МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021 р.

На правах рукопису
УДК 004.056:004.738.5(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система забезпечення інформаційної безпеки локальної мережі

Виконавець: В.Ю. Білий

Керівник: к.т.н., доцент М.Б. Гумен

Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних та комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С.В. Казмірчук
«___» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи
здобувача вищої освіти Білого Віталія Юрійовича

1. Тема: Система забезпечення інформаційної безпеки локальної мережі затверджена наказом в.о. ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: розглянути існуючі загрози інформаційній безпеці локальної мережі, проаналізувати методи поліпшення безпеки інформації, проаналізувати оцінку ризиків, спроєктувати локальну мережу та розробити систему інформаційної безпеки локальної мережі.
4. Зміст пояснювальної записки: дослідження загроз локальній мережі, методи захисту інформації в локальній мережі, розробка системи інформаційної безпеки локальної мережі.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки завдання		*Виконано*
2.	Аналіз літературних джерел		*Виконано*
3.	Обґрунтування вибору рішення		*Виконано*
4.	Збір інформації		*Виконано*
5.	Дослідження загроз інформаційній безпеці		*Виконано*
6.	Дослідження методів та засобів інформаційної безпеки		*Виконано*
7.	Дослідження топології локальної мережі		*Виконано*
8.	Розробка системи забезпечення інформаційної безпеки локальної мережі		*Виконано*
9.	Перевірка на антиплагіат		*Виконано*
10.	Оформлення і друк пояснювальної записки		*Виконано*
11.	Оформлення презентації		*Виконано*
12.	Отримання рецензій від рецензента		*Виконано*

Здобувач вищої освіти _____ В.Ю. Білий
(підпис, дата)

Керівник дипломної роботи _____ М.Б. Гумен
(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи складає 59 сторінок, має 11 рисунків, 1 таблицю та 2 діаграми. Список використаних джерел містить 23 найменувань і займає 2 сторінки. Загальний обсяг роботи 58 сторінок.

Метою дипломної роботи є розробка системи забезпечення інформаційної безпеки локальної мережі.

У роботі розглянуті існуючі загрози, заходи щодо покращення інформаційної безпеки. Проведено аналіз оцінки ризиків системи безпеки підприємства, спроєктовано локальну мережу підприємства та створено систему інформаційної безпеки.

Ключові слова: система захисту інформації, методи забезпечення інформаційної безпеки, локальна мережа.

ЗМІСТ

ВСТУП

Актуальність. Захист інформації в сучасних комп'ютерних інформаційних системах є пріоритетним завданням. Викрадення конфіденційної інформації, знищення даних, викривлення інформації, виведення з ладу комп'ютерних систем – далеко не повний перелік усіх ризиків, що виникають у процесі експлуатації та використання сучасних інформаційних систем. Комплексний характер системи безпеки для протидії різноманітним загрозам системі має забезпечувати контроль за діяльністю службовців, які використовують різноманітні внутрішні ресурси системи, а також мають доступ до Інтернет-додатків. Репутація і безпека сучасних компаній багато в чому залежить від діяльності її співробітників, а системи контролю і введення обмежень для персоналу є важливою складовою комплексу заходів, які спрямовані на підтримку інформаційної безпеки . В цьому напрямку актуальними є не тільки обмеження та фільтрація ресурсів і мережевих сервісів Інтернет з метою захисту корпоративної мережі, але й система, що контролює всі дії користувачів з метою подальшого аналізу й організаційних висновків. Контроль за використанням комп'ютерів і пристроїв у мережі має за мету попередити несанкціонований доступ як до комп'ютерної мережі в цілому, так і до окремих об'єктів спільного доступу, таких як мережеві файлові системи, директорії з конфіденційною інформацією, бази даних, та запобігти втраті чи розголошенню цінної та важливої інформації. Актуальним завданням є також моніторинг дій системних адміністраторів, які зазвичай можуть мати необмежені повноваження в системах та іноді стають джерелом витоку даних з компаній. При цьому важливо мати відповіді на ряд запитань: хто і коли працював у системі; хто мав доступ до баз даних та файлових систем спільного доступу; чим займаються співробітники в певний час; у разі надзвичайної події – чому деякі сервіси перестали бути доступними; які зміни в конфігурації було зроблено, з якої причини і ким? Повний моніторинг дій користувачів системи дасть змогу отримати повну інформацію, що може бути використана

для різноманітних висновків за результатами аналізу діяльності користувачів та результатів їх роботи.

Метою дипломної роботи є розробка системи забезпечення інформаційної безпеки локальної мережі.

Досягнення мети досліджень потребує розв’язання таких задач:

- розглянути методи та засоби захисту інформації в локальній мережі, виявити їх недоліки та переваги;
- провести аналіз існуючих загроз;
- розробити систему інформаційної безпеки.

Об'єкт дослідження: процес захисту інформації в локальній мережі.

Предмет дослідження: системи забезпечення інформаційної безпеки локальної мережі.

Практична цінність полягає у розробці систем забезпечення інформаційної безпеки локальної мережі, що дає змогу зменшити ризики витоку конфіденційної інформації.

Розділ 1. ДОСЛІДЖЕННЯ ЗАГРОЗ ЛОКАЛЬНІЙ МЕРЕЖІ

1.1 Види загроз у локальній мережі

На даний момент можна виділити два фактори вразливості інформації:

- Несанкціонований доступ до інформації з метою видалення, крадіжки або використання в особистих цілях;
- Руйнівна дія шкідливих програмних засобів.

1.1.1 Несанкціонований доступ до інформації

Через своєю багатофункціональність локальна обчислювальна мережа є складною. Це робить її вразливою та дає можливість зловмисникам створювати лазівки для прихованого доступу до інформації. Існує багато прикладів злочинних дій, які свідчать про вразливість локальних мереж.

Існують два напрямки отримання несанкціонованого доступу до інформації:

- Прямий – з фізичним доступом до компонентів локальної мережі;
- Непрямий – без фізичного доступу до компонентів локальної мережі.

Є багато шляхів несанкціонованого доступу до інформації:

- Здійснюються шляхом застосування:
  - Засобів підслуховування;
  - Підкупом осіб конкуруючої фірми;
  - Фотоапаратури;
  - Відеоапаратури;
  - Програм типу «троянський кінь».
- Здійснюються шляхом використання:
  - Недоліків мови програмування;
  - Перехвату ЕМВ;

- Крадіжки носіїв інформації;
- Копіювання інформації;
- Недоліків в операційних системах.

- Здійснюються шляхом використання:
  - Захищених даних за допомогою запитів дозволу;
  - Аналізу виробничих відходів;
  - Відомостей, наявних у засобах масової інформації;
  - Реквізитів розмежування доступу;
  - Таємних паролів.

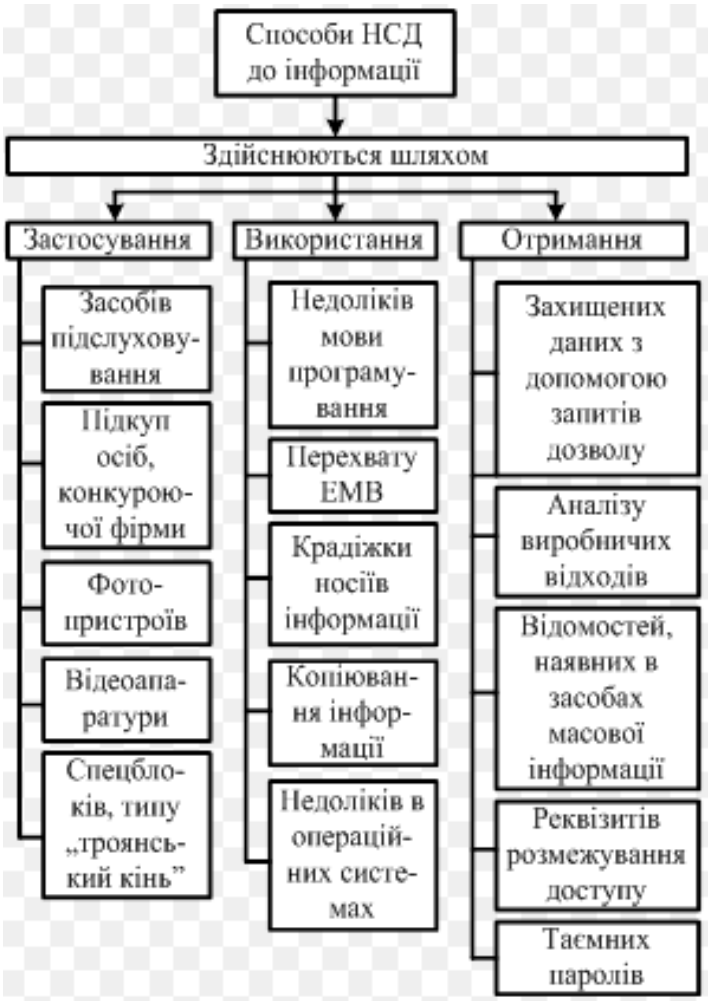


Рис. 1.1 Способи несанкціонованого доступу до інформації

1.1.2 Шкідливі програмні засоби

Шкідливий програмний засіб – програмне забезпечення, що ставить під загрозу нормальне функціонування системи. До нього належать віруси, троянські програми, рекламне програмне забезпечення, клавіатурні логери, руткіти, шпигунські програмні засоби та інше.

Шкідливе програмне забезпечення характеризується:

- стрімким розмноженням у системі шляхом приєднання до інших програм, копіювання себе на інші носії інформації та розсилання по мережі;
- Виконанням будь-яких шкідливих дій, які можуть порушувати нормальну роботу програм або цілої системи, наприклад:
  - Видаленням важливих файлів системи або програмних забезпечень, що порушує їх нормальну функціональність;
  - Внесенням змін у файли;
  - Блокуванням певних програм, наприклад, антивірусів;
  - Використанням ресурсів комп’ютера для своїх цілей, тим самим знижуючи швидкодію системи;
  - Перезавантаженням системи без участі користувача;
  - Збиранням інформації та пересиланням її по мережі.

Можна виділити три основні пункти за рівнем небезпечності дій шкідливих програм:

- Безпечні – не змінюють файли та не пошкоджують їх, не збирають інформацію, можуть проявлятися в аудіо- та відео форматі;
- Небезпечні – використовують ресурси системи, наприклад, забирають оперативну пам’ять, примусово перезавантажують систему, можуть призводити до збоїв системи;
- Дуже небезпечні – можуть пошкоджувати, змінювати та видаляти файли, збирати інформацію та передавати її по мережі.

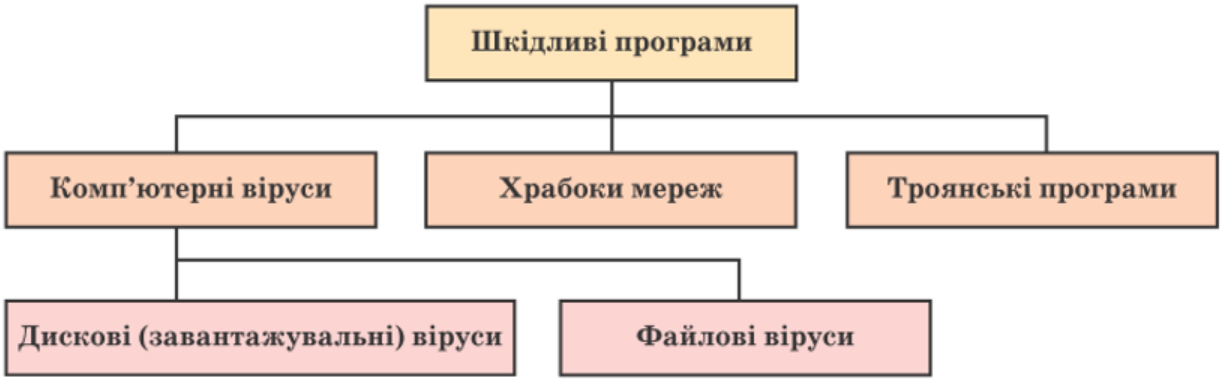


Рис 1.2 Класифікація шкідливого програмного забезпечення за принципами функціональності та розповсюдження

Комп'ютерні віруси – програмне забезпечення, яке виконує несанкціоновані, частіше шкідливі дії по відношенню до системи, здатне до самостійного розповсюдження.

Серед вірусів можна виділити:

- Трояни – як відомо з історії, воїни Трої отримали в подарунок від греків дерев'яного коня, всередині якого розташувалися грецькі воїни. Так само діють троянські програми, проникаючи в систему разом з іншими програмами, які користувач отримує з мережі. Як і інші шкідливі програми, можуть виконувати шкідливі дії, але частіше використовуються у шпигунських цілях;
- Хробаки комп'ютерних мереж – розповсюджуються шляхом пересилання своїх копій комп'ютерними мережами з метою ураження комп'ютерів. Більшість видів поширюються шляхом прикріплення до файлів електронної пошти. Після ураження комп'ютера вони намагаються розповсюджуватися далі. Як і більшість шкідливих програм, можуть виконувати деструктивні дії, характерні шкідливим програмам;
- Поліморфні – під час копіювання змінюються в розмірі, що ускладнює їх виявлення за відомою довжиною коду вірусу. Характеризуються

тим, що для їх виявлення не діють звичайні алгоритми пошуку, так як кожна нова копія вірусу не має зі своїм батьком нічого спільного. Це досягається шифруванням тіла самого вірусу і розшифровувачем, який не має жодного постійного біта в кожному своєму екземплярі;

- Приховані віруси – віруси, які будь-якими способами приховують своє існування в системі. Наприклад, для перевірки антивірусом надається його неуражена копія;
- Дискові віруси – розповсюджуються шляхом копіювання себе в системні ділянки дисків під час спроби читання користувачем ураженого носія;
- Файлові віруси – знаходяться в різних файлах, частіше з розширенням exe або com. Також можуть знаходитись у текстових документах, електронних таблицях, базах даних тощо.

