Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо–кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Розробка рекомендацій щодо захисту інформації в локальній мережі*

Виконавець: студент *2* **курсу, групи** *КБм–21*

Клочко Вікторія Євгенівна
(підпис) (прізвище ім'я по–батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	*Лукова–Чуйко Н.В.*		
Рецензент			
Нормоконтроль			

Київ
2021

Міністерство освіти і науки України

Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова–Чуйко Н.В.

«_____»_____ 20__ року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм–21* (група) *Клочко Вікторії Євгенівні* (прізвище ім'я по–батькові)

Тема дипломної роботи *Розробка рекомендацій щодо захисту інформації в локальній мережі*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 2 від 08.10.2020

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процес захисту інформації , яка обробляється в каналах локальної мережі.

Предмет досліджень засоби та заходи захисту інформації в локальних мережах.

Мета розробка рекомендацій щодо застосування механізмів, та засобів захисту інформації в локальній мережі.

Вихідні дані для проведення роботи Технології локальних мереж, засоби захисту локальних мереж.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення заходів, необхідні для захисту інформації в локальній мережі; розроблення рекомендації щодо захисту інформації в локальній мережі.

Практична цінність Покращення рекомендацій щодо захисту інформації в локальній мережі.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок–кінець)
Розробка плану для досягнення мети роботи	12.10.2020 – 16.10.2020
Аналіз літературних джерел	19.10.2020 – 10.12.2020
Проаналізувати можливі атак на ресурси в локальній мережі	25.01.2021 – 12.02.2021
Проаналізувати існуючі засоби захисту інформаційних ресурсів	15.02.2021 – 26.02.2021
Розроблення рекомендацій	05.04.2021 – 16.04.2021
Оформлення і друк пояснювальної записки	19.04.2021 – 07.05.2021
Підготовка до захисту дипломної роботи	11.05.2021 – 17.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через викрадення, перетворення інформації.

Соціальний ефект Покращення рекомендацій щодо захисту інформації в локальній мережі.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

УДК 004.056.53

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Розробка рекомендацій щодо захисту інформації в локальній мережі»: 88 сторінок, 3 рисунки, 1 додаток та 1 таблиця, 33 літературних джерела.

Об’єкт дослідження – процес захисту інформації , яка обробляється в каналах локальної мережі.

Мета роботи – розробка рекомендацій щодо застосування механізмів, та засобів захисту інформації в локальній мережі.

Методи дослідження – спостереження; аналіз методів доступу до мережі; аналіз методів захисту інформації в локальній мережі.

Наукова новизна одержаних результатів: удосконалення заходів, необхідних для захисту інформації в локальній мережі; розроблення рекомендації щодо захисту інформації в локальній мережі.

Завдання дослідження – провести аналіз можливих атак на інформаційні ресурси в локальних мережах та проблем безпеки локальної мережі. Встановити особливості та напрямки використання різних засобів захисту інформації.

Актуальність теми: Захист інформації в будь–якій локальній мережі має першочергове значення, оскільки більшість цих мереж підключаються до Інтернету для комерційної або дослідницької діяльності. З розвитком інформаційних технологій завдання забезпечення інформаційної безпеки, і зокрема конфіденційності, набуває все більшої значущості. Вона вкрай важлива для будь–якої організації. Тому виникає необхідність аналізувати загрози безпеці інформації в локальних мережах та розробляти рекомендації щодо застосування заходів та засобів захисту інформації в локальній мережі.

Ключові слова: локальна мережа, атаки на мережу, засоби захисту мережі, інформаційні ресурси.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЗЗІ – Засоби захисту інформації

ОС – Операційна система

ПЗ – Програмне забезпечення

ACL – Access Control List

ARP – Address Resolution Protocol

CSMA / CD – Carrier Sense Multiple Access with Collision Detection

DDoS – Distributed Denial of Service

DLC – Data Link Control

DMZ – Demilitarized Zone

DNS – Domain Name System

FDDI – Fiber Distributed Data Interface

FTP – File Transfer Protocol

HTTP – HyperText Transfer Protocol

IP – Internet Protocol

IEEE – Institute of Electrical and Electronics Engineers

ICMP – Internet Control Message Protocol

IDS – Intrusion Detection System

ISO – International Organization for Standardization

ISP – Internet Service Provider

LAN – Local Area Network

LLC – Logical link control

MAC – Media Access Control

MAN – Metropolitan Area Network

MAU – Multistation Access Unit

NetBIOS – Network Basic Input/Output System

NIDS – Network Intrusion Detection System

OSI – Open Systems Interconnection model

PAN – Personal Area Network

PLC – Power line communication

PPP – Point–to–Point Protocol

PPTP – Point–to–Point Tunneling Protocol

PPPoE – Point–to–point protocol over Ethernet

P2P – Peer–to–peer

RFC – Request for Comments

SMTP – Simple Mail Transfer Protocol

SNA – Systems Network Architecture

SSL – Secure Sockets Layer

TCP – Domain Name System

UDP – User Datagram Protocol

USB – Universal Serial Bus

VPN – Virtual Private Network

WAN – Wide Area Network

WEP – Wired Equivalent Privacy

WPA – Wi–Fi Protected Access

ВСТУП

Захист інформації в будь–якій локальній мережі має першочергове значення, оскільки більшість цих мереж підключаються до Інтернету для комерційної або дослідницької діяльності. Сучасні конструкції мереж реалізують три рівня довіри: найбільш надійний, менш надійний і найменш надійний:

- Користувачі, яким довіряють, належать до локальної мережі. Ці користувачі повинні пройти автентифікацію у централізованого адміністратора для доступу до ресурсів в мережі.
- Менш довірені користувачі можуть належать до локальної мережі, зовнішні користувачі, які пройшли перевірку автентичності для доступу до таких ресурсів, як електронна пошта та веб–служби.
- Найменш довірені користувачі – це користувачі, які не пройшли перевірку автентичності, більшість з них просто переглядають ресурси в Інтернеті без злого умислу. Звичайно, деякі сканують ресурси з метою злому і крадіжки даних.

Цілі мережевої безпеки в локальній мережі:

- конфіденційність: тільки авторизовані користувачі мають доступ до мережі;
- цілісність: дані не можуть бути змінені неавторизованими користувачами;
- доступність: безпека повинна бути розроблена таким чином, щоб авторизовані користувачі мали безперервний доступ до даних.

Отже, виходячи з вище сказаного існує необхідність аналізувати рівні захисту інформації в локальних мережах і створювати надійні комплексні методи захисту інформації в мережах.

Метою роботи є розробка рекомендацій щодо застосування механізмів, та засобів захисту інформації в локальній мережі.

Завдання дослідження – провести аналіз можливих атак на інформаційні ресурси в локальних мережах та проблем безпеки локальної мережі. Встановити особливості та напрямки використання різних засобів захисту інформації.

Об’єкт дослідження – процес захисту інформації , яка передається по каналах локальної мережі.

Предмет досліджень – засоби та заходи захисту інформації в локальних мережах.

Методи дослідження – спостереження; аналіз методів доступу до мережі; аналіз методів захисту інформації в локальній мережі.

Наукова новизна одержаних результатів: удосконалення заходів, необхідні для захисту інформації в локальній мережі; розроблення рекомендації щодо захисту інформації в локальній мережі.

Практична цінність полягає в покращенні рекомендацій щодо захисту інформації в локальній мережі.

Апробація роботи була на конференції: Information Technology and Interactions (IT&I–2020), тема роботи: «Collective defense of corporate networks against computer attacks» [1]. Також на IV Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», тема роботи: «Забезпечення безпеки локальних мереж на підприємстві» [2].

РОЗДІЛ 1
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ

1.1 Визначення локальної мережі. Основні схеми локальних мереж

Локальна мережа – це сукупність маршрутизаторів, комутаторів, точок доступу, кабелів, які складають комп'ютерну мережу. Всі ці компоненти комп'ютерної мережі дозволяють пристроям підключатися до веб–серверів і внутрішніх серверів, які знаходяться в межах однієї будівлі. А також дозволяють під'єднатися до інших локальних мереж через глобальні мережі (WAN), або міської мережі (MAN). Зазвичай пристрої, які знаходяться в локальній мережі, такі як персональні комп'ютери та робочі станції, обмінюються файлами і можуть бути доступними один одному через одне підключення до мережі Інтернет.

Такий компонент в локальні мережі, як маршрутизатор призначає IP–адреси кожному пристрою в мережі і забезпечує спільне Інтернет–з'єднання між усіма підключеними пристроями. Мережевий комутатор підключається до маршрутизатора і забезпечує зв'язок між підключеними пристроями, але не перетворює IP–конфігурацію локальної мережі або спільне використання підключень до Інтернету. Комутатори – ідеальні інструменти для збільшення кількості портів LAN, доступних в мережі.

Функція локальних мереж – пов'язувати комп'ютери разом і надавати загальний доступ до принтерів, файлів і інших служб. Архітектура локальної мережі підрозділяється на однорангову або клієнт–серверну.

Клієнт / серверна локальна мережа – це мережа, в якій різні типи різних пристроїв (клієнтів) підключені до централізованого серверу, і цей сервер може обробляти кілька операцій, таких як зберігання даних, доступ до принтера, а також мережевий трафік. Клієнти і сервер пов'язані один з одним дротовим або бездротовим середовищем [3].

У середовищі клієнт / серверної локальної мережі кожен комп'ютер зберігає (або може зберігати) свої (або деякі) ресурси і файли. Інші комп'ютери також можуть отримати доступ до ресурсів, що зберігаються на комп'ютері. Одна з особливостей мережі клієнт / сервер полягає в тому, що файли і ресурси централізовані. Це означає, що комп'ютер–сервер, може їх зберігати, а інші комп'ютери можуть отримати до них доступ. Оскільки сервер завжди включений, клієнтські машини можуть отримувати доступ до файлів і ресурсів, не піклуючись про те, чи включений певний комп'ютер.

Одним з наслідків мережі клієнт / сервер є те, що, якщо сервер вимкнений, його ресурси, а іноді і більшість ресурсів в мережі, недоступні. Фактично, один із способів створення мережі клієнт / сервер – мати більше одного сервера. У цьому випадку кожен сервер може грати свою роль.

Ще одна велика перевага мережі клієнт / сервер полягає в тому, що безпека створюється, управляється і може бути посилена. Для доступу до мережі людина, так званий користувач, повинен надати деякі облікові дані, такі як ім'я користувача і пароль. Якщо облікові дані недійсні, користувачеві заборонений доступ до мережі.

Тип мережі клієнт / сервер також забезпечує безліч інших переваг, таких як централізоване резервне копіювання, можливості локальної мережі, моніторинг Інтернету і т. д. У невеликій мережі всі ці послуги можуть оброблятися одним сервером. У середній і великий мережі може бути багато серверів, кожен з яких виконує своє завдання.

