Бакалаврська робота

Жуль Владислав Володимирович	Дослідження системи фізичного захисту інформації з метою адаптації до загроз і обмежень	КИД-42

2024

ВСТУП

У наш час інформація є дуже цінною і важливою, як і будь-яка інша цінність, люди намагаються вберегти її від сторонніх рук і очей, особливо цінну державну таємницю та приватну комерційну інформацію. У бізнесі добросовісна конкуренція передбачає суперництво, засноване на дотриманні законодавства та загальноприйнятих норм моралі. Однак не секрет, що деякі бізнесмени намагаються за допомогою незаконних операцій отримати інформацію на шкоду інтересам іншої сторони і використати її для отримання переваг на ринку. Причин активності комп'ютерних злочинів і пов'язаних з ними фінансових втрат, по суті, багато:

- Перехід від традиційних "паперових" технологій зберігання та передачі даних до електронних та слабкий розвиток технологій захисту;

- Об'єднання обчислювальних систем, створення глобальних мереж і розширення зовнішнього доступу до інформаційних ресурсів;

- Збільшення складності програмного забезпечення.

Тому основною тенденцією, що характеризує розвиток сучасних інформаційних технологій, є зростання кількості комп'ютерних злочинів і пов'язаних з ними розкрадань конфіденційної та іншої інформації. З розвитком технологій електронних платежів, електронного документообігу та інших бізнес-систем серйозні збої в роботі корпоративних мереж можуть просто паралізувати роботу цілих корпорацій і банків, що призведе до значних матеріальних втрат.

Очевидно, що захист даних в комп'ютерних мережах з розвитком інформаційних систем вийшов на перше місце за важливістю як при організації комп'ютерних мереж, так і при роботі з ними.

Наразі існує три основні принципи інформаційної безпеки, які повинні забезпечувати:

- Цілісність даних (вирішення проблеми захисту від збоїв, які призводять до втрати або зміни інформації);

- Конфіденційність інформації (вирішення проблеми несанкціонованого доступу до інформації);

- Доступність інформації для всіх авторизованих користувачів (вирішення проблеми збою в обслуговуванні).

В даній роботі розглядаються операційні питання захисту інформації в комп'ютерних мережах. Спочатку розглядаються загальні питання безпеки комп'ютерних мереж, аналізуються основні джерела загроз. Другий розділ присвячений аналізу основних методів і засобів підтримки інформаційної безпеки. На основі методів, розглянутих у другому розділі, у третьому розділі проаналізовано підтримку інформаційної безпеки компанії "Інтепс". Оскільки інформація будь-якої компанії, яка зберігається і обробляється в межах локальної мережі, являє собою комерційну таємницю, питання її захисту є надзвичайно важливими і актуальними для адміністрації.

1 ПРОБЛЕМИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Способи та методи несанкціонованого доступу до інформаційних ресурсів комп'ютерних мереж

Одним з найважливіших аспектів проблеми безпеки комп'ютерних мереж є визначення, аналіз і класифікація можливих загроз безпеці комп'ютерних мереж. Перелік значущих загроз, оцінки ймовірностей їх реалізації, а також модель порушника є основою для проведення аналізу ризиків і формулювання вимог до системи захисту комп'ютерних мереж. Більшість сучасних інформаційних мереж обробки інформації, як правило, являють собою територіально розподілені інтенсивно взаємодіючі між собою системи із заданими даними (ресурсами) і оброблювачами (подіями) локальних обчислювальних мереж і окремих комп'ютерів.

Шляхи несанкціонованого доступу до інформації наведені на рисунку 1.1.

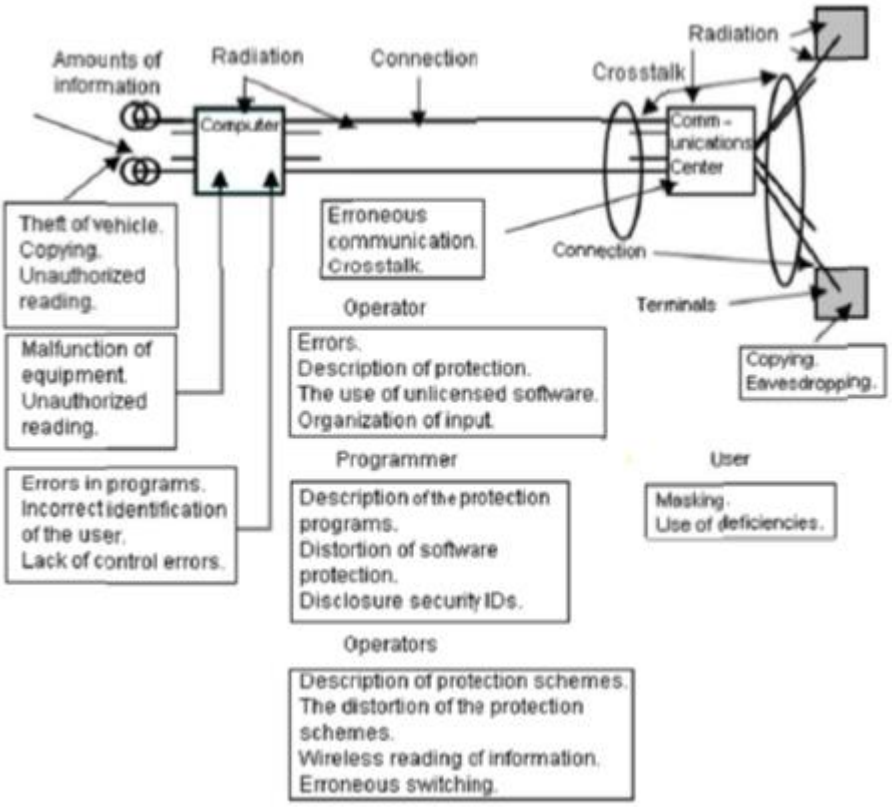


Рисунок 1.1 - Шляхи несанкціонованого доступу до інформації

Для локально-виділених (централізованих) обчислювальних систем можливі всі «традиційні» способи несанкціонованого доступу до інформації в процесі їх експлуатації та доступу до інформації. Крім того, з'явилися нові специфічні способи проникнення в систему і несанкціонованого доступу до інформації.

Наведемо перелік основних ознак виділених комп'ютерних систем:

- Територіальна відокремленість компонентів виділеної системи та інтенсивний інформаційний обмін між ними;

- Широкий спектр можливих способів представлення, зберігання та протоколів передачі інформації;

- Інтеграція даних різного функціонального призначення, що належать різним суб'єктам, в рамках єдиних баз даних або навпаки, розподіл необхідних даних в різних віддалених мережах;

- Абстрагування власників даних від фізичних структур і місця розташування даних;

- Використання методів розподіленої обробки даних;

- Використання автоматизованих систем обробки інформації великої кількості користувачів і персоналу різних категорій;

- Прямий і одночасний доступ до ресурсів (у тому числі цінної інформації) великої кількості користувачів різних категорій;

- Розмаїття різноманітного апаратного та програмного забезпечення;

- Відсутність спеціальних утиліт захисту, які можна було б використовувати в конкретній комп'ютерній мережі.

Загалом система комп'ютерної мережі складається з таких основних функціональних блоків:

- Робочі станції - окремі комп'ютери або мережеві термінали, на яких реалізується автоматизоване робоче середовище користувачів;

- Хост-сервери (файлові, баз даних, сервіси друку та ін.) - високопродуктивні комп'ютери, призначені для реалізації функцій зберігання даних, доступу до них та інших операцій;

- Мережеві пристрої, що забезпечують з'єднання декількох мереж передачі даних;

- Лінії передачі даних (локальні, широкосмугові тощо).

Моделювання процесів порушення інформаційної безпеки доцільно здійснювати за таким логічним ланцюжком: «загроза - джерело загрози - спосіб реалізації - вразливість - наслідки» (рис. 1.2).

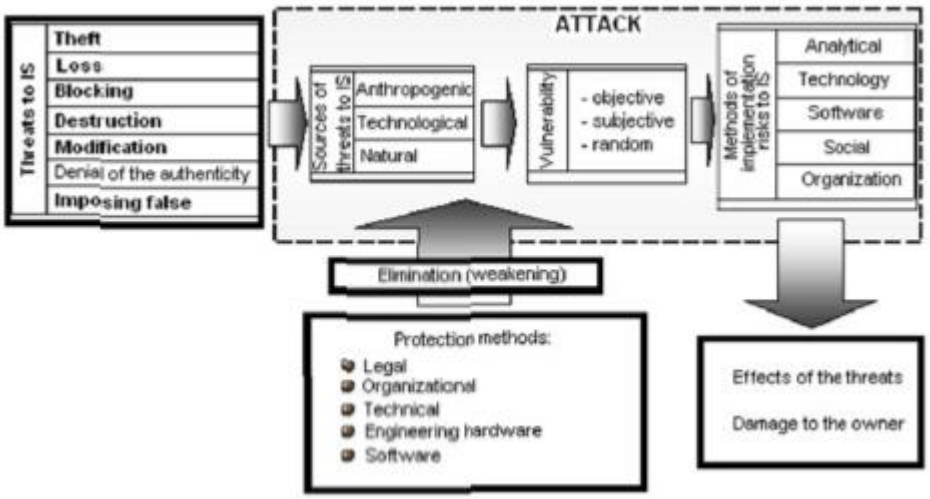


Рисунок 1.2 - Модель реалізації загроз інформаційної безпеки

Несанкціонований доступ до інформації в комп'ютерній мережі відбувається:

- непрямий - без фізичного доступу до вузлів мережі та
- прямий - з фізичним доступом до вузлів мережі.

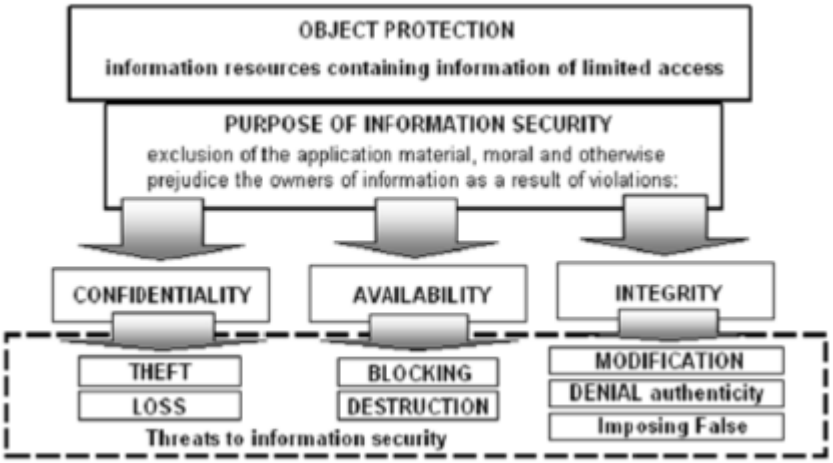


Рисунок 1.3 - Цілі та загрози безпеці інформації

Всі джерела загроз можна розділити на класи за типом носія, класи поділяються на групи за місцем розташування (рис. 1.4.).

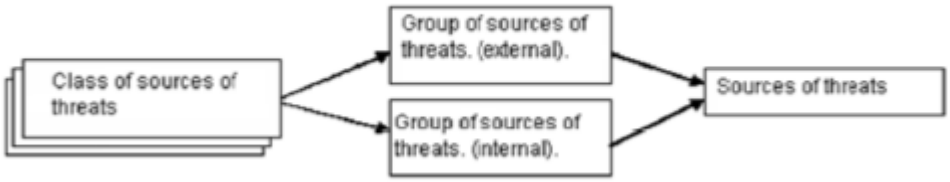


Рисунок 1.4 - Класифікаційна структура «Джерела загроз»

Класифікація можливостей реалізації загрози являє собою сукупність різних операцій джерела загроз за певними методами реалізації з використанням вразливостей, що призводять до реалізації атаки.

1.2 Основні джерела загроз безпеці комп'ютерних мереж

Основними джерелами загроз комп'ютерним мережам та інформації є

- Стихійні лиха та аварії (повінь, ураган, землетрус, пожежа тощо);

- Збої та відмови обладнання (технічних засобів);

- Помилки розробки компонентів комп'ютерних мереж (апаратних засобів, технології обробки інформації, програм, структур даних тощо);

- Помилки експлуатації (користувачів, операторів та іншого персоналу);

- Цілеспрямовані дії порушників (ображених осіб з числа персоналу, злочинців, шпигунів, диверсантів тощо).

Всі види потенційних загроз поділяються на два класи за природою їх виникнення: природні (об'єктивні) та штучні (суб'єктивні).