Деякі шкідливі програми після ураження системи спочатку не виконують ніяких деструктивних дій, а лише розмножуються. Після такої пасивної фази існування через певний час або за вказанням комп'ютера з мережі вони починають діяти, що може призвести до значних неприємностей.

1.2 Напрями захисту інформації

Для захисту інформації сьогодні використовуються апаратні пристрої, а також впроваджуються спеціалізовані технічні засоби та програмне забезпечення. Задля успішної боротьби з несанкціонованим доступом до інформації й перехоплення даних необхідне чітке уявлення про канали витоку.

Захистити інформацію у вашій локальній мережі можуть такі елементи:

1. Перешкода - фізично перекриває шлях зловмиснику до захищеної інформації (на територію та в обладнані кімнати).

2. Контроль доступу - інформація захищається регулюванням доступу до всіх системних ресурсів (обладнання, програмного забезпечення, окремих даних).

Контроль доступу включає такі функції безпеки:

- Ідентифікацію користувачів, персоналу та системних ресурсів, при чому ідентифікація означає присвоєння кожному з вищезазначених об'єктів ім'я, код, пароль та розпізнання суб'єкта чи об'єкта за представленим їм ідентифікатором;
- Перевірка повноважень шляхом перевірки відповідності дати та необхідних ресурсів і процедур встановленим правилам;
- Створення дозволів та умов праці в межах встановлених нормативних правил;
- Реєстрація звернень до захищених ресурсів;
- Швидке реагування на затримку роботи, відмову, вимкнення, сигналізацію при спробах несанкціонованих дій.

3. Маскування - спосіб захисту інформації в локальній мережі шляхом криптографічного перетворення. Коли інформація передається по лініях зв’язку на великі відстані, зашифрувати дані - це єдиний спосіб забезпечити надійний захист.

4. Регламентація - розробка та впровадження в процесі функціонування локальної мережі подій, що створюють такі умови автоматизованої обробки та зберігання захищеної інформації в локальній мережі, в яких можливість несанкціонованого доступу значно зменшується. Для такої ефективності потрібно суворо регламентувати структуру локальної обчислювальної мережі (обладнання приміщень, розміщення апаратури в ньому) та забезпечення комфортних умов для можливості роботи персоналу, відповідних за захист та обробку інформації.

5. Необхідні правила – усі користувачі локальної мережі змушені виконувати встановлені правила обробки та використання конфіденційної захищеної

інформації під загрозою фінансової, адміністративної або кримінальної відповідальності.

Розглянуті методи захисту інформації реалізовані використанням різних можливих засобів захисту інформації. Розрізняють морально-етичні, організаційні, законодавчі, програмні та технічні засоби.

Організаційними засобами захисту можна назвати організаційно-правові заходи, що здійснюються під час створення та функціонування локальної мережі для захисту інформації.

Організаційні заходи охоплюють усі структурні елементи локальної мережі на всіх етапах: будівництво приміщення, проєктування системи, монтаж та налаштування обладнання, випробування та перевірка, експлуатація.

До засобів законодавчого захисту належать законодавчі акти країни, що регулюють правила використання й обробки конфіденційної інформації та відповідальність за порушення цих правил.

Морально-етичні засоби захисту містять усі види норм, які традиційно розвивалися або формувалися в міру поширення обчислювальні можливості певної країни чи суспільства. Ці норми менш обов'язкові, ніж законодавчі, однак їх порушення зазвичай призводять до втрати поваги та авторитету.

1.2.1 Заходи щодо захисту інформації в локальній мережі

Захист інформації на персональному комп'ютері - сукупність певних заходів, засобів та методів запобігання або зменшення шансів утворення каналів витоку та спотворення існуючої інформації, що зберігається на персональному комп'ютері.

1. Організаційний захист – сукупність заходів, що ускладнюють доступ сторонніх осіб до конфіденційної інформації незалежно від методу обробки інформації та каналів витоку інформації. Нижче запропоновані організаційні заходи, які необхідні для підвищення рівня безпеки:

- Донесення до відома співробітників, яка відповідальність слідує за випадкові витоки і навмисні корпоративні «зливи» третім особам;
- Визначення, в яких ситуаціях дійсно потрібно обмінюватися цінною корпоративною інформацією з підлеглими і між підлеглими, щоб не робити цього без необхідності;
- Надання паролів і логінів тим працівникам, які в цього по-справжньому потребують;
- Проведення тренінгів, що підвищують обізнаність співробітників у різних сферах, пов’язаних з безпекою;
- Обмеження кількості точок входу;
- Вимога для гостей – обов'язково заходити на прохідну і розписуватися в журналі відвідувачів перед входом на внутрішню територію;
- Зменшення кількості точок входу в неробочий час, коли навколо не так багато співробітників;
- Проведення обговорень останніх потенційних IT-загроз для підприємства;
- Обмеження доступу до приміщень, в яких може використовуватись або оброблюватись конфіденційна інформація;
- Зберігання магнітних носіїв в закритих та міцних контейнерах;
- Встановлення принтеру, монітора та клавіатури в таких місцях, щоб зменшити можливість несанкціонованого перегляду конфіденційної інформації сторонніми особами;
- Знищення непотрібних матеріалів, які можуть містити в собі цінну інформацію.

Запропоновані заходи допоможуть знизити на підприємстві такі ризики як: ескалація привілеїв та розповсюдження секретної інформації співробітниками, халатність користувачів, злом та проникнення на територію підприємства сторонніх фізичних осіб.

2. Організаційно-технічні засоби захисту - заходи, що стосуються особливостей каналів витоків та способу обробки інформації, що не потребують застосовування нестандартних методів або обладнання. Організаційно-технічні заходи включають:

- Обмеження доступу до внутрішньої частини корпусу персонального комп’ютера шляхом створення механічних замкових пристроїв.
- Знищування всієї секретної інформацію на жорсткому диску комп’ютера за необхідності відправки його на ремонт;
- Організація живлення персонального комп’ютера від окремого джерела живлення або загальної електричної мережі через стабілізатор напруги;
- Використовування рідкокристалічних або плазмових дисплеїв для відображення інформації та струменевих або лазерних принтерів для друку;
- Від’єднання комп'ютера від локальної мережі або мережі віддаленого доступу під час обробки конфіденційної інформації, крім випадку передачі цієї інформації через мережу.
- Встановлення принтера та клавіатури на м’які підставки для зменшення витоку інформації через акустичні канали.
- Під час обробки секретної інформації на комп’ютері увімкнути генератори додаткових фонових шумів (кондиціонери, вентилятори), також можна оброблювати іншу інформацію на сусідніх комп’ютерах.
- Знищення інформації відразу після використання.

3. Заходи технічного захисту - заходи, які суворо пов'язані з характеристиками каналів витоку, для реалізації яких потрібні спеціальні методи, апаратне або програмне забезпечення.

1.3 Висновки до розділу 1

У цьому розділі було розглянуто види загроз локальній мережі, а саме несанкціонований доступ до конфіденційної інформації та руйнівна дія шкідливого програмного забезпечення. Були запропоновані певні заходи щодо захисту інформації в локальній мережі.

Розділ 2. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ

2.1 Ідентифікація та автентифікація

Ідентифікація та автентифікація може розглядатися як опора програмного та апаратного забезпечення, оскільки інші служби призначені для обслуговування так званих іменованих об'єктів. Ідентифікація та автентифікація - це перша лінія оборони, «шлюз» до інформаційного простору організації.

Ідентифікація дозволяє суб’єкту (користувачеві, процесу, що діє від імені конкретного користувача, або іншому обладнанню та програмному забезпеченню) називати (повідомляти своє ім’я). Завдяки автентифікації інша сторона переконується, що суб’єкт дійсно є тим, ким він або вона себе представляє.

Автентифікація буває односторонньою (зазвичай клієнт перевіряє свою справжність на сервері) та двосторонньою (взаємною). Прикладом односторонньої автентифікації є процедура входу користувача в систему.

У мережевому середовищі, де сторони ідентифікації / автентифікації розподілені географічно, сервіс має два основні аспекти:

- що служить автентифікатором (тобто використовується для підтвердження справжності особи суб’єкта);
- як організований (і захищений) обмін даними ідентифікації / автентифікації.

Суб'єкт може підтвердити свою справжність, надавши, принаймні, одну з наступних сутностей:

- дещо, що він знає (пароль, персональний ідентифікаційний номер, криптографічний ключ тощо);
- щось, що йому належить (особиста картка чи інший пристрій подібного значення);

- щось, що є частиною його самого (звук, відбитки пальців тощо, тобто власні біометричні характеристики).

У відкритому мережевому середовищі між сторонами автентифікації / автентифікації немає надійного маршруту, це означає, що в цілому дані, які передаються суб'єктом можуть не збігатися з даними, отриманими та використаними для перевірки справжності. Потрібно забезпечити захист від пасивного та активного прослуховування мережі, тобто від перехвату, зміни та / або відтворення даних. Передання паролів у відкритому вигляді, очевидно, незадовільне; не рятує становище і шифрування паролів, оскільки воно не захищає від відтворення. Потрібні більш складні протоколи автентифікації.

Надійна ідентифікація ускладнена не тільки через мережеві загрози, а й з багатьох інших причин. По-перше, майже всі автентифікаційні сутності автентифікації можуть бути виявлені, викрадені або підроблені. По-друге, існує протиріччя між надійністю автентифікації, з одного боку, та зручністю користувача й адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити облікові дані (адже на його місце могла сісти інша людина), а це не тільки клопітно, але й збільшить ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніші засоби захисту, тим дорожчі.

Сучасні засоби ідентифікації / автентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід – це, насамперед, вимога зручності для користувача. Якщо в корпоративній мережі є багато інформаційних сервісів, до яких можна отримати незалежний доступ, то багаторазова автентифікація / автентифікація стає надто обтяжливою. На жаль, поки що не можна сказати, що єдиний вхід у мережу став нормою, домінуючі рішення ще не сформувалися.

Таким чином, потрібно шукати компроміс між надійністю, доступністю за ціною та зручністю використання й адмініструванням засобів ідентифікації та автентифікації.

Цікаво відзначити, що сервіс ідентифікації / автентифікації може стати ціллю атак на доступність. Якщо система налаштована на блокування пристрою введення облікових даних (наприклад, терміналу) після певної кількості невдалих спроб, зловмисник може зупинити законного користувача кількома натисканнями клавіш.

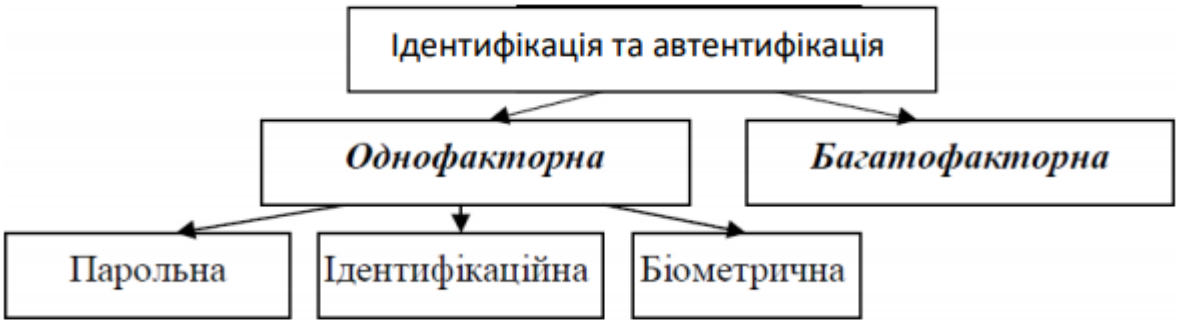


Рис.2.1 Система технології ідентифікації та автентифікації

2.1.1 Автентифікація за допомогою пароля

Основними перевагами автентифікації за допомогою пароля є простота та звичність. Паролі вже давно вбудовані в операційні системи та інші сервіси. За правильного використання паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Однак, за сукупністю характеристик, їх слід визнати найслабшим засобом автентифікації.

Щоб зробити пароль незабутнім, його часто роблять простим (ім’я подруги, назва спортивної команди тощо). Однак простий пароль не складно вгадати, особливо якщо ви знаєте пристрасті користувача. Існує класична історія про радянського розвідника Річарда Зорге, суб'єкт уваги якого через слово говорив «карамбу»; звичайно, цим самим словом відкривався секретний сейф.

Іноді паролі не шифруються з самого початку, оскільки вони містять стандартні значення, що вказані в документації і не завжди змінюються після встановлення системи.

Введення пароля можна підглянути. Для підглядання іноді навіть використовують оптичні прилади.

Паролями часто діляться колеги, щоб ті могли, наприклад, підмінити на деякий час власника пароля. Теоретично в таких випадках краще використовувати засоби управління доступом, але на практиці цього ніхто не робить; і таємниця, що відома двом, вже не є таємницею.

Пароль можна вгадати «методом грубої сили», використовуючи, скажімо, словник. Якщо файл пароля зашифрований, але доступний для читання, його можна завантажити на свій комп'ютер і спробувати підібрати пароль, програмуючи повний перебір (припускається, що алгоритм шифрування відомий).

