонніх провідниках;
- просочування інформаційних сигналів в лінії електроживлення;
- просочування інформаційних сигналів у колі заземлення;
- знімання інформації з використанням закладних пристроїв «жучків».

-Параметричні - перехоплення інформації шляхом «високочастотного опромінення» ТЗПІ.

-Вібраційні - відповідність між роздрукованим символом і його акустичним образом.

2) Технічні канали витоку інформації при передачі її по каналам зв'язку

-Електромагнітні канали: електромагнітні випромінювання передавачів зв'язку, модульовані інформаційним сигналом (прослуховування радіотелефонів, стільникових телефонів, радіорелейних ліній зв'язку).

-Електричні канали: підключення до ліній зв'язку.

-Індукційний канал: ефект виникнення навколо високочастотного кабелю електромагнітного поля при проходженні інформаційних сигналів.

-Паразитні зв'язки: паразитні ємнісні, індуктивні і резистивні зв'язки і наведення близько розташованих один від одного ліній передачі інформації.

3) Технічні канали витоку мовної інформації:

- Акустичні канали: середовище поширення - повітря.

- Віброакустичні канали: середовище поширення - огороджувальні будівельні конструкції.

- Параметричні канали: результат впливу акустичного поля на елементи схем, що призводить до модуляції високочастотного сигналу інформаційним сигналом.

- Акустоелектричні канали: перетворення акустичних сигналів в електричні.

- Оптико-електронний (лазерний) канал: опромінення лазерним променем вібруючих поверхонь (зазвичай – вікон).

4) Технічні канали витоку видової інформації (зображеня)

- Спостереження за об'єктами. Використовуються: вдень - оптичні прилади і телевізійні камери; вночі - прилади нічного бачення, тепловізори, телевізійні камери.

- Зйомка об'єктів. Використовуються: телевізійні і фотографічні засоби. Для зйомки об'єктів вдень з близької відстані застосовуються портативні камуфльовані фотоапарати і телекамери, суміщені з пристроями відеозапису.

- Зйомка документів: здійснюється з використанням портативних фотоапаратів

4.1.2. Засоби виявлення каналів витоку інформації

Принцип дії більшості індикаторів електромагнітного поля заснований на широкосмуговому детектуванні електричного поля.

Індикатори забезпечують можливість виявлення радіопередавальних прослуховуючих пристроїв з будь-якими видами модуляції.

Індикатори електромагнітного поля

Принцип дії більшості індикаторів електромагнітного поля заснований на широкосмуговому детектуванні електричного поля. Індикатори забезпечують можливість виявлення радіопередавальних прослуховуючих пристроїв з будь-якими видами модуляції.

Приклад: Індикатор поля-частотомер SEL SP-71M «Оберіг» є мікропроцесорним індикатором поля та призначений для миттєвого виявлення будь-яких джерел радіовипромінювання: радіомікрофонів, радіостанцій, мобільних телефонів.

Скануючі радіоприймачі

У процесі контролю радіоефіру основними діями є пошук, виявлення і прийом необхідних радіосигналів.

Скануючі приймачі:

AR5001D і ICOM IC-R10

Слід зазначити, що скануючі приймачі в руках зловмисників можуть служити розвідувальним засобом.

Аналізатори спектру, радіочастотоміри

Характерною особливістю більшості таких пристроїв є їх портативне виконання і висока чутливість.

-Радіочастотоміри призначені для вимірювання частоти джерела радіосигналу - приклад: «3000A Plus».

-Аналізатори спектра дозволяють аналізувати спектр прийнятих сигналів в заданому діапазоні частот. Приклади:

- - «HP8591E HP»;
- - «ESA-L1500A».

Аналізатори спектра призначені для вимірювання електромагнітних випромінювань і наводок; для контролю радіоелектронної обстановки в приміщеннях.

-Радіотестери вимірюють параметри сигналів, працюють з усіма типами модуляції.

Багатофункціональні комплекти для виявлення каналів витоку інформації

1)Портативний комплект для виявлення засобів знімання інформації і виявлення каналів її витоку «ПКУ-6М». Система містить комплект датчиків, що дозволяють:

-виявити канали витоку акустичної інформації через наскрізні щілини і тріщини огороджувальних конструкцій;

-оцінити вібро-акустичні властивості огороджувальних конструкцій та інженерних комунікацій;

-виявити електричні сигнали в слабкострумових лініях;

-виявити електричні сигнали в потужнострумових лініях;

-виявити оптичне випромінювання освітлювальних приладів, індикаторів, датчиків сигналізації, у видимому і інфрачервоному діапазонах.

2)Портативний комплект для виявлення засобів знімання інформації та виявлення каналів її витоку «Піранья»

Прилад складається з основного блоку управління і індикації, комплекту перетворювачів і дозволяє працювати в наступних режимах:

-високочастотний детектор-частотомір;

-скануючий аналізатор дротових ліній;

-детектор ІК-випромінювань;

-детектор низькочастотних магнітних полів;

-диференційний низькочастотний підсилювач;

-віброакустичний приймач;

-акустичний приймач.

3)Крім того, застосовуються:

-Багатофункціональний комплекс радіомоніторингу і виявлення каналів витоку інформації «АРК-Д1ТІ»

-Комплекс RS turbo

-Комплекси вимірювання ПЭМИН

-Програмно-аппаратний комплекс «СИГУРД»

-Аналізатор спектру “НАВИГАТОР-П6Г»

Нелінійні локатори

Істотною відмінністю нелінійної локації від класичного спостереження (виявлення) об'єктів з активною відповіддю є пряме перетворення падаючої на об'єкт енергії зондуючого сигналу в енергію вищих гармонік.

Вимірювач вторинних полів (детектор нелінійних переходів) «NR 900 EM» призначений для пошуку електронних пристроїв, що містять напівпровідникові компоненти, незалежно від їх функціонального стану.

Комплекс для вимірювання характеристик акустичних сигналів СПРУТ- 7

Металодетектори

Різновидами магнітних методів є індукційні струмовихрові з різними видами намагнічення поля і магнітоелектричні з використанням природного геомагнітного поля землі або штучного магнітного поля.

-Досмотрово-сигнальні комплексі «АКА 7202М» та «ADAMS AD18»

-Селективний виявитель зброї у ручній поклажі РУБЕЖ-Д

-Комп’ютеризований металодетектор «КОРНЕТ»

-Портативна рентгенотелевізійна установка «НОРКА»

-Досмотрові ендоскопи

4.1.3. Методи та системи захисту інформації.

Приховання та захист інформації від витоку технічними каналами

За функціональним призначенням засоби інженерно-технічного захисту поділяються на такі групи:

-інженерні засоби - різні пристрої і споруди, які протидіють фізичному проникненню зловмисників на об'єкти захисту;

-апаратні засоби (вимірювальні прилади, пристрої, програмно-апаратні комплекси та ін.) - призначені для виявлення каналів витоку інформації, оцінки їх характеристик і захисту інформації;

-програмні засоби, програмні комплекси і системи захисту інформації в

інформаційних системах різного призначення і в основних засобах обробки даних;

-криптографічні засоби інформації, що передаються по відкритих каналах і мережах зв'язку.

Способи захисту інформації

Всі способи захисту діляться на дві групи:

1. Приховування:
   - пасивне приховування;
   - активне приховування;
   - спеціальний захист.
2. Дезінформація:
   - технічна дезінформація;
   - імітація;
   - легендування.

Пасивне приховування:

- зниження контрастності демаскуючих ознак приховуваних видових об'єктів, застосування маскувальних покриттів, камуфлювання техніки;

- зниження рівня інформаційних фізичних полів, створюваних функціонуючим об'єктом;

- застосування екранованих камер і споруд, що виключають електромагнітні випромінювання в навколишній простір.

Активне приховування - створення маскуючих шумових перешкод різної фізичної природи. Застосовується як додатковий захід до пасивного приховування.

Спецзахист - кодування цифрової інформації, скремблювання телефонних переговорів, та ін.

Екранування електромагнітних хвиль

Для зниження наводок необхідно усувати або послаблювати до допустимих значень паразитні зв'язки: паразитна ємкість, взаємна індуктивність і паразитний опір.

Наступний етап - екранування і розв'язуючі фільтри.

Екранування - це захист приладів від впливу зовнішніх полів і локалізація електромагнітної енергії в межах певного простору шляхом перешкодження її поширення.

Розв'язуючий фільтр - це пристрій, що обмежує поширення перешкоди по дротах, які є загальними для джерела і приймача наводки (приклад: оптроелектронна пара – «оптрон»).

Для зниження паразитної ємності між електричними ланцюгами вводиться струмопровідний екран, з'єднаний із загальним проводом.

Для зниження величини магнітних полів використовують два види екранування: магнітостатичне і динамічне.

Магнітостатичне екранування засноване на застосуванні екранів з феромагнітних матеріалів з великою магнітною проникністю. Лінії магнітного поля як би втягуються в матеріал з більш високою магнітною проникністю, в результаті всередині екрану поле послаблюється.

Сутність динамічного екранування полягає в тому, що змінне магнітне поле послаблюється у міру проникнення в металевий екран, так як внутрішні шари екрануються вихровими струмами, що виникають в шарах, розташованих ближче до поверхні.

Екрануються не тільки окремі блоки апаратури і їх сполучні лінії, а й приміщення в цілому.

У звичайних приміщеннях основний екрануючий ефект забезпечують залізобетонні стіни будинків. Екрануюча властивість дверей і вікон гірше. Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, в тому числі:

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори з металізованої тканини;
- металізоване скло (наприклад, з двоокису олова), що встановлюється в металеві або металізовані рами.