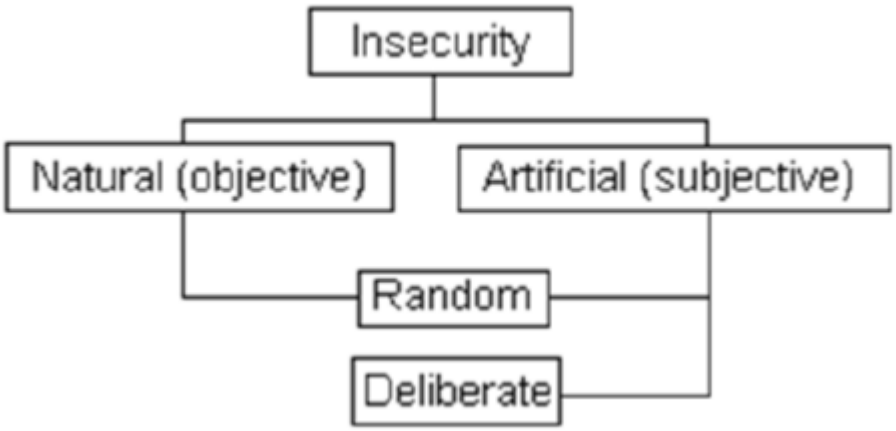


Рисунок 1.5 - Класифікація загроз за джерелами та мотивацією

Природні загрози - це загрози, викликані впливом на комп'ютерну мережу об'єктивних фізичних процесів або стихійних природних явищ чи катастроф, що не залежать від людини.

Штучні загрози, викликані діяльністю людини. Класифікація загроз за мотивацією. Серед них можна виокремити такі, що впливають на операційну діяльність:

- Ненавмисні, випадкові загрози, викликані помилками при проектуванні мережі, помилками в програмному забезпеченні, помилками персоналу тощо;

- Свідомі (навмисні) загрози - загрози, викликані корисливими, ідеологічними або іншими прагненнями людей (зловмисника).

По відношенню до комп'ютерної мережі джерела загроз можуть бути зовнішніми або внутрішніми (компоненти самих мереж - обладнання, програми, персонал, кінцеві користувачі).

Найбільш поширеними штучними загрозами комп'ютерних мереж є (операції, що здійснюються людьми випадково, через незнання, необережність або некомпетентність, але без злого умислу):

1) Ненавмисні операції, що призводять до часткового виходу системи з ладу або пошкодження апаратних, програмних, інформаційних ресурсів системи;

2) Небезпечне відключення обладнання або зміна режиму роботи пристроїв і програм;

3) Ненавмисне пошкодження джерела інформації;

4) Системне програмне забезпечення, яке здатне при некомпетентному використанні викликати збій системи або здійснити незворотні зміни в системі;

5) Нелегальне встановлення та використання неофіційних програм з подальшим необґрунтованим витрачанням ресурсів;

6) Зараження комп'ютера вірусами;

7) Необережні дії, що призводять до поширення та розголошення конфіденційної інформації;

8) Розголошення, передача або втрата інформації доступу (паролів, ключів шифрування, ідентифікаційних карток, цифрових сертифікатів тощо);

9) Розробка архітектури системи, розробка технології обробки даних, розробка додатків, з можливостями небезпеки для системи та безпеки інформації;

10) Незнання обмежень компанії (корпоративних правил);

11) Вхід в систему в обхід мостів захисту (завантаження сторонньої операційної системи зі змінних носіїв інформації тощо);

12) Некомпетентне використання, налаштування або відключення системи захисту співробітниками служби безпеки;

13) Передача даних на неправильну адресу (пристрою, клієнта тощо);

14) Неправильне введення;

15) Ненавмисне пошкодження каналів передачі даних.

На основі досліджень Гундара, основними можливими шляхами навмисної дезорганізації, виведення системи з ладу, проникнення в систему та несанкціонованого доступу до інформації є наступні:

1) Фізичне пошкодження (псування, знищення тощо) найважливіших компонентів комп'ютерної системи (пристроїв, носіїв важливої системної інформації тощо);

2) Відключення або виведення з ладу підсистем функціонування (джерел живлення та охолодження, ланцюгів зв'язку тощо);

3) Дезорганізація функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, створення потужних активних радіозавад на частотах роботи пристроїв тощо);

4) Впровадження агентів як співробітників (у тому числі керівної групи, яка відповідає за безпеку);

5) Вербування (шляхом підкупу, шантажу тощо) персоналу або окремих користувачів з певними повноваженнями;

6) Прослуховування, дистанційна фото- та відеозйомка тощо

7) Перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку, а також наведення активних випромінювань на допоміжні елементи, які не беруть безпосередньої участі в обробці інформації (телефонні лінії, електропостачання, опалення тощо);

8) Перехоплення інформації, що передається каналами зв'язку. Подальший аналіз з метою з'ясування протоколів обміну даними, правил авторизації в каналі для подальшого проникнення в систему;

9) Викрадення носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, накопичувачів і всього комп'ютера);

10) Несанкціоноване копіювання носіїв інформації;

11) Крадіжка промислового брухту (списки, записи, утилізовані документи і тощо);

12) Доступ до решти інформації з оперативної пам'яті та зовнішніх накопичувачів;

13) Зчитування інформації з оперативної пам'яті, що використовується операційною системою (в тому числі підсистемою безпеки) або іншими користувачами, в асинхронному режимі з використанням недоліків багатозадачних операційних систем та систем програмування;

14) Незаконне отримання паролів та іншої інформації доступу з подальшим маскуванням під зареєстрованого користувача;

15) Несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку тощо;

16) Розголошення алгоритму шифрування зашифрованої інформації або її кодів;

17) Розгортання "спеціального програмного забезпечення" та "вірусів" ("троянів" та "бекдорів"), що дозволяють гальмувати систему безпеки, нелегально та приховано надавати доступ до системних ресурсів з метою запису та передачі конфіденційної інформації;

18) Несанкціоноване підключення до ланцюгів зв'язку з метою роботи "між лініями". ", використання пауз в операціях реального користувача від його імені з подальшим введенням неправдивих звітів або модифікацією переданих повідомлень;

19) Несанкціоноване підключення до каналів зв'язку для прямої підміни реального користувача шляхом його фізичного відключення після входу в систему та успішної аутентифікації з введенням дезінформації та нав'язуванням неправдивих звітів.

Таблиця 1.1 - Класифікація різновидів порушення працездатності систем та несанкціонованого доступу до інформації за об'єктами впливу та способами нанесення шкоди безпеці

Ways of plotting of a damage	Objects of effects			
	The equipment	Programs	Data	Staff
Disclosure (leak) of the information	Plunder of media, connection to the communication circuit, unapproved usage of resources	Unapproved copying interception	Plunder, copying, interception	Transmission of data on protection, disclosure, negligence
Information integrity loss.	Connection, modification, activeX applications, change of operating modes, unapproved usage of resources	Implantation of Trojans and bugs	Distortion, modification	Staff recruitment, "masquerade"
Violation of working capacity of the automated system	Change of modes of functioning, output out of operation, plunder, corrupting	Distortion, removal, substitution	Distortion, removal, imposing of the false data	Maintenance, physical elimination
Illegal duplicating of the information	Manufacture of clones without licenses	Usage of illegal copies	The publication without the knowledge of authors	

Узагальнена класифікація віддалених атак:

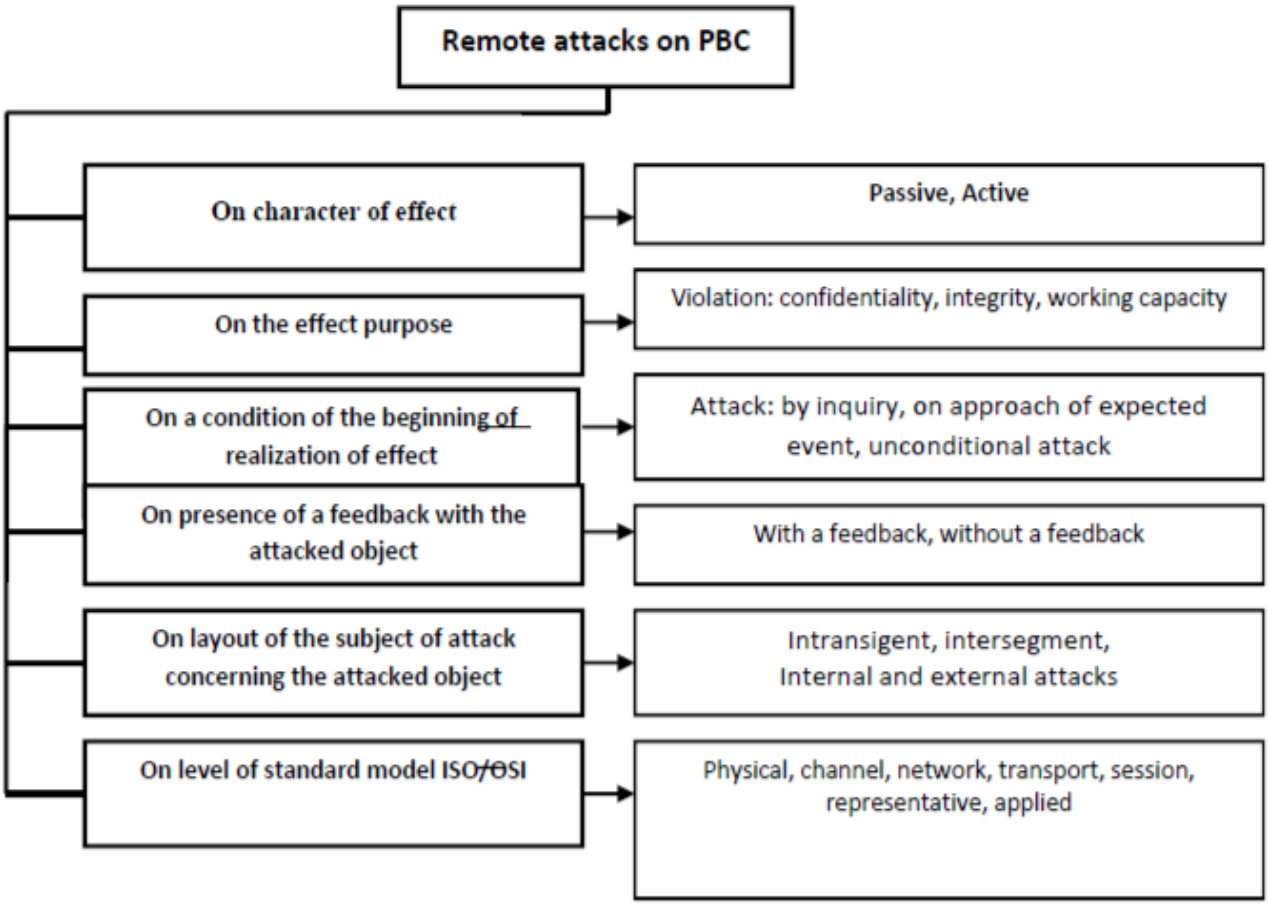


Рисунок 1.6 - Класифікація стандартних віддалених атак

1.3 Характеристика та механізми реалізації стандартних віддалених атак

Корпоративна мережа може бути ізольованою від зовнішнього світу (що є дуже умовним), а може мати зв'язок з Інтернетом. Типова конфігурація корпоративної мережі представлена на рис. 1.7.

Підключаючись до мереж загального користування, організації переслідують певні цілі і намагаються ефективно вирішити наступні завдання:

- Надання внутрішнім користувачам доступу до зовнішніх ресурсів. Це, в першу чергу, WWW - ресурси, FTP - архіви тощо;

- Надати доступ користувачам із зовнішньої мережі до деяких внутрішніх ресурсів (корпоративний WEB-сервер, FTP-сервер тощо);

- Забезпечити взаємодію з віддаленими філіями та офісами;

- Організувати легкий доступ до ресурсів внутрішньої мережі з будь-якого місця.

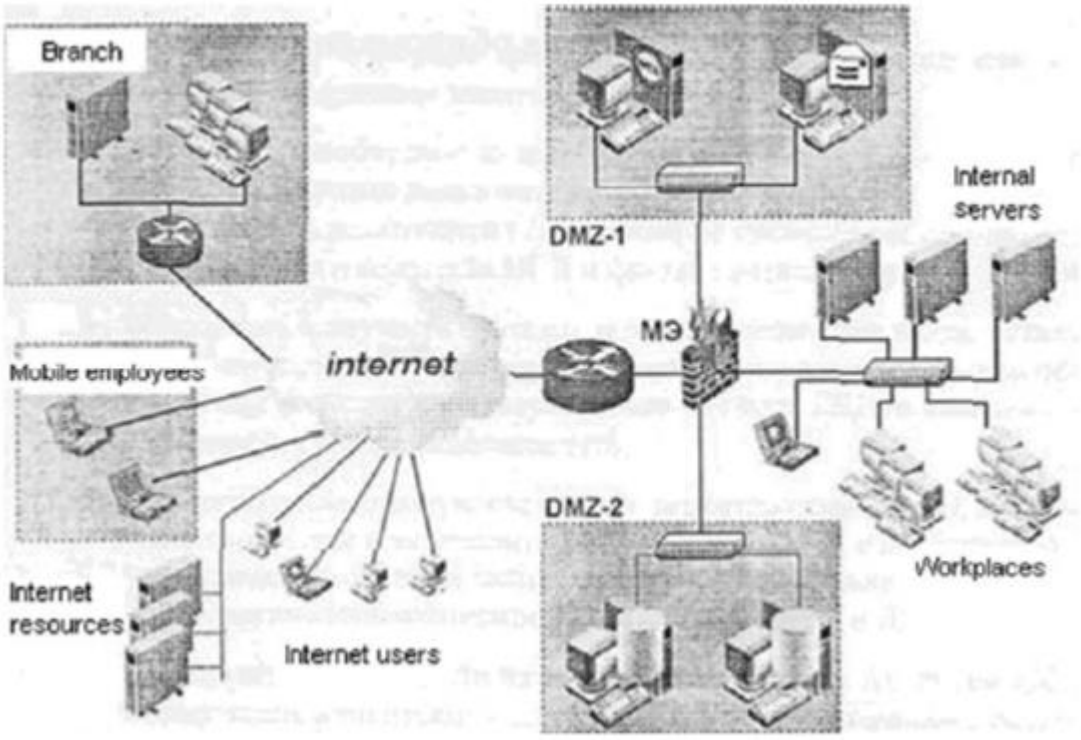


Рисунок 1.7 - Типова мережева конфігурація організації

Вирішуючи перелічені завдання, організація стикається з низкою проблем безпеки. Взаємодія з віддаленими філіями та мобільними користувачами через відкриті канали створює загрозу перехоплення переданої інформації. Виділення загального доступу до внутрішніх ресурсів створює загрозу зовнішніх вторгнень і перехоплення конфіденційної інформації.