Клієнти зазвичай спілкуються з серверами за допомогою набору протоколів TCP / IP. TCP – це протокол, орієнтований на з'єднання, що означає, що з'єднання встановлюється і підтримується до тих пір, поки прикладні програми на кожному кінці не закінчать обмін повідомленнями. Він визначає, як розбивати дані додатки на пакети, які можуть доставляти по мережі, відправляє пакети і приймає пакети від мережевого рівня, керує управлінням потоком і обробляє повторну передачу відкинутих або перекручених пакетів, а також підтвердження всіх вхідних пакетів. У моделі взаємодії відкритих систем (OSI) TCP охоплює частини рівня 4, транспортного рівня, і частини рівня 5, тобто сесійний рівень [4].

IP – це протокол без встановлення з'єднання, що означає, що немає постійного з'єднання між кінцевими точками, які обмінюються даними. Кожен пакет, який проходить через Інтернет, розглядається як незалежна одиниця даних, яка не має ніякого відношення до будь–якої іншої одиниці даних. (Причина, по якій пакети розміщуються в правильному порядку, полягає в TCP.) У моделі взаємодії відкритих систем (OSI) IP знаходиться на рівні 3, мережевому рівні.

Однорангова локальна мережа – в якій не потрібно централізований серверний комп'ютер, тому він не може витримувати величезне робоче навантаження в порівнянні з клієнт–серверної локальною мережею. Відповідно до цієї концепції, кожен комп'ютер та інші пристрої пов'язані між собою паралельно.

Кожен пристрій в мережі вважається одноранговим вузлом з функціями, які вносять свій внесок в мережу. Кожен пристрій в мережі P2P розділяє частину своїх ресурсів з іншими комп'ютерами в мережі. Ці ресурси можуть включати сховище, смугу пропускання і обчислювальну потужність.

Деякі основні особливості цієї мережі включають в себе:

- Кожен пристрій в мережі P2P надає ресурси мережі і споживає ресурси, які надає мережа.
- У мережі P2P файли розподіляються між різними комп'ютерами.
- Будучи частиною P2P–мережі, можна спільно використовувати таке обладнання, як принтери, між різними пристроями в мережі.
- Для настройки тимчасової мережі потрібне спеціалізоване програмне забезпечення.
- Деякі мережі P2P формуються шляхом накладання віртуальної мережі на фізичну мережу. Мережа використовує фізичне з'єднання для передачі даних, тоді як віртуальне накладання дозволяє комп'ютерам в мережі взаємодіяти один з одним.

Завдяки своїй архітектурі P2P–мережу може запропонувати користувачам безліч переваг, в тому числі:

- Простий обмін файлами: розвинена мережа P2P дозволяє швидко обмінюватися файлами на великих відстанях.

- Зниження витрат: немає необхідності вкладати кошти в окремий комп'ютер для сервера при налаштуванні P2P–мережі.
- Адаптивність: P2P–мережа легко розширюється для включення нових клієнтів. Ця перевага робить ці мережі більш гнучкими, ніж мережі клієнт–сервер.
- Надійність: на відміну від мережі клієнт–сервер, яка може вийти з ладу при виході з ладу центрального сервера, мережа P2P, ймовірно, залишиться працездатною навіть у випадку відмови центрального сервера.
- Висока продуктивність: в той час як мережа клієнт–сервер працює менш ефективно, коли до неї приєднується більше клієнтів, мережа P2P може поліпшити свою продуктивність, коли до неї приєднається більше клієнтів. Це пов'язано з тим, що кожен клієнт в мережі P2P також є сервером, який надає ресурси мережі.
- Ефективність: P2P–мережі дозволяють співпрацювати між пристроями, що мають різні ресурси, що може принести користь всієї мережі.

Програми, що працюють на сервері локальної мережі, надають такі послуги, як доступ до бази даних, спільне використання документів, електронна пошта і друк. Пристрої у тимчасовій локальної мережі обмінюються даними безпосередньо з комутатором або маршрутизатором без використання центрального сервера [5].

Локальні мережі можуть з'єднуватися з іншими локальними мережами через виділені лінії і послуги або через Інтернет за допомогою технологій віртуальних приватних мереж. Ця система підключених локальних мереж класифікується як глобальна локальна мережа або міська мережа. Локальні і глобальні мережі розрізняються за своїм діапазоном.

1.2 Мережеві протоколи локальної мережі

Мережевий протокол визначає, як мережа буде вирішувати такі проблеми та завдання:

- помилки лінії зв'язку;
- регулювання потоку інформації (щоб запобігти переповненню буферів);

- виявлення несправностей;
- інтерпретація повідомлень.

Еталонна модель OSI. Модель OSI ділить функції, які протоколи повинні виконувати, на семи ієрархічних рівнях. Кожен рівень взаємодіє тільки зі своїми сусідніми шарами і не знає про існування інших верств. Модель OSI додатково поділяє другий (канальний) рівень на два підрівні, які називаються управлінням доступом до середовища (MAC) і управлінням логічним каналом (LLC), відповідно. У мережевих протоколах фізичний рівень (рівень 1) і підрівень управління доступом до середовища зазвичай реалізуються за допомогою обладнання, а інші рівні реалізуються за допомогою програмного забезпечення. Апаратні компоненти рівнів 1 і управління доступом до середовища зазвичай називаються модемами і драйверами (або контролерами) відповідно.

Строго кажучи, для роботи мережі потрібні тільки рівні моделі: фізичний, канальний та прикладний. Інші рівні додаються тільки в міру необхідності додаткових послуг (наприклад, безпомилкова доставка, маршрутизація, управління сеансом, перетворення даних і т. д). Більшість сучасних локальних мереж містять всі або більшу частину рівнів OSI, що дозволяють підключатися до інших мереж і пристроїв.

Модель OSI включає архітектуру, якої дотримуються більшість стандартів протоколів. Кожен стандарт повинен бути відкритим, щоб можна було поєднувати мережеві пристрої різних виробників. Спеціалізовані технічні організації, на відміну від комітетів по стандартизації, таких як ISO, доклали максимальних зусиль для стандартизації мережевих протоколів. Однак ISO прийме і підтвердить мережевий стандарт, якщо він відповідає архітектурі протоколу, певною моделлю OSI.

Стандарти IEEE:

- IEEE 802.3. IEEE, відповідно до ISO, погодився нести відповідальність за специфікацією локальних мереж, швидкість передачі яких становить від 1 до 20 мегабіт / сек. Стандарт IEEE 802.3, який ISO прийняв в якості власного стандарту (ISO 8802), регулює фізичний рівень та рівень управлінням доступом до середовища моделі OSI.

Стандарт IEEE 802.3 визначає, що доступ до мережі повинен здійснюватися через CSMA / CD з використанням топології шини зі швидкістю від 1 до 20 мегабіт / сек (основна смуга) або 10 мегабіт / сек (широкосмугова). Широко використовувана мережа Ethernet відповідає стандарту IEEE 802.3. ISO прийняв Ethernet як стандарт, ISO 8802.3. У системах управління мережу Ethernet (802.3) в першу чергу підходить для некритичних додатків, таких як диспетчерський моніторинг і управління програмами.

- IEEE 802.4 та 802.5. Стандарт IEEE 802.4 визначає мережу токенів з різною швидкістю передачі базової та широкосмугової передачі, ніж стандарт IEEE 802.3. Стандарт 802.4 використовується багатьма виробниками, як структура протоколу нижчих рівнів своїх локальних мереж. Крім того, інший стандарт IEEE, IEEE 802.5, визначає токен кільцеву мережу з меншими швидкостями передачі для базових смуг кабелів. IBM прийняла стандарт 802.5 для протоколу передачі токенів із кільцевою топологією.

Протокол TCP/IP. Більшість виробників, які пропонують Ethernet–сумісність для реалізації наглядових функцій над обладнанням використовують протокол TCP / IP для рівнів 3 і 4 (мережевий та транспортний) моделі OSI. На сьогоднішній день протокол TCP / IP використовується в Інтернет–мережі передачі даних.

У протоколі TCP / IP TCP гарантує контроль наскрізних з'єднань. TCP робить доступними для користувача декілька послуг, таких як встановлення мережевих з'єднань та роз'єднань, гарантоване послідовність передачі даних, захист від втрати послідовності, контроль часу з'єднання та прозоре мультиплексування та транспортування даних. IP (протокол Інтернету) виконує додаткові функції, такі як адресація мережевих даних, розподіл пакетів даних та маршрутизація даних у мультимережевих системах.

Іноді розділ TCP / IP у контрольній мережі замінюється іншим протоколом – протоколом специфікації виробничих повідомлень, який використовується пристроями для обміну даними через мережі 802.3.

1.3 Методи доступу до мережі

Існує багато методів доступу, найчастіше використовуються опитування, виявлення зіткнень та передача маркера.

Метод доступу, який найчастіше використовується у головних / ведених протоколах, – опитування. Під час опитування ведучий опитує кожну станцію послідовно, щоб перевірити, чи є у нього дані для передачі. Ведучий надсилає повідомлення певній станції і чекає на відповідь фіксований час. Пристрій повинен відповісти, надіславши або дані, або коротке повідомлення про те, що у нього немає даних для відправки. Якщо пристрій не відповідає протягом відведеного часу, ведучий припускає, що пристрій не працює, і продовжує опитування інших пристроїв. Взаємозв'язок між станціями в конфігурації ведучий / ведений є неефективним, оскільки опитування вимагає, щоб дані спочатку надсилалися ведучому, а потім приймаючому пристрою. Оскільки конфігурації ведучий / ведений використовують цей прийом, опитування часто називають методом доступу ведучий / ведений.

Виявлення зіткнень зазвичай називають CSMA / CD (багаторазовий доступ до сенсора перевірки з виявленням зіткнень). У цьому методі доступу кожен вузол із повідомленням про відправлення чекає, поки в мережі не буде трафіку, а потім передає. Поки вузол передає, його схема виявлення зіткнень перевіряє наявність іншого передавача. Якщо схема виявляє зіткнення (два вузли, що передають одночасно), вузол відключає свій передавач і чекає випадкову кількість часу, перш ніж повторити спробу. Цей метод працює добре, якщо мережа не має надмірного обсягу трафіку.

Кожне зіткнення та повторна спроба використовує час, який не можна використовувати для передачі даних; отже, пропускна здатність мережі зменшується, а час доступу збільшується зі збільшенням трафіку. З цієї причини виявлення зіткнень не є популярним у мережах управління. У промислових додатках виявлення зіткнень може використовуватися для збору даних та

обслуговування програм у великих системах та розподілених додатках управління в режимі реального часу з відносно невеликою кількістю вузлів [6].

Передача токена – це техніка доступу, яка виключає суперечки між станціями PLC, які намагаються отримати доступ до мережі. У цій техніці PLC передають маркер, який є повідомленням, що надає запитуваній станції ексклюзивне, але тимчасове право управління мережею (тобто передавати інформацію). Станція з токеном має ексклюзивне право передавати по мережі інформацію, однак він повинен відмовитись від цього права наступному призначеному вузлу після припинення передачі. Таким чином, передача токенів насправді є розподіленою формою опитування. Метод доступу, що передає маркер, є кращим у розподілених програмах управління, які мають багато вузлів або жорсткі вимоги до часу відгуку.