Безпека оптоволоконних кабельних систем (ОКС)

Оптоволокно - це прозорий матеріал, що передає електромагнітну енергію в інфрачервоному діапазоні хвиль. За рахунок повного внутрішнього відбиття хвилі від оболонки, випромінювання назовні практично не просочується. Ефективне перехоплення інформації можливий тільки шляхом фізичного підключення до оптоволоконної лінії.

Однак якщо ОКС розглядати як систему, що містить робочі станції, сервери, інтерфейсні карти, концентратори і інші мережеві активні пристрої, які самі є джерелом випромінювань як в радіочастотному, так і в оптичному діапазонах, то проблема витоку інформації стає актуальною.

Заземлення технічних засобів і придушення інформаційних сигналів в ланцюгах заземлення

Екранування ТЗПІ та з'єднувальних ліній ефективно тільки при правильному їх заземленню:

- опір заземлюючих провідників, а також земляних шин повинні бути мінімальними;
- в системі заземлення мають бути відсутні замкнуті контури;
- мінімальний опір контактів (краще пайка);
- забороняється використовувати в якості заземлювачів нульові фази, металеві оболонки підземних кабелів, металеві труби водо- і теплопостачання.

Для ефективного придушення інформативних сигналів в ланцюгах заземлення та електроживлення застосовують електричне зашумлення від

генераторів шуму.

Фільтрація інформаційних сигналів

Випромінювання та наводки в ланцюгах електроживлення, в сигнальних ланцюгах інтерфейсу і на друкованих платах, в проводах заземлення від пристроїв електронно-обчислювальної техніки модульовані корисним сигналом, і можуть бути перехоплені зловмисником.

Фільтрація є основним і ефективним засобом придушення (ослаблення) наводок.

Для фільтрації сигналів використовуються розділові (разделительные) трансформатори і перешкодо-пригнічуючі фільтри - пригнічують сигнали в заданый смузі частот.

Активні методи захисту. Просторове і лінійне зашумлення

Фільтрація - пасивний метод захисту. Коли фільтрації недостатньо, то вдаються до активних методів захисту, заснованих на створенні перешкод, що перевищують рівні побічних випромінювань та наводок.

У системах просторового зашумлення використовуються перешкоди типу «білого шуму», який має рівномірно розподілений енергетичний спектр у всьому робочому діапазоні або «синфазні перешкоди», тобто імпульси випадкової амплітуди, що збігаються за формою і часом існування з імпульсами корисного сигналу.

Системи лінійного зашумлення застосовуються для зашумлення наведених небезпечних сигналів в сторонніх провідниках і сполучних лініях, що виходять за межі контрольованої зони (в основному, лінії електроживлення)

Випускаються генератори шуму СУПЕРНИК та SI-8001, які призначені для захисту електромережі змінного струму 220В/ 50Гц та не впливають на роботу обчислювальної техніки.

Приховування і захист від витоку інформації по акустичному і віброакустичному каналам

Якщо акустичні і віброакустичні характеристики приміщень , що захищаються не відповідають вимогам щодо захисту мовної інформації, то застосовують активні засоби захисту, які забезпечують необхідний захист при мінімальному шумі в приміщенні, що практично не впливає на комфортність розмов.

Вони є генераторами акустичного і віброакустичного маскуючого шуму, що містять аудіо- та вібровипромінювачі та дозволяють нейтралізувати такі види підслуховування як:

- безпосереднє підслуховування в умовах поганої звукоізоляції приміщення;
- застосування радіо- і дротових мікрофонів, встановлених в порожнинах стін, над стелею, в вентиляційних коробах і т.п .;

- застосування стетоскопів, встановлених на стінах (стелях, підлогах), трубах водо- (тепло-, і газо-) постачання) і т.п.;

- застосування лазерних і мікрохвильових систем знімання аудіоінформації з вікон і елементів інтер'єру.

Найбільш відомими генераторами є «СОНАТА - АВ 1М» і «ШОРОХ-3».

Захист мовної інформації в телефонних системах з використанням криптографічних методів (кодування вхідного сигналу – передача – декодування).

Приклади пристроїв:

- Пристрої захисту мовної інформації в відкритих каналах зв'язку: СКРИПТ – 6401 та ОРЕХ-2

- Шифратор PRAGMA (включається замість звичайного модему) призначений для гарантованого криптографічного захисту телефонних каналів зв'язку, факсу, ПК.

- Пристрої захисту переговорів в каналах мобільного зв'язку стандарту GSM: «Альфа-С», УКС-001, РЕЗЕДА - сумісні з мобільними телефонами.

4.2. Принципи криптографічного захисту інформації

4.2.1.Поняття криптографії.

Криптографічні методи захисту інформації - «тайнопис» з'явились більш ніж п'ять тисяч років тому – (древні цивілізації Єгипту, Месопотамії, Індії, Греції, Риму).

Під час другої світової війни були винайдені електромеханічні шифратори на комутаційних дисках та на цевочних дисках.

В наші часи криптографія остаточно оформилась як математична наука, вона орієнтована на сучасні засоби обчислювальної техніки та телекомунікацій.

Історія криптографії починалась із використання криптоалгоритмів заміни одного символа іншим по спеціальним правилам (приклад - шифр Цезаря). Розкриття цих алгоритмів третій стороні автоматично приводило до розкриття шифротексту (обмежені за функціональними можливостями і в сучасній криптографії не використовуються).

Наприкінці XIX сторіччя криптографія починає переходити до криптоалгоритмів з ключем.

Шифрування з ключем (key coding) – це методи кодування, особливістю яких є обов'язкове збереження ключа в таємниці від третьої сторони, збереження криптографічного алгоритму при цьому не обов'язково.

Ключ - це конкретний секретний стан певних параметрів алгоритму криптографічного перетворення даних.

Криптографічний захист забезпечує конфіденційність і цілісності даних, що передаються у відкритих мережах, а також анонімність об'єкта й умови його причетності до дій, що здійснюються в ТКС.

Криптографія - це сукупність методів перетворення даних (шифрування та дешифрування), спрямованих на приховання їх інформаційного змісту в разі перехоплення повідомлення зловмисником.

Криптоаналіз – це наука, що займається вивченням та розробкою методів та засобів розкриття шифрів.

Криптографічна система захисту інформації - це сукупність криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів.

Узагальнена схема криптосистеми представлена на рис. 4.1.

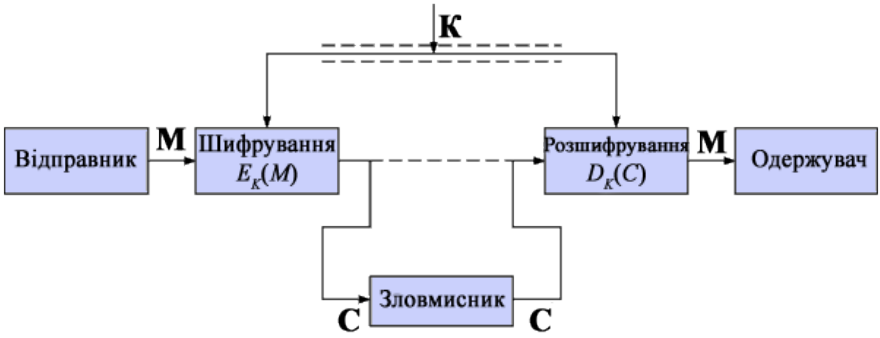

Рисунок 4.1. - Узагальнена схема криптосистеми

M - відкритий текст (повідомлення). Це може бути потік бітів, текстовий файл, бітове зображення, оцифрований звук, цифрове відеозображення й ін.

C – зашифрований текст.

К – ключ шифру.

$C = E_к(M)$ - функція шифрування; $M = D_к(C)$ - функція розшифрування;

Для відновлення первісного відкритого тексту має виконуватися тотожність:

$$D_к\,(E_к\,(M)) = M.$$

4.2.2. Симетричні та асиметричні криптографічні системи. Ефективність захисту

Криптографічні системи, у загальному випадку, класифікуються на основі таких трьох незалежних характеристик:

1. тип операцій для перетворення відкритого тексту в шифрований (алгоритм шифрування);
2. число ключів, що використовуються;
3. метод обробки відкритого тексту.

1)Типи операцій при шифруванні

При шифруванні використовуються наступні операції:

- Заміни або підстановки - символи вихідного тексту замінюються на символи іншого (або того ж) алфавіту відповідно до заздалегідь визначеного правила, яка є ключем даного шифру.

- Перестановки - символи оригінального тексту міняються місцями за певним правилом, що є секретним ключем.

- Гамування - символи вихідного тексту складаються з символами випадкової послідовності.

- Алгоритми, засновані на аналітичних перетвореннях даних (використовуються властивості простих чисел алг. RSA).

- Комбіновані методи. Послідовне шифрування вихідного тексту за допомогою двох і більше алгоритмів.

2)Число ключів, що використовуються

Якщо і відправник, і одержувач інформації використовують той самий ключ або однакові ключі, які легко виводяться один з одного, система називається симетричною, системою з одним ключем, системою із секретним ключем або схемою традиційного шифрування.

Якщо відправник і одержувач використають різні ключі (один відкритий, а інший секретний), причому жоден із ключів не може бути обчислений з іншого за певний час, система називається асиметричною, системою із двома ключами або схемою шифрування з відкритим ключем.

3)Методи обробки відкритого тексту:

- Блочне шифрування передбачає обробку відкритого тексту блоками, так що в результаті обробки кожного блоку виходить блок шифрованого тексту.