Виділивши деякі рівні інформаційної інфраструктури, зручно розглянути питання безпеки корпоративних мереж:

- Рівень персоналу
- Рівень додатків
- Рівень СУБД
- Рівень операційної системи
- Мережевий рівень

До мережевого рівня відносяться мережеві протоколи (TCP IP, NetBEUI, IPX/SPX), кожен з яких має свої особливості, вразливості та пов'язані з ними можливі атаки.

Операційні системи (Windows, UNIX тощо), встановлені на вузлах корпоративної мережі, відносяться до рівня операційних систем (ОС).

Необхідно виділити також рівень систем управління базами даних (СУБД), оскільки вони є невід'ємною частиною будь-якої корпоративної мережі.

На четвертому рівні знаходяться всі можливі додатки, що використовуються в корпоративній мережі. Це може бути програмне забезпечення веб-серверів, різноманітні офісні додатки, браузери тощо.

І, нарешті, на верхньому рівні інформаційної інфраструктури знаходяться користувачі та обслуговуючий персонал автоматизованої системи.

Можна виділити деякі загальні етапи проведення атаки на корпоративну мережу:

- Збір даних

- Спроба отримати доступ до найменш захищеного вузла (можливо, з мінімальними привілеями)

- Спроба підвищення рівня привілеїв або використання вузла як платформи для дослідження інших вузлів мережі

- Отримання повного контролю над одним або декількома вузлами

Зловмисник переслідує певні цілі, здійснюючи ці атаки. У загальному вигляді це можуть бути:

- Порушення нормального функціонування об'єкта атаки (відмова в обслуговуванні, Dos)

- Отримання контролю над об'єктом атаки

- Отримання конфіденційної інформації

- Модифікація та фальсифікація даних

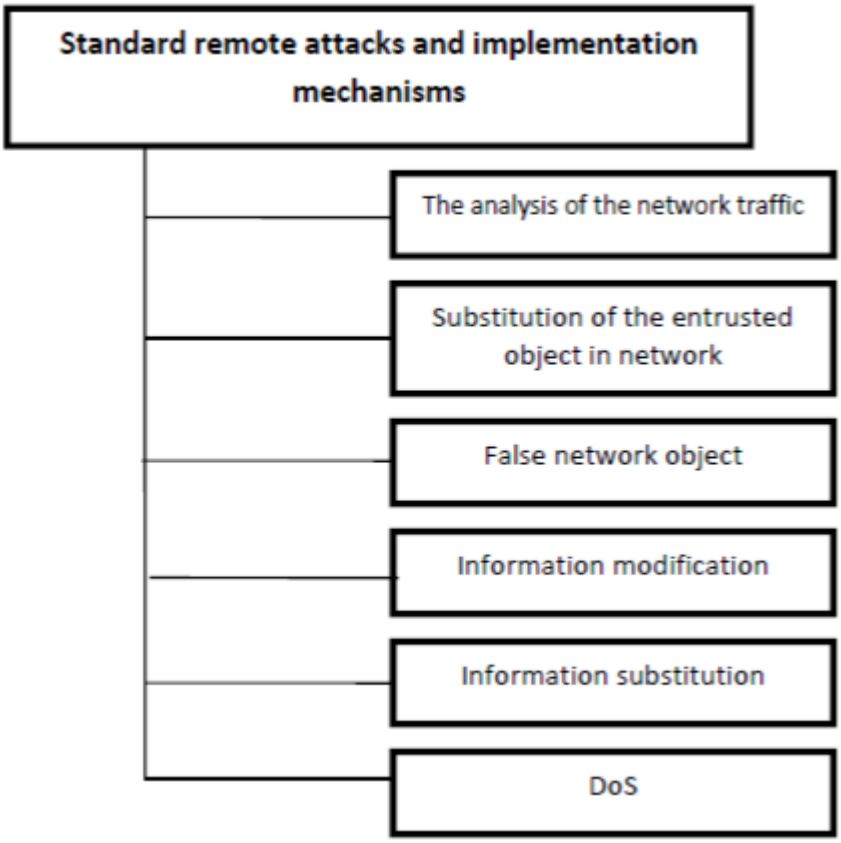


Рисунок 1.8 - Класифікація стандартних віддалених атак на розподілені мережеві системи

Наступний можливий варіант класифікації атак за місцем знаходження порушника:

- В одному сегменті з об'єктом атаки;

- У різних сегментах з об'єктом атаки.

Механізм реалізації атаки залежить від взаємного розташування атакуючого та жертви. Зазвичай реалізація міжсегментної атаки є більш складною.

Найбільш важливою для розуміння можливих атак є класифікація атак за механізмами їх реалізації:

- Пасивне прослуховування

Приклад: перехоплення мережевого трафіку

- Підозріла активність

Приклад: сканування портів (сервісів) об'єкта атаки, спроба підбору пароля (брутфорс).

- Марне витрачання обчислювального ресурсу.

Приклад: вичерпання ресурсів атакованого вузла або групи вузлів, що призводить до деградації (переповнення запитів на з'єднання тощо).

- Порушення навігації (створення хибних об'єктів і шляхів)

Приклад: Зміна шляху мережевих пакетів таким чином, щоб вони проходили через хости та маршрутизатори порушника, зміна відповідних карт умовних інтернет-імен та IP-адрес (DNS-атака) тощо.

- Виведення з ладу

Приклад: передача на атакований вузол пакетів певного типу, що призводить до відмови вузла або сервісів на ньому (WinNuke, програми для DoS-атак тощо)

- Запуск додатків на об'єкті атаки

Приклад: виконання шкідливої програми в оперативній пам'яті об'єкта атаки (трояни, передача управління шкідливій програмі шляхом переповнення буфера, виконання шкідливого коду на Java або ActiveX тощо).

Найбільш повна класифікація атак здійснюється за механізмами їх реалізації. Інші приклади використання деяких механізмів:

1) Сніфінг трафіку - перехоплення та аналіз мережевого трафіку, заснований на можливості переведення мережевого адаптера в неселективний режим роботи.

Призначення: Отримання конфіденційної та критичної інформації

Механізм реалізації: Пасивне обнюхування

Використовувана уразливість: Базується на загальному середовищі технології передачі даних (Ethernet)

- Недолік проектування, передача конфіденційної інформації без шифрування.

Рівень інформаційної інфраструктури: мережевий.

Рівень ризику: високий.

2) Сканування портів - підключення до вузла мережі та пошук у вибраному діапазоні портів для виявлення працюючих сервісів.

Мета: отримання конфіденційної та критичної інформації.

Використовувана вразливість: помилки в роботі сервісів, встановлені, але не використовувані сервіси.

Рівень інформаційної інфраструктури: мережевий.

Рівень ризику: низький.

3) ARP-атака - підміна - додавання фальшивих записів до таблиці, що використовується при роботі протоколу ARP.

Мета: порушення нормального функціонування об'єкта атаки.

Механізм реалізації: порушення навігації.

Використовувана вразливість: недолік проектування протоколу ARP

Рівень інформаційної інфраструктури: мережа.

Ступінь ризику: високий

IISDOS-атака - Відправлення некоректно сконструйованого HTTP-запиту призводить до перевитрати ресурсів WWW-сервера.

Мета: порушення нормального функціонування об'єкту атаки.

Механізм реалізації: марна витрата ресурсів сервера.

Використана уразливість: помилка реалізації Microsoft Internet Information Server.

Рівень інформаційної інфраструктури: Додатки.

Рівень ризику: Середній

1.4 Канали витоку інформації на фізичному рівні

Канал витоку інформації (КВІ) - це сукупність джерела інформації, матеріального носія або середовища розповсюдження сигналу, що несе цю інформацію, та засобів зняття інформації з сигналу або носія. Відома наступна КВІ (рис. 1.9):

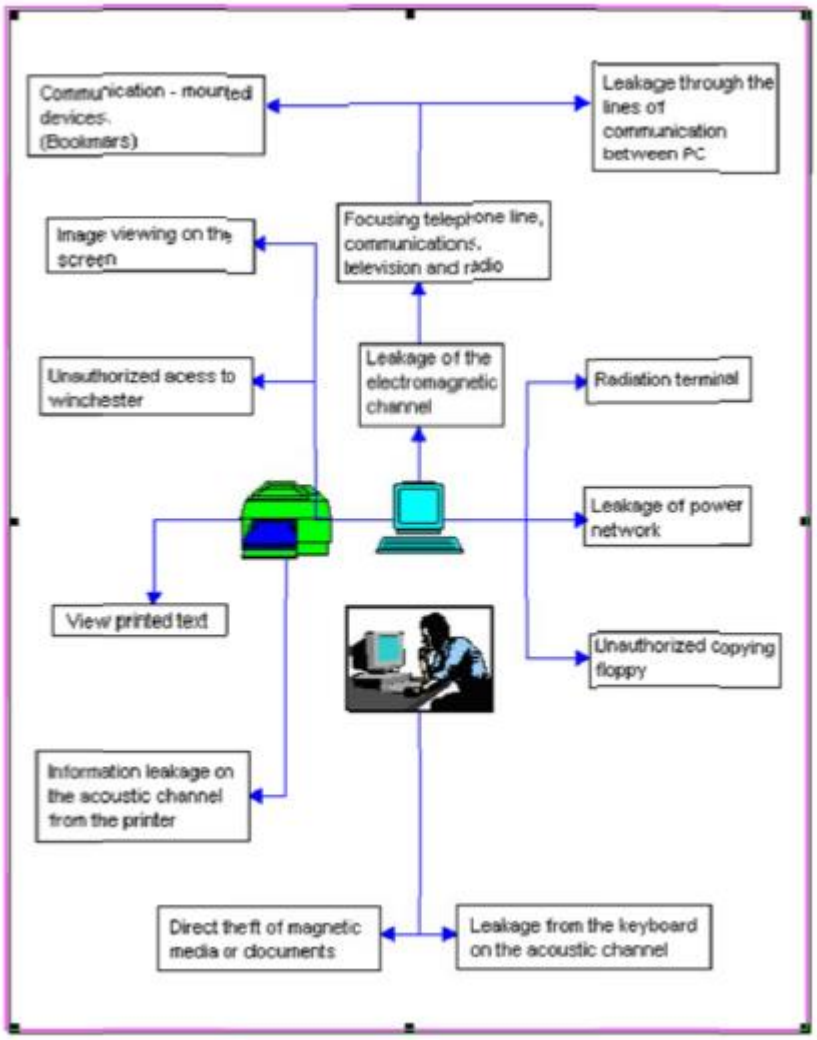


Рисунок 1.9 - Основні канали витоку інформації при обробці на комп'ютері

1. Електромагнітний канал. Причиною її виникнення є електромагнітне поле, пов'язане з електричним струмом в пристроях під час обробки інформації. Електромагнітне поле може індукувати струми в близько розташованих проводах. Електромагнітний канал може бути:

- Радіоканал (високочастотні випромінювання).
- Низькочастотний канал.
- Мережевий канал.
- Канал заземлення.
- Лінійний канал (ланцюг зв'язку між ПК).

2. Акустичний канал. Пов'язаний з поширенням звукових хвиль у повітрі або пружних коливань в інших середовищах, що виникають при роботі дисплеїв.

3. Канал несанкціонованого копіювання.

4. Канал несанкціонованого доступу.

1.5 Віруси та шкідливі програми

1.5.1 Поняття та види комп'ютерних вірусів

Комп'ютерні віруси - це програми або фрагменти програмного коду, які, потрапивши на комп'ютер жертви, можуть виконувати проти волі користувача різні операції на цьому комп'ютері - створювати або видаляти об'єкти, оновлювати файли даних або програмні файли, здійснювати операції у власному розповсюдженні через локальні мережі або в Інтернеті. Модифікація програмних файлів, файлів даних або завантажувальних секторів дисків таким чином, що вони самі стають носіями вірусного коду, називається зараженням і є основною функцією комп'ютерних вірусів.