У загальній конфігурації мережі шини, що використовує техніку передачі токенів, кожна станція ідентифікується адресою. Під час роботи маркер послідовно переходить від однієї станції до наступної. Вузол, що передає маркер, також знає адресу наступної станції, яка прийме маркер. Мережа циркулює передані дані в одному або декількох інформаційних пакетах, що містять дані джерела, пункту призначення та контролю. Кожен вузол отримує цю інформацію та за потреби використовує її. Якщо вузол має інформацію для надсилання, він надсилає її в новому пакеті [7].

1.4 Технології локальних мереж

1.4.1 Техніка спільної локальної мережі (мультипротоколи)

Мережі локальної мережі, такі як Token Ring (IEEE 802.5), Ethernet V2, IEEE 802.3 та FDDI, дозволяють спільне використання підмережі. Для Token Ring і FDDI, цей протокол доступу базується на передачі маркера алгоритму; як для Ethernet V2, так і для IEEE 802.3, схема виявлення зіткнень під назвою CSMA / CD використовується для надання доступу до локальної мережі. Оскільки локальні мережі лише визначаються через рівень OSI 2 (Data Link Control), будь–який

транспортний протокол вищого рівня може використовувати цю підмережу. Як випливає з терміна локальна мережа, вузли повинні знаходитися в безпосередній фізичній близькості один від одного, як правило, в межах однієї будівлі. На рисунку 1.1, програми А у лівому вузлі повинні спілкуватися за допомогою транспортного протоколу А зі своїм партнером у правому вузлі (програми Б).

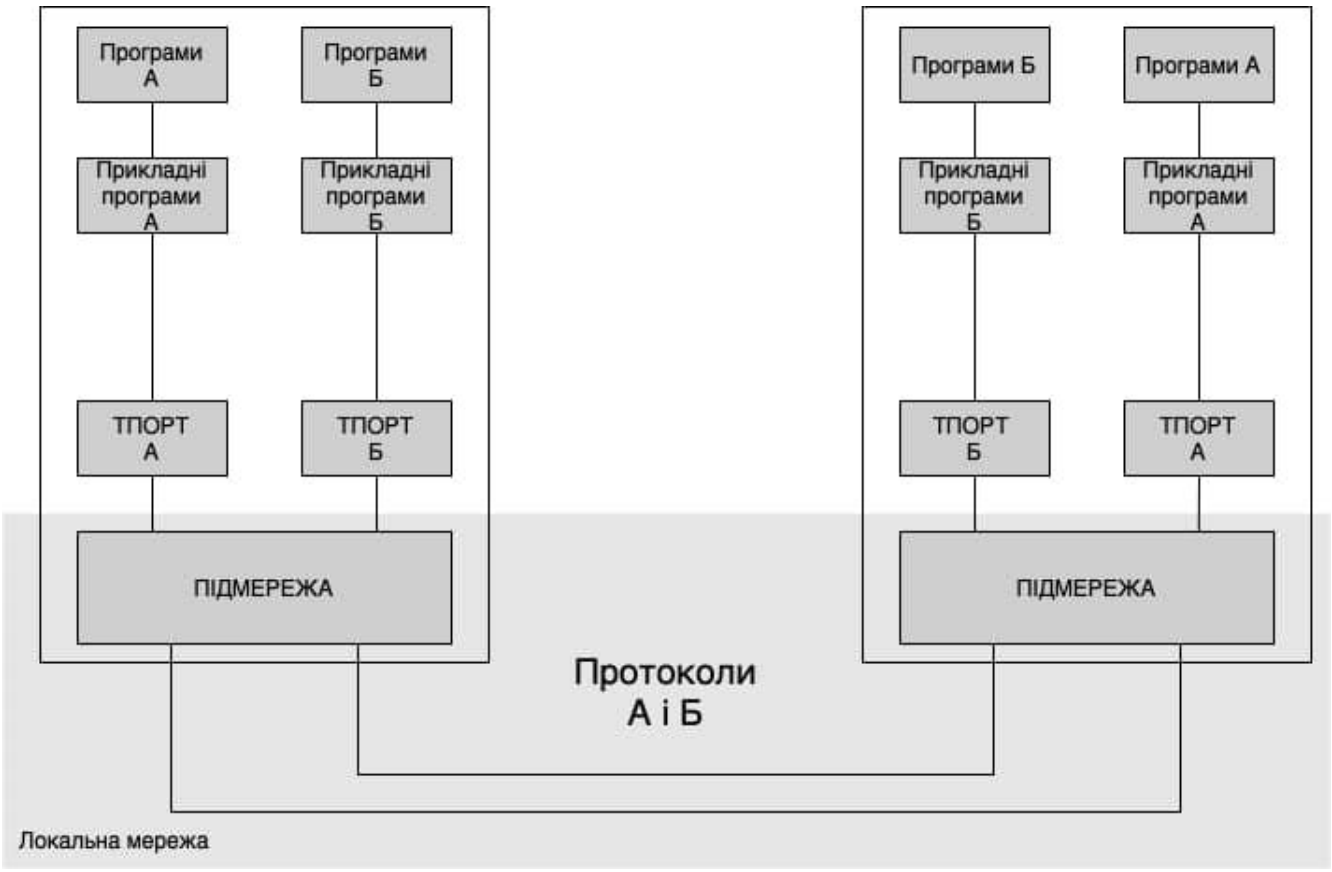

Рисунок 1.1 – Схема спільної локальної мережі (мультипротоколи)

Мережі локальної мережі історично використовувались для підключення робочих станцій людей у межах організації, яким потрібно часто спілкуватися разом та обмінюватися даними та використовувати певні ресурси. Зазвичай ці локальні мережі створюють разом відомчі лінії, вважаючи, що люди в одному відділі потребують спочатку спілкуватися між собою.

Незважаючи на те, що додавання локальної мережі не вплине на програми безпосередньо, для налаштування локальної мережі потрібне додаткове обладнання. Електропроводка між вузлами повинна бути встановлена, кожна робоча станція повинна мати інтерфейсну адаптерну карту для конкретного протоколу локальної мережі [8].

Переваги спільних підмереж: локальні мережі:

- Дозволяє спільне використання однієї підмережі кількома протоколами, зменшення фізичних мережевих витрат, таких як проводка, адаптерні карти та інше.
- Можна використовувати спільні кадрові ресурси, оскільки це може робити одна група людей, керувати адмініструванням та управлінням мережею для всіх програм в мережі.
- Не потрібні спеціальні пристрої для встановлення логічних зв'язків між ними, не потрібні проміжні вузли маршрутизації.

Недоліки спільних підмереж: локальні мережі:

- Локальні мережі обмежені на обмежені відстані.
- Може знадобитися спільний доступ до однієї мережевої інтерфейсної карти для декількох транспортних протоколів, що може вплинути на продуктивність певної програми.
- Використання спільного носія іноді впливає на пропускну здатність додатків. Якщо в даний момент одна програма використовує мережу (наприклад, для передачі файлів TCP / IP FTP), то для іншої програми може відзначатися низька продуктивність.
- Якщо локальна мережа з якихось причин не працює, користувачі програм, як А, так і Б можуть не працювати.

1.4.2 Техніка спільної локальної мережі (Local Bridge)

Як згадувалося в попередньому описі локальної мережі, всі локальні мережі працюють на рівні OSI 2, рівні управління передачею даних. Підшар управління доступом до мультимедіа DLC визначає формати кадрів, адресацію та протоколи доступу для кожного конкретного типу локальної мережі. Якщо дві локальні мережі потрібно підключити, щоб забезпечити зв'язок між подібними програмами, тоді можна використовувати локальний міст. Місцевий міст працює на рівні MAC, і його часто називають мостом MAC [9].

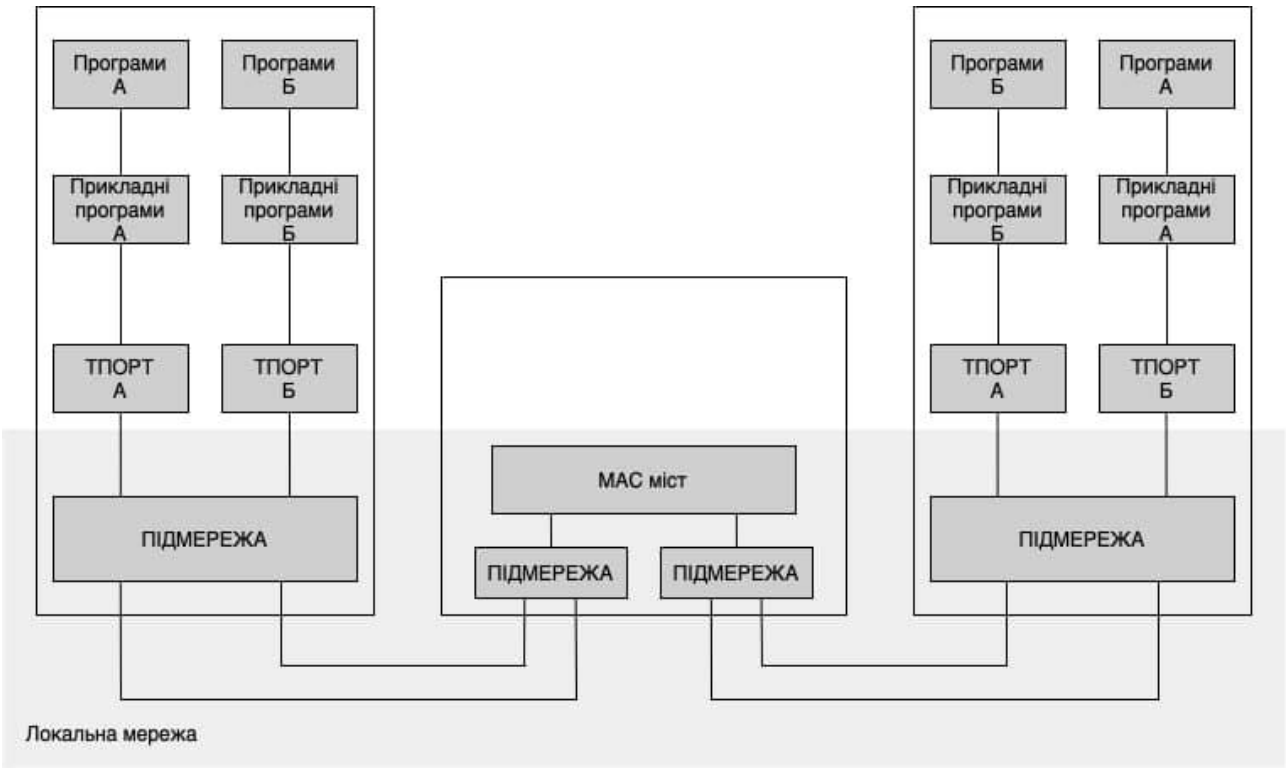

Рисунок 1.2 – Схема спільної локальної мережі (Local Bridge)

На рисунку 1.2, якщо два показані вузли розташовані на двох окремих сегментах локальної мережі (можливо, ці локальні мережі належать двом різним підрозділам компанії в будівлі), Як показано на цій схемі, для забезпечення цього зв'язку було обрано міст MAC. Міст MAC зможе виявити, що кадри потрібно перенаправляти з лівого сегмента на правий сегмент. Міст робить це визначення за допомогою свого «мостового протоколу», наприклад, мосту вихідного маршруту для локальних мереж Token Ring та прозорого мосту для локальних мереж Ethernet. Якщо два сегменти локальної мережі однакового типу, наприклад, два Token Ring, то ця переадресація може бути надзвичайно швидкою, оскільки формати кадру та протокол мостів однакові з обох сторін.