- При потоковому шифруванні шифрування всіх елементів відкритого тексту здійснюється послідовно, одне за іншим, у результаті чого на кожному етапі отримують по одному елементу шифрованого тексту.

Вимоги до шифрів

До шифрів, які використовуються для криптографічного захисту інформації, висувають низку вимог:

- статистична безпека алгоритмів;
- надійність математичної бази алгоритмів;
- простота процедур шифрування й розшифрування;
- незначна надмірність інформації за рахунок шифрування;
- простота реалізації алгоритмів на різній апаратній базі.

Приклади популярних криптоалгоритмів/схем шифрування приведені в таблиці 4.1.

Таблиця 4.1. - Приклади популярних криптоалгоритмів / схем шифрування

Назва	Довжина ключа, біт	Розробник
Симетричні		
Rijndael (AES)	128—256	J. Daemon, V.Rijmen, Бельгія
SNOW	128, 256	Lund University, Швеція
RC6	128—256	RSA Security, США
3DES	168	Стандарт ANSI X9.52-1998
MARS	128—400	IBM Corporation, США
TwoFish	128—256	B. Schneir, США
SERPENT	128—256	R. Anderson, E. Biham, L. Knudsen
ДСТУ 28147:2009	256	Стандарт СРСР - ГОСТ 28147-89
Асиметричні		
RSA	1024—4096+	RSA Laboratories, США
RSA-OAEP	1024—4096+	RSA Laboratories Europe, Швеція
ACE Encrypt	1024—4096+	IBM Zurich Research Laboratory, Швейцарія
EPOC	1024—4096+	Nippon Telegraph and Telephone, Японія

Стійкість криптографічної системи захисту інформації

Стійкість криптографічної системи захисту інформації є її здатність протистояти атакам порушника на інформацію, що захищається.

Вона може бути поділена на:

- безумовна стійкість - не залежить ні від яких можливостей порушника (єдина умова: порушник не знає секретний ключ) й умов її визначення й не може бути зменшена за жодних умов;
- умовна стійкість - залежить від можливостей протиборчої сторони й умов її визначення, а її оцінки можуть змінюватися залежно від багатьох факторів.

4.2.3. Генерація ключів та обмін ключами.

Стійкість криптографічної системи значною мірою пов’язана з процедурами роботи з ключовою інформацією. Крім безпосередньо застосування ключа необхідно забезпечити коректність таких процедур: генерації, поширення, зберігання, заміни, депонування та знищення ключів.

Порушнику набагато простіше провести атаку на підсистему роботи із ключами , а не на сам алгоритм криптографічного захисту.

Якісний ключ, призначений для використання в рамках симетричної криптосистеми, являє собою випадковий двійковий набір та не знижує теоретичну стійкість криптосистеми.

Якщо потрібен ключ розрядністю n, у процесі його генерації з однаковою ймовірністю повинен виходити кожен з 2^n можливих кодів.

Генерація ключів для асиметричних криптосистем - процедура більш складна, оскільки ключі, які застосовуються в таких системах, повинні мати унікальні властивості.

Для генерації ключової інформації в криптосистемах, застосовуються такі методи (у порядку зростання якості):

- програмна генерація, що передбачає обчислення чергового псевдовипадкового числа як функції часу, послідовності символів, заданих користувачем, особливостей його клавіатурного почерку тощо;
- програмна генерація, заснована на моделюванні якісного генератора псевдовипадкових послідовностей (ГПВП) з рівномірним законом розподілу (приклад-RANDOM);
- апаратна генерація з використанням якісного ГПВП;
- апаратна генерація з використанням генераторів випадкових послідовностей, побудованих на основі фізичних генераторів шуму і якісних ГПВП.

Обмін ключами

Для симетричних криптосистем кожна сторона використовує один і той же секретний ключ для шифрування/розшифрування, і якщо він періодично змінюється (максимум – в кожному сеансі), то учасники повинні обмінюватися ключами (зловмисник може «підслухати»).

Тому для формування спільного ключа використовують асиметричну схему Діффі – Хеллмана, у якій є два відкритих для всіх числа: просте число p (ділиться тільки на себе та 1) й ціле число q, що є первинним коренем p ($q^p \pmod p = 1$).

Примітка: $B = A \pmod p$ – залишок від цілочисельного ділення A на p, приклад $B = 19 \pmod 5 = 4$.

Припустимо, користувачі A й B мають намір обмінятися ключами. Користувач A вибирає випадкове ціле число $A < p$ і обчислює $Y_A = q^A \pmod p$;

Користувач B незалежно вибирає випадкове ціле число $B < p$ і обчислює $Y_B = q^B \pmod p$;

Кожна сторона зберігає значення (А і В) в таємниці а значення Y передає іншій стороні.

Користувач A обчислює ключ за формулою

$$K=Y_B^A \pmod p = q^{BA} \pmod p;$$

Користувач *B* - за формулою

$$K=Y_A^B \pmod p = q^{AB} \pmod p.$$

Ці дві формули обчислення дають однакові результати, отже кожен користувач отримав ключ, який використовується для подальшого симетричного шифрування.

Зловмисник може перехопити параметри *p*, *q*, *A* і *B*, але обчислити ключ йому дуже важко, тому що ступінь за модулем деякого простого числа обчислюється відносно легко, але зворотня операція - дискретні логарифми є неоднозначною і для великих простих *p* є обчислювально складним завданням (не вирішується за допустимий час).

У багатосерверних системах застосовується схема відновлення майстер-ключа системи декількома учасниками.

Схема управляється авторизованим дилером, основне завдання якого - поділ секрету на компоненти («тіні») і розподіл їх серед учасників так, що будь-які *m* (і більше) учасників, зібравшись разом і пред'явивши тіні, можуть відновити секретний ключ. Але будь-які (*m* – 1) і менше учасників не можуть це зробити.

4.2.4. Електронний цифровий підпис і функція хешування.

Хеш-функції

Для контролю цілісності інформації, яка передається, використовується механізм створення цифрових відбитків повідомлень (message digiting). за допомогою криптографічних хеш-функцій.

Така функція, $H(D_m)$ застосовується до повідомлення D_m довільної довжини M й обчислює значення S_h фіксованої довжини h – хеш сума або дайджес повідомлення D_m (ґрунтується на ідеї стиснення D_m).

Дайджес S_h передається разом з повідомленням.

Найпопулярнішими на сьогодні є функції хешування MD5, SHA-1, SHA-2, Whirlpool, ГОСТ 34.311—95 й RIPEMD.

Хеш - функція повинна володіти властивостями:

- Хеш-функцію H(Dm) досить просто обчислити для будь якого Dm.
- Хеш-функція повинна бути чутлива до всіляких змін в тексті, таким як вставки, викиди, перестановки і т. п.
- Хеш-функція є незворотною, іншими словами, підбір документа D'm , який володів би необхідним значенням хеш функції H(Dm), є обчислювально нерозв'язною задачею, хоча теоретично можливо (з мізерною ймовірністю),

що два різних повідомлення Dm і D’m можуть бути стиснуті в одну і ту ж згортку (так звана колізія, або «зіткнення»).

Електро́нний цифрови́й пі́дпис

Електро́нний цифрови́й пі́дпис (ЕЦП) (англ. digital signature) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який підтверджує його цілісність та ідентифікує підписувача.

Функціонально цифровий підпис аналогічний звичайному рукописному підпису і володіє його основними перевагами:

- засвідчує, що підписаний текст виходить від особи, яка його поставила;
- не дає цій особі можливості самій відмовитися від зобов'язань, пов'язаних з підписаним текстом;
- гарантує цілісність підписаного тексту.

До обчислення ЕЦП в файл, що підписується (або в окремий файл ЕЦП) додається інформація, яка однозначно ідентифікує автора підписаного документа і забезпечує її цілісність.

Кожен підпис містить наступну інформацію:

- дату підпису;
- термін закінчення дії ключа даного підпису;
- інформацію про особу, яка підписала файл (П.І.Б., посада, коротке найменування фірми);
- ідентифікатор підписанта (відкритий ключ);
- власне цифровий підпис.

Технологія застосування системи ЕЦП передбачає наявність мережі абонентів, що посилають один одному підписані електронні документи. Для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом в таємниці і використовується ним для формування ЕЦП. Відкритий ключ відомий всім іншим користувачам і призначений для перевірки ЕЦП одержувачем підписаного електронного документа.

Система ЕЦП включає дві основні процедури:

- формування цифрового підпису;
- перевірки цифрового підпису.

Схема формування цифрового підпису представлена на рис. 4.2., схема перевірки цифрового підпису – на рис. 4.3.

Фальсифікація можлива у двох випадках: або підпис підроблено, або змінено зміст повідомлення.