Залежно від типів інфікованих об'єктів існують різні типи комп'ютерних вірусів:

- Поліморфні віруси
- Комп'ютерні віруси MtE (Mutation Engine віруси)
- Резидентний вірус пам'яті
- Скриптовий вірус
- Стелс-віруси
- Зашифровані віруси
- Антивірусний вірус, ретровірус
- Антивірусний вірус
- Вірус-черв'як
- Вірус-містифікатор (Hoax)
- Вірус-компаньйон
- Dropper
- Вірус-зоопарк

Залежно від типу заражених об'єктів, комп'ютерні віруси можна розділити на наступні типи:

- Файлові комп'ютерні віруси (File viruses),
- Завантажувальні комп'ютерні віруси (Boot віруси),
- Макрокомандні комп'ютерні віруси (макровіруси).

1.5.2 Класифікація комп'ютерних шкідливих програм

Антивірусні лабораторії класифікують комп'ютерні шкідливі програми за різними алгоритмами роботи:

- Зомбі - невеликі комп'ютерні програми, що розповсюджуються в Інтернеті вірусами-черв'яками. Програми-зомбі встановлюються в атаковану систему і чекають подальших команд для роботи.

- Перехоплювачі клавіатури (клавіатурні шпигуни) - різновид троянських програм, основною функцією яких є перехоплення даних, що вводяться користувачем за допомогою клавіатури. Цільові програми - персональні та мережеві паролі, дані для входу в систему, кредитні картки та інша особиста інформація.

- Логічні бомби - різновид троянських програм - приховані блоки, вбудовані в раніше розроблені і широко використовувані програми. Вони є ресурсами комп'ютерних диверсій. Такі програми нешкідливі до настання певної події, при якій вони запускаються (натискання користувачем певних клавіш на клавіатурі, зміни у файлі або настання певної дати чи часу).

- Бекдори - програми, що забезпечують вхід в систему або отримання ексклюзивних прав в обхід існуючої системи безпеки. Вони часто використовуються для обходу існуючої системи безпеки. Бекдори не заражають файли, а реєструються в реєстрі, оновлюючи ключі реєстру.

- Поштові бомби - одна з елементарних мережевих атак. Зловмисник розсилає на комп'ютер або поштовий сервер компанії одне величезне повідомлення або набір поштових повідомлень (десять тисяч), які виводять систему з ладу.

- Руткіт - шкідлива програма, призначена для перехоплення системних функцій операційної системи APl з метою приховування своєї присутності в системі. Крім того, руткіт може маскувати процеси інших програм, різні ключі реєстру, папки і файли. Руткіти поширюються як самостійні програми, так і у вигляді додаткових компонентів у складі інших шкідливих програм - бекдорів, поштових черв'яків та інших. За принципом дії руткіти умовно поділяються на дві групи: User Mode Rootkits (UMR) - руткіт, що працює в режимі користувача, і Kernel Mode Rootkit (KMR) - руткіт, що працює в режимі ядра. Робота UMR заснована на перехопленні функцій бібліотек користувацького режиму, а робота KMR - на встановленні в систему драйвера, який виконує перехоплення функцій на рівні ядра системи, що значно ускладнює його виявлення та знешкодження.

- Трояни (троянські коні) - шкідливі програми, що містять прихований модуль, який виконує несанкціоновані операції в комп'ютері. Ці дії завжди спрямовані на те, щоб завдати шкоди користувачеві. Троянські програми підміняють деякі часто запускаються програми, виконують їх функції або імітують таку роботу, одночасно виконуючи деякі шкідливі операції. Деякі троянські програми містять механізм оновлення компонентів з Інтернету.

- Аплети - додатки, невеликі Java-додатки, які вбудовуються в HTML-сторінку. Самі по собі ці програми не є шкідливими, але можуть бути використані в зловмисних цілях. Особливо аплети небезпечні для любителів он-лайн ігор, оскільки там використовуються аплети на мові Java. Аплікатори можуть використовуватися для відправки зібраної на комп'ютері інформації третім особам.

- Веб-баги - ресурс для відстеження користувачів мережі Інтернет. Зазвичай це прозорі графічні файли розміром 1x1 піксель, які використовуються для збору статистичної інформації про користувача під час його перебування на веб-сайті. Вони можуть збирати різну інформацію - дату і час, тип браузера, налаштування екрану, JavaScript налаштування, файли cookie, IP-адресу, тип операційної системи. Спамери використовують такі помилки, вкладаючи їх в електронні листи, які дають їм можливість визначити існування адреси.

- Перехоплювачі сторінок (викрадачі) - різновид небажаних комп'ютерних програм, мета яких встановити потрібну сторінку в якості стартової на комп'ютері, куди може потрапити троян. Програми використовують уразливості в безпеці інтернет-браузерів і реєструються в реєстрі. Зазвичай ручне очищення реєстру не допомагає, такі трояни мають функцію відновлення необхідних даних в реєстрі і маскуються під системні файли.

- Файли cookie - файли, які складаються з даних про користувача, зібраних веб-серверами і зберігаються на жорсткому диску комп'ютера. Під час відвідування будь-якого веб-сервера спеціальні файли cookie зберігають інформацію про відвідувача, яка використовується для ідентифікації користувача сервером. Дані, отримані від файлів cookie, використовуються спамерами для складання списків розсилок.

- Шпигуни - не віруси, зазвичай використовуються хакерами для відстеження працездатності мережі.

- Шпигунські програми - небезпечні для користувача програми (не віруси), призначені для стеження за системою і відправки зібраної інформації третій стороні - творцю або замовнику цієї програми. Наявність шпигунського програмного забезпечення на комп'ютері призводить до нестабільної роботи браузера та уповільнення роботи системи.

2 МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Модель загроз корпоративної комп'ютерної мережі

Виходячи з проведеного аналізу, всі джерела загроз безпеці інформації, що з'являються в корпоративній мережі, можна розділити на три основні групи:

1. Загрози, викликані діяльністю суб'єкта.

2. Загрози, викликані апаратними засобами (техногенні загрози).

3. Загрози, викликані спонтанними джерелами (стихійні лиха)

Дії зловмисників, що можуть призвести до порушення безпеки інформації, можуть бути зовнішніми:

1. Кримінальні структури;

2. Рецидивісти та потенційні злочинці;

3. Недобросовісні партнери;

4. Конкуренти;

5. Політичні опоненти;

А також внутрішні:

1. Співробітники компанії;

2. Співробітники філій;

3. Агенти конкурентів.

За результатами міжнародного досвіду, дії зловмисників можуть призвести до низки небажаних наслідків, серед яких стосовно корпоративної мережі можна виокремити наступні:

1. Крадіжка

- Апаратне забезпечення (жорсткі диски, ноутбуки, системні блоки);

- Носії інформації (паперові, магнітні, оптичні тощо);

- Інформація (читання та несанкціоноване копіювання);

- Інформації про доступ (ключі, паролі тощо);

2. Заміна (модифікація)

- Операційні системи;

- Системи управління базами даних;
- Програми;
- Інформація (дані);
- Паролі та правила доступу;

3. Знищення (пошкодження)
- Апаратні засоби (жорсткі диски, ноутбуки, системні блоки);
- Носії інформації (паперові, магнітні, оптичні тощо);
- Програмне забезпечення (ОС, СУБД, операційне програмне забезпечення)
- Інформація (файли, дані)
- Паролі та ключова інформація.

4. Порушення стабільної роботи (переривання)
- Швидкість обробки інформації;
- Пропускна здатність каналів передачі даних;
- Розміри вільної оперативної пам'яті;
- Розміри вільного дискового простору;
- Блоки живлення апаратних засобів;

5. Помилки
- При встановленні програмного забезпечення, ОС, СУБД;
- При розробці програмного забезпечення;
- При обслуговуванні обладнання;

6. Перехоплення інформації (несанкціоноване)
- За допомогою специфічного обладнання;
- За рахунок наведень від ліній електропередач;
- За рахунок наведень від сторонніх провідників;
- Акустичним каналом з вихідних носіїв;
- Аудіоканалом при обговоренні питань;
- Підключенням до каналів передачі інформації;
- порушення правил доступу (хакерство);

До другої групи належать загрози менш прогнозовані, які безпосередньо залежать від технічних властивостей і, відповідно, потребують особливої уваги.

Технічні засоби, що містять потенційні загрози безпеці інформації, можуть бути як внутрішніми, так і зовнішніми:

1. Неякісними апаратними засобами обробки інформації;

2. Неякісне програмне забезпечення обробки інформації;

3. Допоміжні засоби (системи охорони, сигналізації);

4. Інші засоби, що застосовуються в офісах;

І зовнішні:

1. Засоби зв'язку;

2. Закрити виділені небезпечні виробництва;

3. Сервісні лінії (енерго- та водопостачання, водовідведення);

4. Транспорт.

Наслідками застосування таких засобів, що безпосередньо впливають на безпеку інформації, можуть бути

1. Порушення стабільності роботи

- Порушення працездатності систем обробки даних;

- Порушення працездатності телекомунікацій;

- Старіння медіа-ресурсів;

- Порушення існуючих правил доступу;

2. Знищення (пошкодження)

- Програмне забезпечення, ОС, СУБД;

- Ресурсів обробки інформації (відключення електроенергії, витоки);

- Приміщення

- Інформації (розмагнічування, випромінювання, витоки тощо);

- Персоналу

3. Модифікація

- Програмне забезпечення, ОС, СУБД;

- Інформація, що передається каналами передачі даних та лініями зв'язку.

Третю групу складають загрози, які неможливо передбачити, а отже, завжди слід здійснювати моніторинг їх потенційної активності.

До непередбачуваних загроз зазвичай відносять стихійні лиха, такі як:

1. Пожежі;

2. Землетруси;

3. Повені;

4. Урагани;

5. Різні непередбачувані обставини;

6. Незрозумілі явища.

Зазначені стихійні лиха та незрозумілі явища як вплив на інформаційну безпеку є небезпечними для всіх підрозділів корпоративної мережі і можуть призвести до знищення та втрати важливої інформації, обладнання, співробітників тощо.

2.2 Основні механізми захисту комп'ютерних систем

Для захисту комп'ютерних систем від несанкціонованого втручання в процеси їх функціонування та інформації використовуються такі основні методи захисту:

- Ідентифікація (називання та ідентифікація), аутентифікація (підтвердження автентичності) користувачів системи;

- Розмежування доступу користувачів до ресурсів системи та авторизація (призначення прав) користувачів;

- Реєстрація та повідомлення про події, що відбуваються в системі;

- Криптографія даних, що зберігаються і передаються по каналах зв'язку;

- Контроль цілісності та автентичності даних;

- Виявлення та знешкодження дій комп'ютерних вірусів;

- Перезапис решти інформації на носії даних;

- Виявлення вразливостей (слабких місць) систем;

- Ізоляція комп'ютерних мереж (фільтрація трафіку, приховування внутрішньої структури та адресації тощо);

- Виявлення атак та оперативне реагування;

- Резервне копіювання;

- Маскування.

Перераховані механізми захисту можуть застосовуватися в конкретних засобах і системах захисту в різних комбінаціях і варіаціях. Найбільший ефект досягається при їх постійному використанні з іншими видами захисту. Розглянемо перераховані механізми захисту більш детально.

2.2.1 Ідентифікація та аутентифікація користувачів

З можливістю розмежування доступу до ресурсів комп'ютерної мережі та можливістю реєстрації кожного доступу (співробітника, користувача, процесу) і ресурсу автоматизованої системи, що захищається, повинна бути забезпечена ідентифікація. Для цього в системі повинні зберігатися спеціальні мітки кожного суб'єкта та об'єкта, за якими вони можуть бути ідентифіковані.

Ідентифікація - це, з одного боку, присвоєння суб'єктам і об'єктам системи індивідуальних імен, номерів або спеціальних пристроїв (ідентифікаторів), а з іншого - їх ототожнення за присвоєними їм унікальними ідентифікаторами. Наявність ідентифікатора дозволяє спростити процедуру виділення конкретного суб'єкта з множини однотипних суб'єктів. В якості ідентифікаторів найчастіше застосовуються числа або символи у вигляді набору символів.

Аутентифікація - це підтвердження достовірності ідентифікації суб'єкта або об'єкта системи. Мета автентифікації суб'єкта - переконатися, що суб'єкт є саме тим, за ким його ідентифікували. Мета автентифікації об'єкта - переконатися, що це саме той об'єкт, який потрібен.

Зазвичай здійснюється аутентифікація користувачів:

- Шляхом перевірки знання ними паролів (спеціальних конфіденційних рядків символів);

- Шляхом перевірки наявності у них будь-яких спеціальних пристроїв (карток, ключів тощо) з унікальними мітками;

- Перевіряючи унікальні фізичні характеристики та параметри (наприклад, відбитки пальців, тощо) користувачів за допомогою спеціальних біометричних пристроїв.

Введення ідентифікатора і пароля користувачем обробляється частіше за все з клавіатури. Однак багато сучасних систем захисту використовують також інші типи ідентифікаторів - магнітні картки, радіочастотні картки, смарт-картки.

Біометричні методи характеризуються високим рівнем надійності ідентифікації користувача. Існує також можливість помилок розпізнавання (пропуск або помилкова тривога), а також вища вартість самих систем.

Ідентифікація та аутентифікація користувачів повинна здійснюватися при кожному їх вході в систему та при відновленні роботи після короткочасної перерви, після періоду неактивності.