Тим не менш, запропоновані нижче заходи можуть значно покращити надійність захисту паролем:

- введення технічних обмежень (пароль не повинен бути занадто коротким, він повинен містити літери, цифри, розділові знаки тощо);
- управління періодом дії паролів, їх періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження кількості невдалих спроб входу (це ускладнює застосування «методу грубої сили»);
- навчання користувачів;
- використання програмних генераторів паролів (така програма, що заснована на простих правилах, може генерувати лише пам'ятні паролі).
- завжди рекомендується використовувати вищезазначені заходи, навіть якщо на додаток до паролів використовуються інші методи автентифікації.

Рис. 2.1.1 Парольна автентифікація

2.1.2 Одноразові паролі

Розглянуті вище паролі можна назвати багаторазовими. Їх розкриття дозволяє зловмиснику діяти від імені законного користувача. Одноразові паролі - набагато потужніший інструмент, який витримує пасивне підслуховування мережі.

Найвідомішим програмним генератором OTP є система Bellcore S / KEY. Ідея системи така: нехай буде односторонньою функцією f (тобто функцією, обчислити зворотну якої неможливо за прийнятний час). Ця функція відома як користувачеві, так і серверу автентифікації. Нехай далі є в наявності секретний ключ K, який знає лише користувач.

На початковій фазі адміністрування користувача функція f застосовується до клавіші K n разів, після чого результат зберігається на сервері. Далі процедура автентифікації користувача така:

- сервер надсилає номер (n-1) в користувацьку систему;

- користувач застосовує функцію f до секретного ключа K (n-1) і надсилає результат на сервер автентифікації через мережу;
- сервер застосовує функцію f до значення, отриманого від користувача, і порівнює результат із раніше збереженим значенням. У разі збігу справжність користувача вважається встановленою, сервер запам'ятовує нове значення (надіслане користувачем) і зменшує лічильник на одиницю (n).

Насправді реалізація дещо складніша (поруч із лічильником сервер надсилає значення ядра, що використовується функцією f), але це для нас зараз не важливо. Оскільки функція f незворотна, перехоплення пароля та доступ до сервера автентифікації не дозволяє йому знати секретний ключ K та передбачити наступний одноразовий пароль.

Система S / KEY знаходиться в стані Інтернет-стандарту (RFC 1938).

Іншим підходом до надійної автентифікації є створення нового пароля через короткий час (наприклад, кожні 60 секунд), для чого можуть бути використані програми або спеціальні інтелектуальні карти (на практиці такі паролі можна розглядати як одноразові паролі). Сервер автентифікації повинен знати алгоритм генерації паролів та його параметри; крім того, годинник клієнта та сервера повині бути синхронізовані.

2.1.3 Ідентифікація / автентифікація за допомогою біометричних даних

Біометрія - це сукупність автоматизованих методів ідентифікації та / або автентифікації людей на основі їх фізіологічних та поведінкових характеристик. Фізіологічні характеристики включають відбитки пальців, характеристики сітківки та рогівки очей, геометрію руки та обличчя тощо. До поведінкових характеристик належать динаміка підпису (вручну), стиль роботи з клавіатурою. На місці стику фізіології та поведінки знаходиться аналіз особливостей голосу й розпізнавання мови.

Біометрією по всьому світу займаються дуже давно, але довгий час все було складно і дорого. На сьогодні попит на біометричні продукти дуже інтенсивно зростає, особливо в контексті розвитку електронної комерції. Це зрозуміло, оскільки користувачеві набагато зручніше представлятися, ніж щось запам’ятовувати. Попит створює пропозицію, і на ринку з’явилися відносно недорогі апаратно-програмні продукти, зосереджені головним чином на розпізнаванні відбитків пальців.

Загалом робота з біометричними даними організована наступним чином. Спочатку створюється та ведеться база даних характеристик потенційних користувачів. Для цього знімаються біометричні характеристики користувача, обробляються, результат обробки (так званий біометричний шаблон) реєструється в базі даних (необроблені дані, такі як сканування пальців або рогівки, зазвичай не зберігаються).

Надалі, щоб ідентифікувати (і одночасно автентифікувати) користувача, процес видалення та обробки буде повторений з подальшим пошуком у базі даних шаблонів. У разі успішного пошуку особистість та справжність користувача вважаються встановленими. Для автентифікації достатньо порівняти обраний біометричний шаблон на основі раніше введених даних.

Біометричні дані зазвичай використовуються разом з іншими автентифікаторами, такими як інтелектуальні карти. Іноді біометрична автентифікація - це лише перша лінія захисту і використовується для активації інтелектуальних

карт, що зберігають криптографічні секрети; у цьому випадку біометричний шаблон зберігається на тій же карті.

У галузі біометрії активність дуже висока. Створено відповідний консорціум, активно проводяться роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу тощо), публікується безліч рекламних статей, в котрих біометрія подається як інструмент забезпечення надбезпеки, що став доступним широким масам.

Слід зазначити, що з біометричними даними необхідно поводитися дуже обережно. Потрібно мати на увазі, що вони зазнають тих самих загроз, що й інші методи автентифікації. По-перше, біометричний шаблон порівнюється не з результатом початкової обробки характеристик користувача, а з результатом місця порівняння. І як відомо, багато чого може трапитися на цьому шляху .... По-друге, біометричні методи не є надійнішими, ніж шаблонна база даних. По-третє, повинна бути врахована різниця між використанням біометричних даних у контрольованій зоні, моніторингом безпеки та «польовими» умовами, коли, наприклад, до пристрою сканування рогівки можна піднести муляж тощо. По-четверте, біометричні дані людини змінюються, тому базу даних шаблонів потрібно підтримувати. Це спричиняє певні проблеми як для користувачів, так і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка «діра» для біометрії є фатальною. Паролі, незважаючи на їх ненадійність, можуть бути змінені в крайньому випадку. Втрачену картку автентифікації можна анулювати та завести нову. Не можна змінити палець, око чи голос. Якщо біометричні дані пошкоджені, потрібно, принаймні, серйозне оновлення всієї системи.

Рис 2.1.3 Класифікація методів біометричної ідентифікації користувачів

2.2 Управління доступом

Традиційно контроль доступу дозволяє визначати та контролювати дії, які суб'єкти (користувачі та процеси) можуть виконувати над об'єктами (інформацією та іншими комп'ютерними ресурсами). У цьому розділі йдеться про логічне управління доступом, яке на відміну від фізичних рішень, реалізується програмними засобами. Логічне управління доступом є основним механізмом для багатокористувацьких систем, що покликані забезпечити конфіденційність та цілісність об'єктів і, певною мірою, їхню доступність (шляхом заборони обслуговування сторонніх користувачів).

Розглянемо формальну постановку проблеми в традиційному тлумаченні. Існує сукупність предметів і набір об’єктів. Завдання логічного управління доступом полягає у визначенні набору дозволених операцій для кожної пари «пре-

дмет-об'єкт» (можливо, залежно від деяких додаткових умов) та у перевірці реалізації встановленої послідовності.

Тема логічного управління доступуом є однією з найскладніших у галузі інформаційної безпеки. Той факт, що поняття об'єкта (і тим більше типи доступу) змінюється від сервісу до сервісу. Для операційної системи об’єкти містять файли, пристрої та процеси. Для файлів та пристроїв, як правило, включені дозволи на читання, запис, виконання (для програмних файлів), іноді видалення та додавання. Окремим правом може бути можливість передання прав доступу іншим суб'єктам (так зване право власності). Процеси можна створювати та знищувати. Сучасні операційні системи також підтримують інші об'єкти.

Для реляційних систем управління базами даних об’єктом є база даних, таблиця, подання, збережена процедура. Пошук, додавання, модифікація та видалення даних стосується таблиць, інші об’єкти мають різні типи доступу.

Різноманітність об'єктів та операцій, які можуть бути застосовані до них, призводять до базової децентралізації логічного управління доступом. Кожен сервіс сам вирішує, чи дозволяти певному об'єкту виконувати ту чи іншу операцію. Теоретично це відповідає сучасному об’єктно-орієнтованому підходу, але призводить до значних труднощів на практиці. Основна проблема полягає в тому, що до багатьох об’єктів можна отримати доступ за допомогою різних сервісів (можливо, доведеться подолати деякі технічні труднощі). Отже, можна не тільки використовувати СУБД для доступу до реляційних таблиць, але й безпосередньо читати файли або розділи диска, що підтримуються операційною системою (як тільки ви зрозумієте структуру зберігання об’єктів бази даних). Як результат, під час визначення матриці доступу слід враховувати не лише принцип розподілу привілеїв для кожного сервісу, але й існуючі взаємозв’язки між сервісами (потрібно забезпечити узгодженість різних частин матриці). Подібна складність виникає під час експорту / імпорту даних, коли інформація про права доступу зазвичай втрачається (оскільки це не має сенсу для нової послуги). Отже, обмін даними між різними серверами створює особливий ризик для

управління доступом, а проєктування та реалізація різнорідної конфігурації повинна забезпечувати постійне розподілення та мінімізацію прав доступу суб'єктів до об'єктів, способів експорту / імпорту даних.

Під час вирішення питання про надання доступу зазвичай аналізується така інформація:

- ідентифікатор суб’єкта (ідентифікатор користувача, адреса комп'ютерної мережі тощо) Такі ідентифікатори складають основу для довільного (або дискреційного) управління доступом;
- атрибути суб’єкта (тег безпеки, група користувачів тощо). Теги безпеки є основою для примусового (обов'язкового) управління доступом.

Матрицю доступу нерозумно зберігати у виді двовимірного масиву. Зазвичай вона зберігається у стовпцях, тобто для кожного об’єкта існує список «дозволених» суб’єктів та їх прав. Елементами списку можуть бути назви груп та шаблони суб’єктів, що є великою підмогою для адміністратора. Деякі проблеми виникають лише у разі видалення суб’єкта, коли доводиться видаляти його ім'я з усіх списків доступу; однак ця операція проводиться рідко.

На закінчення слід наголосити на важливості контролю доступу не тільки на рівні операційної системи, але й у рамках інших служб, які є частиною сучасних додатків. Саме тут на перший план виходить уніфікована політика безпеки організації, а також професійне системне адміністрування.

2.3 Протоколювання та аудит

Протоколювання - збір та накопичення інформації про події в інформаційній системі компанії. Кожен сервіс має власний набір подій, але вони можуть бути підрозділені на зовнішні - спричинені діями інших серверів, внутрішні - спричинені діями самого сервісу та клієнтські – спричинені діями користувачів та адміністраторів.

Аудит – аналіз накопичуваної інформації, який проводиться майже в реальному часі або періодично.

Реалізація протоколювання та аудиту має наступні цілі:

- забезпечення підзвітності користувачів та адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушення інформаційної безпеки;
- надання інформації для виявлення та аналізу проблем.

Забезпечення підзвітності насамперед важливе як інструмент стримання. Якщо користувачі та адміністратори знають, що вся їх діяльність зареєстрована, вони, можливо, втримаються від незаконних операцій. Якщо є підстава підозрювати якогось користувача в нечесності, його дії можна реєструвати особливо детально. Це не лише надає можливість для розслідування випадків порушення безпеки, а також скасування неправильних змін. Це забезпечує цілісність інформації.

Реконструкція послідовності подій дозволяє виявити слабкі місця в захисті сервісів, знайти винуватця вторгнення, оцінити масштаби спричиненого пошкодження та повернутися до нормальної роботи.

Виявлення та аналіз проблеми можуть допомогти покращити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переналаштувати або переконфігурувати систему та знову заміряти продуктивність тощо.

Рис. 2.3 Реєстрація та аудит

2.4 Шифрування

Один з найсильніших методів забезпечення конфіденційності та цілісності інформації - це шифрування. Цей спосіб відіграє центральну роль у програмному та апаратному забезпеченні безпеки.

Існує два основних методи шифрування, які називаються симетричними й асиметричними. У першому використовується той самий ключ для шифрування та дешифрування повідомлень. Існують також дуже ефективні симетричні методи шифрування.

Основним недоліком симетричного шифрування є те, що секретний ключ має бути відомим як відправнику, так і одержувачу. З одного боку це створює нову проблему розсилки ключів. З іншого одержувач, який має зашифроване та розшифроване повідомлення, не може засвідчити, що його було отримано від конкретного відправника, оскільки він сам міг згенерувати таке повідомлення.

У асиметричних методах використовуються два ключа. Один з них - несекретний, використовується для шифрування та може бути опублікований разом з адресою користувача, інший - секретний, використовується для розшифрування і відомий лише одержувачу. Найпопулярнішим є асиметричний Метод RSA (Raivest, Shamir, Adleman), заснований на великих операціях з великими (100-значними) простими числами.

Асиметричні методи шифрування дозволяють реалізувати електронний підпис або електронну сертифікацію повідомлення. Ідея складається з того, що відправник надсилає дві копії повідомлення - відкриту та розшифровану за допомогою секретного ключа (звичайно, дешифровка незашифрованого повідомлення насправді є формою шифрування). Одержувач може зашифрувати за допомогою відкритого ключа відправника дешифровану копію та порівняти з відкритою. Якщо вони збігаються, особистість і підпис відправника вважається встановленим.

Істотним недоліком асиметричних методів є те, що в них низька швидкість, тому їх поєднують із симетричними, при цьому не слід забувати, що асиметричні методи на 3-4 порядки повільніші симетричних. Тож для вирішення задачі розсилки ключів повідомлення спочатку симетрично шифрують відкритим асиметричним ключем отримувача, після чого повідомлення і ключ відправляються по мережі.

Криптографічні методи дозволяють надійно контролювати цілісність інформації. На відміну від традиційних методів контролю сумування, яке може протистояти лише випадковим помилкам, криптографічна контрольна сума, розрахована на основі використання секретного ключа практично виключає всі можливості непомітної зміни даних.