Однак деякі локальні мости також виконують певну кількість перетворень, щоб можна було підключати різні типи сегментів, наприклад, кільце символів до Ethernet V2. У цьому випадку формати кадрів різні, і потрібно здійснити перетворення. Крім того, мостові протоколи можуть відрізнятися. Поки перетворення відбувається строго на рівні OSI 2, можна вважати цю функцію головним чином "мостом", а не функцією "маршрутизатора".

Хоча для забезпечення цієї функціональності потрібно буде додати локальний міст, це не матиме впливу на кінцеві вузли. Міст потрібно буде приєднати до кожного сегмента локальної мережі як звичайний пристрій сегмента локальної мережі, і, отже, потрібно планувати, щоб забезпечити його приєднання до обох сегментів локальної мережі. Наприклад, якщо локальний міст з'єднував два символьні кільця, він повинен розташовуватися в будівлі так, щоб проводка для обох сегментів локальної мережі могла до нього дійти, плюс він повинен приєднуватися до багатостанційного блоку доступу (MAU) Token Ring №1 і MAU Token Ring №2.

Переваги локального мосту:

• Оскільки мости працюють на рівні OSI 2, вони не чутливі до вибору транспортних протоколів. Таким чином, мости можуть пересилати рамки для всіх транспортних протоколів.

• Мости можуть перенаправляти кадри дуже швидко, оскільки мало, якщо взагалі є, конверсії.

• Мости можна використовувати для ізоляції сегментів великої “локальної мережі” з метою покращення загальної ефективності, де два сегменти визначають власні логічні робочі групи.

Недоліки локального мосту:

- Оскільки мости не є чутливими до транспортних протоколів, вони не можуть виявити проблеми. Наприклад, у мережах TCP / IP цілком можливо отримати «широкомовні шторми», коли один користувач може завантажити мережу сторонніми повідомленнями. Маршрутизатори, чутливі до транспортного протоколу, можуть запобігти виникненню таких проблем.
- Вбудовані обмеження мостового протоколу можуть заборонити розширене підключення. Наприклад, міст вихідного маршруту обмежений реалізацією лише семи послідовних мостів у мережі (сім "стрибків"); прозорий міст обмежений одним активним мостом у будь–який час між двома сегментами. Ці обмеження вплинуть на дизайн та розширюваність будь–яких великих локальних мереж.

- Оскільки весь трафік може проходити через міст, організаційне розділення за адресами чи підмережами не відбувається.

1.4.3 Техніка спільної локальної мережі (віддалений / розділений міст)

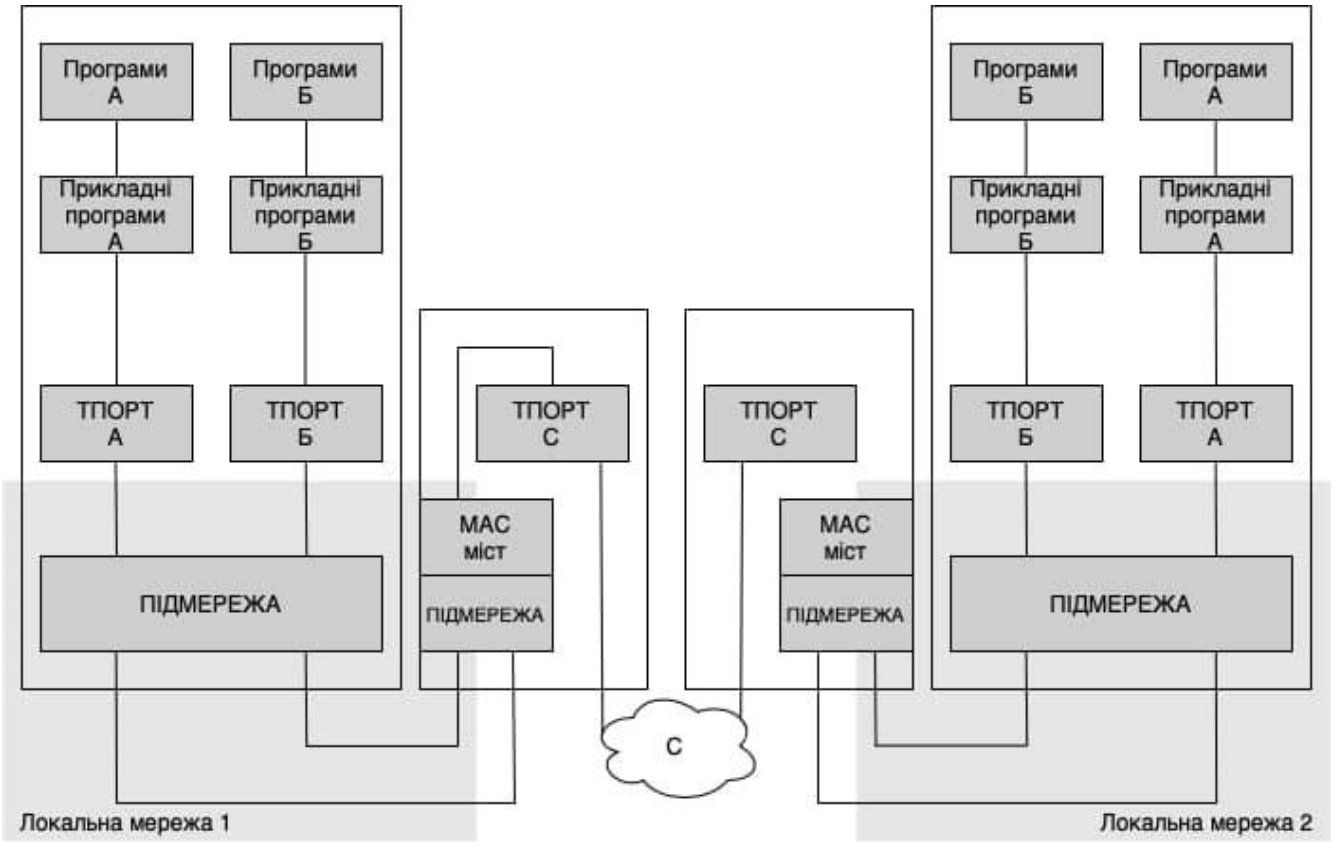

Рисунок 1.3 – Схема спільної локальної мережі (віддалений / розділений міст)

Ця техніка є особливим випадком розширення локальних мереж за допомогою мостів через широку мережу. Ці мости називаються віддаленими або розділеними мостами. Суттєвою особливістю цієї техніки є те, що кадри беруться з локальної мережі на підрівні MAC рівня OSI 2. Потім ці кадри надсилаються як дані через глобальну мережу, де вони відновлюються як MAC–кадри в цільовій локальній мережі. Підходи інкапсуляції зазвичай використовуються мостами для передачі цих кадрів через глобальну мережу. Встановлюється зв’язок між двома віддаленими мостовими партнерами, який мультиплексує весь трафік між двома локальними мережами. Один віддалений міст може з'єднувати кілька локальних мереж і може

мультиплексувати всі ці локальні мережі через одне з'єднання з мостом–партнером – це називається багатопортовим мостом [10].

Як і у випадку з іншими методами інкапсуляції, протокол з'єднання між партнерськими мостами, як правило, є приватним. Як показано на рисунку 1.3, ці мости показані як справжні мости MAC для відключення трафіку від підключеної локальної мережі, тоді задіяний додатковий стек протоколів, щоб забезпечити функцію інкапсуляції в глобальній мережі, використовуючи транспортний протокол C. Може бути деяка фільтрація трафіку локальної мережі, щоб затоплення проміжної широкосмугової мережі непотрібними трансляціями (наприклад, трансляціями для визначення партнера сеансу з токен–рингом). Цей тип фільтрації виконується лише на рівні Data Link Control (рівень OSI 2), і рідко такі віддалені мости фільтруються на верхніх шарах (рівень 3 і вище), таким чином, вони не залежать від транспортних протоколів.

Віддалені мости трапляються попарно (звідси і назва розділений міст, що вказує на "розкол" між двома партнерами). Між мостами потрібні точкові з'єднання. Деякі реалізації дозволяють одному фізичному мосту мати кілька з'єднань, але це завжди відбувається у точці до точки з партнерами.

Зазвичай кінцеві вузли чи програми не змінюють. Для забезпечення функції віддаленого мосту знадобиться додаткове обладнання та програмне забезпечення, також ці пристрої повинні мати можливість підключення до відповідних локальних мереж. Між партнерськими мостами зазвичай є орендована лінія.

Переваги віддаленого (розділеного) мосту:

- Транспортний протокол є незалежним.
- Можливо, буде здійснено деяку фільтрацію повідомлень трансляції по локальній мережі, що зменшить трафік широкосмугової мережі.
- Ці віддалені мости, як правило, недорогі і демонструють хорошу продуктивність при заданій швидкості зв'язку між віддаленими мостами.

Недоліки віддаленого (розділеного) мосту:

- Адекватна фільтрація не може бути виконана мостами на рівні Data Link Control або на більш високих рівнях, внаслідок чого сторонній трафік може

заполонити проміжну мережу широкої зони. Цей сторонній трафік може впливати на критичні таймери сеансів для певних конфіденційних транспортних протоколів (таких як SNA та NetBIOS), що спричиняє скасування сеансів.

- Оскільки підхід інкапсуляції та протокол сеансу між мостами–партнерами часто є власністю, все обладнання має закуповуватися у одного постачальника. Однак це може змінитися, оскільки нові стандарти, такі як PPP, стають все більш популярними.
- Може бути дорого підключити кожен міст фізично до кожного іншого мосту в точці до точки через орендовані лінії.
- Може бути обмежений, якщо такий є, контроль над потоком на нижчій швидкості зв'язку між партнерськими мостами.
- Існують обмеження щодо розширюваності та / або масштабованості цих мереж через обмеження кількості переходів (як для кільця токенів) та / або проблеми, викликані великою кількістю потенційних партнерів (кінцеві станції та / або мости).

1.5 Процес атаки локальної мережі

Оскільки більшість антивірусного програмного забезпечення та брандмауерів досить добре налаштовані проти зовнішнього вторгнення, і внутрішній нагляд іноді є відносно вільним. Тоді ініціалізація серійної атаки буде набагато простішою в певних точках. Весь процес атаки може бути розбитий на три основні фази. Це може не стосуватися особливих випадків, однак є актуальними для більшості [11].