2.2.2 Розмежування доступу зареєстрованих користувачів до ресурсів комп'ютерної мережі

Розмежування доступу до ресурсів комп'ютерної мережі - це такий порядок використання ресурсів автоматизованої системи, при якому суб'єкти отримують доступ до об'єктів системи в суворій відповідності до встановлених прав. Права розмежування доступу - це сукупність правил, що регламентують права доступу суб'єктів до об'єктів у системі.

Авторизація користувачів здійснюється з використанням наступних механізмів реалізації розмежування доступу:

- Механізми вибіркового управління доступом, засновані на використанні таблиць атрибутів, списків прав доступу тощо;

- Механізми управління проксі-доступом, засновані на використанні міток конфіденційності ресурсів і рівнів толерантності користувачів;

- Механізми підтримки закритого середовища ввіреного програмного забезпечення (індивідуальні списки для кожного користувача дозволених до

використання програм), підкріплені механізмами ідентифікації та аутентифікації користувачів при їх вході в систему.

Апаратні засоби розмежування доступу до ресурсів комп'ютерної мережі слід розглядати як складову єдиної системи моніторингу доступу користувачів:

- На контрольованій території;

- В окремих будівлях та філіях організації;

- До мережевих блоків та блоків системи захисту інформації (фізичний доступ);

- До інформаційних та мережевих програмних ресурсів.

Механізми управління доступом користувачів до об'єктів доступу виконують домінуючу роль у підтримці внутрішньої безпеки комп'ютерних систем. В основі їх роботи лежить концепція єдиного диспетчера доступу. Суть цієї концепції полягає в тому, що менеджер доступу виступає посередником-контролером при всіх зверненнях суб'єктів до об'єктів.

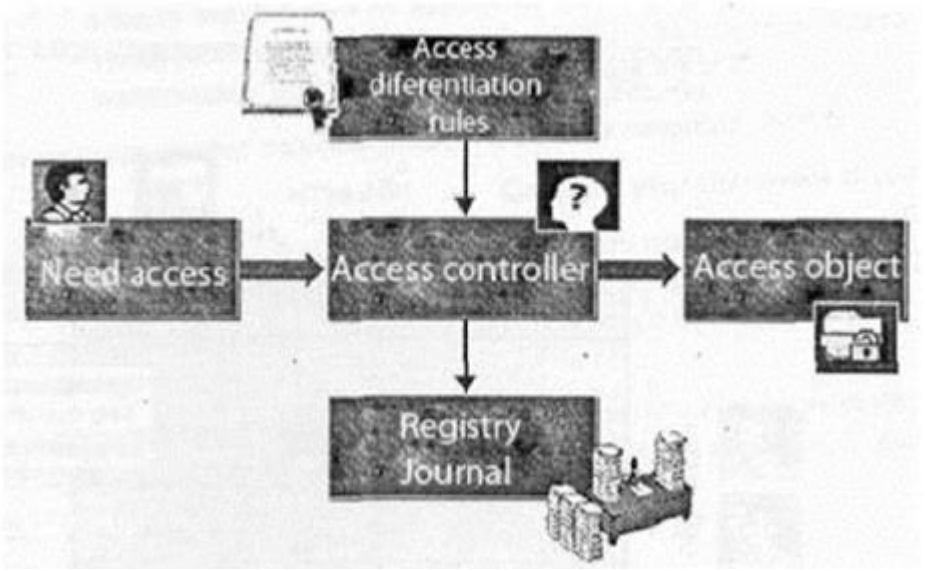


Рисунок 2.1 - Схема роботи механізму розмежування доступу

Основні функції менеджера доступу:

- Перевіряє права доступу кожного суб'єкта до конкретного об'єкта на основі інформації, що міститься в базі даних системи захисту;

- Дозволяє або забороняє (блокує) доступ суб'єкта до об'єкта;

- При необхідності реєструє факт доступу та його параметри в системному журналі (в тому числі спроби несанкціонованого доступу з перевищенням прав).

Основними вимогами до реалізації диспетчера доступу є

- Повнота контрольованих операцій (перевірці підлягають всі операції всіх суб'єктів над усіма об'єктами системи - обхід менеджера передбачається неможливим);

- Можливість формальної перевірки функціонування;

- Мінімізація ресурсів, що використовуються менеджером.

У загальному вигляді операція розмежування доступу суб'єктів до об'єктів базується на перевірці даних, які зберігаються в базі даних безпеки. Під базою даних безпеки розуміється база даних, що зберігає інформацію про права доступу суб'єктів до об'єктів. Для модифікації бази даних розмежування доступу необхідно передбачити ресурси для ексклюзивних користувачів (менеджерів безпеки, власників тощо) на ведення цієї бази. Такий контроль доступу повинен забезпечувати можливість виконання наступних операцій:

- Додавання і видалення об'єктів і суб'єктів;

- Перегляд та зміна відповідних прав доступу суб'єктів до об'єктів.

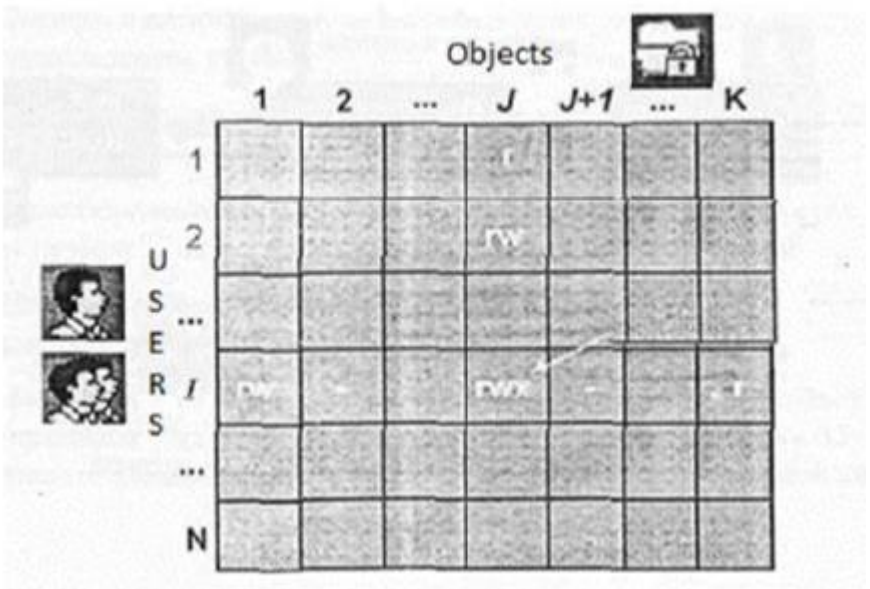


Рисунок 2.2 - Матриця вибіркового розмежування доступу

В основу розмежування доступу до ресурсів бази даних, як правило, покладено абстрактну матрицю доступу або її реальні представлення. Кожен рядок цих матриць відповідає суб'єкту, а стовпець - об'єкту мережевої системи. Кожна одиниця цієї матриці являє собою впорядковану сукупність значень, що визначають права доступу (для всіх можливих режимів доступу - читання, модифікація, видалення тощо) певного суб'єкта до певного об'єкта.

2.2.3 Реєстрація та негайне сповіщення про події безпеки

Методи реєстрації призначені для отримання та накопичення (з метою подальшого аналізу) до стану інформації про ресурси системи та про дії суб'єктів, визнаних адміністрацією системи потенційно небезпечними для системи. Аналіз зібраної ресурсами реєстрації інформації дозволяє виявити факти порушень, наслідки для системи та визначити, наскільки далеко зайшло порушення, підказати метод його розслідування та пошуку порушника і шляхи виправлення ситуації. Крім того, реєстраційні ресурси дозволяють отримувати вичерпну статистику про використання цих ресурсів, трафік мережі, використання інструментів, спроби несанкціонованого доступу тощо. Крім запису даних про конкретні події в спеціальні журнали для подальшого аналізу, ресурс реєстрації подій може забезпечувати і оперативне сповіщення менеджерів безпеки про стан ресурсів, спроби несанкціонованого доступу та інші порушення.

При реєстрації подій безпеки в системному журналі зазвичай збирається наступна інформація:

- Дата і час;

- Ідентифікатор суб'єкта (користувача або програми), що виконує цю операцію;

- Самостійна робота.

Механізми реєстрації дуже тісно пов'язані з іншими захисними механізмами. Сигнали про події, що відбуваються, і детальну інформацію про них механізми

реєстрації отримують від механізмів контролю (підсистем розмежування доступу, контролю цілісності ресурсів та інших).

У найбільш розвинених системах захисту підсистема сповіщення пов'язана з механізмами оперативного автоматичного реагування на певні події.

Основні способи реагування на виявлені факти несанкціонованого доступу:

- Тривожний сигнал;
- Повідомлення менеджера з безпеки;
- Повідомлення власнику інформації в цій системі;
- Вилучення програмного забезпечення (процесів) з подальшого виконання;
- Відключення (блокування) терміналу або комп'ютера, з якого здійснюється спроба несанкціонованого доступу до інформації;
- Виключення порушника зі списку зареєстрованих користувачів тощо.

2.2.4 Криптографічні методи захисту інформації

Криптографічні методи захисту ґрунтуються на можливості здійснення деякої операції перетворення інформації, яка може бути виконана одним або декількома користувачами системи, що володіють деяким секретним ключем, без якого неможливо здійснити цю операцію.

У класичному методі криптографії одиницею секретної інформації є ключ, знання якого дозволяє відправнику зашифрувати інформацію, а одержувачу - розшифрувати її. Ці операції шифрування з високою ймовірністю є нездійсненними без знання секретного ключа. Оскільки обидві сторони, що володіють ключем, можуть як зашифрувати, так і розшифрувати інформацію, такі алгоритми перетворення називають симетричними або алгоритмами з секретним ключем. У криптографії з відкритим ключем доступні два ключі, принаймні один з яких неможливо обчислити з іншого. Один ключ використовується відправником для шифрування інформації, яку необхідно надати. Інший ключ використовується одержувачем для розшифрування отриманої інформації. Існують додатки, в яких один ключ повинен бути відкритим, а інший - конфіденційним. Алгоритми

перетворення з відкритим і секретним ключами називають асиметричними, оскільки ролі сторін, що володіють різними ключами з пари, різні.

Методи криптографії загалом стосуються:

- Шифрування (дешифрування) інформації;

- Створення та перевірка цифрового підпису електронних документів.

Застосування методів і засобів криптографії дозволяє забезпечити вирішення наступних завдань із захисту інформації:

- Запобігання можливості несанкціонованого ознайомлення з інформацією при її зберіганні в комп'ютері або на відчужених носіях, а також при передачі по каналах зв'язку;

- Підтвердження автентичності електронного документа, доказ авторства документа і факту його отримання від відповідного джерела інформації;

- Підтримка гарантій цілісності - виключення можливості несанкціонованої зміни інформації;

- Посилення автентифікації користувачів системи - власників закритих ключів.

Основною перевагою криптографічних методів захисту інформації є те, що вони забезпечують високу гарантовану захищеність, яка може бути обчислена і виражена в числовому вигляді (середня кількість операцій або необхідний час для розкриття зашифрованої інформації або ключів).

Основні недоліки методів криптографії:

- Великі витрати ресурсів (часу, продуктивності) на виконання криптографічних перетворень інформації;

Труднощі з розповсюдженням зашифрованої інформації;

- Високі вимоги до безпеки закритих ключів та захисту відкритих ключів від підміни;

2.2.5 Контроль цілісності та автентичності даних, що передаються каналами зв'язку

Електронний цифровий підпис - це послідовність символів, отримана в результаті перетворення в апаратних засобах певного інформаційного вмісту за математичною алгоритм з використанням ключів, що мають незмінний зв'язок з кожним символом даного інформаційного вмісту.

Застосування електронного цифрового підпису дозволяє

- Забезпечення автентичності інформації;

- Забезпечити контроль цілісності (в т.ч. дійсності) інформації;

- Вирішення питання про юридичний статус документів, отриманих з автоматизованої системи.

- Методи контролю цілісності системних ресурсів призначені для своєчасного виявлення модифікації системних ресурсів.

- Дозволяє забезпечити стабільне функціонування системи захисту та цілісність оброблюваної інформації.

Повинен бути забезпечений контроль цілісності програмного забезпечення, оброблюваної інформації та засобів захисту, для підтримки інваріантності програмного середовища, визначеного передбаченою технологією обробки, і захист від несанкціонованого коригування інформації:

- Ресурси розмежування доступу, що забороняють модифікацію або видалення захищеного ресурсу

- Ресурси зіставлення критичних ресурсів з їх стандартними копіями (та відновлення у разі порушення цілісності);

- Ресурси підрахунку контрольної суми (підписів тощо);

- Ресурси електронного цифрового підпису.

Міжмережеві екрани, встановлені в точках з'єднання з мережею Інтернет - забезпечують захист зовнішнього периметру мережі фірми та захист власних Інтернет - серверів, відкритих для загального користування, від несанкціонованого доступу. Основними методами захисту є:

- Трансляція адрес для приховування структури та адресації внутрішньої мережі;

- Фільтрація трафіку;

- Обробка списків доступу на маршрутизаторах;

- Додаткова ідентифікація та аутентифікація користувачів стандартних послуг;

- Аудит вмісту інформаційних пакетів, виявлення та знешкодження комп'ютерних вірусів;

- Віртуальні приватні мережі (для захисту потоків даних, що передаються у відкритих мережах - підтримки конфіденційності, - застосовуються методи криптографії, розглянуті вище);

- Протидія атакам на внутрішні ресурси.