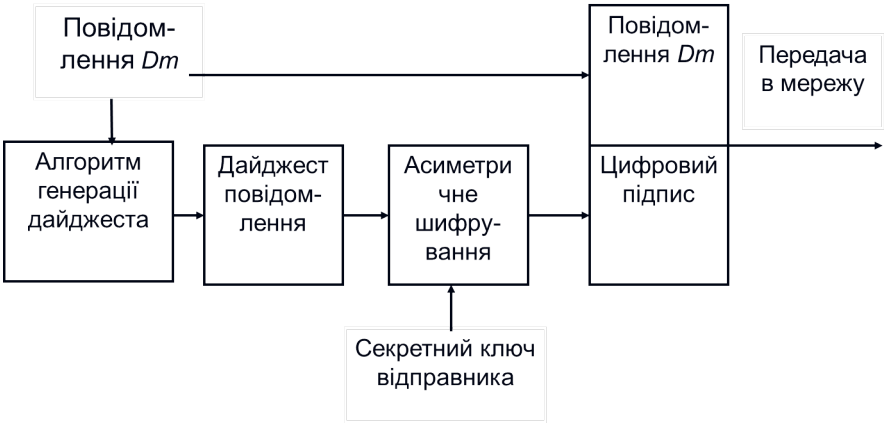

Рисунок 4.2. - Формування цифрового підпису

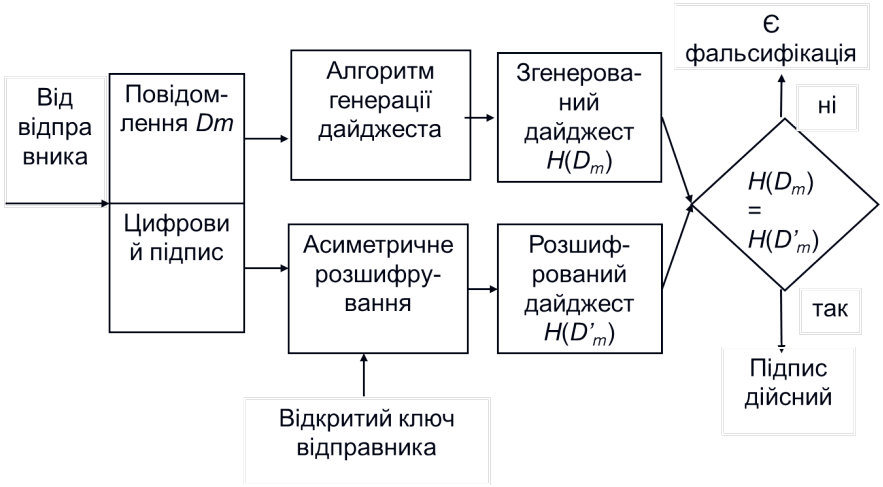

Рисунок 4.3. - Перевірка цифрового підпису

4.3. Антивірусний захист

Комп'ютерний вірус – це програма, яка написана програмістом, і на відміну від звичайних програм, ніколи не зберігає себе у вигляді окремих файлів, здатна створювати власні копії (розмножуватися), впроваджувати їх у файли, системні області комп'ютера або комп'ютерних мереж та чинити деструктивні дії.

Ведуть себе комп'ютерні віруси точно так само, як віруси живі: вони ховають свій код в тілі «здорової» програми і при кожному її запуску активуються і починають бурхливо «розмножуватися», безконтрольно поширюючись по всьому комп'ютеру.

Після зараження комп'ютера вірус може активізуватися і почати виконувати шкідливі дії по знищенню програм і даних.

Активізація вірусу може бути пов'язана з різними подіями:

- настанням певної дати або дня тижня
- запуском програми
- відкриттям документа ...

Історія виникнення вірусів

Перша «епідемія» комп'ютерного вірусу сталася в 1986 році, коли вірус на ім'я Brain (англ. «мозок») «заражав» дискети персональних комп'ютерів.

В даний час відомо кілька десятків тисяч вірусів, що заражають комп'ютери і розповсюджуються по комп'ютерних мережах.

Ознаки зараження

Основні симптоми зараження комп'ютера вірусом є:

- Уповільнення роботи програм;
- Збільшення розмірів деяких файлів і зміна часу їх створення;
- Поява не існуючих раніше «дивних» файлів;
- Зменшення обсягу доступної оперативної пам'яті;
- Раптово виникають різноманітні відео-та звукові ефекти.
- Деякі файли і диски виявляються зіпсованими;
- Комп'ютер перестає завантажуватися з жорсткого диска.

4.3.1. Класифікація комп'ютерних вірусів.

Віруси можна розділити на класи за такими ознаками:

1. По середовищу перебування вірусу;
2. За способом зараження середовища перебування;
3. По деструктивним можливостям;
4. За особливостями алгоритму вірусу.

1) Середовище перебування

По середовищу перебування віруси можна розділити на:

-Файлові - впроваджуються у виконувані програми (*.exe – файли)

-Мережеві - поширюються по комп'ютерній мережі (виділяють «почтові віруси»).

-Завантажувальні - у завантажувальний сектор логічного диска (Boot-сектор) або в системний завантажувач вінчестера (Master Boot Record) – більш детально в курсі «Архітектура обчислювальних систем» -5 семестр.

-Макровіруси.

2) Способи зараження

Способи зараження діляться на резидентний і нерезидентний.

- Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до вимикання або перезавантаження комп'ютера.

- Нерезидентні віруси не заражають пам'яті комп'ютера і є активними обмежений час.

3) Деструктивні можливості

За деструктивним можливостям віруси можна розділити:

- Нешкідливі - ніяк не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширення);

- Безпечні, вплив яких обмежується зменшенням вільної пам'яті на диску і графічними, звуковими й іншими ефектами;

- Небезпечні, які можуть призвести до серйозних збоїв у роботі;

- Дуже небезпечні, в алгоритм роботи яких свідомо закладені процедури які можуть призвести до втрати програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті (неперевірена комп'ютерна легенда - вводити в резонанс і руйнувати голівки деяких типів вінчестерів).

4) Особливості алгоритму

За особливостями алгоритму виділяються групи вірусів:

-«Паразитичні» - класичний тип вірусів, які при поширенні своїх копій обов'язково змінюють вміст дискових секторів або файлів.

-«Перезаписуючі» - віруси даного типу записують своє тіло замість коду програми, не змінюючи назви виконуваного файлу, внаслідок чого при запуску програми виконується код вірусу, а сама програма перестає запускатися.

-«Компаньйон-віруси» - вірус, виконуваний файл якого має те ж ім'я, що і додаток, але інше розширення. Часто замість розширення .EXE вірус-компаньйон розташовується в файлі з розширенням .COM, що забезпечує його завантаження і запуск при активізації програми по імені.

- «Віруси-черв'яки» - віруси, які поширюються в комп'ютерній мережі, і так само як і «компаньйон-віруси», не змінюють файлів і секторів на дисках.

- «Стелс-віруси» (віруси-невидимки), що представляють собою досить досконалі програми, які перехоплюють звернення ОС до уражених файлів або дисків і «підставляють» замість себе незаражені ділянки інформації.

- «Поліморфік-віруси» - їх складно детектувати, тому що вони не мають сигнатур, тобто не містять жодної постійної ділянки коду. Два зразки того самого поліморфік-вірусу не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

- «Студентські» - вкрай примітивні віруси, часто нерезидентні і містять велику кількість помилок.

- «Віруси-ланки» - не змінюють код програми, а змушують ОС виконати свій код, змінюючи адресу місця розташування на диску зараженої програми, на власну адресу.

- «Віруси, що вражають вихідний код програми» - Віруси даного типу вражають вихідний код програми або її компоненти (*.OBJ, *.LIB, *.DCU). Після компіляції програми, віруси виявляються вбудованими в неї.

- «Макровіруси» - віруси цього сімейства заражають не програми (*.EXE –файли), а дані, впроваджуючись в файли даних в вигляді макросів. Макро-віруси є програмами на макро-мовах, вбудованих в багато систем обробки даних (текстові редактори, електронні таблиці і т. д.). Для свого розмноження такі віруси використовують можливості макро-мов і за їх допомогою переносять себе з одного зараженого файлу (документа або таблиці) в інші. Найбільшого поширення набули макро-віруси для Microsoft Word, Excel. Існують також макро-віруси, що заражають бази даних Microsoft Access.

4.3.2. Файлові та бутові віруси, мережеві «черв'яки», «троянський кінь».

Файлові віруси

Впроваджуються в програми і активізуються при їх запуску. Після запуску зараженої програм можуть заражати інші файли до моменту вимикання комп'ютера або перезавантаження операційної системи.

За способом зараження файлові віруси поділяються на:

-Перезаписуючі віруси.

-Віруси-компаньйони.

-Файлові черви створюють власні копії з привабливими для користувача назвами в надії, що він їх запустить.

-Віруси-ланки.

-Паразитичні віруси.

-Віруси, що вражають вихідний код програми.

Мережні віруси

Розрізняють:

-Мережні черви.

-Троянські програми.

-Утиліти хакерів і інші шкідливі програми.

«Троянський кінь» - таємний, підступний задум. Троянські програми здійснюють різні несанкціоновані користувачем дії:

-збір інформації та її передача зловмисникам;

-руйнування інформації або зловмисна модифікація;

-порушення працездатності комп'ютера;

-використання ресурсів комп'ютера в зловмисних цілях.

Утиліти хакерів і інші шкідливі програми.

До даної категорії відносяться:

-утиліти автоматизації створення вірусів, червів і троянських програм;

-програмні бібліотеки, розроблені для створення шкідливого ПЗ;

-хакерські утиліти приховування коду заражених файлів від антивірусної перевірки;

-програми, що повідомляють користувачу свідомо помилкову інформацію про свої дії в системі;

-інші програми, які тим чи іншим способом навмисно завдають прямого або непрямого збитку даному або віддаленим комп'ютерам.

Шляхи проникнення вірусів

- Глобальна мережа Internet
- Електронна пошта
- Локальна мережа
- Комп'ютери «Загального призначення»
- Піратське програмне забезпечення
- Ремонтні служби
- Знімні накопичувачі

1)Глобальна мережа Internet

Основним джерелом вірусів на сьогоднішній день є глобальна мережа Internet.