Останнім часом поширення набуло симетричне шифрування, засноване на використанні складових ключів. Ідея полягає в тому, що секретний ключ розділений на дві частини, які зберігаються окремо. Кожна частина не дозволяє окремо виконати дешифрування. Якщо особа підозрюється у використанні якогось ключа правоохоронними органами, вони можуть отримати половину ключа і потім діяти звичним до симетричного розшифрування методом.

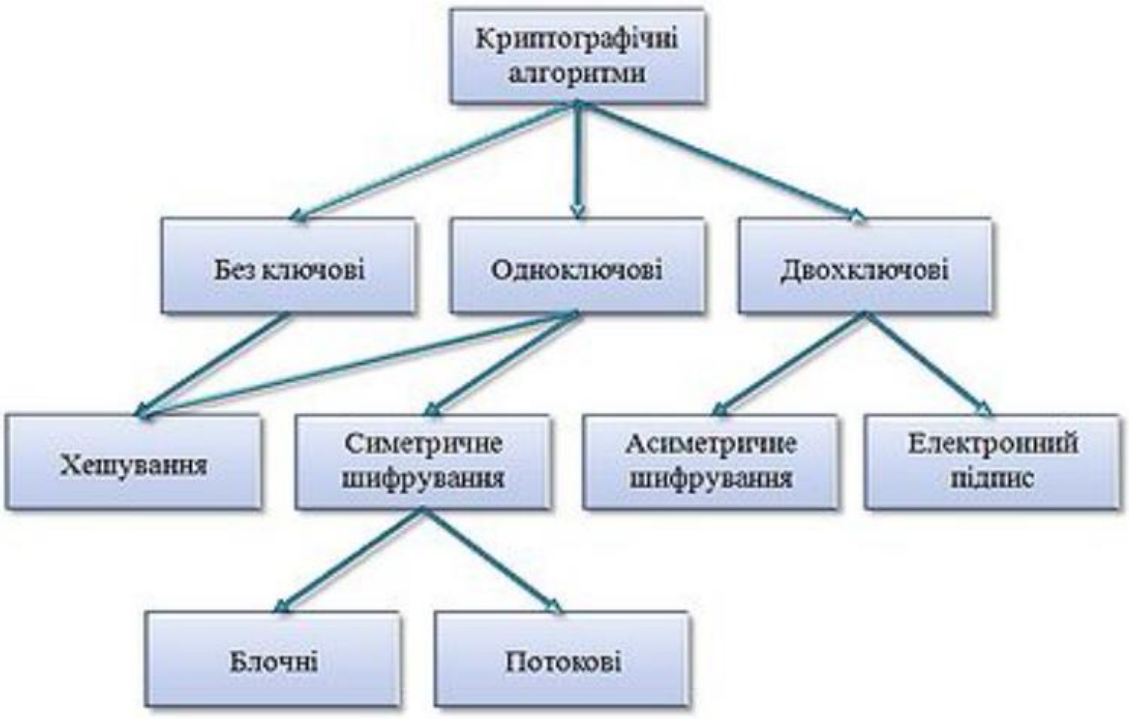


Рис. 2.4 Класифікація криптографічних алгоритмів

2.5 Екранування

Екран використовується для розрізнення доступу клієнтів з однієї групи серверів до серверів іншої групи. Екран виконує свої функції, контролюючи всі потоки інформації між двома системними групами.

У найпростішому випадку екран складається з двох механізмів, один з яких обмежує переміщення даних, а інший, навпаки, йому сприяє. У більш загальному випадку екран або напівпроникну оболонку зручно уявити собі як послідовність фільтрів. Кожен з них може затримати дані або відразу "перекинути" їх на інший бік. Крім того, допускається передання порції даних на наступний фільтр для продовження аналізу та обробка даних від імені одержувача й повернення результату відправнику.

Окрім функцій розмежування доступу, екрани здійснюють також протоколювання обмінів інформацією.

Екран, як правило, не є асиметричний, для нього визначені поняття "всередині" і "зовні". У цьому випадку задача екранування формується як захист внутрішньої області від потенційно ворожої зовнішньої. Таким чином, брандмауери встановлюються для захисту локальної мережі організації, що має доступ до такого відкритого середовища як Інтернет. Ще один приклад екрану - пристрій захисту порту, який контролює доступ до комунікаційного порту комп'ютера до і після, незалежно від усіх інших системних засобів захисту.

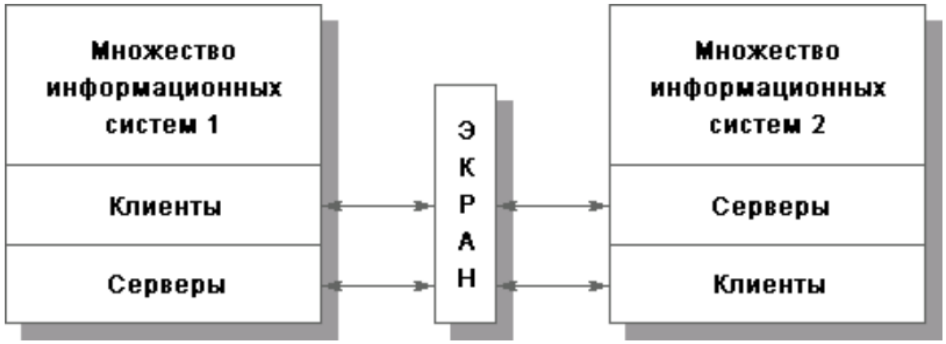


Рис. 2.5 Екран як засіб розмежування доступу

2.6 Висновки до розділу 2

У другому розділі були розглянуті основні методи забезпечення інформаційної безпеки, а саме:

- Автентифікація та ідентифікацію, їх види;
- Управління доступом;
- Протоколювання та аудит;
- Криптографічний метод;
- Екранування.

Розділ 3. РОЗРОБКА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Види структур локальної мережі

У великих агентствах існує гостра необхідність об’єднувати різних фахівців у відділи та чіткіше визначати обов’язки. Актуальність дослідження полягає в тому, що воно може запропонувати модель розвитку інформаційної інфраструктури. Важливим аспектом є побудова локальної мережі та забезпечення швидкісного доступу до глобальної мережі. Реалізація запропонованого проєкту дозволить скоротити документообіг в організації, збільшити продуктивність роботи та скоротити час обробки інформації.

Комп’ютерну мережу можна розглядати як підключення двох або більше комп’ютерів за допомогою кабельної або телефонної лінії та модему, при якому можливий обмін даними між ними. Комп’ютери, розташовані в одній кімнаті або будівлі і з’єднані між собою, називаються локальною мережею (LAN – Local Area Network). Кількість комп'ютерів, підключених до такої мережі, обмежена використовуваною кабельною системою та мережевим обладнанням. Кілька локальних комп’ютерних мереж разом утворюють кампусну мережу (CAN – Campus Area Network), наприклад, локальні мережі сусідніх будівель або будівель одного підприємства чи навчального закладу. MAN (Metropolitan Area Network) - це мережа міського рівня, до якої можуть бути підключені декілька локальних або кампусних мереж підприємств та організацій. WAN (Wide Area Network) - це широкомасштабна мережа, яка охоплює, наприклад, кілька міст, регіонів або провінцій.

CAN (Global Area Network) - це об’єднання багатьох великих комп’ютерних мереж, наприклад, на національному рівні. І нарешті, мережею всіх мереж є Інтернет, що включає всесвітню павутину, систему електронної пошти та інші системи, що зберігають та передають інформацію.

Встановлення локальної мережі забезпечує компанії наступні переваги:

- Можливість сумісного використання елементів локальної мережі працівниками;
- Швидкий доступ до необхідної інформації;
- Зберігання та резервне копіювання даних, надійність захищеної інформації;
- Використовування сучасних технології в повсякденній роботі (доступ до Інтернету, електронний документообіг тощо)

Для забезпечення стабільності роботи всіх відділів та служб, доступних у компанії, необхідно, щоб локальна мережа відповідала певним вимогам:

- Ефективність (мінімальна вартість за високої якості);
- Можливість модернізації (за необхідності до локальної мережі можна підключити додаткові пристрої без зміни технічних або програмних параметрів мережі);
- Гнучкість (збій елемента мережі не потребує переривати всю локальну мережу).

Окрім комп’ютерів працівників, локальна мережа складається з ряду взаємопов’язаних елементів. Це мережеві кабелі, маршрутизатори, контролери, панелі та пульти управління.

Не існує універсальної структури локальної мережі. Кожен проєкт розгортання локальної мережі - це ексклюзивний продукт, який розробляється з урахуванням особливостей конкретного підприємства. Однак існує три основних види структури локальної мережі.

3.1.1 Топологія «Зірка»

Переваги топології локальної мережі "Зірка" полягають у тому, що нові вузли можуть підключатися до мережі, не перериваючи інші елементи. Єдиний мінус - коли HUB виходить з ладу. Це порушує роботу всієї локальної мережі. Можливість підключення нових станцій не перериваючи роботу всієї системи, а також відносно низька вартість цього типу локальної мережі сприяли її популярності.

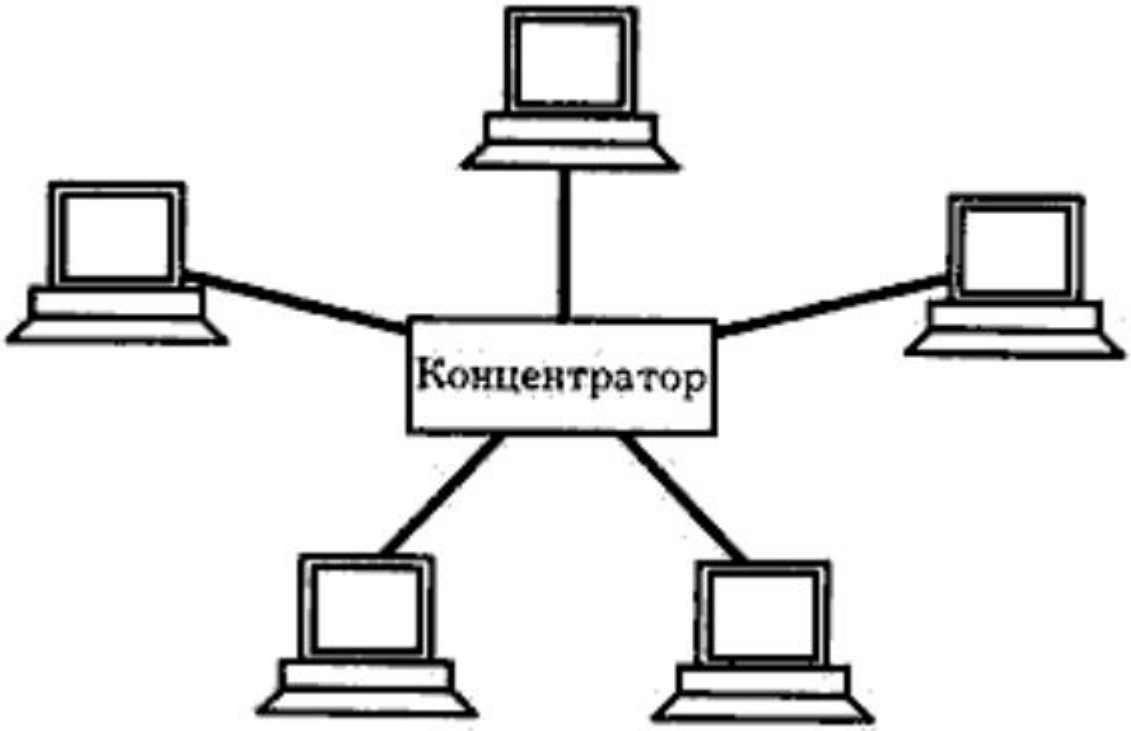


Рис 3.1.1 Топологія «Зірка»

3.1.2 Топологія «Кільце»

При такій структурі локальної мережі всі комп’ютери підключені послідовно. Сигнал передається в одному напрямку навколо кільця, кожен комп’ютер виконує роль підсилювача. Недоліками цієї структури є відносно низька швидкість передачі даних з одного комп'ютера на інший, а також переривання всієї локальної мережі, коли хоча б один підключений до неї комп'ютер виходить з ладу.