Приєднання до мережі. Для внутрішньої ініціалізації атаки першим кроком було б спробувати проникнути в мережу, щоб стати одним із звичайних користувачів. Кабель Ethernet можна отримати в більшості офісних середовищ, як тільки це відбудеться зловмисник стане законним членом інтрамережі, який спостерігає за функціональною мережевою інфраструктурою. Це надає можливість зловмисникам перейти до наступного кроку. Але дуже мало ймовірності того, що це станеться, оскільки зловмисники прагнуть не викриватися фізично, оскільки може

бути шанс отримати відеозапис для подальших довідок. Натомість вони могли б віддавати перевагу використанню чогось невидимого для проникнення в мережу, в цьому випадку Wi–Fi – це чудовий вибір.

Сигнал Wi–Fi можна повністю розпізнати в межах діапазону, якого може досягати потужність сигналу. Незважаючи на те, що функцію трансляції автосигналу можна вимкнути, все одно можна відсканувати її за допомогою певних карток Wi–Fi у режимі моніторингу. Коли сигнал виявляється, перший аналіз починає працювати на його криптографії. Якщо використовується метод шифрування WEP, тоді ефективний процес злому дозволить «розрахувати» пароль для приєднання до мережі за значний короткий проміжок часу, іноді його можна обчислити навіть за секунди. Замість шифрування WEP, адміністратори мережі завжди хотіли б надати перевагу методу шифрування WPA / WPA2, оскільки вони дуже добре знайомі з тим, як швидко WEP можна зламати.

WPA / WPA2 не було б легко розрахувати за допомогою алгоритму. Однак все ще може бути три можливості його зламати. За допомогою грубої сили – це завжди одна з можливостей. Однак усі символи можуть використовуватися в системі, включаючи алфавіти, цифри, знаки, можливо, всі використовуються паролем, отже, незліченна кількість комбінацій тесту та витрати часу зробили грубу силу майже неможливою. «Словник» – один із методів. Вже складений список слів "вгадування" використовується програмою засобів атаки як "словник". Це програмне засіб буде намагатися відповідати кожній фразі, які зберігаються в файлі словника з сигналом, щоб перевірити, яке словом є правильною «здогадкою». Насправді цей метод має величезні випадкові ситуації. Величезний файл списку слів (іноді може складати кілька гігабайт простого текстового файлу), що містить мільйони фраз, можливо, потребує днів, щоб перевірити його за допомогою сигналу навіть без одного збігу, тоді як інший "словник", що містить лише потрібне слово, спрацьовує на сигнал протягом декількох секунд. Використовуючи цей метод, все покладається на файл словника, незалежно від того, містить він „потрібну” фразу чи ні. Третя можливість – використання функції WPS як єдиного експлоїту. Насправді WPS було винайдено для зручності. Гостям не потрібно знати пароль хосту, щоб приєднатися до хост–

мережі Wi–Fi одним натисканням кнопки «швидке посилання». Цю функцію може використовувати програмне забезпечення для проникнення для злому шифрування WPA / WPA2.

Експлойт відкриття. Коли хакери знаходяться в інтрамережі, перед тим, як вносити будь–які зміни чи пошкодження в мережевій інфраструктурі, вони, як правило, намагаються переконатися, що їх подальші дії не будуть записані. Іншим словом, система реєстрації буде першою метою, яку хакери хочуть закрити. Ця функція зазвичай вбудована в маршрутизатор або комутатор. Таким чином, дуже мало хакерів залишають комутатор і маршрутизатор у спокої одразу після потрапляння доступу в мережу. Якщо використовуються "слабкі" назви користувача та пароль (наприклад, звичайні фрази, що існують "root", "admin" або налаштування за замовчуванням.), то хакер отримає бажану привілею з самого початку. Це призведе до досить простого та швидкого процесу атаки, крім того, журнали можна стирати після їхніх атак. В іншому випадку, якби маршрутизатор або система входу до комутатора були модифіковані для досягнення відносно безпечного рівня, зловмисники все одно не ігнорували б можливості збереження журналів, щоб повідомити, хто здійснив атаку. У цьому випадку сам журнал, не містив би правдиву інформацію, для подальшого ознайомлення з нею адміністратором, оскільки хакери будуть фальсифікувати дані в системі реєстрації. Замість запису IP–адреси щодо того, що вона зробила, система реєстрації, ймовірно, встановить запис MAC–адреси на тих, хто торкнувся чутливих системних модулів. MAC–адреса – це унікальний відбиток одного мережевого інтерфейсу. Однак цю ідентичність можна змінити в ОС зловмисників. У середовищі Linux будуть сторонні програми, які виконують цю роботу, тоді як середовище Windows дозволяє користувачеві змінювати його за властивістю мережевого інтерфейсу. Незважаючи на те, що більшість постачальників мережевих інтерфейсів усвідомлювали, що, мабуть, не є гарною ідеєю дозволяти користувачам змінювати MAC–адресу, а функція модифікації в драйверах зазвичай видаляється, все одно можна "розблокувати" це обмеження шляхом невеликих змін реєстру системи Windows.

Коли хакери впевнені в тому, що “засліплюють” мережеві прилади, комутатори або маршрутизатори, настав час внести більше змін до інтрамережі. Сканування портів зазвичай є першим вибором – від хакерів до ініціалізації послідовної атаки. У деяких випадках конкретні порти, які відкриваються, може бути набагато легше використовувати як експлойти. Крім того, деякі порти дуже унікальні для ОС, тому хакер може визначити, яку ОС використовує жертва, щоб підготуватися до наступного кроку. Одне сканування порту може надати досить багато цінної інформації про цільову ОС.

Якщо хакер хоче отримати ім’я користувача та пароль, наприклад, електронної скриньки жертви, оскільки зазвичай скринька електронної пошти може містити багато корисної особистої інформації, яку можна використовувати для багатьох цілей. Перший крок – фішинговий веб–сайт повинен бути створений якомога подібніший до реального. Це змусить жертву повірити у фішинг–сайт, що він вводить ім’я користувача та пароль на справжньому сайті. Певне програмне забезпечення може завантажувати та клонувати той самий веб–сайт, що і цільовий.

Оригінальні функції пошуку DNS зазвичай вбудовані всередині комутатора або маршрутизатора. Він відправить користувачеві мережеві запити до реального загальнодоступного DNS, щоб отримати результат, а потім поверне правду назад користувачеві. Для зловмисників вони не дозволяють надсилати запит користувача на справжній DNS. Вони воліють щось вигадувати і повертати назад жертві. Жертва повірить у те, що вони повернули, і починає це відвідувати.

Коли жертви потрапляють на підроблений веб–сайт поштової скриньки, вони починають вводити ім’я користувача та пароль. У серверній панелі реєстратор ключів записує те, що вони ввели, і надсилає на вказану адресу (зазвичай це мережевий інтерфейс зловмисника). Але підроблений веб–сайт, який клонували, не працює, але виглядає однаково. Це може спричинити обережність жертви, якщо кілька разів натискання кнопки входу не відобразить справжній процес входу з правильним ім’ям користувача та паролем [12].

Насправді інше програмне забезпечення спрямовує веб–сайт із клонованого на справжній DNS–сервер і, нарешті, веде до справжньої електронної скриньки після

першого запиту на вхід від користувача. Таким чином, жертва може просто бачити веб–сайт оновленим один раз після того, як вони ввели ім’я користувача та пароль. Вони можуть ввести його ще раз, оскільки здогадка про їх власне помилкове введення і вхід справді стануть успішними після другої спроби. На жаль, хоча веб–сторінка оновлюється після першої спроби, хакери вже отримали ім’я користувача та пароль, показані на їх екрані як звичайні тексти.

Технічне обслуговування систем жертв. Попередній метод може бути різним у різних ситуаціях. Іноді це може бути атакою соціальної інженерії, коли жертва видає ім'я користувача та пароль для входу в ОС. Тоді хакер налаштує віддалений зв’язок між собою та жертвою. Цей нелегальний мережевий сеанс був би використаний для передачі даних або навіть вузла для бот–мережі, яка готується до наступної атаки або масивної DDoS–атаки. Весь процес досить складний і обмежений багатьма змінними. Таким чином, повністю функціональна жертва дуже цінна для хакера. Вони точно не хотіли б повторити той самий процес атаки ще раз, і не хотіли забути жертву, оскільки могли б принести більше користі. Таким чином, хакери намагатимуться встановити один невидимий інтерфейс для жертви для підключення в майбутньому. Кілька алгоритмів використовуються для того, щоб приховати типові характеристики бэкдор–вірусу від виявлення, та знищення антивірусним програмним забезпеченням в ОС жертви. Цей процес дуже схожий на встановлення VPN–з'єднання між жертвою та хакером. Таким чином, процес технічного обслуговування також називають тунелюванням. На ОС жертв працює вірус зворотного підключення, це значно споживає чимало обчислювальних ресурсів. Якщо жертви знають трохи про управління завданнями в системі Windows, існує ймовірність того, що вони можуть провести розслідування та з’ясувати, який процес є найбільш енергоємним і припинити його. Тоді жертва може перервати процес тунелювання. Отже, вони перенесуть процес вірусу з самого себе на системний процес, тому жертва не зможе легко його закінчити, якщо не вимкнути всю систему. З налаштуванням самозапуску під час завантаження ОС жертва буде під наглядом хакера, як тільки у нього буде з’єднання з Інтернетом.

Будь–який з найпоширеніших методів атак потребує передумови. Це те саме, що виявити експлойт в процесі атаки. Крім того, коли хакери хочуть підтримувати жертв, їм може знадобитися надіслати корисні навантаження, що містять вірусні та шкідливі коди. Це все подібність між будь–якими методами чи процесами атаки [13].

1.6 Загальні методи атаки

Всі різноманітні методи, як правило, отримують однакові результати. Загалом, їх мета – отримати відносно високий привілей незаконним шляхом, щоб мати право на розгортання даних, які не можна чіпати, крім адміністраторів. Зрозумівши типові представники потенційних загроз безпеці, є можливість їх запобігання. Крім того, існує два способи атак, які є або офлайн, або онлайн.

Троянська вірусна програма, одна з найвідоміших шкідливих програм за всю історію. Він не дублює себе зазвичай, як інші віруси. Отримуючи несанкціоновані відносно високі привілеї проникнути в хост–операційну систему жертви, вона, як правило, генерує та об’єднує один або кілька шкідливих корисних навантажень, в більшості випадків, для першочергового надання доступу до незаконних віддалених з’єднань буде включений бэкдор, що значно уповільнить робочу швидкість ОС. Однак, на відміну від загальних комп'ютерних вірусів, більшість троянських програм не сприяють адсорбції в інших файлах і роблять ін'єкції. Таким чином, виявити без зразка бази даних антивірусного програмного забезпечення може бути досить важко.

Оскільки їх принцип функціонування полягає в ініціативі підключення до зовнішніх інтерфейсів, таким чином їх відносно легко виявити, коли вони починають працювати, хоча вони добре скомпільовані, щоб уникнути першого етапу сканування антивірусним програмним забезпеченням. Принаймні більшість антивірусного програмного забезпечення помітить користувача системи, і один підозрілий процес, який намагався підключитися до випадкових рідкісних портів [14].