2.3 Робота з методами захисту

Конкуренція в галузі розробки систем захисту комп'ютерних систем неминуче призводить до уніфікації переліку загальних вимог до таких ресурсів. Один з пунктів такого уніфікованого переліку практично завжди може містити вимогу контролю за всіма наявними захисними механізмами. На жаль, розробники систем безпеки приділяють основну увагу реалізації захисних механізмів, а не засобам управління ними. Незнання, нерозуміння або недооцінка більшістю проектувальників і розробників психологічних і технічних перешкод, що виникають при впровадженні розроблених систем захисту. Успішно подолати ці перешкоди можна, лише забезпечивши необхідну гнучкість поводження з цими системами захисту.

Недостатня увага до проблем і побажань замовників, до підтримки зручності експлуатації системи безпеки часто є причиною відмови від використання конкретних систем захисту.

У наш час в більшості випадків установка засобів захисту проводиться на вже функціонуючі комп'ютерні системи. Захищена комп'ютерна система використовується для вирішення важливих прикладних завдань, в безперервному робочому циклі, більшість власників і користувачів вкрай негативно ставляться до будь-яких, навіть короткочасних, перерв в її функціонуванні для установки і налаштування засобів захисту або часткової втрати працездатності системи, викликаної некоректною роботою засобів захисту.

Впровадження систем захисту ускладнюється тим, що правильно налаштувати систему безпеки з першого разу неможливо. Зазвичай це пов'язано з відсутністю у замовника повного детального переліку всіх засобів захисту апаратні, програмні та інформаційні ресурси системи, а також готовий перелік прав доступу кожного користувача до ресурсів системи.

Таким чином, етап імплантації засобів захисту для деяких включає в себе операції з первинного виявлення та відповідної зміни налаштувань засобів захисту. Ці операції повинні проходити для власників і користувачів системи з якомога меншим клопотом.

Очевидно, що одні й ті ж операції адміністратор безпеки повинен часто повторювати і на етапі експлуатації системи, щоразу при зміні структури апаратного забезпечення, програмного забезпечення, персоналу, користувачів тощо. Такі зміни відбуваються досить часто, тому засоби керування системою захисту повинні забезпечувати зручність реалізації необхідних при цьому змін налаштувань системи захисту. Якщо система захисту не враховує цю діалектику, вона не володіє достатньою гнучкістю і не забезпечує зручність перенастроювання - така система дуже швидко стає не помічником, а лише клопотом для всіх, в тому числі і для адміністраторів.

Ті рішення, які зрозумілі для одного окремого комп'ютера або невеликої мережі з 10-15 робочих станцій, зовсім не підходять для обслуговуючого персоналу (включаючи адміністраторів) великих мереж з сотнями робочих станцій.

Для вирішення проблем управління засобами захисту в системі великих мереж необхідно передбачити наступні можливості:

- Повинні підтримуватися можливості керування механізмами захисту як в режимі on-line (віддалено, з робочої станції), так і локально (безпосередньо з конкретної робочої станції). Причому будь-які зміни налаштувань захисних механізмів, внесені в режимі on-line, повинні автоматично поширюватися на всі робочі станції, яких вони стосуються (незалежно від стану робочої станції в момент модифікації центральної бази даних). Аналогічно, частина змін, зроблених локально, повинна автоматично відображатися в центральній базі даних захисту, а при необхідності також розсилатися на всі інші сервери, яких вони стосуються. Наприклад, при зміні пароля користувачем на одній з робочих станцій, нове значення пароля цього користувача повинно бути відображено в центральній базу даних захисту мережі, а також розсилається на всі робочі станції, на яких збирається працювати користувач;

- Робота з механізмами захисту конкретного сервера повинна здійснюватися незалежно від його активності. Після включення неактивного сервера всі зміни налаштувань, що стосуються його механізмів захисту, повинні автоматично переноситися на нього.

- У великих системах модернізація засобів захисту вимагає від обслуговуючого персоналу великих трудовитрат і пов'язана з необхідністю обходу всіх робочих станцій для отримання до них локального доступу. Проведення таких замін може бути викликано як необхідністю усунення виявлених помилок інсталяції, так і необхідністю вдосконалення і розвитку системи (встановлення нових, більш досконалих версій програмного забезпечення);

- Для великих комп'ютерних мереж особливого значення набуває оперативний контроль за станом робочих станцій і роботою користувачів в мережі.

Тому система захисту повинна включати в себе підсистему оперативного контролю стану робочих станцій мережі та стеження в структурі за роботою користувачів.

3 РОЗВИТОК СКЛАДНОСТІ РЕСУРСІВ, ЩО ЗАБЕЗПЕЧУЮТЬ БЕЗПЕКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Опис локальної обчислювальної мережі підприємства "Інтепс"

Розглянемо локальну обчислювальну мережу компанії "Інтепс". Дана компанія спеціалізується на розробці та виробництві сучасних джерел безперебійного живлення. Компанія має декілька виробничих приміщень. В компанії працює близько 40 інженерів та програмістів. Основними завданнями компанії є розробка і тестування нових моделей джерел безперебійного живлення, а також створення програмного забезпечення для цих джерел.

При розробці локальної мережі для цієї компанії необхідно було врахувати деякі особливості використання комп'ютерного обладнання. Справа в тому, що на в центрі розробники нової техніки та програмісти користуються комп'ютерами.

Якщо програмісти зайняті роботою на ПК постійно і мають відповідно обладнані місця, то інженери використовують комп'ютери час від часу, в першу чергу для аналізу розрахунків, робочих креслень, операцій з тестування розроблених виробів. Загалом у філії задіяно п'ять стаціонарних комп'ютерів і 22 портативних.

Пересилання один одному робочих креслень, ескізів і розрахункових файлів, виконаних в таких програмах, як AutoCAD, SolidWork і MathCAD, а також перегляд електронної пошти і матеріалів в Інтернеті було основним способом обміну даними всередині компанії. Обсяг матеріалів, що передаються, фактично виявився незначним, а інтенсивність використання не зростає, тому високі вимоги до мережі не пред'являлися. Мережа була розроблена з використанням обладнання HomePlug AV, що має забезпечити реальну швидкість передачі даних у локальній мережі до 85 Мбіт/сек. При створенні мережі був використаний інженерний галоп компанії "Інтепс":

1. Будівля підключена до промислових ліній електропередач.

2. У будівлі фактично виділено дві паралельні лінії електроживлення - користувацька (розетки 220 В) і лінія, що забезпечує живлення освітлювальних приладів. Другий контур проходить під стелею будівлі.

3. Проводка в будівлі виконана прихованим способом в стінах, використовувався алюмінієвий дріт.

Схему електропостачання будівлі інженерного центру представлено на рисунку 3.1 у зменшеному вигляді. Використовуються наступні позначення:

- Desktop

- The computer (as we see, not on all desktops there is a necessity of usage of computers)

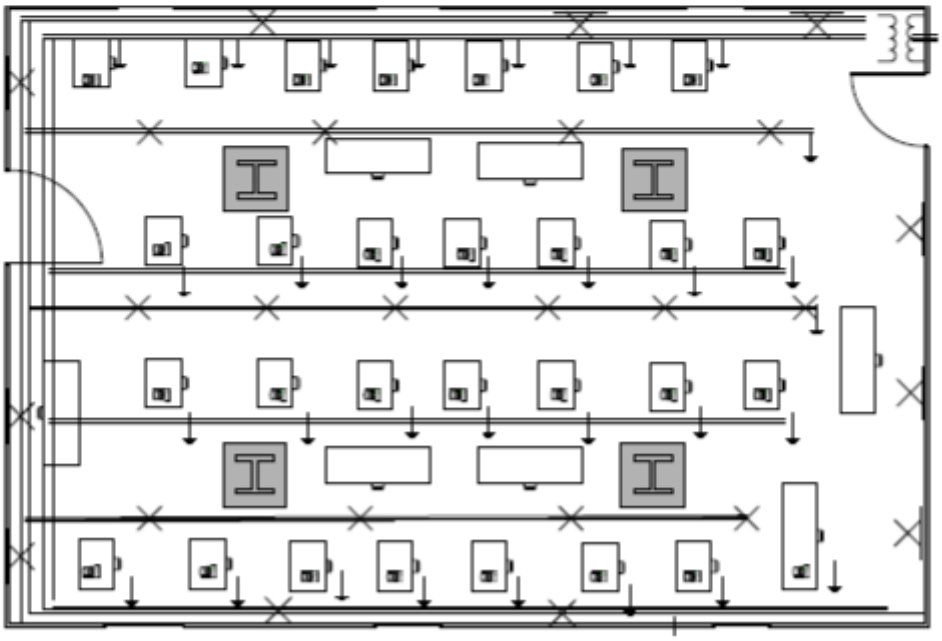
- The entry transformer

- The wall lights

- The ceiling lights

- Grounding

- Two-phase electrical line, 220 V



-

Рисунок 3.1 - План електропостачання будівлі інженерного центру

В даному випадку для реалізації мережі PLC в будівлі були використані наступні основні підходи:

1. Мережа PLC використовує в якості несучого середовища тільки нижній контур джерел живлення

2. Технологія мережі - шина з використанням виділеного сервера, що забезпечує доступ до мережі Інтернет, виконує функції поштового сервера та файлового сервера. На цьому ж комп'ютері було встановлено допоміжне програмне забезпечення для підтримки інформаційної безпеки локальної мережі.

3. Живлення пристроїв на робочих станціях здійснюється від мережі нижнього контуру з обов'язковим використанням діодних фільтрів при підключенні до електричної мережі кожної робочої станції. Фільтр і PCL-адаптер на робочих місцях підключаються окремо, що забезпечує захист несучої мережі від перешкод, що генеруються на робочих місцях співробітників, зокрема, при використанні персональних комп'ютерів та інших пристроїв.

Для підтримки надійної роботи мережі і виключення негативного впливу перешкод, пов'язаних з використанням на робочих столах комп'ютерів та інших пристроїв, що створюють електромагнітні перешкоди, на кожній робочій станції використовується діодний фільтр, що виключає проникнення перешкод в несучу мережу. Схема підключення наведена на рисунку 3.2.

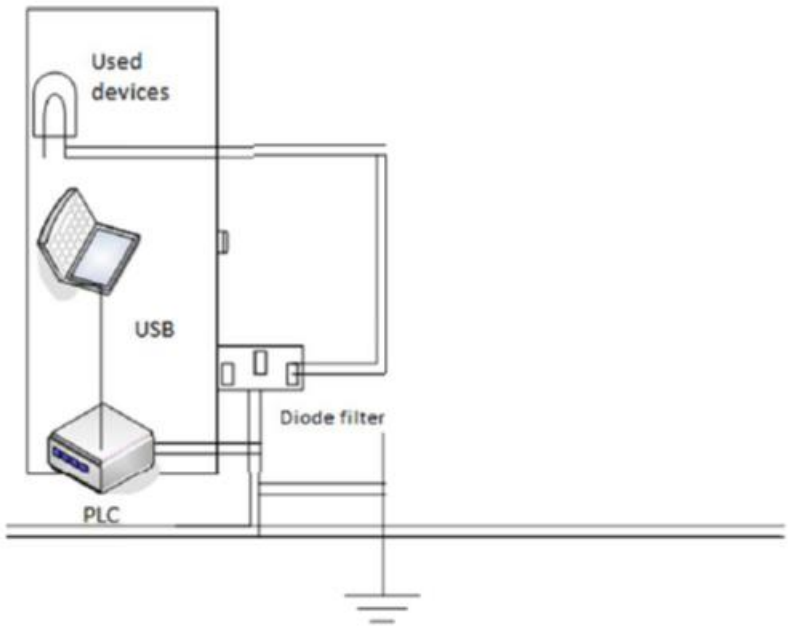


Рисунок 3.2 - Схема підключення терміналів до мереж PLC

Загальна схема локальної обчислювальної мережі представлена на рисунку 3.3.