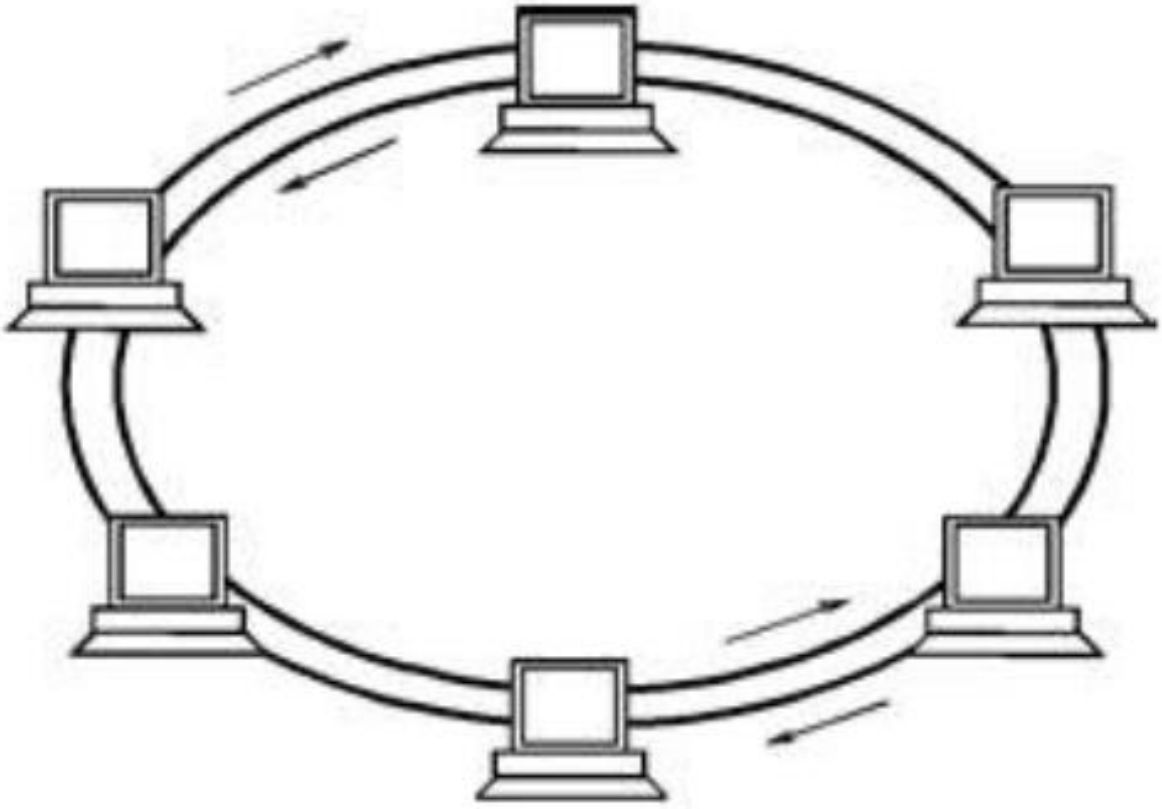


Рис 3.1.2 Топологія «Кільце»

3.1.3 Топологія «Шина»

За допомогою топології локальної мережі «шина» кожен комп'ютер підключений до загального кабелю - шини даних. Основним недоліком є залежність усіх комп’ютерних комунікацій від одного кабелю. Якщо локальна мережа розроблена відповідно до такої топології, повинна бути забезпечена цілісність шини; на цьому компоненті не можна заощадити. Крім того, якщо виникає необхідність підключення нового комп'ютера, то під час встановлення зв'язок між комп'ютерами через локальну мережу повинен бути перерваний.

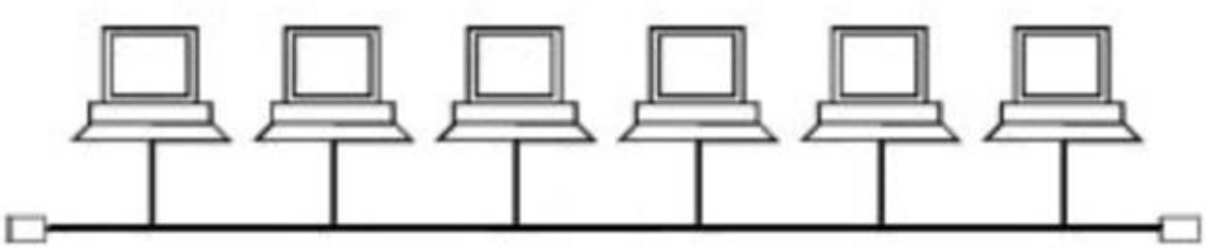


Рис 3.1.3 Топологія «Шина»

Хоча кожна топологія локальної мережі має свої недоліки, можна реалізувати проєкт, який повністю відповідає унікальним потребам компанії. Складні багатошарові локальні мережі зазвичай використовують кілька топологій. Так, наприклад, комп'ютери одного відділу підключені за типом "Зірка", комп'ютери у другому відділі з'єднані послідовно, а всі ПК у наступних відділах підключені до загальної шини. Ця топологія називається топологією деревоподібною. Крім того, комп’ютери кожного відділу (або поверху) можуть мати окремий сервер. Розділення всіх комп’ютерів у локальній мережі згідно з топологією дерева - це рішення, яке забезпечує зручне адміністрування всієї системи.

Незалежно від обраного методу організації локальної комп'ютерної мережі, слід мати на увазі, що її функціональність та надійність залежать не тільки від топології, а й від надійності обладнання та рівня підготовки фахівців, які беруть участь в установці та налаштуванні локальної мережі. Очевидно, що монтаж повинен виконуватися компетентними фахівцями.

Також були розглянуті декілька видів побудови топології локальної мережі та важливість її детального проєктування для забезпечення найбільш вдалого захисту конфіденційної інформації.

3.2 Оцінка ризиків спроєктованої системи безпеки

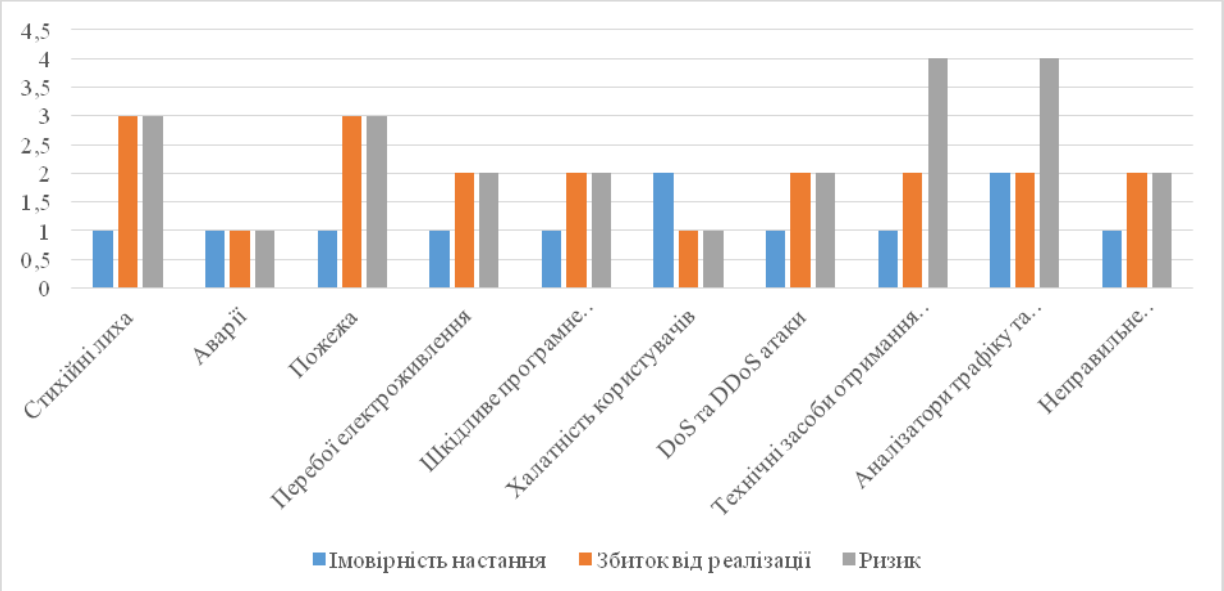
Серед загроз, крім відносно стандартних, таких як стихійні лиха, аварії, пожежі; ненавмисні помилки користувачів; перебої електроживлення; шкідливе програмне забезпечення; халатність користувачів; вказано й більш притаманні для конкретного підприємства (пов'язані зі специфікою роботи, розповсюдженістю комп'ютерної мережі, наявними ресурсами та іншими вхідними даними).

У таблиці присутні коефіцієнт імовірності настання і коефіцієнт збитку від реалізації кожної загрози за 3-х бальною шкалою. Добуток цих складових дозволить визначити ризик. Розраховано загальну суму ризиків. На основі отриманих даних виділено три типи ризику: низький (1,2), середній (3,4), високий (6,9). Побудована діаграма оцінки ризиків за категоріями.

Таблиця 1. Оцінка ризиків існуючої системи безпеки підприємства.

Назва загрози	**Імовірність настання**	**Збиток від реалізації**	**Ризик**
Стихійні лиха	1	3	3
Аварії	1	1	1
Пожежа	1	3	3
Перебої електрожив-	1	2	2

лення			
Шкідливе програмне забезпечення	1	2	2
Халатність користувачів	2	1	1
DoS та DDoS атаки	1	2	2
Технічні засоби отримання інформації	1	2	4
Аналізатори трафіку та прослуховуючі програми	2	2	4
Неправильне налаштування апаратури	1	2	2
Сума ризиків:			**24**