При віддаленому підключенні до головної ОС, зловмисники, швидше за все, можуть повністю контролювати жертви (наприклад, захоплення вікна, передача файлів, зміна налаштувань ОС, викрадення особистої інформації про обліковий запис тощо).

Flame – шкідлива програма, яка використовуються з метою кібершпіонажу. Заражена ОС буде намагатися заразити через локальну мережу або USB. Використовуючи незаконно отриманий привілей, буде зроблена спроба активувати будь–який протокол передачі для завантаження інформації про контакти. Bluetooth є одним із способів отримання інформації про найближче оточення. Після того, як інформація буде зібрана і прихована, ці пакети будуть завантажені на віддалені сервери по всьому світу, щоб підготуватися до наступного використання.

Хробак – один з найвідоміших комп'ютерних вірусів. У нього сильна здатність до самовідтворення. На відміну від троянської вірусної програми, одна з його основних функцій – це автоматичне поширення файлів, що містять шкідливі коди, в інші каталоги в ОС хоста або навіть в іншу ОС через локальну мережу. Як і інші віруси, черв'як має всі стандартні корисні навантаження (наприклад, видалення файлів, шифрування неавторизованих файлів, спам даних по електронній пошті). На відміну від інших вірусів, хробакові не потрібно хост–програма або процес в ОС. Як тільки він виявляє і заражає «наступну» жертву, він зазвичай завершує свою роботу, тому підозрілий процес зникає або змінюється. Найбільш часто використовуваний порт для хробаків – 1434. Хробаки зазвичай споживають досить багато мережевих ресурсів, тому для інших процесів, яким теж потрібні мережеві ресурси, залишається зовсім небагато.

Відмова в обслуговуванні (DoS). Троянська вірусна програма або черв'як – типові представники шкідливих програм або вірусів, які поширюються через Інтернет, але можуть заразити користувача тільки в тому випадку, якщо вони їх запустять.

Щоб перервати або призупинити процес, який передбачав підключення користувачів або клієнтів до Інтернету або інших мережних служб, атака типу «відмова в обслуговуванні» (DoS) є сумнозвісним рішенням. Націлювання на

споживання більшої частини мережевих ресурсів жертви насправді є одним з багатьох способів DoS–атак. Як тільки атака може викликати у жертви проблеми або призупинити її надання послуг, навіть якщо вона буде скинута, вона може належати до категорії DoS–атак. У деяких випадках атаці важко працювати з одним або обмеженим обчислювальним ресурсом (наприклад, для атаки на величезну корпоративну мережу.

Способи ініціювання DoS–атаки можуть бути різними для досягнення різних цілей. DoS–атаки можна ідентифікувати в основному за трьома ключовими категоріями властивостей: статичним, динамічним і інтерактивним. Аналізуючи властивості, властиві DoS–атакам, їх можна класифікувати окремо. Властивості, які зазвичай не змінюються під час однієї безперервної атаки, які зазвичай встановлювалися перед атакою, називаються статичними властивостями атаки. Це визначається хакерами і самою атакою, що є фундаментальною властивістю. З іншого боку, властивості, які можуть змінитися під час атаки, відомі як динамічні властивості атаки (наприклад, мета, час, вибір вузла і т. д.). Властивості, які не тільки відносяться до ініціатора атаки, але також обмежуються специфікацією, скануванням безпеки і можливістю надання послуг з боку жертви, визначаються як властивості взаємодії атак [15].

Статичні властивості атак зазвичай містять режим управління атакою, атакуючий режим зв'язку, технічні принципи атаки, протоколи атак та шари атаки.

1. Режим управління атакою строго обмежує секретність джерела атаки. Залежно від різних методів атаки, режим управління жертвою можна розділити в основному на прямий, непрямий або автоматичний.

На ранній стадії DoS, від встановлення мети, реалізації атаки до остаточного припинення, атаки зазвичай налаштовувалися хакером вручну. Зовнішнім організаціям легше відстежувати і проводити розслідування. Це становило небезпеку для хакерів, тому атаки були розпочаті з використанням багаторівневої структури. Метод прямої ієрархії зажадав величезної кількості роботи, щоб простежити шлях до вихідного хакера, який все ще використовується в наші дні, а також автоматичний режим. Методи атаки були налаштовані ще до того, як вірус

було скомпільовано і випущено. Недолік цього режиму в тому, що він явно вимагає від ініціатора атаки великої кількості технічних знань.

2. У режимі непрямого управління атакою може бути багато способів зв'язку між зловмисником і жертвою. Ці способи дозволять судити про складність зворотного відстеження. Зазвичай можна розуміти як двосторонню, монозв'язок або непрямий зв'язок.

Пакети даних, які отримують жертви, містять реальну IP–адресу верхнього рівня ієрархії атак, який можна легко відстежити. Другий спосіб означає, що справжня ідентифікаційна інформація хакера не буде активована в пакети даних, що відправляються жертвам, зазвичай фальшива IP–адреса буде додана до UDP–пакета перед відправкою. Однак є кілька обмежень для використання цього способу зв'язку, наприклад, хакеру складно контролювати жертву по її відгуками і статусу. Друге, непряме звернення, як особливий спосіб двостороннього спілкування, використовує третю сторону для узгодження сеансів з жертвами. Цей шлях прихований, його складно відстежити або контролювати і фільтрувати. Записи, які реєструють жертви, дуже обмежені (іноді тільки на випадковий загальнодоступний сервер для проміжного обміну даними).

3. Технічні принципи атаки. Семантичний і грубий – це два основних принципи, які активно використовуються. Семантика зазвичай використовує існуючі недоліки і лазівки для DoS–атак. Жертви можуть легко уникнути цього типу атак, регулярно встановлюючи оновлення.

Метод грубої перевірки не вимагає, щоб жертва сама мала експлойти, а відправляє жертві величезну кількість запитів на обслуговування, щоб вичерпати свій ресурс і знищити його (так звана штормова атака). Щоб уникнути цього типу, власної сили з боку жертви недостатньо. Це також вимагає, щоб маршрутизатор верхнього рівня жертви (може бути ISP) мав функції фільтрації. Деякі атаки поєднують ці два принципи разом, щоб бути ще сильнішими проти рішень (наприклад, SYN Flood.). Навіть деякі зловмисники знайомі з фізичними вадами або недоліками протоколу, існуючими в конструкції жертви, тому атака навіть створить

додатковий потік даних, щоб зруйнувати жертву. Це здається однією з грубих атак, але її можна виправити, тільки спочатку виправивши помилку в протоколі.

4. Протоколи атак. Під час однієї безперервної атаки будуть задіяні численні протоколи, такі як SMTP, ICMP, UDP і HTTP з верхнього рівня. В принципі, чим вище рівень, на якому задіяні ці протоколи, тим більше ресурсів жертва споживає для аналізу пакетів, відправлених зловмисниками.

5. Шари атак. Зазвичай атаки з використанням TCP / IP виходять від рівня передачі даних, мережі, транспорту і додатків. Атаки на рівень передачі даних (відомий як рівень 2) відбуватимуться тільки всередині LAN через обмеження протоколів. Це рідко можна побачити, але легко випустити з уваги. Більшість атак націлені на мережевий рівень, а також на додаток.

В основному розглядаються три категорії динамічної властивості: тип адреси джерела, генерація пакетів даних, тип цілі.

1. Тип адреси джерела. Ініціатор атаки може використовувати в якості вихідної адреси справжні або підроблені типи. Як згадувалося вище, можна використовувати справжню IP–адресу, але його легше відстежити. Підроблені типи вирішать цю проблему, або збільшать труднощі для жертв при здійсненні аналізу та фільтрації пакетів. Однак в деяких випадках необхідно використовувати дійсну IP–адреса джерела. Через високу ймовірність розкриття вихідної інформації, швидкість її використання знижується. Як правило, фальшиві адреси – це ті, які вже були призначені легальним користувачам, але будуть повторно використані зловмисником незаконно вдруге, або ті, які зарезервовані в мережі і ніколи нікому не були призначені.

2. Генерація пакетів даних. Дані всередині атакуючих пакетів в основному існують в п'яти різних режимах: нема жодного, унікальний, випадковий, словниковий і функціональний.

Як згадувалося раніше в процесі штормової атаки, зловмисникові необхідно відправляти масивні пакети цілі. Інформаційне навантаження даних усередині пакетів може створюватися в різних режимах. Різні режими будуть впливати на перевірку жертв і фільтрувати дії з пакетами. Завантаження пакетів може бути

проведена чотирма різними способами. По–перше, відправка пакетів з однаковим навантаженням. Пакети такого типу будуть мати типові характеристики, які можна визначити з перших кроків. По–друге, відправка пакетів з випадковим завантаженням. Незважаючи на те, що ці пакети, можливо, можуть бути розпізнані за допомогою «розпізнавання режиму», їх легко відфільтрувати, оскільки більшість з них генеруються випадковим чином без практичного сенсу, але зловмисник все ж може спроектувати спосіб випадкової генерації. В цьому випадку жертва буде розпізнавати пакети, що містять шкідливу інформацію, до тих пір, поки вони не будуть проаналізовані на рівні додатку, що значно ускладнило їх фільтрацію. По–третє, зловмисник буде підбирати певне навантаження, яке він вважає значущими, кожен раз, коли він формує пакет, дотримуючись певних правил, щоб додати набір пакетів. По–четверте, останній спосіб – кожен раз генерувати різне навантаження. Це досить складно зробити, висновок, оскільки кожна функція, яка використовується для генерації різного навантаження, в кінцевому підсумку призведе до різних труднощів при виявленні.

3. Тип цілі. Зловмисник вибере мету випадковим чином, але, швидше за все, це додаток, система, критичний мережевий ресурс, мережа, мережева інфраструктура або Інтернет.

Найпоширеніший спосіб атакувати – зосередитися на додатках. Зазвичай вони націлені на лазівку в одному конкретному додатку і продовжують проводити DoS–атаки. Вичерпання ресурсу жертви – цілком типовий випадок для систем (типу SYN–штурму, UDP–штурму). Деякі атаки націлені тільки на критично важливі ресурси, особливо це може бути сервер доменних імен (DNS) або маршрутизатори. У той час як ті, які націлені на мережу, повинні мати достатньо ресурсів і методів (зазвичай сервер кореневого домена, основний маршрутизатор магістралі, відомий сервер цифрових сертифікатів). Цей тип атак не дуже поширений на практиці, але безумовно смертельний, якщо він відбудеться. Мета в Інтернеті – це черв'як або троян, які будуть масово поширюватися всюди, що призведе до появи величезної кількості хостів та мереж з ефектом відмови в обслуговуванні. Цей тип приніс би мало не найстрашніші пошкодження.

Властивості взаємодії при атаці: або статичні, або динамічні властивості атак не тільки обмежуються методами і можливостями реалізації їх ініціатора, але також обмежуються можливостями цільових користувачів. Це може в основному: виявлення можливостей і ефекти атаки.