Можливе зараження через сторінки Інтернет через наявність на сторінках всесвітньої павутини різного «активного» вмісту: скриптів, ActiveX-компонентів, Java-аплетів.

У цьому випадку використовуються уразливості ПЗ, встановленого на комп'ютері користувача, або уразливості в ПЗ власника сайту, а нічого не підозрюючі користувачі зайшовши на такий сайт ризикують заразити свій комп'ютер.

2)Електронна пошта

Один з основних каналів розповсюдження вірусів.

Зазвичай віруси в листах електронної пошти маскуються під безневинні вкладення: картинки, документи, музику, посилання на сайти.

У деяких листах можуть міститися дійсно тільки посилання, тобто в самих листах може і не бути шкідливого коду, але якщо відкрити таке посилання, то можна потрапити на спеціально створений веб-сайт, що містить вірусний код.

Багато поштових вірусів, потрапивши на комп'ютер користувача, потім використовують адресну книгу з встановлених поштових клієнтів для розсилки самого себе далі.

3)Локальна мережа

Третій шлях «швидкого зараження» - локальні мережі. Якщо не приймати необхідних заходів захисту, то заражена робоча станція при вході в мережу заражає один або кілька службових файлів на сервері.

На наступний день користувачі при вході в мережу запускають заражені файли з сервера, і вірус, таким чином, отримує доступ на комп'ютери користувачів.

4)Персональні комп'ютери «загального користування»

Небезпеку становлять також комп'ютери, встановлені в навчальних закладах. Якщо один з учнів приніс на своїх носіях вірус і заразив який-небудь навчальний комп'ютер, то чергову «заразу» отримають і носії всіх інших учнів, які працюють на цьому комп'ютері.

Те ж відноситься і до домашніх комп'ютерів, якщо на них працює більше однієї людини.

5)Піратське програмне забезпечення

Нелегальні копії програмного забезпечення, як це було завжди, є однією з основних «зон ризику». Часто піратські копії на дисках містять файли, заражені найрізноманітнішими типами вірусів.

6)Ремонтні служби

Досить рідко, але досі цілком реально зараження комп'ютера вірусом при його ремонті або профілактичному огляді. Ремонтники - теж люди, і деяким з них властиво байдуже ставлення до елементарних правил комп'ютерної безпеки.

7)Знімні накопичувачі

В даний час велика кількість вірусів розповсюджується через знімні накопичувачі, включаючи: флеш-память, цифрові фотоапарати, цифрові відеокамери, цифрові плеєри (MP3-плеєри), стільникові телефони.

Методи захисту:

-Захист локальних мереж

-Використання дистрибутивного ПЗ

-Резервне копіювання інформації

-Використання антивірусних програм

-Не запускати неперевірені файли.

4.3.3. Принципи побудови антивірусних програм.

Антивірусна програма - спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом, та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики - запобігання зараження (модифікації) файлів чи операційної системи шкідливим кодом.

Нині існує багато антивірусних програм, найбільш популярними в нашій країні є комплекти: Антивірус Касперського, Dr Web, NOD32, Avira, Norton Antivirus, AidsTest, Avira Free Antivirus та інші.

Антивірусні програми можуть виконувати такі дії:

-знаходячись резидентно в оперативній пам'яті, перевіряти в режимі реального часу на наявність вірусів усі об'єкти, до яких звертається користувач;

-проводити евристичний аналіз, тобто здійснювати пошук нових вірусів за стандартними діями вже відомих;

-сканувати інтернет-трафік, вхідну і вихідну електронну пошту, поштові бази даних;

-виконувати пошук вірусів у архівах;

-виконувати лікування об'єктів – видаляти віруси із файлів та системних областей, відновлюючи їх функціональність;

-виконувати за встановленим розкладом повну перевірку комп'ютера, оновлення антивірусних баз та інше;

-створювати карантинну зону для підозрілих об'єктів;

-блокувати несанкціоновані користувачем дії по відправленню даних на віддалений комп'ютер, запуску програм, завантаженню з віддалених комп'ютерів різноманітних даних та інше.

Методи знаходження вірусів

Антивірусні програми використовують два різних методи:

а)Перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в антивірусній базі.

б)Знаходження підозрілої поведінки будь-якої з програм, що схожа на поведінку зараженої програми.

а)Відповідність визначенню вірусів в антивірусній базі.

При цьому методі антивірусна програма під час перегляду файлу звертається до антивірусної бази, що складена авторами програми-антивірусу. У разі відповідності якоїсь ділянки коду програми, що проглядається, відомому коду (сигнатурі) вірусу в базі, може виконуватися одна з наступних дій:

-Видалити інфікований файл

-Відправити файл у карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу).

-Намагатися відтворити файл, видаливши сам вірус з тіла файлу.

б)Підозріла поведінка програмних забезпечень.

Антивіруси, що використовують метод знаходження підозрілої поведінки програм, не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується (EXE - файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити.

На відміну від методу відповідності визначенню вірусів в базі, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів. Однак треба враховувати, що програми, побудовані на цьому методі, видають також велику кількість помилкових попереджень.

Класифікація антивірусних програм

Розрізняють такі антивірусні програми:

- сканери (детектори) – програми, що здатні проводити перевірку комп'ютера на наявність шкідливих програм і повідомляти користувача про їх наявність. У ході перевірки програми використовують дані з антивірусних баз – дані про відомі на даний момент часу шкідливі програми;

- лікарі – програми, що здійснюють «лікування» комп'ютерів від виявлених шкідливих програм, тобто знешкоджують їх, а при неможливості знешкодження можуть видаляти заражені об'єкти або розташовувати їх у спеціальних папках. Як і детектори, лікарі використовують антивірусні бази для оновлення даних про способи боротьби зі шкідливими програмами;

- монітори – програми, що постійно (резидентно) знаходяться в оперативній пам'яті комп'ютера з моменту завантаження операційної системи і перевіряють усі файли і диски, до яких іде звертання, блокують дії, що можуть ідентифікуватись як дії шкідливої програми;

- ревізори – програми, які аналізують стан системних файлів і папок та порівнюють їх зі станом, що був на початку роботи антивірусної програми. При певних змінах, які характерні для діяльності шкідливих програм, програма-ревізор виводить повідомлення про можливість ураження шкідливою програмою;

- блокувальники – програми, які аналізують обмін даними комп'ютера користувача з іншими комп'ютерами в мережі. Програма блокує з'єднання з певним комп'ютером у мережі, якщо фіксує дії, які характерні для шкідливих комп'ютерних програм, і виводить повідомлення про намагання їх проникнення на комп'ютер користувача.

- сучасні антивірусні програми – це комплексні програми, що мають властивості всіх перерахованих видів, а також засоби поновлення антивірусних баз та модифікацію антивірусних програм через електронну пошту.

4.4. Захист операційних систем та програмного забезпечення.

4.4.1. Засоби захисту в складі обчислювальної системи.

Власний захист програм - це ті елементи захисту, які притаманні самому програмному забезпечення або супроводжують його продаж і перешкоджають незаконним діям користувача. До них відносяться:

-Документація на ПЗ, яка є суб'єктом авторського права і може виконувати функції захисту.

-Обмежене застосування - реалізується в тому випадку, коли ПЗ використовується невеликим числом користувачів, кожен з яких відомий по імені.

-Замовне проектування - розробка програмного забезпечення для спеціальних цілей.

-Індивідуальні мітки в стандартних програмних модулях для кожної копії програми.

Засоби захисту ПЗ в складі обчислювальної системи

Ця категорія засобів захисту включає:

-Захист дискових накопичувачів;

-Захистні характеристики пристроїв ПК;

-Замки захисту;

-Зміна функцій штатних пристроїв.

При використанні таких засобів виконання програми залежить від певних дій, спеціальних запобіжних заходів і умов, що гарантують захист.

1) Захист дискових накопичувачів

Методи захисту дисків використовують два принципи:

- завадити копіювання програми на інший диск;

-перешкодити перегляду або операції зворотного ассемблювання (дезассемблювання).

Основна техніка захисту інсталляційних накопичувачів полягає у форматуванні диска спеціальними способами, які оберігають операційну систему від копіювання. Це:

-нестандартне визначення форматів даних або каталогів,

-зміна розмірів секторів,

-збільшення числа синхронізуючих бітів,

-заміна інформаційних заголовків.

Перераховані методи стають неефективними при використанні систем побітового копіювання.

2) Захистні характеристики пристроїв

Використання спеціальних характеристик апаратури ПК для захисту програм - досить потужний, але дорогий засіб. Практичний інтерес представляють:

-Унікальний диск (вартість реалізації досить низька). Принцип полягає в тому, щоб заборонити запис інформації в деякі сектори доріжки (Раніше-механічне стирання магнітного шару поверхні, пізніше - лазерним променем), що створює унікальний формат кожного диска. Порівнюючи швидкості читання різних дисків, розрізняють оригінальний диск від його копії.

-У той час як спеціалізований комп'ютер економічно невигідний для забезпечення захисту програм, спеціалізований мікропроцесор на одному чіпі придатний для цих цілей. Для захисту програми від зчитування по шині даних ПК, виконання програми реалізується в чіпі (реалізація процедур шифрування і дешифрування програм або даних, які використовує програма).

3) Замки захисту

Замки захисту використовуються для того, щоб заборонити доступ до програми, якщо при спробі звернення до неї не виконані деякі перевірки:

-Контроль граничного часу або дати використання згідно з ліцензією, при цьому еталоном служать годинник комп'ютера.

-Замок на основі унікального для кожного комп'ютера серійного номера. Програма функціонує тільки на тих комп'ютерах, серійні номери яких включені в ліцензію.