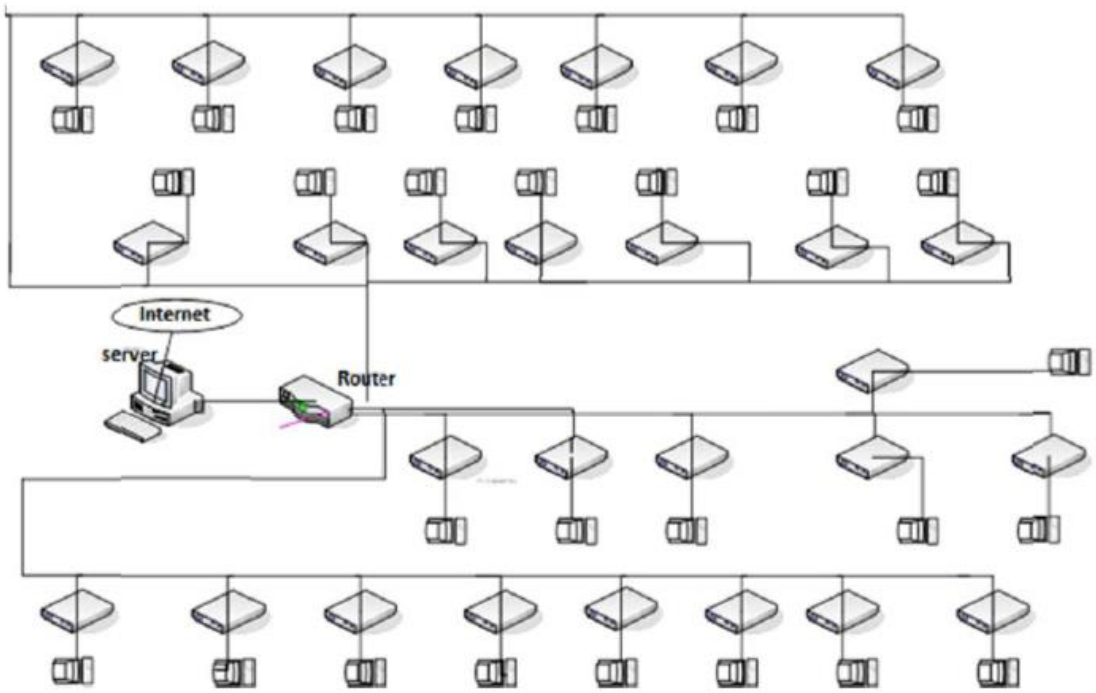


Рисунок 3.3 - Загальна схема локальної обчислювальної мережі інженерного центру "Інтепс"

3.2 Аналіз інформаційної безпеки локальної обчислювальної мережі в інженерному центрі "Інтепс"

Далі будуть розглянуті основні загрози безпеки мережі та надані рекомендації по зниженню рівня загроз.

По-перше, основний трафік в мережі формують процеси обміну робочою документацією, що використовується при проектуванні та випробуванні нових зразків продукції на даному підприємстві. Більшість документів є робочими і не становлять інтересу для третіх осіб. Однак можливість несанкціонованого доступу до всієї проектної документації може становити серйозну небезпеку для організації. До політики безпеки в локальній обчислювальній мережі інженерного центру "Інтепс" слід враховувати наступні вимоги:

1. Виключення можливого несанкціонованого доступу до повної конструкторської документації

2. Підтримка цілісності інформації в мережі

Розглянемо лише випадки несанкціонованого доступу з прямим підключенням до мережі (з метою перехоплення інформації, пошкодження даних, імплантації вірусів і т.д.), методи захисту яких зводяться до використання одних і тих же програмних і апаратних засобів.

1. Доступ до мережі з використанням електромагнітних випромінювань і перешкод

Фізично мережа організована в окремій будівлі на промисловій території фірми. Територія охороняється, тому доступ сторонніх осіб на територію ускладнений. Електроживлення будівлі здійснюється через понижуючий трансформатор, що виключає можливість підключення до мережі через дроти, виведені за межі будівлі.

У приміщенні при роботі на комп'ютерах не використовуються спеціальні пристрої, що екранують випромінювання від екранів моніторів ПК та інші електромагнітні перешкоди. Однак територіальне розміщення будівель на території, що охороняється, та відсутність місць прямого візуального контакту в

межах розумної видимості за межами території робить практично неможливим зчитування даних з екранів комп'ютерів або перехоплення електромагнітних завад при роботі на клавіатурі тощо.

Крім того, слід врахувати, що ноутбуки з LCD-моніторами мають дуже низький рівень випромінювання, що унеможливлює будь-які перешкоди.

Також необхідно зазначити, що кожне робоче місце в мережі заземлено, що згідно з міркуваннями, викладеними в пункті 2.2. передбачає підключення захисного заземлення до кожного блоку локальної обчислювальної мережі через фільтр, який має великий опір в широкій смузі, але малий опір на частоті 50 Гц. Дана схема підключення дозволяє істотно знизити рівень магнітного випромінювання працюючих в мережі комп'ютерів, що особливо важливо, оскільки, на відміну від класичних мереж, мережі, побудовані за технологією PLC, використовують екрановані кабелі.

В якості фізичного середовища передачі використовується неекранований кабель.

Тим не менш, складна структура електропроводки в будівлі теоретично допускає приховане підключення до мережі або безпосередньо через проведення чи розміщення в безпосередній близькості до електропроводки пристроїв, що здійснюють перехоплення наведених електромагнітних випромінювань. У зв'язку з цим виникає проблема несанкціонованого доступу до мережі.

2. Несанкціонований доступ до мережі.

Не зупиняючись окремо на способах захисту від несанкціонованого доступу до інформаційних потоків у мережі з використанням терміналів мережі (оскільки засоби боротьби з цією загрозою є стандартними для всіх видів мереж), розглянемо більш детально загрози, пов'язані з несанкціонованим підключенням безпосередньо до мережі. У цьому випадку важливо, щоб адміністратор (або використовувана для оперативного реагування на виникаючі загрози програма контролю) вчасно отримав попередження про атаку. В локальній мережі інженерного центру компанії використовується програма мережевого моніторингу Alchemy Aye, яка здійснює в режимі реального часу моніторинг переданих пакетів

на різних ділянках мережі і, в разі виявлення втрат пакетів або їх затримок, видає попередження на файловий сервер. Відзначимо, що про порушенні передачі пакетів на одній з підчастот мережі дана частота тимчасово блокується, а мережеві адаптери надалі використовують інші несучі частоти для відправки та отримання пакетів. Всього використовується 1536 підчастот (як заявляють розробники стандарту, блокування до 50% підчастот не повинно впливати на швидкість обміну даними в мережі), тому важко очікувати є, що зловмисник зможе організувати одночасно атаку з використанням хоча б половини частотного спектру.

В якості додаткового захисту в мережі використовується спеціальний блок Alchemy Eye Noise Filter, робота якого ініціюється безпосередньо програмою мережевого монітора в разі виявлення потенційного зовнішнього втручання в роботу мережі. Цей пристрій є джерелом інформаційних маскувальних шумів. Параметри шуму програмно оптимізуються відповідно до параметрів мережі, передача шуму здійснюється на частотах зі спектром, що повторює спектр шумового сигналу.

Однак, при мережевих атаках, в ході яких виявляється задіяною значна кількість підчастот, падає швидкість передачі пакетів, а втрати пакетів починають перевищувати деяке критичне значення (встановлюється адміністратором мережі), робота мережі буде заблокована до усунення джерел стороннього втручання в роботу мережі.

Даний алгоритм захисту буде виконаний в будь-якому випадку, незалежно від того, що було порушенням нормальної роботи мережі - несанкціоноване підключення периферійних пристроїв до кабельної системи або збої в роботі джерел живлення в результаті зовнішньої техногенної або природної аварії.

3. Пошкодження даних в мережі, загроза втрати даних

При отриманні зловмисником доступу до мережі можливе проведення інформаційних атак, наприклад, відправка в мережу надлишкових масивів інформації (інформаційна бомба), впровадження програм віруси тощо.

Однак у мережі, організованої за технологією PLC стійкість мережі до такого роду впливів виявляється навіть більшою, ніж для аналогічних мереж,

організованих за класичними схемами (наприклад, кабельних мереж Ethernet). Справа в тому, що при надсиланні "інформаційних бомб" відповідні підчастоти відразу ж блокуються, а надіслані пакети в такій мережі знищуються.

Крім того, в мережах PLC використовується апаратне шифрування даних, що передаються, за допомогою алгоритму AES. Виключається передача в мережу незашифрованих повідомлень (що є звичайною практикою в локальних мережах стандарту Ethernet). Як наслідок, по-перше, зловмисник навряд чи доб'ється розкриття отриманих даних за розумний період часу без додаткового впливу на мережу, а, по-друге, у разі імплантації зловмисникові необхідно буде провести шифрування своїх програм в мережу, а для цього необхідно заволодіти ключами шифрування, що при несанкціонованому доступі в мережу навряд чи можливо. Таким чином, локальна обчислювальна мережа, побудована на технології PLC, показує високу стійкість до зовнішніх атак, спрямованих як на отримання інформації з мережі, так і на порушення роботи мережі, спотворення даних в мережі.

Пакетні фільтри, що використовуються в комп'ютерній мережі цієї компанії, здійснюють аналіз інформації мережевого і транспортного рівнів моделі OSI. Це мережеві адреси (наприклад, IP) відправника і одержувача пакета, кількість портів відправника і одержувача, прапори TCP протокол, опція IP, типи ICMP. Фільтри пакетів будуть організовані за ресурсами маршрутизаторів. Часто використовуються штатні ресурси операційних систем.

Пакети перевіряються за трьома ланцюжками правил, налаштованих менеджером. В якості міжмережевого екрану першого рівня в комп'ютерній мережі компанії "Інтепс" використовується ОС Linux, що працює за принципом фільтра. Схема його роботи представлена далі.

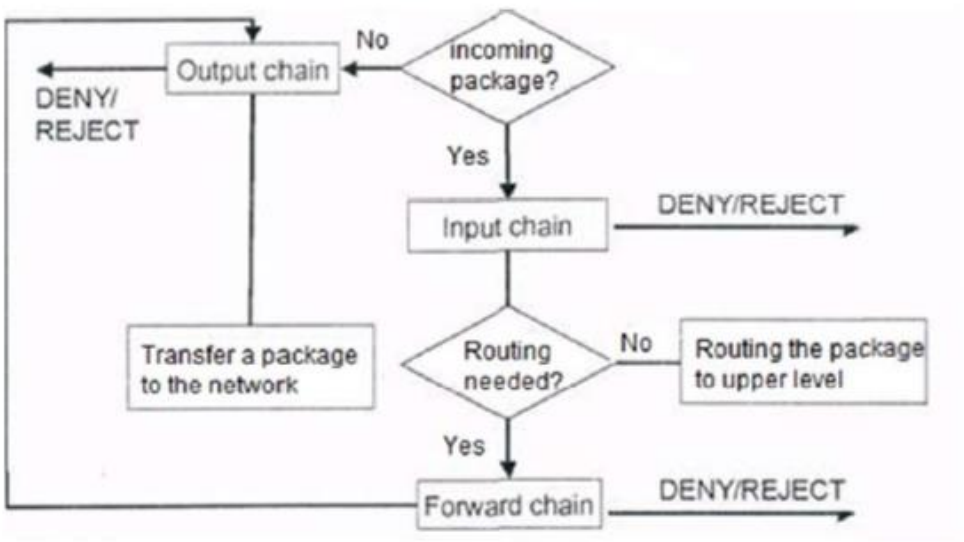


Рисунок 3.4 - Принцип використання ОС Linux в якості фільтра пакетів

Цей тип міжмережевого екрану заснований на використанні так званого принципу посередництва, тобто запит приймається міжмережевим екраном, аналізується і тільки потім передається на реальний сервер. Перш ніж дозволити встановлення TCP-з'єднання між комп'ютерами внутрішньої і зовнішньої мережі, посередники рівня з'єднання спочатку як мінімум реєструють клієнта. При цьому не дуже важливо, з якого боку (зовнішнього чи внутрішнього) знаходиться даний клієнт. При позитивному результаті реєстрації між зовнішнім і внутрішнім комп'ютерами організується віртуальний канал, по якому пакети передаються між мережами.

В якості сервера-шлюзу з'єднання в мережі даної компанії використовується сервер-шлюз з перетворенням IP-адрес (Network Address Translation, NAT). Проксі-сервери рівня додатків, які часто називають проксі-серверами, перевіряють і фільтрують інформацію на рівні мережевих додатків. Вони розрізняються за підтримуваними протоколами прикладного рівня. HTTP, FTP, SMTP, POP3/IMAP, NNTP, Gopher, telnet, DNS, RealAudio / RealVideo сервіси підтримується в комп'ютерній мережі цієї компанії. Коли клієнт внутрішньої мережі звертається, наприклад, до веб-сервера, його запит потрапляє до веб-посередника (або перехоплюється ним). Він встановлює з'єднання з сервером від імені клієнта, а

отриману інформацію передає клієнту. Для зовнішнього сервера посередник представляє себе як клієнт, а для внутрішнього клієнта - як веб-сервер.