1. Виявлення можливостей. Жертв можна розділити на категорії за їхньою здатністю виявляти шкідливі пакети: фільтровані, нефільтрованого і невимовні.

Іноді для жертв атакуючі пакети мають досить типові характеристики, які необхідно виявити. Захист від атак може бути реалізовано ефективно, щоб забезпечити нормальне надання послуг, шляхом фільтрації цих пакетів. Однак характеристики, які були додані в фільтр, можуть одночасно впливати на звичайні пакети і навіть впливати на нормальне надання послуг. Це в точності та ж мета, яку хоче досягти зловмисник. Таким чином, в певному сенсі наосліп додати ці характеристики до фільтру не вийде. Найгірше те, що атакуючі пакети не мають такої типової особливості, як звичайні пакети. Це призведе до того, що жертви будуть повністю незахищеними перед атакуючими пакетами хакерів.

2. Ефект атаки. Різні рівні ефектів атаки – від відсутності, деградації, самовідновлення, відновлення вручну – допоможуть класифікувати всіх жертв.

Якщо цільова система як і раніше може надавати ті ж послуги, що і під час атаки, це можна визначити як відсутність ефектів. Якщо сили атаки недостатньо для створення повного DoS, але за рахунок деякого уповільнення здатності обслуговування, деградація є справедливою назвою для цих атак. Коли атака досягає масштабу, необхідного для створення повного DoS, це означає, що сервісний збиток успішно завданий. Типові DDoS–атаки, такі як категорії штормів, не викличуть серйозного впливу на жертву. Зазвичай вони відновлюються самостійно. Використання деяких лазівок в системі може привести до збою, перезапуску або припинення роботи сервера. Починаючи з цього моменту цільовій жертві може знадобитися викликати інженерів для ручного відновлення. Хоча деякі інші атаки безпосередньо знищують системні файли, це може привести до критичної втрати даних. У цьому випадку сервер може не надавати ті ж послуги навіть після перезавантаження вручну [16].

Фішинг. Починаючи від троянських вірусних програм, хробаків, закінчуючи DoS–атаками або DDoS–атаками, активні методи атак використовуються вже понад пару десятиліть. Кваліфікації, встановлені для сканування та фільтрації пакетів, надзвичайно жорсткі та розумні, наскільки це можливо.

Фішинг – це техніка, яка намагається приховати справжню особистість хакера, щоб викрасти особисту конфіденційну інформацію. Найпоширеніший спосіб розповсюдження фішингової інформації – це електронні листи, іноді також за допомогою миттєвих повідомлень. Майже точно такі ж інтерфейси входу були клоновані хакерами і були присутніми перед кінцевими жертвами, тому вони не будуть різнитися і твердо вводити туди свою приватну інформацію. Незважаючи на те, що протокол криптографії Secure Sockets Layer (SSL) використовується для ідентифікації сервера, який в даний час надає послугу входу, все одно дуже важко виявити, розпізнати та повністю уникнути фішингових атак.

Посилаючи електронну пошту, електронні листи можна отримати лише досить обмежені результати. Існує спосіб зробити фішинговий електронний лист, щоб він виглядав більш реалістичним – на основі попереднього реального електронного листа, надісланого офіційним джерелом, до нього буде внесено крихітні зміни. Це може містити приховуване гіперпосилання під звичайними текстами. Адреса електронної пошти відправника зазвичай відображається як ім’я чи група, а не як справжній формат електронної адреси, крім того, користувачі можуть не перевірити, чи гіперпосилання призведе їх туди, куди вони думали. Цей тип фішингу все ще широко використовується сьогодні (відомий як клонування).

У мережевому середовищі, яке наповнене плагінами браузера для захисту від фішингу, хакери переходять з тексту на зображення, тому фішинг–фільтри не зможуть його правильно виявити. Крім того, програми, які можуть всебічно перевірити веб–сайт, стають дедалі досконалішими.

Методів фішингу незліченна кількість і ці методи швидко розвиваються. Незалежно від того, яким чином хакери використовують методи, мета у них завжди однакова, конфіденційна інформація.

Не атакуючи недозволену лазівку, не використовуючи оригінальний недолік дизайну, фішинг зовсім відрізняється від активних методів атаки. Натомість для ініціювання можливої атаки, яка, ймовірно, принесе великі збитки жертві, не потрібно надто багато технічного досвіду. Для великої групи користувачів, якій не вистачає довіри або розвитку мережі, приносить небезпеку, і є предметом, який набагато складніший, ніж передбачалося.

Загрози при транспортуванні. Мережева карта (NIC) кожного хоста в мережі ідентифікується за допомогою апаратної адреси. Мережева карта буде запрограмована на прийом тільки пакетів, адресованих: апаратною адресою одноадресної розсилки, відповідному хосту, широкомовною апаратною адресою. Здатний зловмисник може перепрограмувати NIC з апаратною адресою іншого хоста і приймати пакети, адресовані цьому хосту. Щоб не бути спійманим, зловмисник може повернути копію пакета в мережу [17].

Прослуховування телефонних розмов – це процес добування інформації, переданої по мережі. Процес прослуховування різниться в залежності від використовуваного засобу зв'язку. У кабелях можна встановити засоби прослуховування за рахунок використання аналізатора пакетів або індуктивності. Сніффер пакетів – це комп'ютерне програмне забезпечення або обладнання, яке може перехоплювати трафік, що проходить через кабель локальної мережі. Аналізатор пакетів може використовуватися як для корисних, так і для зловмисних цілей:

- для аналізу мережевих проблем і моніторингу використання мережі,
- для фільтрації підозрілого контенту з мережевого трафіку,
- для вивчення структури заголовків пакетів різних протоколів, використовувані в мережі,
- для виявлення спроб вторгнення в мережу,
- для збору інформації для здійснення мережевого вторгнення.

Оскільки звичайний провід випромінює випромінювання при проходженні через нього електричних сигналів, зловмисник може торкнутися дроту і прочитати, що випромінюються сигнали через індуктивність, не вступаючи у фізичний контакт

з кабелем. Зловмисник, що перехоплює сигнали з широкосмугового кабелю, повинен відокремити цільової сигнал від всіх мультиплексованих сигналів.

Бездротові сигнали передаються через відкритий простір і більш уразливі для прослуховування. Чим ширше шлях проходження сигналу, тим легше зловмисникові перешкодити прямої видимості передачі між відправником і отримувачем, а також вловити всю передачу від антени, розташованої близько до одержувача.

Smurf Атака. Зловмисник може запустити атаку Smurf, відправивши підроблене повідомлення Echo–Request на широкомовний IP–адрес мережі. У підробленому повідомленні Echo–Request, як вихідний IP–адреси використовується IP–адреса жертви. Отже, кожен хост, який одержує широкомовне повідомлення Echo–Request, відправить жертві повідомлення Echo–Reply. Жертва буде завалена потоком повідомлень Echo–Reply. Таким чином, атака Smurf є різновидом атаки типу відмова в обслуговуванні (DoS). Є два рішення для запобігання атаки Smurf:

- Маршрутизатори не пересилають дейтаграми, що мають адресу призначення в якості широкомовної IP–адреси,
- хости налаштовані не відповідати на повідомлення Echo–Request, які були отримані як широкомовне повідомлення.

Перенаправлення трафіку. Скомпрометований маршрутизатор може відправляти повідомлення про оновлення маршруту всім своїм сусіднім маршрутизаторам, інформуючи їх про те, що він знаходиться на найкоротшому шляху до кожної мережі в Інтернеті. Сусідні маршрутизатори пересилають всі свої вхідні пакети даних цього скомпрометованого маршрутизатора, який в кінцевому підсумку буде заповнений пакетами даних і почне їх відкидати. Пакети даних не доходять до місця призначення.

Атаки на службу доменних імен (DNS). DNS–сервер – це машина, на якій зберігається таблиця (звана DNS–кешем), що відображає доменні імена в IP–адреси. Сервер запитує інші DNS–сервери, розташовані вище в ієрархії доменних імен, для розв'язання доменних імен, для яких у нього немає запису IP–адреси в кеші DNS, і оновлює свій кеш з урахуванням отриманого зіставлення. Отруєння кеша DNS – це

атака, за допомогою якої DNS–сервер змушують вважати зіставлення доменного імені та IP–адреси справжнім, хоча насправді це не так. Після зараження кешу DNS запис залишається в кеші деякий час і впливає на клієнтів, які в цей час використовують DNS–сервер. Наприклад, зловмисник може замінити інформацію про IP–адресу цільового файлового сервера на IP–адресу скомпрометованого файлового сервера, яким він керує. Зловмисник створює підроблені записи на зламаному сервері з іменами файлів, відповідними іменами на цільовому сервері. Ці файли можуть містити шкідливий вміст, таке як черв'як або вірус. Користувачі, які хочуть завантажувати файли з цільового файлового сервера, можуть через незнання завантажувати файли з шкідливим вмістом зі скомпрометованого файлового сервера.

Атака Syn Flood. Під час процесу встановлення TCP–з'єднання сервер підтримує чергу SYN_RECV, щоб відстежувати запити з'єднання, для яких він виділив ресурси і відповів повідомленням SYN / ACK, але відповідний ACK від клієнта ще не отримано. В кінцевому підсумку сервер втрачає час очікування пакета ACK і видаляє незавершений запит на з'єднання зі своєї черги. Зловмисник може запустити DDOS–атаку, відправивши кілька повідомлень із запитом на з'єднання SYN, використовуючи підроблені неіснуючі IP–адреси, і ніколи не відповісти повідомленнями ACK. Черга SYN_RECV сервера заповнюється повідомленнями з неповними запитами на з'єднання. Незважаючи на те, що ці неповні запити на з'єднання відкидаються після тайм–ауту, якщо справжній клієнт намагається встановити TCP–з'єднання з сервером в цей час, сервер відхиляє SYN–запит від цього клієнта [18].

1.7 Висновки за першим розділом

Переваги LAN:

- Все налаштування LAN займає невелику область, тому керувати цією мережею – нескладне завдання.

- Завдяки мережевий операційній системі легко налаштувати локальну мережу.
- LAN має високу швидкість з підтримкою кабелів Ethernet. Наприклад – в сучасній версії Ethernet.
- Він може підтримувати швидкість до гігабіта в секунду.
- Деякі захисні протоколи забезпечують відмінний захист від зловмисників.
- Завдяки хорошій швидкості, він забезпечує високу продуктивність малих і великих організацій.
- Це відмінна стабільна мережа в порівнянні з іншими, такими як WAN, MAN, PAN і т. Д.

Недоліки LAN (Local Area Network):

Є деякі обмеження мереж LAN, такі як –

- Обмеження географічного регіону – Локальні мережі в основному пов'язані на невеликій території, наприклад, в невеликому будинку, підприємстві.
- Проблема безпеки. Якщо комп'ютер централізованого сервера не налаштований належним чином, його дані можуть бути втрачені. Таким чином, зловмисник може скористатися перевагами і захопити ваші дані. Якщо будь–який комп'ютер заразиться вірусом, він зможе легко відтворити всю мережу.
- Залежність від сервера – якщо в будь–який момент централізований серверний комп'ютер вийде з ладу, вся система LAN може працювати належним чином. Таким чином, вся мережа LAN залежить від центральної серверної машини.
- Спочатку установка локальної мережі є дорогою – на початковому етапі для створення локальної мережі необхідно використовувати програмне забезпечення спеціального типу, таке як мережна операційна система, і інші компоненти мережевого обладнання, такі як концентратори, повторювачі, комутатори, кабелі і т. Д. Таким чином, ці апаратні і програмні компоненти мережі є дорогими.