-Запис з частковим руйнуванням інформації в оперативній пам'яті (ОЗП). Блоки динамічної пам'яті повинні періодично відновлюватися шляхом регенерації. Якщо сигнал регенерації переривати на деякий час, то інформація в ОЗП руйнується специфічним чином для кожного конкретного модуля пам'яті. Це дає унікальний ключ захисту, який охороняє програму від функціонування на іншому комп'ютері.

4) Зміна функцій штатних пристроїв

Існує ряд методів захисту, які засновані на чергуванні дій ключів та функцій системи.

Ці чергування можуть запобігти перегляду програмного лістингу або призупинити виконання підпрограм копіювання. Зміни повинні бути непомітними для користувача, наприклад, якщо змінити імена файлів, що виводяться на екран монітора, то випадковий користувач не зможе викликати такі файли.

Функціональні особливості апаратури можуть використовуватися для захисту програм. Будь-яка програма, розміщена в ПЗП, відображає його

властивість - тільки читання інформації. Спроби обійти цю властивість програмним способом будуть безуспішні, якщо тільки не скопіювати програму в пам'ять, яка допускає запис, де незаконна копія може бути змінена.

4.4.2. Засоби захисту із запитом інформації

Програма вимагає для своєї роботи введення додаткової інформації:
- паролі, номера ключів і т.п.
- сигнатури
- апаратура захисту

1)Паролі

Паролі повинні бути прості для запам'ятовування, щоб не записувати їх, і не повинні бути настільки очевидними, щоб порушник міг вгадати - вони не повинні бути пов'язані з адресою або назвою фірми.

Використання в якості пароля окремих елементів умовного слова, наприклад першої та п'ятої літери, запобігає ситуацію, коли ціле слово могло б бути випадково почуте.

Одноразовий блокнот - більш надійний механізм формування паролів, в цьому випадку пароль є складовим, на зразок листків блокнота, які відкриваються одночасно.

Сюди ж відносяться питально-відповідні системи, які запитують місце народження, дівоче прізвище і т.п.

2)Сигнатури

Сигнатура - унікальна характеристика комп'ютера або інших пристроїв системи, яка не схильна до змін і сама не впливає на нормальне функціонування програмного забезпечення і може бути використана для захисту і перевірена програмним способом.

Якщо характеристики унікальні для даної обчислювальної системи, нормальне проходження програми може бути виконано тільки на ній.

Приклади сигнатур: MAC- та IP-адреса, серійний №, унікальне форматування диска та ін.

3)Апаратура захисту

Електронні пристрої захисту (ЕПЗ) зазвичай приєднуються через стандартні інтерфейси COM, LPT, USB і відгукуються на запит у вигляді деякого псевдовипадкового числа або їх послідовності.

Недолік - доступ до цього пристрою з програми, і хакер може передбачити обхід запиту (включається звернення до підпрограми, яка імітує функцію ЕПЗ). Можна також стежити за лінією зв'язку і фіксувати числа, а потім генерувати таблицю для вторгнення в програму.

Тому розроблені ЕПЗ з елементами інтелекту з вбудованим

мікропроцесором для реалізації складних алгоритмів захисту (генерація запиту на доступ кілька разів випадковим чином в випадкові моменти часу і самознищення програми при виявленні обходів).

4.4.3. Засоби активного захисту.

Засоби захисту ініціюються при виникненні особливих обставин - спроби несанкційованого доступу, введення неправильного пароля, вказівки неправильної дати або часу або інших подібних умов.

Засоби активного захисту діляться на дві групи: внутрішні (в складі комп'ютера) і зовнішні.

Внутрішні засоби активного захисту:

-блокують або знищують програму (для ліцензійних програм);

-попередження, дружнє нагадування, організація спостереження (несанкційований доступ).

Зовнішні засоби активного захисту - сигнали тривоги, викликані різними ситуаціями, які переводять в стан готовності засоби захисту.

4.4.4. Засоби пасивного захисту.

До засобів пасивного захисту відносяться методи, спрямовані на пошук доказів копіювання програми, а саме:

- Ідентифікація оригінальних програм:

■.....Кореляційні характеристики оригіналу відрізняються від копій.

■.....«Рідні плями» - з'являються в процесі розробки програми: стиль програмування, помилки і надмірності (підпрограми, які були необхідні для налагодження, а потім не були видалені).

■.....«Відмінні мітки» (вводяться спеціально) - при нормальному функціонуванні не «проявляють» себе. Закодовані відмінні мітки залишаються доступними і в машинному коді.

-Контроль і реєстрації подій, процедур або доступу до даними.

-Водяні знаки, етикетки.

4.4.5. Електронні ключі.

Контроль доступу до комп'ютерів, ідентифікація і аутентифікація, а також ряд інших захисних функцій, виконуються за допомогою електронного ключа і пристроїв введення ідентифікаційних ознак (ПВІО) до завантаження ОС.

За способом зчитування ПВІО поділяються на:

- контактні,

- дистанційні (радіочастотним або інфрачервоним методом)
- комбіновані.

ПВІО можуть бути електронними, біометричними та комбінованими. Електронні ПВІО містять мікросхему пам'яті ідентифікаційної ознаки.

Одним з найбільш потужних інструментів захисту ПЗ і БД - інструментальна система Hardlock з електронним ключем Hardlock - високий рівень захисту програм і апаратне шифрування файлів даних.

Ключі Hardlock випускаються в наступних конфігураціях:

-зовнішні ключі на COM, LPT, USB порти

-внутрішні ключі на системну шину ПК;

-мережеві ключі - зовнішній або внутрішній.

4.4.6. Технологія захисту інформації на основі смарт-карт.

Технологія смарт-карт (СК), заснована на картах з вбудованим мікропроцесором, використовується в банківській системі.

СК можуть бути виготовлені тільки промисловим шляхом і, отже, не можуть бути скопійовані.

За технологією СК розроблені персональні ідентифікатори iKey компанії Rainbow - недорогі брелки, які можуть використовуватися на будь-якій робочій станції, що має USB шину.

iKey 2000 створює потужну систему захисту і криптографічного кодування безпосередньо всередині апаратного пристрою.

4.4.7. Створення захищеної операційної системи.

Захищені ОС стали розроблятися для персональних комп'ютерів, робочих станцій і для мережевих систем.

В даний час є два принципово різних методів проектування захищених операційних систем:

-Розробка захищеної системи «з нуля», і в цьому випадку для неї спеціально розробляються захищені додатки. Внаслідок значної трудомісткості і вартості такий підхід прийнятний для заможних виробників.

-Доопрацювання системи-прототипу з метою поліпшення її характеристик захисту. Найбільш часто основою для розробки захищених ОС служить UNIX.

Всі захищені ОС в загальному реалізують один і той же набір захисних функцій - управління доступом і контроль за його здійсненням, ідентифікація і аутентифікація, аудит, пряму взаємодію і т.д.

Це пов'язано з тим, що всі розробники орієнту-ються на відповідні розділи стандартів інформаційної безпеки.

Однак способи реалізації цих функцій, як і реалізований ними рівень захисту, відрізняються від системи до системи навіть в рамках одного класу вимог.

Найпрогресивнішою технологією побудови захищеної ОС є технологія мікроядра.

На відміну від традиційної архітектури, в якій ОС являє собою монолітне ядро, що реалізує основні функції з управління апаратними ресурсами і організації середовища для виконання процесів користувача, мікроядерна архітектура розподіляє функції ОС між мікроядром і системними сервісами, що входять до складу ОС (процеси, рівноправні з додатками користувача).

В результаті такі важливі компоненти ОС як файлова система, мережева підтримка і т.д. перетворюються в незалежні модулі, які функціонують як окремі процеси і взаємодіють з ядром і один з одним на загальних підставах.

Чіткий розподіл програмного забезпечення на системні і прикладні програми тепер розмивається, тому що між процесами, що реалізують функції ОС, і прикладними процесами, які виконують програми користувача, немає ніяких відмінностей.

Всі компоненти системи використовують засоби мікроядра для обміну повідомленнями, але взаємодіють безпосередньо. Микроядро лише перевіряє законність повідомлень, пересилає їх між компонентами і забезпечує доступ до апаратури.

Інша зміна в технології побудови ОС, пов'язана виключно з впровадженням технології мікроядра, це організація взаємодій між процесами і ядром за допомогою універсального механізму передачі інформації - обміну повідомленнями, який прийшов на зміну техніці системних викликів.

Для захищених систем така архітектура є оптимальною, тому що вона дозволяє досить просто і ефективно вирішити цілий ряд питань, що неминуче виникають при реалізації захищених систем.

У мікроядерній системі мікроядро виконує лише функції:

-управління фізичної апаратурою (оперативною пам'яттю, процесорами, зовнішніми пристроями);

-розподіл ресурсів апаратної платформи між процесами (час процесора, пам'ять і т.д.);

-ізоляція процесів;

-організація взаємодії між процесами;

-управління процесами (створення, знищення, перемикання).

Ядро є своєрідним арбітром, роль якого зводиться до підтримки деякого набору «правил гри» всередині операційної системи, всі інші традиційні функції ОС реалізуються поза ядром.

Програмно-апаратний комплекс «Акорд - 1.95»

Програмно-апаратний комплекс засобів захисту інформації від несанкційованого доступу «Акорд - 1.95», призначений для застосування на ПК типу IBM PC з метою захисту ПК та інформаційних ресурсів від несанкціонованого доступу і забезпечення конфіденційності інформації при багатокористувацькому режимі її експлуатації.