Заснований на технології перевірки пакетів з урахуванням стану протоколу, міжмережевий екран забезпечує найвищий рівень безпеки. Метод stateful inspection передбачає збір інформації з пакетів даних, як комунікаційного, так і прикладного рівня, що досягається шляхом збереження та накопичення її в спеціальних контекстних таблицях, які динамічно оновлюються. Такий підхід забезпечує максимально можливий рівень безпеки, перевіряючи з'єднання на рівнях від 3 до 7 мережевої моделі OSI, тоді як проксі-посередники можуть перевіряти з'єднання лише на 5-7 рівнях. Обробка нового з'єднання, таким чином, відбувається наступним чином:

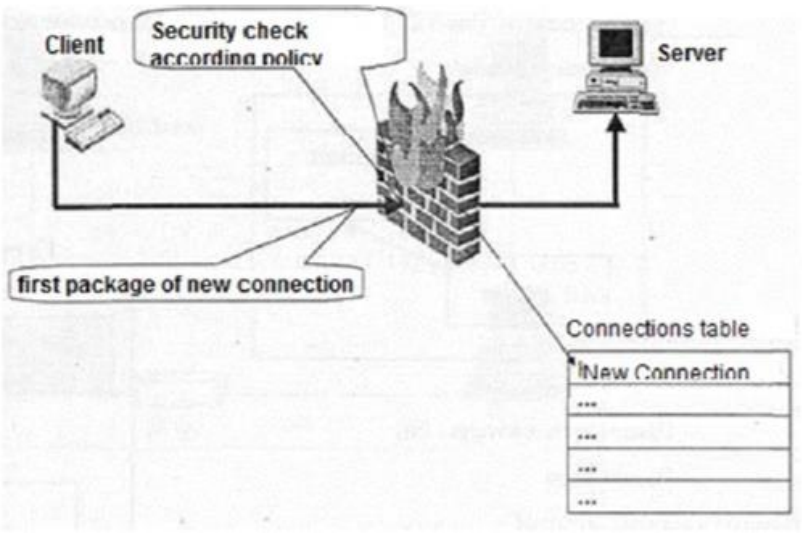


Рисунок 3.5 - Обробка нового з'єднання в комп'ютерній мережі компанії

Після того, як з'єднання занесено в таблицю, обробка наступних пакетів цього з'єднання відбувається на основі аналізу таблиць. У зв'язку з вищевикладеним можна стверджувати, що PLC центру інжинірингу будівельних мереж компанії "Інтепс" відрізняється високою стійкістю до зовнішніх впливів, а використання апаратного шифрування високої глибини виключає вплив людського фактору при роботі з інформацією, що вимагає підвищеного захисту.

3.3 Політика інформаційної безпеки в компанії " Інтепс"

Для безпосередньої організації (побудови) та ефективного функціонування комплексної системи захисту інформації в комп'ютерній мережі компанії "Інтепс" повинна бути створена спеціальна служба безпеки інформації (служба комп'ютерної безпеки).

Служба комп'ютерної безпеки являє собою штатний або позаштатний підрозділ, створений для організації кваліфікованої розробки системи захисту інформації та підтримки її нормального функціонування.

На цей підрозділ необхідно покласти вирішення наступних основних завдань:

- Визначення вимог до системи захисту інформації, її носіїв та процесів обробки, розробка політики безпеки та процесів обробки, розробка політики безпеки;

- Організація заходів щодо реалізації прийнятої політики безпеки, надання методичної допомоги і координація робіт по створенню і розвитку комплексної системи захисту;

- Контроль за дотриманням встановлених правил безпечної роботи в системі, оцінка ефективності та достатності вжитих заходів і застосованих засобів захисту.

Основні функції служби на ТОВ "Інтепс" перераховані нижче:

- Формування вимог до системи захисту при створенні та розвитку мережевої системи;

- Участь у проектуванні системи захисту, її випробуваннях та прийнятті в експлуатацію;

- Планування, організація та підтримка функціонування системи захисту інформації в процесі функціонування мережевої системи;

- Навчання користувачів і персоналу комп'ютерної мережі правилам безпечної обробки інформації та обслуговування компонентів мережевої системи;

- Розподіл між користувачами необхідних засобів доступу до ресурсів мережевої системи;

- Контроль за дотриманням користувачами та персоналом мережі встановлених правил поводження із захищеною інформацією в процесі її автоматизованої обробки;

- Взаємодія з відповідальними за безпеку інформації в підрозділах;

- Регламентація роботи та контроль за менеджерами баз даних,

Сервери та мережеві пристрої (для співробітників, що забезпечують коректність застосування наявних у складі ОС, СУБД та ін. засобів розмежування доступу та інших засобів захисту інформації);

- Вжиття заходів при спробах несанкціонованого доступу до інформації та при порушеннях правил функціонування системи захисту;

- спостереження за роботою системи захисту та її підрозділів і організація перевірок надійності їх функціонування.

Організаційно-правовий статус служби захисту інформації компанії "Інтепс" визначається наступним чином:

- Служба повинна підпорядковуватися начальнику служби безпеки даного підприємства, тобто особі, яка несе персональну відповідальність за дотримання правил поводження з інформацією, що захищається;

- Співробітники служби повинні мати право доступу до всіх приміщень, де встановлено мережеве обладнання, і право вимагати від керівництва підрозділів припинення автоматизованої обробки інформації за наявності прямої загрози для інформації, що захищається;

- Право забороняти включення в число експлуатованих нових одиниць комп'ютерної мережі, якщо вони не відповідають вимогам захисту інформації, повинно бути надано керівнику служби захисту і це може призвести до серйозних наслідків у разі реалізації значних загроз безпеки;

- чисельність служби повинна бути достатньою для виконання всіх перерахованих вище функцій;

- штатний персонал служби не повинен мати інших обов'язків, пов'язаних з функціонуванням мережі;

- працівникам служби повинні бути забезпечені всі умови, необхідні для виконання ними своїх функцій.

Для вирішення завдань, покладених на підрозділ захисту інформації, його співробітники повинні мати наступні права:

- Визначати необхідність, розробляти, представляти на узгодження та затвердження керівництву нормативні та організаційно-розпорядчі документи, що стосуються питань захисту інформації, у тому числі документи, що регламентують діяльність працівників інших підрозділів;

- Отримувати від працівників інших підрозділів необхідну інформацію з питань застосування інформаційних технологій та обслуговування комп'ютерних мереж, щодо обов'язків кінцевого користувача;

- Брати участь в опрацюванні технічних рішень, що стосуються обов'язків кінцевого користувача, при проектуванні та розробці нових підсистем і комплексів задач;

- Брати участь у випробуваннях розроблюваних підсистем і комплексів задач щодо оцінки якості реалізації вимог до обов'язків кінцевого користувача;

- Перевіряти діяльність співробітників інших підрозділів організації щодо дотримання правил кінцевих користувачів.

Природно, що всі ці завдання не під силу одній людині, особливо в такій великій організації, як компанія " Інтепс". Крім того, обслуговування комп'ютерної безпеки можуть бути співробітники з різними функціональними обов'язками. До складу цього підрозділу повинні входити наступні фахівці:

- Керівник, який безпосередньо відповідає за стан інформаційної безпеки та організацію робіт зі створення комплексних систем захисту інформації в комп'ютерній мережі;

- Аналітики з питань комп'ютерної безпеки, стану інформаційної безпеки, відповідальні за аналіз, визначення вимог до безпеки різних підсистем комп'ютерної мережі та шляхів підтримки їх захисту, а також за розробку необхідних нормативно-методичних та організаційно-розпорядчих документів з питань захисту інформації;

- Менеджери засобів захисту інформації, керівники та фахівці, які відповідають за підтримку та адміністрування конкретних засобів захисту інформації та ресурсів аналізу захищеності підсистем;

- Менеджери засобів криптографічного захисту, відповідальні за встановлення, налаштування, зняття засобів криптографічного захисту, генерацію та розподіл ключів і т.д.;

- Відповідальний фахівець за вирішення питань захисту інформації в розроблюваних програмістами і впроваджуваних додатках (участь у розробці технічних завдань щодо захисту інформації, у виборі засобів і методів захисту, участь у випробуваннях нових додатків з метою перевірки виконання вимог щодо захисту і т.д.);

- Фахівці із захисту інформації від витоку технічними каналами;

- відповідальний виконавець за організацію конфіденційного діловодства тощо.

3.4 Методика реалізації політики безпеки інформації в компанії "Інтепс"

Тепер розглянемо цілі інформаційної безпеки в компанії "Інтепс":

Конфіденційність - забезпечення доступу до інформації лише тим особам, які уповноважені на отримання такого доступу. Зберігання та перегляд цінних

Доступ до інформації мають лише ті особи, які мають на це службові обов'язки та повноваження.

Цілісність - збереження цілісності цінної та секретної інформації означає, що вона захищена від несанкціонованої модифікації. Існує певний набір типів інформації, які мають цінність тільки тоді, коли ми можемо гарантувати, що вони правильні. Загальна мета політики інформаційної безпеки компанії повинна гарантувати, що інформація не була пошкоджена, знищена або змінена в будь-який спосіб.

Придатність - підтримка того, щоб інформаційні та розвідувальні системи були доступними і готовими до роботи завжди, як тільки в них виникне потреба. У цьому випадку основною метою політики інформаційної безпеки компанії повинна бути гарантія того, що інформація завжди доступна і підтримується в належному стані.

Досягається безперервність процесу функціонування комп'ютерної мережі фірми і своєчасність відновлення її працездатності:

- Проведення спеціальних організаційних заходів і розробка організаційно-розпорядчих документів щодо забезпечення обчислювального процесу;

- Сувора регламентація процесу обробки інформації із застосуванням комп'ютера та роботи системи персоналу, включаючи кризові ситуації;

- Призначення та підготовка посадових осіб, відповідальних за організацію та реалізацію практичних заходів з безпеки інформаційно-обчислювального процесу;

- Точне знання і суворе дотримання всіма посадовими особами, які використовують комп'ютерні пристрої в мережі, вимог керівних документів з безпеки;

- Застосуванням різних способів резервного копіювання апаратних ресурсів, стандартних програм копіювання та страхового копіювання ресурсів інформаційної системи;

- Постійне підтримання необхідного рівня безпеки компонентів системи, безперервний контроль та управлінська підтримка коректного застосування засобів захисту,

- Проведення постійного аналізу ефективності вжитих заходів і застосовуваних засобів і ресурсів безпеки мережі, розробка і реалізація пропозицій щодо їх вдосконалення.

У концепції інформаційної безпеки даної компанії слід виділити наступні питання:

- Характеристика комп'ютерної мережі в організації, як об'єкта інформаційної безпеки (об'єкта захисту):

- Призначення, цілі створення та обслуговування комп'ютерної мережі фірми

- Структура і розміщення основних мережевих елементів організації, інформаційні зв'язки з іншими об'єктами

- Категорії інформаційних ресурсів, які підлягають захисту

- Категорії фахівців-користувачів організації, режими використання та рівні доступу до інформації

- Інтереси, що враховуються при обслуговуванні фахівцем організації суб'єктів інформаційних відносин;

- Вразливість основних компонентів організації

- Цілі та завдання підтримки інформаційної безпеки організації та основні шляхи їх досягнення (вирішення завдань системи захисту)

- Перелік основних небезпечних факторів впливу та суттєвих загроз інформаційній безпеці:

- зовнішні та внутрішні фактори впливу, загрози безпеці інформації та їх джерела

- Навмисні дії опосередкованих осіб, зареєстрованих користувачів і обслуговуючого персоналу

- Витік інформації технічними каналами

- Неформальна модель можливих порушників

- Підхід до оцінки ризиків в комп'ютерній мережі організації;

- Основні положення технічної політики у сфері захисту інформації компанії

- Принципи підтримки інформаційної безпеки організації;

- Основні заходи та методи (способи) захисту від загроз, ресурси підтримки необхідного рівня захищеності ресурсів:

- Організаційні (управлінські) заходи захисту

- Структура, функції та повноваження підрозділу підтримки інформаційної безпеки;

- Фізичні засоби захисту

- Технічні (апаратно-програмні) засоби захисту

- Системний контроль безпеки інформації

- Контроль ефективності системи захисту

- Першочергові заходи щодо забезпечення безпеки інформації компанії

- Перелік нормативних документів, що регламентують діяльність у сфері захисту інформації.

ВИСНОВКИ

У найближчому майбутньому прогрес в області розвитку засобів обчислювальної техніки, програмного забезпечення і мережевих технологій дасть поштовх до розвитку засобів захисту, що зажадає багато в чому перегляду існуючої наукової парадигми інформаційної безпеки. Новий погляд на змістовні положення про безпеку:

- Дослідження та аналіз причин порушення безпеки комп'ютерних систем;

- Розробка ефективних моделей безпеки, адекватних сучасному рівню розвитку програмних і апаратних засобів, а також можливостям зловмисників;

- Створення методів і засобів коректної імплантації моделей безпеки в існуючі методи, з можливістю гнучкого управління, забезпеченням безпеки в залежності від висунутих вимог, допустимого ризику і витрат ресурсів;

- Необхідність розвитку засобів аналізу безпеки комп'ютерних систем шляхом реалізації тестових впливів (атак).

Широка інформатизація суспільства, впровадження комп'ютерних технологій у сферу управління об'єктами, стрімке зростання темпів науково-технічного прогресу поряд з позитивними досягненнями в інформаційних технологіях, створюють реальні передумови для витоку конфіденційної інформації.

Основною метою роботи була розробка загальних рекомендацій щодо захисту інформації в комп'ютерних мережах та розвиток можливостей забезпечення інформаційної безпеки. Отримані наступні результати:

1. Розглянуто основні шляхи захисту від несанкціонованого доступу до інформації, що циркулює в системах обробки.

2. Проведено класифікацію способів та засобів захисту інформації.

3. Проведено детальний аналіз методів захисту інформації в процесорних системах.

4. Розглянуто основні напрямки захисту інформації в комп'ютерних мережах.

5. Розроблено концепцію безпеки локальних обчислювальних мереж інженерного корпусу компанії " Інтепс" та питання безпеки при груповій обробці даних у службах і підрозділах фірми.

6. Здійснено формування політики безпеки конкретної фірми та наведено методику реалізації цієї політики.

7. Розроблено документи з інформаційної безпеки в компанії " Інтепс".