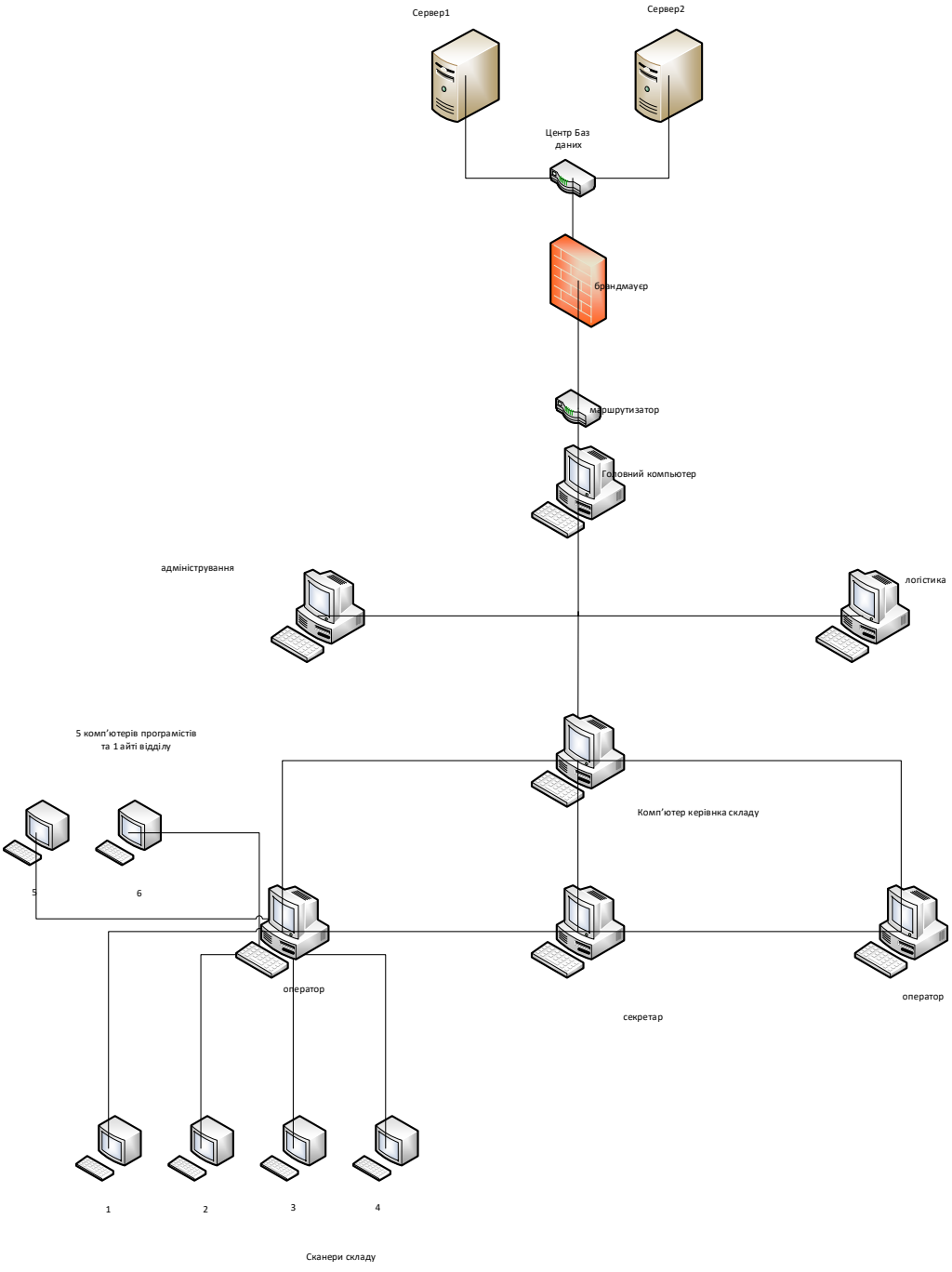


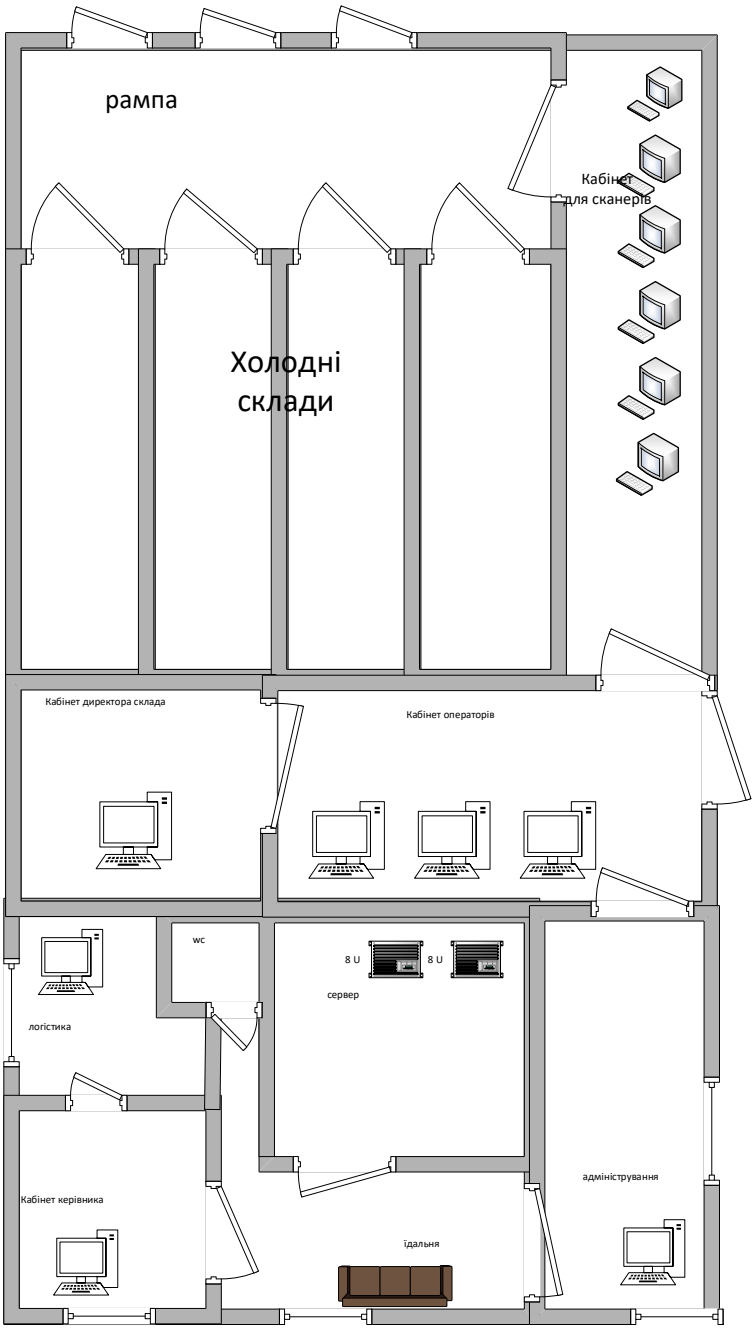
На основі інформації в першому та другому розділі було виявлено ризики інформаційної безпеки підприємства. Після впровадження запропонованих заходів безпеки сума риків зменшилась, що дає змогу стверджувати про доцільність їх використання. Хоча ризики і залишаються, слід зазначити, що домогтися стовідсоткової безпеки неможливо.

3.3 Розробка системи безпеки локальної мережі

3.3.1 Проєктування локальної мережі

За допомогою програми Visio спроєктував локальну мережу вигаданого підприємства. При цьому врахував та показав розміщення в будівлі всього обладнання даної мережі.





Також детально вказав усе обладнання мережі, а саме:

- усі комп’ютери мережі:

У мережі знаходиться 7 комп’ютерів: 1 головний, який розташований у кабінеті власника фірми; 2 комп’ютери, які обслуговують склади і забезпечують інформацією стосовно заказів та підтримку працездатності системи; 2 комп’ютери операторів, 1 комп’ютер директора складу, 1 - у секретарів.

- усі пристрої (зокрема, й мережеві), необхідні для функціонування локальної та глобальної мереж:

2 сервери для надійності та стабільної працездатності системи у разі збою 1-го сервера або профілактичних робіт; 1 центр баз даних для з'єднання 2-х серверів та направлення потрібної інформації в її місце. Сканери потрібні для сканування товару на складі, для контролю кількості товару та внесення його в базу даних. Маршрутизатор, що роздає інтернет для комп'ютерів .

- вказано за якою технологією організована локальна мережа фірми:

Fast Ethernet (Швидкий Ethernet) - набір стандартів Ethernet для пакетного передання даних з номінальною швидкістю 100 Мбіт/с, що в 10 разів швидше за початкову для Ethernet швидкість у 10 Мбіт/с

- все обладнання, яке забезпечує на даний момент захист інформації в мережі даної фірми:

Брандмауер для захисту з'єднання та забезпечення цілісності та конфіденційності інформації й доступу до серверів та виходу до інтернету.

Маршрутизатор:

- Системний журнал;
- SNTP (англ. Simple Network Time Protocol) - протокол синхронізації часу по комп'ютерній мережі. Є спрощеною реалізацією протоколу NTP . Використовується у вбудованих системах і пристроях, що не вимагають високої точності, а також у призначених для користувача програмах точного часу. SNTP протокол є окремим випадком NTP протоколу з деякими спрощеннями. Таким чином SNTP клієнт може звертатися до будь-якого NTP сервера, як до сервера SNTP.
- Моніторинг роботи центрального процесора;
- Traceroute - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передання даних у залежності

від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE;

- SNMP - стандартний інтернет-протокол для управління пристроями в IP-мережах на основі протоколів TCP / UDP. До підтримуючих SNMP пристроїв відносяться маршрутизатори, комутатори, сервери, робочі станції, принтери тощо;
- SNMP-пастка (SNMP-trap) - це особливий сигнал, що відправляється пристроєм з підтримкою протоколу SNMP. Як правило, подібні сигнали відправляються пристроями для того, щоб оповістити адміністратора мережі про настання якихось критичних подій. Наприклад, деякі види джерел безперебійного живлення (UPS) можуть відправляти SNMP-trap у разі, коли обладнання переходить у режим харчування від батареї UPS. Як правило, подібні ситуації вимагають негайного втручання обслуговуючого персоналу і тому пристрій сам ініціює відправку сигналу по протоколу SNMP. Ще як приклад можна навести деякі моделі датчиків відкриття приміщень і стійок обладнання. Ці датчики можуть бути підключені до локальної мережі і підтримувати відправку SNMP-trap в критичних ситуаціях, таких як несанкціоноване відкриття дверей, наприклад.
- RMON (англ. Remote Network Monitoring - дистанційний моніторинг мережі) - протокол моніторингу комп'ютерних мереж, розширення SNMP, розроблене IETF. В основі RMON, як і в основі SNMP, лежить збір і аналіз інформації про характер даних, що передаються по мережі. Як і в SNMP, збір інформації здійснюється апаратно-програмними агентами, дані від яких надходять на комп'ютер, де встановлено додаток управління мережею. Відмінність RMON від свого попередника полягає, в першу чергу, у характері збірки: якщо в SNMP ця інформація характеризує тільки події, що відбуваються на тому пристрої, де

встановлений агент, то RMON вимагає, щоб ці дані характеризували трафік між мережевими пристроями.

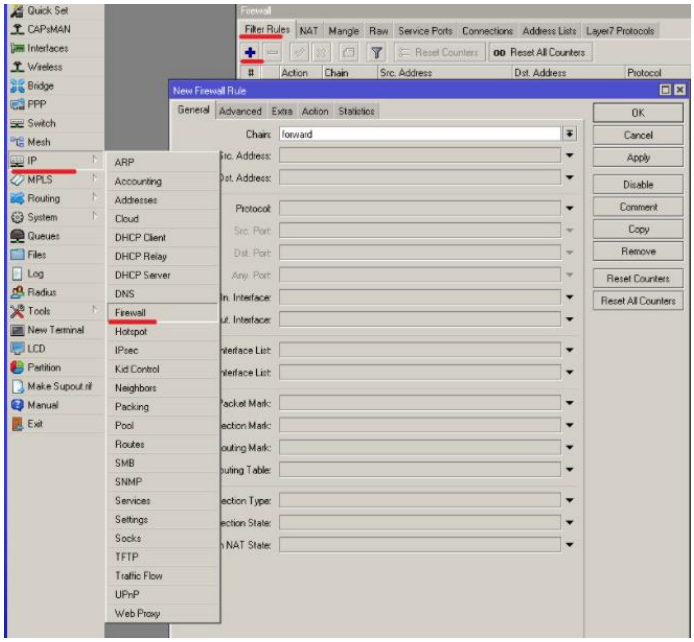
- Link Layer Discovery Protocol (LLDP) - протокол канального рівня, що дозволяє мережевому обладнанню сповіщати обладнання, яке працює в локальній мережі, про своє існування і передавати йому характеристики, а також отримувати від нього аналогічні відомості.
- Якщо після отримання підтвердження (DHCPACK) від сервера клієнт виявляє, що вказана сервером адреса вже використовується в мережі, він розсилає широкомовне повідомлення відмови DHCP (DHCPDECLINE), після чого процедура отримання IP-адреси повторюється. Використання IP-адреси іншим клієнтом можна виявити, виконавши запит ARP .

3.3.2 Встановлення Firewall на маршрутизатор

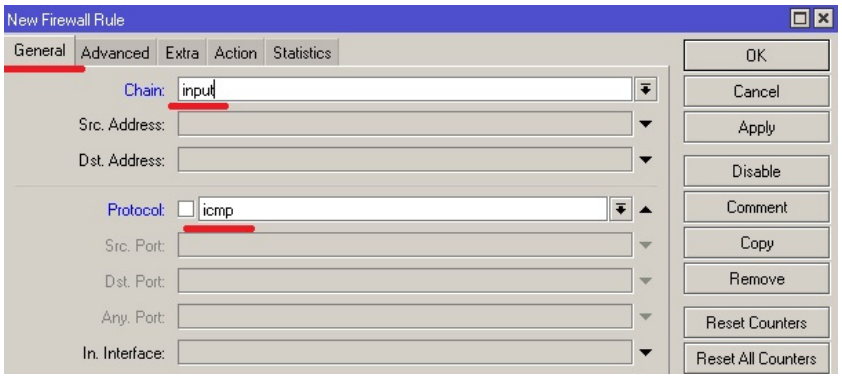
Спочатку потрібно налаштувати безпеку маршрутизатора, для цього зробимо наступні кроки:

- Заборонимо пінгувати наш пристрій;
- Заборонимо доступ до маршрутизатора всім, крім учасникам локальної мережі та дозволених ip адресів;

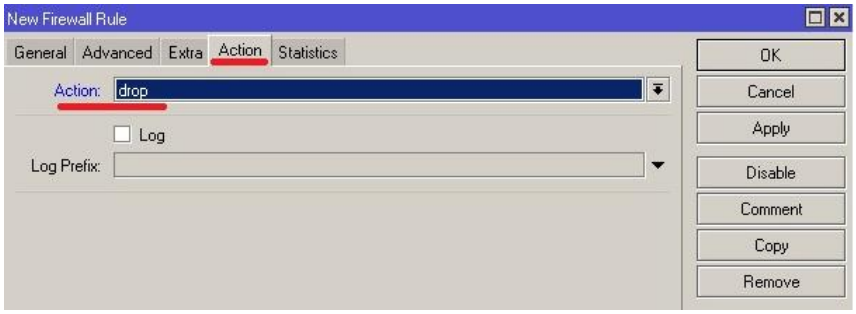
Для налаштування підключаємося до маршрутизатора за допомогою додатка winbox, далі меню IP-Firewall. Вкладка Filter Rules, натискаємо додати:



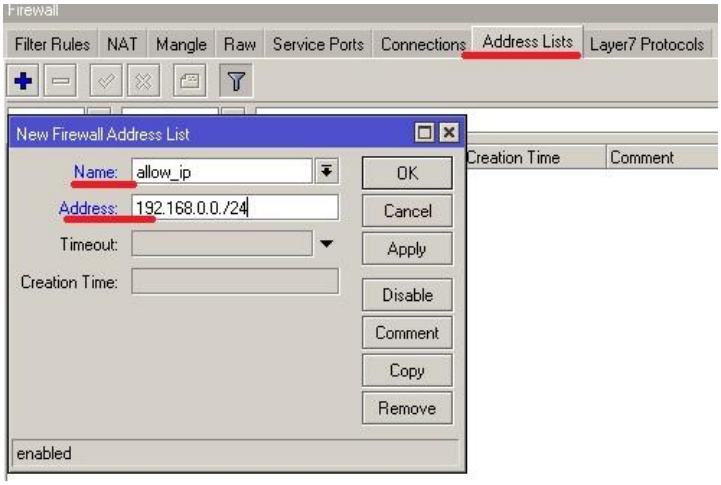
Забороняємо пінг на маршрутизатор, для цього на вкладці general, chain вибираємо input protocol icmp:



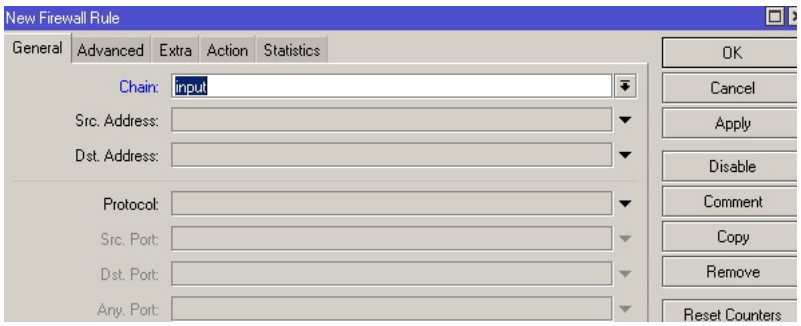
На вкладці Action вибираємо drop



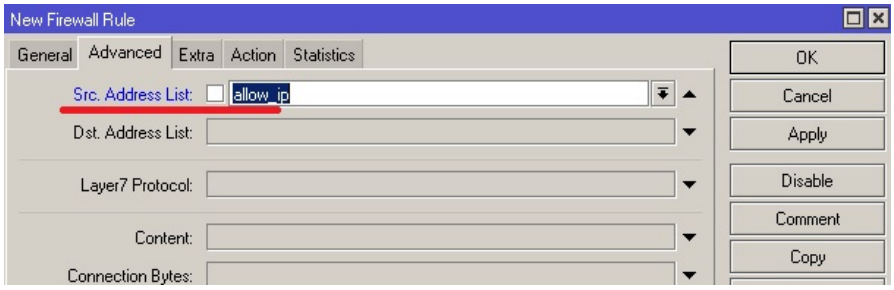
Забороняємо доступ до управління маршрутизатором. Спочатку налаштовуємо лист з адресами, які мають доступ, далі переходимо до IP Firewall, вкладка Address Lists та додаємо новий лист:



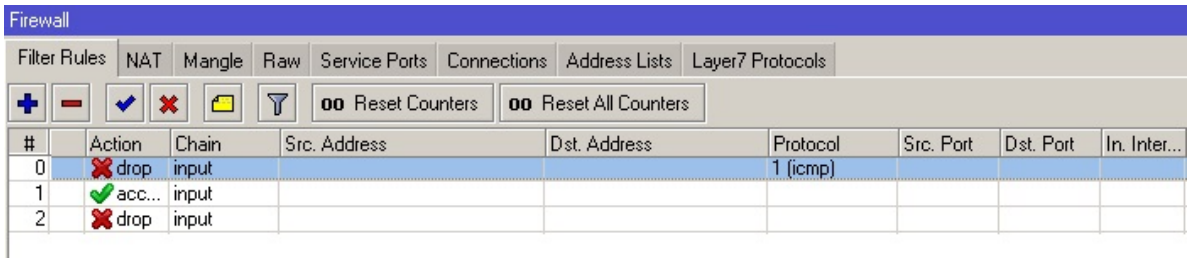
Далі створюємо нове правило та знову переходимо до Filter rules та додаємо його:



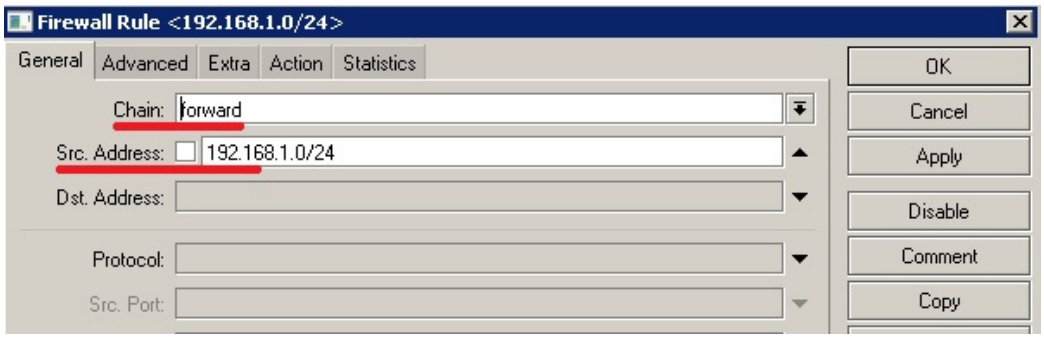
Далі переходимо до вкладки Advanced і в якості Src. Address List вибираємо створений щойно лист:



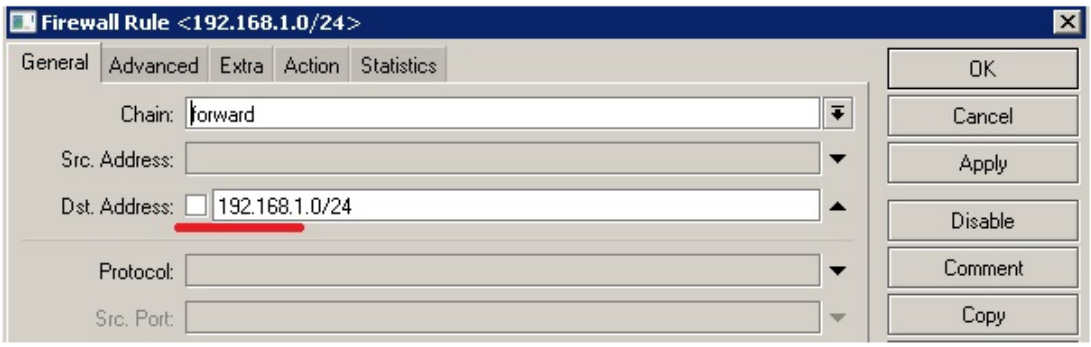
Далі забороняємо вхідні повідомлення. Додаємо правило на chain input і в дії ставимо drop:



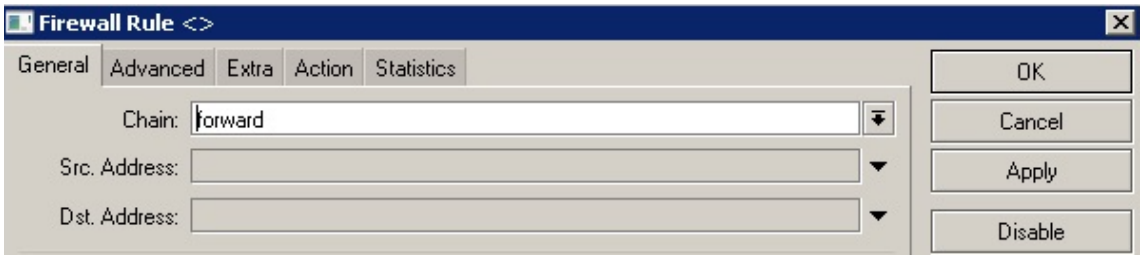
Розглянемо ситуацію, коли нам потрібно дати доступ тільки конкретній мережі. Для цього створюємо два правила в chain forward. Перше правило дозволяє вихідний трафік з нашої мережі:



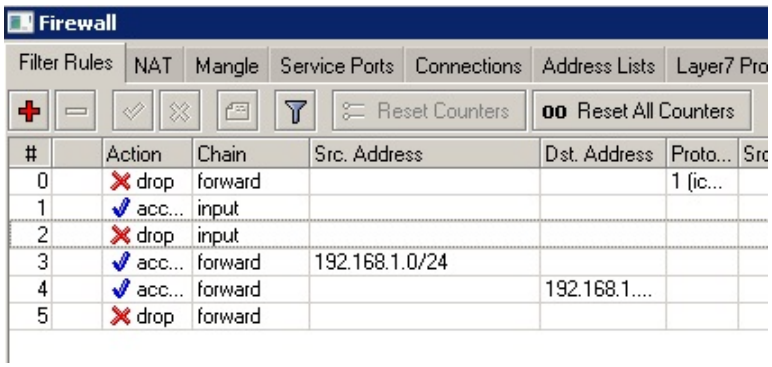
Action ставимо accept. Можна вказати Src. Address або використати Address Lists, як ми робили раніше. Наступним правилом дозволяємо вхідний трафік пакетів до нашої мережі:



Наступним правилом забороняємо всі інші мережі:



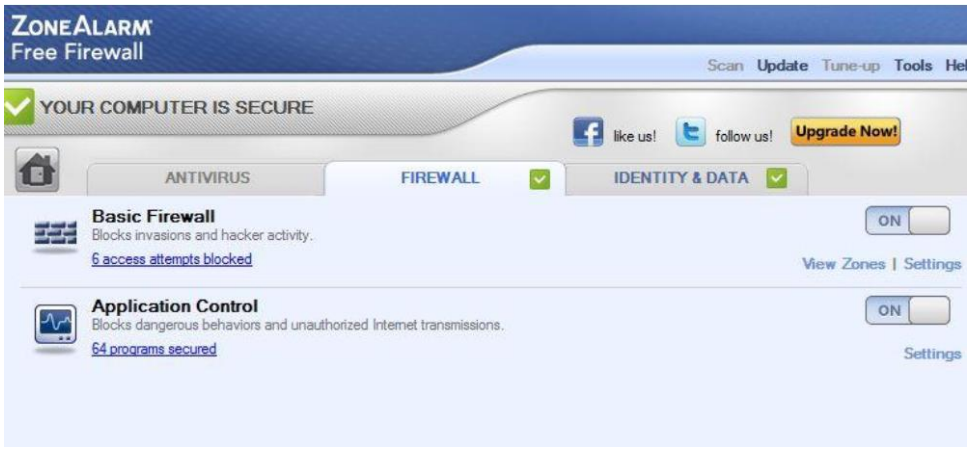
Action вибираємо drop. В результаті вийшло наступне:



3.3.3 Встановлення Firewall на комп'ютер

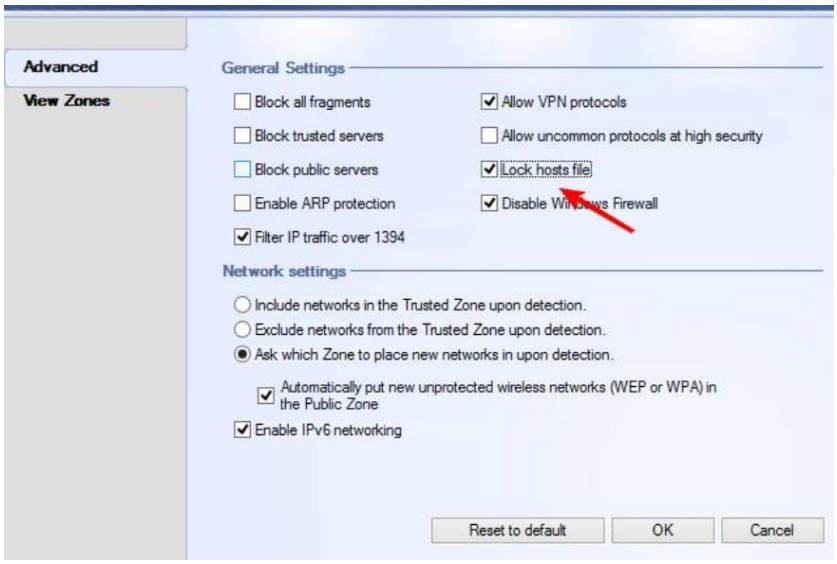
Насправді у Windows є свій влаштований брандмауер, але толку від нього мало. Розглянемо непоганий Firewall Zone Alarm. Головне меню:

Перейдемо до налаштувань:



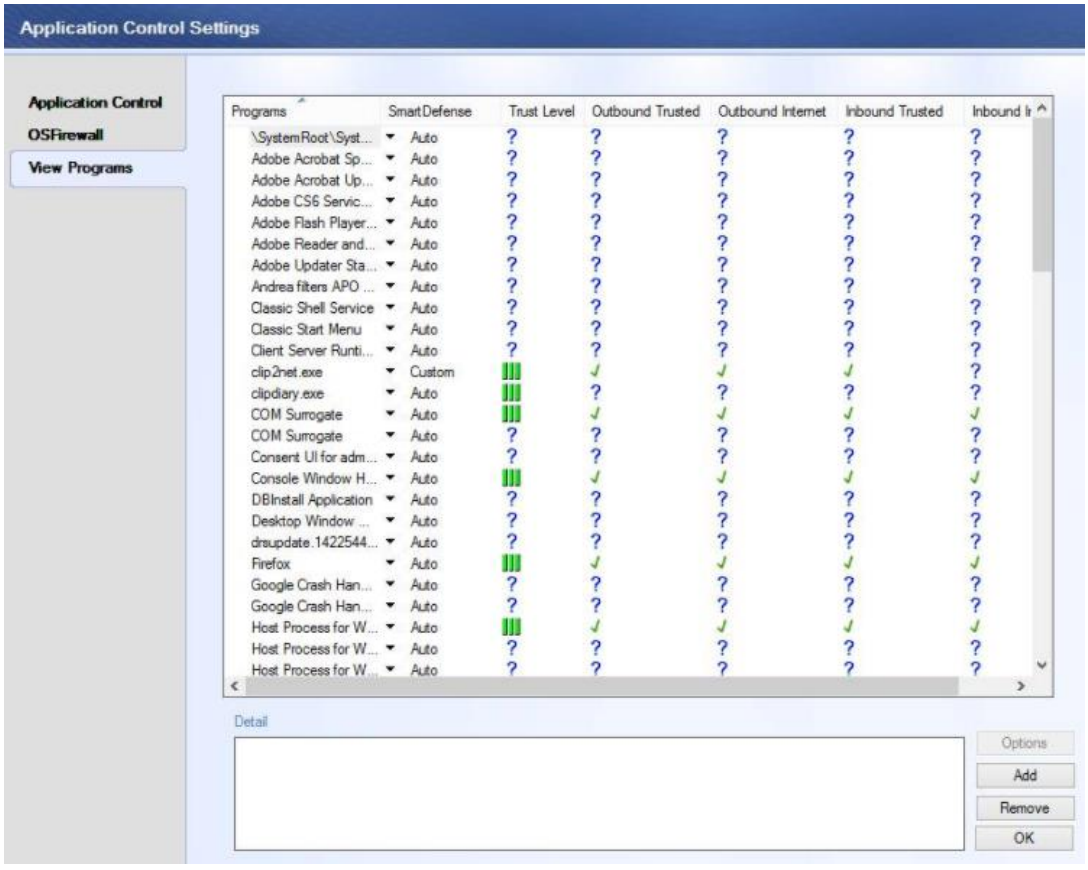
Тиснемо View Details та відкриваємо вкладку з розділами, далі тиснемо першу кнопку Settings навпроти розділу Basic Firewall:

Тиснемо Advanced Settings



Ставимо галочку Lock hosts file, що захищає цей файл від перезапису, далі тиснемо ok та переходимо до другої Settings:

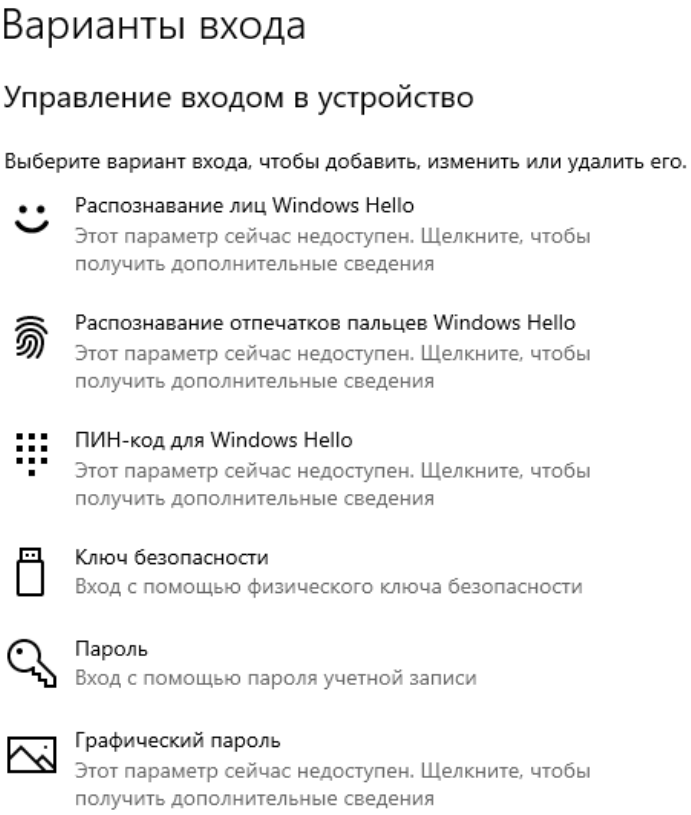
Тиснемо View Programs:



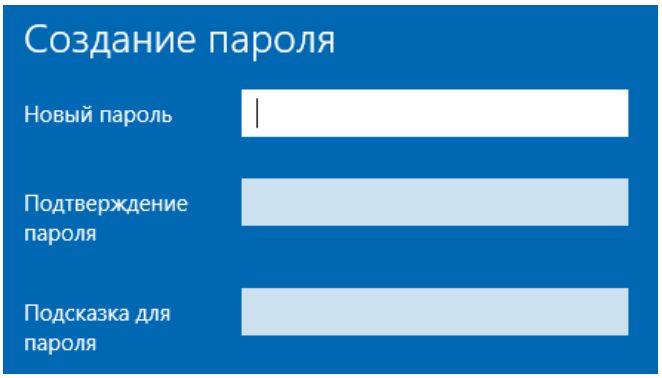
Ця вкладка відповідає за допуски в інтернет усіх програм на комп’ютері. Якщо її немає, можна додати.

3.3.4 Способи автентифікації Windows

Для того, щоб інша особа не змогла зайти до вашого облікового запису та не наробити шкоди, існують декілька способів автентифікації, в нашому випадку це ключ безпеки або пароль:

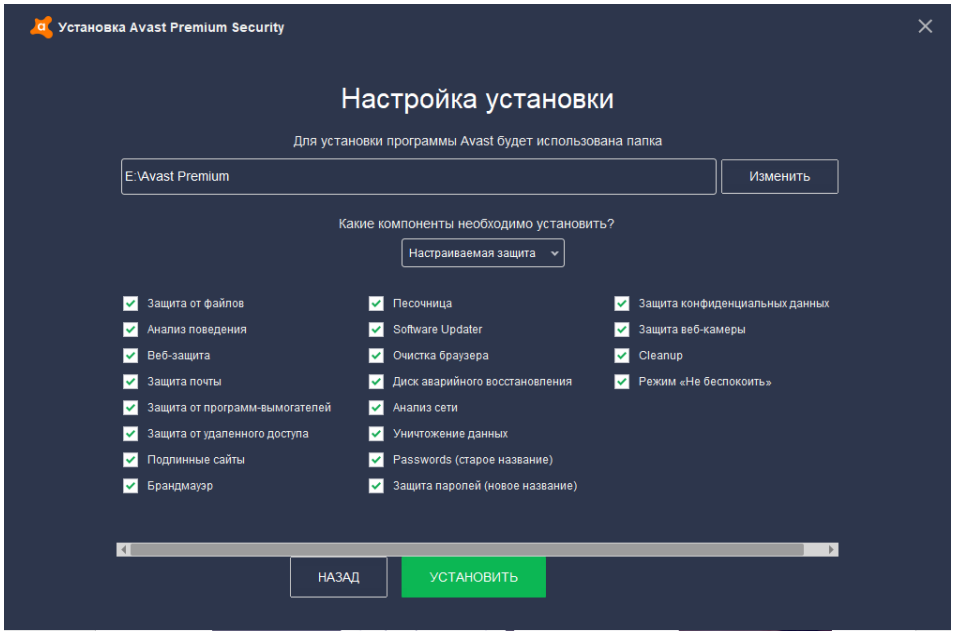


Найпрактичнішим способом є створення паролю, легко і швидко:

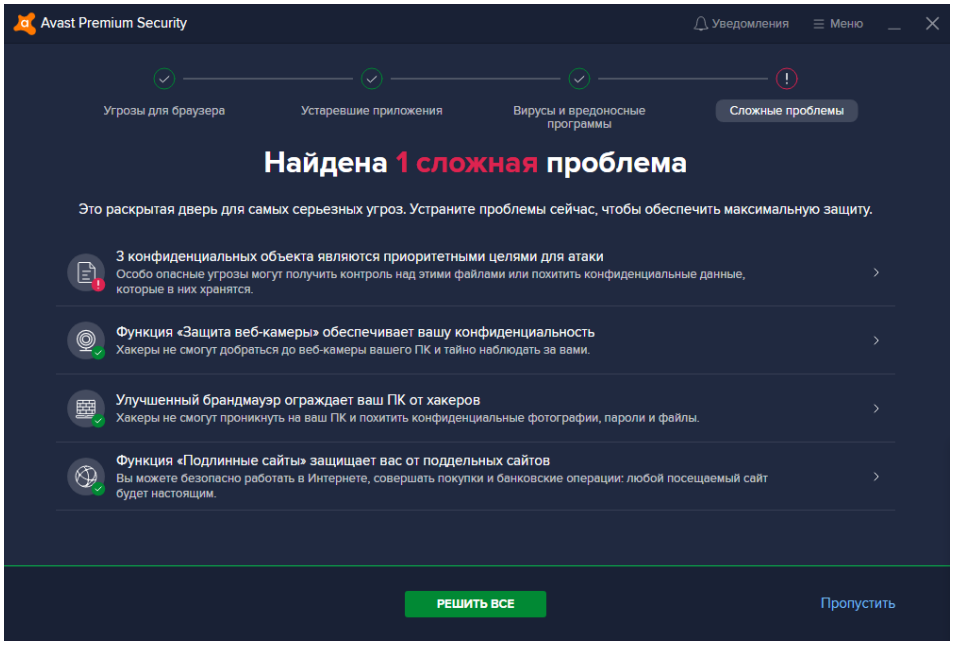


3.3.5 Встановлення антивірусу

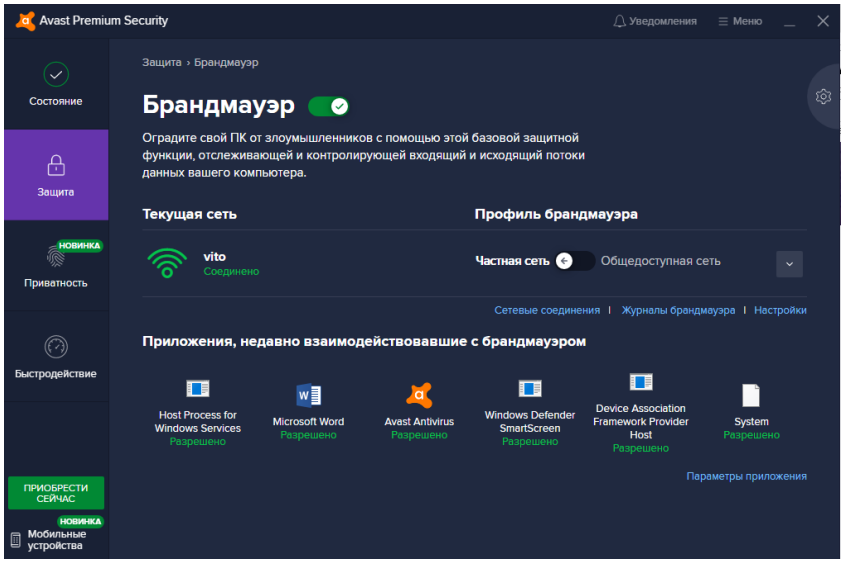
Налаштування встановлення:



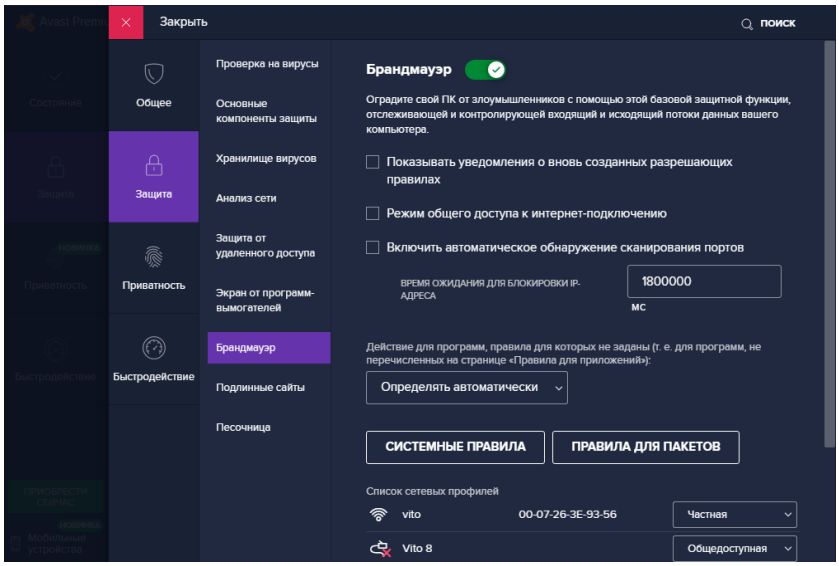
Одразу після встановлення програми було запропоновано просканувати систему:



Меню брандмауера:



Налаштування:



3.4 Висновки до розділу 3

У третьому розділі були розглянуті види топології локальних мереж, проаналізовані та оцінені ризики системи безпеки, також спроєктовано локальну обчислювальну мережу підприємства, описано обладнання та його характеристики, продемонстровані роботи Firewall на маршрутизаторі та комп'ютері, метод автентифікації користувача та функції антивірусу.

ВИСНОВКИ

Дипломна робота присвячена розробці системи забезпечення інформаційної безпеки локальної мережі. Були розглянуті ймовірні загрози системі захисту конфіденційної інформації, розглянуті методи щодо запобігання цим загрозам, рекомендації для зменшення шансів витоку секретної інформації.

Розглянуто основні види топології для побудування локальної мережі, створено систему інформаційної безпеки, а саме: спроєктовано локальну мережу зі вказанням усієї апаратури та їх характеристики та продемонстровано роботу методів захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дронов, В. Современные методы защиты информации / Дронов В. – Москва: изд. БХВ-Петербург, 2009. – 544 с.
2. Холмогоров, В. Уязвимости в сети / В. Холмогоров. – СПб.: Питер, 2012. – 272 с.
3. Хофман, Л. Дж. Современные методы защиты информации / Л. Дж. Хофман. – Москва: Советское радио, 1994. – 264 с.
4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К.: ДСТСЗІ СБ України, 1999. – 12 с.
5. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / А.Г. Корченко, В.П. Щербина, С.В. Казмирчук // Захист інформації – 2012. – №1. – С. 126-139.
6. Вихорев, С. Как определить источники угроз / С. Вихорев, Р. Кобцев // Открытые системы. – 2002. – №07-08. – С. 43.
7. Основы информационных технологий. [Електронний ресурс]. – Режим доступу до ресурсу: http://master.cmc.msu.ru/files/Laponina-1.pdf
8. Левин, В. К. Защита информации в информационно-вычислительных системах и сетях / В. К. Левин // Программирование. – 2009. – №3. – С. 67.
9. НД ТЗІ 2.5-004-99 — Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу‖. [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835
10. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. – Феникс, 2008 г.

11. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса «Основы информационной безопасности». – Интернет Университет Информационных Технологий, 2010г.
12. Infowatch. Глобальні дослідження витоків інформації починаючи з 2007 року. 2018. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.infowatch.ru/analytics/leaks_monitoring
13. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Санкт Петербург: Питер, 2016. 992 с.
14. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. Санкт Петербург: Изд-во Политехн. ун-та, 2009. 126 с.
15. Захист інформації в локальних мережах. [Електронний ресурс]. – Режим доступу до ресурсу: https://uadoc.zavantag.com/text/8659/index-1.html?page=2
16. Кулаков Ю. А., Луцкий Г. М. Компьютерные сети. – К.: Юниор, 1998. – 380 с.
17. Бэрри Нанс. Компьютерные сети / Пер. с англ. – К.: Бином, 1995. – 214 с.
18. Захист інформації в локальних обчислювальних мережах. [Електронний ресурс]. – Режим доступу до ресурсу: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-setyakh/v-lokalnykh-vychislitelnykh-setyakh/
19. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов – М: ДМК Пресс, 2010. – 314 с.
20. Соколов А.В., Защита информации в распределенных корпоративных сетях и системах / — М.: ИЛ, 2015. — 656 с.
21. Рассел Д., Локальная вычислительная сеть / — М.: Книга по Требованию, 2012. — 102 с.
22. Нанс Б.А, Компьютерные сети / — М.: Наука, 2014. — 400 с.
23. А.В. Гаврилов «Локальные сети ЭВМ». — М.: Издательство «Мир», 2007