Комплекс «Акорд» складається з програмно-апаратних засобів «Акорд АМДЗ» і ПЗ розмежування доступу «Акорд 1.95-00 ».

Характеристики комплексу:

- Для установки апаратної частини необхідний вільний слот ISA або PCI;
- Використовують для ідентифікації персональні ТМ-ідентифікатори DS 199х з об'ємом пам'яті до 64 Кбіт.
- Використовують для аутентифікації пароль до 12 символів.
- Блокують завантаження з FDD, CD ROM, ZIP Drive.
- Передбачають реєстрацію від 16 до 32 користувачів.
- Мають апаратний датчик випадкових чисел (ДВЧ).
- Забезпечують контроль цілісності програм, даних і системних областей жорстких дисків.
- Мають внутрішню енерго-незалежну пам'ять для зберігання даних про зареєстрованих користувачів і журналу реєстрації подій.

4.5.Безпечна взаємодія в комп’ютерних мережах

4.5.1. Типи атак в КМ.

Загальна класифікація атак на інформаційні ресурси була розглянута в п. 2.1.7. Розглянемо особливості атак в комп’ютерних мережах:

-Розподілені IP-мережі насамперед схильні до віддалених атак (прослуховування та активний вплив), оскільки зазвичай використовуються відкриті канали передачі даних.

-В локальних мережах на перше за значимістю місце виходять порушення зареєстрованих користувачів, оскільки в цьому випадку канали передачі даних локальної мережі знаходяться на контрольованій території і захист від несанкціонованого підключення до них реалізується адміністративними методами

Найбільш поширені в КМ такі атаки:

1)Підслуховування (sniffing) – шляхом перехоп-лення всіх мережевих пакетів, які передані через певний домен та password sniffing- перехоплення незашифрованого пароля.

2)Аналіз мережевого трафіку.

3)Підміна довіреного суб'єкта - некоректне привласнення, або фальсифікація IP-адреси.

4)Посередництво в обміні незашифрованими ключами (атака man-in-the-middle). Для проведення атаки man-in-the-middle (людина-в-середині) зловмисникові потрібен доступ до пакетів, що передаються по мережі. Для атак цього типу часто використовуються сніфери пакетів, транспортні протоколи і протоколи маршрутизації

5)Відмова в обслуговуванні (Denial of Service, DoS). DoS атака відрізняється від атак інших типів: вона не націлена на отримання доступу до мережі або на отримання з цієї мережі будь-якої інформації. Атака DoS робить мережу (сервер) недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, ОС або додатків (переповнення трафіку). По суті, вона позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації. Якщо атака цього типу проводиться одночасно через багато пристроїв, то говорять про розподілену атаку відмови в обслуговуванні DDoS (distributed DoS).

6)Перехоплення сеансу (session hijacking). Після закінчення початкової процедури аутентифікації з'єднання, встановлене законним користувачем, наприклад з поштовим сервером (а в гіршому випадку з сервером банку), перемикається зловмисником на свій хост, а вихідному серверу видається команда розірвати з'єднання. В результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

7)Атаки на рівні додатків полягають у використанні відомих слабкостей серверного ПЗ (FTP, HTTP, web-сервера). Головна проблема з атаками на рівні додатків - вони часто користуються портами, яким дозволений прохід через міжмережевий екран.

8)Мережева розвідка - збір інформації про мережу за допомогою запитів DNS, ехо-тестування (ping sweep) і сканування портів:

- Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені.

- ехо-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі.

- Отримавши список хостів, зловмисник використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами.

В результаті видобувається інформація, яку можна використовувати для злому мережі.

4.5.2. Захист КМ за допомогою сканерів

Сканери стали грізною зброєю як захисту так і нападу (при використанні зловмисником) в Internet.

Сканер - це програма, призначена для автоматизації процесу пошуку слабкостей у захисті комп'ютера, підключеного до мережі відповідно до протоколу TCP / IP.

Найбільш досконалі сканери звертаються до портів TCP / IP віддаленого комп'ютера і в деталях протоколюють відгук, який вони отримують від цього комп'ютера.

Запустивши сканер на своєму комп'ютері, користувач може знайти проломи в захисних механізмах віддаленого сервера.

Більшість сканерів призначений для роботи в середовищі операційної системи UNIX, хоча на теперішній час такі програми є для будь-якої ОС.

Можливість запустити сканер на конкретному комп'ютері залежить від:

- версія ОС, під управлінням якої працює цей комп'ютер;
- параметри підключення до Internet (швидкість не менше 14400 біт / с);
-обсяг ОЗУ комп'ютера - менший обсяг вимагають сканери, які управляються за допомогою командного рядка, «ненажерливі» - з віконним графічним інтерфейсом користувача.

Зазвичай сканери створюються і використовуються фахівцями в області мережевої безпеки. щоб з їх допомогою системні адміністратори могли перевіряти комп'ютерні мережі на наявність в них вад.

Для ефективного використання сканерів на практиці необхідно правильно інтерпретувати зібрані з їх допомогою дані, а це можливо тільки при наявності глибоких знань в області мережевої безпеки і багатого досвіду.

Однак деякі сканери в процесі пошуку проломів в захисті мереж виконують деструктивні дії:

-несанкціонований доступ до інформації;

-створення, використання і поширення шкідливих програм;

-знищення, блокування, модифікація або копіювання інформації, що зберігається в електронному вигляді

4.5.3.Захист від аналізаторів протоколів.

В даний час найпоширеніша технологія побудови локальних комп'ютерних мереж є Ethernet.

Однак технологія Ethernet не позбавлена істотних недоліків. Основний з них - передана інформація не захищена. Комп'ютери мережі можуть перехоплювати інформацію, адресовану сусідам, тому що в мережі використовується широкомовний (широковещательный) механізм обміну

повідомленнями.

Комп'ютери мережі, як правило, спільно використову-ють один і той же кабель, який служить середовищем для пересилання повідомлень між ними:

- коаксіальний – топологія «шина»,

- вита пара – топологія «зірка» з центральним концентратором або комутатором.

Якщо комп'ютер, підключений до мережі Ethernet, нічого не передає сам, він, тим не менш, продовжує «слухати» всі повідомлення, що передаються іншими комп'ютерами.

Помітивши в заголовку передаваємої порції даних свою мережеву адресу, комп'ютер копіює ці дані в свою локальну пам'ять.

Крім того, переважна більшість сучасних Ethernet-адаптерів допускають функціонування в особливому режимі, званому «безладним». При використанні даного режиму адаптер копіює в локальну пам'ять комп'ютера всі без винятку передані через мережу кадри даних.

Спеціалізовані програми, що переводять мережевий адаптер в «безладний» режим і збирають весь трафік мережі для подальшого аналізу, називаються аналізаторами протоколів.

Адміністратори мереж широко використовують аналізатори протоколів для здійснення контролю за роботою цих мереж і визначення їх перевантажених ділянок.

На жаль, аналізатори протоколів використовуються і зловмисниками, які проникають в мережу ззовні (наприклад, якщо мережа має вихід в Internet), та з їх допомогою можуть перехопити чужі паролі та іншу конфіденційну інформацію.

Аналізатори протоколів існують для будь-якої платформи. Аналізатор протоколів може бути встановлений в будь-якому вузлі мережі і звідти перехоплювати мережевий трафік.

Рекомендовані засоби захисту:

- Встановити мережевий адаптер, який принципово не може функціонувати в «безладному» режимі. (Існують адаптери які не підтримують безладний режим на апаратному рівні, інші забезпечуються драйвером, що не допускає роботу в безладному режимі).

- Встановити сучасний мережевий інтелектуальний комутатор, який буферизує кожен пакет в пам'яті і відправляє його в міру можливості точно за адресою (немає «прослуховування» мережним адаптером всього трафіку.

- Не допускайте несанкціонованого встановлення аналізаторів протоколів на комп'ютери мережі. Для цього слід застосовувати засоби боротьби з програмними закладками.

- Шифрування всього трафіка мережі.

4.5.4. Міжмережеві екрани.

Міжмережеві екрани (МЕ), в літературі фігурують також firewall, брандмауери у загальному випадку, є засобом розмежування доступу клієнтів з однієї мережі до інформації, що зберігається на серверах в іншій мережі.

У цьому сенсі МЕ можна уявити як набір фільтрів, що пропускають через себе весь трафік, аналізують інформацію і приймають рішення: пропустити інформацію або її заблокувати.

Одночасно з цим проводиться реєстрація подій і тривожна сигналізація в разі виявлення загрози.

Зазвичай МЕ роблять несиметричними (визначаються поняття «всередині» і «зовні»), причому в завдання екрану входить захист внутрішньої мережі від потенційного ворожого оточення.

Крім того, МЕ може використовуватися в якості корпоративної відкритої частини мережі, видимої з боку Інтернету.

Так, наприклад, у багатьох організаціях МЕ використовуються для зберігання даних з відкритим доступом, як, наприклад, інформація про продукти та послуги, і т.п.

Сучасні вимоги до міжмережевих екранів:

- Основна вимога - забезпечення безпеки внутрішньої (що захищається) мережі і повний контроль над зовнішніми підключеннями і сеансами зв'язку.
- Екрануюча система повинна мати могутні і гнучкі засоби керування для простого і повного втілення в життя політики безпеки організації.
- МЕ повинен працювати непомітно для користувачів локальної мережі і не ускладнювати виконання ними легальних дій.
- Процесор МЕ повинен бути швидкодіючим і встигати обробляти весь вхідний і вихідний потік в пікових режимах, щоб його не можна було блокувати DoS -атаками і порушити його роботу.
- Система забезпечення безпеки повинна бути надійно захищена від будь-яких несанкціонованих впливів, оскільки вона є ключем до конфіденційної інформації організації.
- Система управління екранами повинна мати можливість централізовано забезпечувати проведення для віддалених філій єдиної політики безпеки.
- Брандмауер повинен мати засоби авторизації доступу користувачів через зовнішні підключення, що є необхідним в разі роботи співробітників організації в відрядженнях.

4.5.5. Управління криптографічними ключами

Всі криптографічні системи засновані на використанні криптографічних ключів. У симетричній криптосистемі відправник і одержувач використовують один і той же секретний ключ, який повинен підлягати періодичному оновленню щоб уникнути його компрометації.

Несиметрична криптосистема використовує два ключі - відкритий (передається по мережі) і секретний (особистий).

Управління ключами включає в себе наступні функції:

-генерація ключів;

-зберігання ключів;

-розподіл ключів.

1) Генерація ключів.

Так як від криптографічного ключа залежить безпека криптографічного алгоритму, то якісні криптографічні ключі повинні мати достатню довжину і випадкові значення бітів.

Для генерації ключів використовують апаратні і прогамні засоби, здатні формувати псевдовипадкові числа (ПВЧ).

Для регулярної заміни ключа необхідно проводити процедуру його модифікації. Під модифікацією ключа розуміють генерування нового ключа з попереднього за допомогою деякої односпрямованої функції.

2) Зберігання ключової інформації.

Під зберіганням ключів розуміють організацію їх безпечного зберігання, облік та видалення. Секретні ключі ніколи не повинні записуватися в явному вигляді на носій, який може бути прочитаний або скопійований.

Носієм ключової інформації може бути:

- пристрій зовнішньої пам’яті (з‘ємний магнітний диск, флеш-память)

- пристрій зберігання ключів типу Touch Мемогу,

- пластикова смарт – картка, яка дозволяє ідентифікувати і аутентифікувати користувачів, зберігати криптографічні ключі, паролі і коди.

Пристрій зберігання ключів типу Touch Мемогу (ТМ) являє собою енерго-незалежну пам'ять, розміщену в металевому корпусі. У структуру ТМ входять наступні основні блоки:

- Постійний запам'ятовуючий пристрій (ПЗП), який зберігає унікальний 64-розрядний код, що складається з 8-бітового коду типу приладу, 48-бітового унікального серійного номера і 8-бітової контрольної суми.

- Оперативна пам'ять (ОЗП) ємністю від 128 до 8192 байт.

- Вбудована мініатюрна літієва батарейка з терміном служби не менше 10 років, яка забезпечує живлення всіх блоків пристрою.

3) Розподіл ключів.

Будь-яка інформація про використовувані ключі повинна бути

захищена, зокрема зберігатися в зашифрованому вигляді.

Необхідність в зберіганні і передачі ключів, зашифрованих за допомогою альтернативних джерел, призводить до концепції ієрархії ключів:

- головний ключ (ГК),
- ключ шифрування ключів (КК),
- ключ шифрування даних (КД).

Ієрархія ключів може бути дворівнева (КК / КД), або трирівнева (ГК / КК / КД).

Самим нижнім рівнем є робочі або сеансові КД, які застосовуються для шифрування даних, персональних ідентифікаційних номерів (PIN) і аутентифікації повідомлень.

Для шифрування ключів з метою захисту при передачі або зберіганні, застосовують ключі наступного рівня - ключі шифрування ключів КК, які ніколи не повинні використовуватися як сеансу КД.

У більшості випадків в каналі застосовуються два ключа для обміну між вузлами мережі, по одному в кожному напрямку (ключ відправлення і ключ отримання).

На верхньому рівні ієрархії ключів знаходиться головний ключ (майстер-ключ) ГК, який шифрує КК, якщо потрібно зберегти їх на диску.

Для виключення перехоплення ГК поширюється між учасниками обміну неелектронним способом.

Криптографічний блок може бути спроектований як єдина НВІС і поміщений в фізично захищене місце.

Важливою умовою захисту інформації є періодичне оновлення ключової інформації. В особливо відповідальних випадках оновлення КД бажано робити щодня.

Розподіл ключів - найвідповідальніший процес в управлінні ключами. До нього ставляться такі вимоги:

- оперативність і точність розподілу;
- скритність розподілу ключів.

Розподіл ключів між користувачами комп'ютерної мережі реалізується двома способами:

- використанням одного або декількох центрів розподілу ключів;
- прямим обміном сеансовими ключами КД між користувачами мережі.

В обох випадках повинна бути забезпечена достовірність сеансу зв'язку. Це можна здійснити, використовуючи:

- механізм запиту-відповіді;
- механізм позначок часу.

а)Механізм запиту-відповіді полягає в наступному. Користувач А включає в посилаєме повідомлення (запит) для користувача В непередбачуваний елемент (наприклад, випадкове число).

При відповіді користувач В повинен виконати деяку операцію з цим елементом (наприклад, додати одиницю), що неможливо здійснити заздалегідь, оскільки невідомо, яке випадкове число прийде в запиті. Після отримання результату дій користувача В (відповідь) користувач А може бути впевнений, що сеанс є справжнім.

б)Механізм позначок часу передбачає фіксацію часу для кожного повідомлення.

Це дозволяє кожному суб'єкту мережі визначити, наскільки старе повідомлення, що прийшло і відкинути його, якщо виникнуть сумніви в його автентичності.

При використанні позначок часу необхідно встановити допустимий часовий інтервал затримки.

В обох випадках для захисту елемента контролю використовують шифрування, щоб бути впевненим, що відповідь надіслано не зловмисником і не змінений штемпель позначки часу.

Завдання розподілу ключів зводиться до побудови протоколу розподілу ключів, що забезпечує:

- взаємне підтвердження автентичності учасників сеансу;
- підтвердження достовірності сеансу механізмом запиту-відповіді або позначки часу;
- використання мінімального числа повідомлень при обміні ключами;
- можливість виключення зловживань з боку центру розподілу ключів (аж до відмови від нього).

При цьому відділяється процедура підтвердження справжності партнерів від процедури власне розподілу ключів.

Контрольні питання

1. Приведіть класифікацію технічних каналів витоку інформації.
2. Назвіть засоби виявлення каналів витоку інформації.
3. Які багатофункціональні комплекти для виявлення каналів витоку інформації є найпоширенішими?
3. Чим відрізняються активне та пасивне приховування інформації та якими технічними засобами воно виконується?
4. Дайте визначення поняттю криптографії.
5. Приведіть узагальнену схему криптосистеми.
6. Чим відрізняються симетричні та асиметричні криптосистеми?
7. Приведіть схему формування та перевірки електронного цифрового підпису.
8. Дайте визначення комп’ютерного вірусу.
9. Приведіть класифікацію комп'ютерних вірусів.

10. Назвіть основні шляхи проникнення вірусів.

11. Які два основних метода знаходження вірусів використовуються в антивірусних програмах?

12. Які засоби власного захисту програм існують?

13. Які методи захисту дискових накопичувачів використовуються?

14. Назвіть засоби захисту програм із запитом інформації.

15. Чим відрізняються засоби активного та пасивного захисту програм?

16. Чому найпрогресивнішою технологією побудови захищеної ОС вважається технологія мікроядра?

17. Назвіть основні типи атак в комп'ютерних мережах (КМ).

18. Як виконується захист КМ за допомогою сканерів?

19. Що таке аналізатори протоколів? Які функції вони виконують?

20. Як аналізатори протоколів використовуються зловмисниками і які засоби захисту від них існують?

21. Які сучасні вимоги ставляться до міжмережевих екранів?

22. Що таке трьох-рівнева ієрархію ключів? Для чого вона використовується?

СПИСОК ЛІТЕРАТУРИ

1. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 118 с.

2. Замула О.А. Захист держаних секретів. Навчальний посібник. ХНУРЕ – 2004.– 206 с.

3. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Електронна версія. Монографія. Харків. Форт. 2016, 902с.

4. Закон України “Про інформацію” від 02.10.1992 року.

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31.05.2005 року, №2594- IV, К., 2005.

6. Про заходи щодо захисту інформаційних ресурсів держави. Затверджено Указом Президенту України №582 від 10.04 2000 року

7. Сенів М.М. Безпека програм та даних: навч. посіб. / М.М. Сенів, В.С. Яковина; М-во освіти і науки України, Нац. ун-т "Львівська політехніка". – Львів: Вид-во Львівської політехніки, 2015. – 256 с.

8. Постанова КМУ від 29.03.2006р. № 373 «Правила забеспечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ».

9. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 3.1-003-2005.

10. Олейніков А.М. Методи та засоби захисту інформації. Навчальний посібник для студентів вищих навчальних закладів. - Харків: НТМТ , 2014. – 299 с.

11. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ Іваненко С.О., Гавриленко О.В., Липский О.А., Швецов А.С. - Київ, ІСЗЗІ НТУУ «КПІ», 2016.- 104 с.

12. Носов В.В., Манжай О.В. Організація та забезпечення безпеки інформації. Навч. посібник: - Харків, Вид-во Харків, Нац. ун-ту внутр. справ, 2007. - 216 с.

13. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

14. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

Навчальне видання

ПОВОРОЗНЮК Анатолій Іванович
ПОВОРОЗНЮК Оксана Анатоліївна

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчальний посібник

Роботу до видання рекомендував проф. М. Й. Заполовський

В авторській редакції