- Конфіденційність порушена – адміністратор локальної мережі має право переглядати всі дані кожного підключеного користувача.

РОЗДІЛ 2
ІСНУЮЧІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ

Заходи, що забезпечують захист інформації в локальній мережі повинні бути представлені у вигляді плану, та бути попередньо опрацьованими. Профілактика виникнення критичних ситуацій є однією з найважливіших заходів.

Для забезпечення захисту повинні бути створені фізичні перешкоди для перешкоджання проникнення зловмисників до апаратури. Також повинен здійснюватися контроль над усіма ресурсами системи. З метою маскування інформації, яка передається по лініям зв'язку на великі відстані виконується криптографічне перетворення інформації. Заключним етапом є: створення сукупності правил безпеки, та забезпечення їх виконання співробітниками організації [19].

2.1 Проблеми безпеки локальних мереж

З точки зору безпеки локальні мережі мають наступні проблеми:

- відсутність механізму налаштування доступу декількох користувачів до різних ресурсів на одному комп'ютері;

- необхідність підготовлення користувача до різних адміністративних заходів – відновлення антивірусної бази, архівування даних, визначення механізмів доступу до ресурсів;
- поділ ресурсів і завантаження розподіляються по різних вузлах мережі, багато користувачів мають потенційну можливість доступу до мережі як до єдиної комп'ютерної системи;
- операційна система, що представляє складний комплекс взаємодіючих програм. В силу цього обставина важко сформулювати чіткі вимоги безпеки, особливо до загально цільових мереж, розроблялися без урахування безпеки;
- невизначена периферія сильно впливає на неможливість визначення, в більшості випадків, точних меж мережі. Один і той же вузол може одночасно працювати в декількох мережах, і, отже, ресурси однієї мережі цілком можуть використовуватися з вузлів, що входять в іншу мережу. Таке широкомасштабне поділ ресурсів, безсумнівно, перевага;
- множинність точок атаки в комп'ютерній системі, можна контролювати доступ до системи користувачів, оскільки цей доступ здійснюється з терміналів комп'ютерної системи. Ситуація в мережі зовсім інша: до одного і того ж файлу може бути затребуваний так званий віддалений доступ з різних вузлів мережі. Тому, якщо адміністратор окремої системи може проводити чітку політику безпеки щодо своєї системи, то адміністратор вузла мережі позбавлений такої можливості;
- не визначений розподіл траєкторії доступу. Користувач або загарбник може зажадати доступ до ресурсів деякого вузла мережі, з яким даний вузол не пов'язаний безпосередньо мережею. У таких випадках доступ здійснюється через певний проміжний вузол, пов'язаний з обома вузлами, або навіть через кілька проміжних вузлів. У комп'ютерних мережах вельми непросто точно визначити, звідки саме прийшов запит на доступ, особливо якщо загарбник докладе трохи зусиль до того, щоб приховати це;
- слабка захищеність лінії зв'язку. Мережа тим і відрізняється від окремої системи, що неодмінно включає в себе лінії зв'язку, по яких між вузлами

передаються дані. Це може бути елементарний провід, а може бути лінія радіозв'язку, в тому числі і супутниковий канал. При наявності певних умов (і відповідної апаратури) до провідника можна непомітно (або майже непомітно) під’єднатись, радіохвилю можна успішно прослуховувати.

2.2 Основні принципи забезпечення інформаційної безпеки

Основні принципи забезпечення інформаційної безпеки:

- Системність підходу.

Захист інформації передбачає необхідність врахування всіх взаємопов'язаних елементів, умов і чинників, істотно значущих для розуміння і вирішення проблеми забезпечення інформаційної безпеки.

При створенні системи захисту необхідно враховувати всі слабкі і найуразливіші місця системи обробки інформації, а також характер можливих об'єктів і порушення атак на систему з боку порушника, шляхи проникнення в систему для несанкціонованого доступу до інформації.

Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення, але і з урахуванням можливості появи переважно нових шляхів реалізації загроз безпеки.

Системний підхід також передбачає несуперечливість застосовуваних засобів захисту [20].

Тимчасова системність (принцип безперервності функціонування системи захисту):

Захист інформації це не разові заходи, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу захисту системи. Розробка системи захисту повинна починатися з моменту проектування системи захисту, а її адаптація та доопрацювання повинна здійснюватися протягом усього часу функціонування системи.

Зокрема за часом доби система захисту повинна функціонувати цілодобово. Дійсно, більшості засобів захисту для виконання своїх функцій необхідна підтримка

(Адміністрування), зокрема для призначення і зміни паролів, призначення секретних ключів, реакції на факти несанкціонованого доступу і т.д. перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу захищаються систем і ЗЗІ (засобів захисту інформації). Такі перерви в роботі ЗЗІ можуть використовуватися для внесення закладок, здійснення несанкціонованого доступу і т.д.

- Комплексні рішення.

У розпорядженні фахівців перебуває широкий спектр заходів, методів і засобів захисту інформаційних систем. Комплексне їх використання або комплексування передбачає узгоджене застосування різнорідних засобів захисту при забезпеченні інформаційної безпеки. Даний принцип передбачає врахування усієї сукупності можливих загроз при реалізації систем захисту.

- Розумна достатність засобів захисту.

Створити абсолютно непереборну систему захисту принципово неможливо. Тому при проектуванні системи безпеки має сенс вести мову про деяке її прийнятному рівні. При цьому необхідно розуміти, що високоефективна система захисту дорого коштує, може істотно знижувати продуктивність, що захищається і створювати відчутні незручності для користувача. Важливо правильно вибрати той правильний рівень захисту, при якому витрати, ризик злому і розмір можливих збитків були б прийнятні.

- Розумна надмірність засобів захисту.

Особливістю функціонування системи захисту є те, що рівень захищеності безперервно знижується в процесі функціонування системи. Це викликано тим, що будь–яка атака на систему як успішна, так і немає, дає інформацію зловмисникові. Накопичення інформації призводить до успішну атаку.

Сказане знаходиться в протиріччі з принципом розумної достатності. Вихід тут в розумному компромісі – на етапі розробки системи захисту в неї повинна закладатися якась надмірність, яка б дозволила збільшити термін її життєздатності.

- Гнучкість управління та застосування.

Як правило, система захисту проектується в умовах великої невизначеності. Тому що встановлюються засоби захисту можуть забезпечувати як надмірний, так і достатній рівень захищеності. Тому повинні бути реалізовані принципи гнучкості управління, що забезпечують можливість налаштування механізмів в процесі функціонування системи. Так, введення будь–якого нового вузла в мережі або зміну діючих умов не повинно знижувати досягнутого рівня захищеності корпоративної мережі в цілому.

- Відкритість алгоритмів і механізмів захисту.

Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок секретності, структурної безпеки і алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливість подолання системи захисту (Навіть автору).

- Простота застосування захисту, засобів і заходів.

Механізми захисту повинні бути інтуїтивно зрозумілі і прості в використанні. Вони повинні володіти інтуїтивно зрозумілим інтерфейсом, автоматичної і автоматизованої настройки. Система захист повинен по можливості мінімально заважати роботі користувачів, тому вона повинна функціонувати в «фоновому» режимі, була непомітною і ненав'язливою.

- Уніфікація засобів захисту.

Сучасні системи захисту відрізняються високим рівнем складності, що вимагає високої кваліфікації обслуговуючого персоналу.

З метою спрощення адміністрування систем безпеки доцільно прагнути до їх уніфікації, в межах підприємства. Наприклад, багато фірм–розробники ЗЗІ прагнуть до уніфікації журналів реєстрації систем виявлення атак, міжмережевих екранів [21].

2.3 Програмні засоби захисту

Програмне забезпечення для захисту інформації включає програми ідентифікації користувачів, засоби управління доступом, інформацію про шифрування, видалення залишкової (активної) інформації, наприклад, тимчасових файлів, тестового контролю системи захисту та ін.

Основні напрямки використання програмного захисту інформації:

- захист інформації від несанкціонованого доступу,
- захист програм від копіювання,
- захист інформації від руйнування,
- захист інформації від шкідливих програм,
- захист програм від шкідливих програм,
- програмний захист каналів зв'язку.

Програмні засоби захисту інформації можна розділити на наступні:

- вбудовані засоби захисту інформації;
- антивірусна програма – програма для виявлення комп'ютерних шкідливих програм і лікування інфікованих файлів, а також для профілактики – запобігання зараженню файлів або операційної системи шкідливим кодом.

Якщо мова йде про ПК, який здатний обмінюватись інформацією зі зовнішніми джерелами, то без антивірусної програми, яка є основним елементом в антивірусному захисті, не можливо говорити про ефективну антивірусну безпеку. Без використання антивірусної програми не можна гарантувати відсутність шкідливих програм, навіть якщо користувач буде дотримуватись всіх правил безпеки.

Антивірусне програмне забезпечення – це досить складний програмний комплекс, для його створення потрібні зусилля команди висококваліфікованих вірусних аналітиків, експертів і програмістів з багаторічним досвідом і вельми специфічними знаннями та вміннями. Основна технологія антивірусної перевірки – сигнатурний аналіз має на увазі безперервну роботу з моніторингу вірусних інцидентів і регулярний випуск оновлень антивірусних баз. З огляду на ці та інші причин, антивірусні програми не вбудовуються в операційні системи. Вбудованим

може бути тільки найпростіший фільтр, що не забезпечує повноцінної антивірусної перевірки [22].

Заходи захисту:

• Профілактика, до профілактичних засобів відносяться:

- перекриття шляхів проникнення шкідливих програм в комп'ютер;
- виключення можливості зараження і псування шкідливими програмами, які проникли в комп'ютер, інших файлів.

• Діагностика:

- діагностичні засоби дозволяють виявляти шкідливі програми в комп'ютері і розпізнавати їх тип.

• Лікування:

- лікування полягає у видаленні шкідливих програм із заражених програмних засобів і відновленні уражених файлів.

Захисний комплекс ґрунтується на застосуванні антивірусних програм і проведенні організаційних заходів.

- міжмережеві екрани (так звані брандмауери або фаєрволи). Між локальною та глобальною мережами створюються спеціальні проміжні сервери, які фільтрують весь трафік, який проходить через них, трафік мережевого / транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищений різновид методу – це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік посилається від імені firewall–сервера, роблячи локальну мережу практично невидимою;
- Proxy–servers (proxy – довіреність, довірена особа). Весь трафік мережевого / транспортного рівнів між локальною та глобальною мережами забороняється повністю – маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери–посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях – наприклад, на рівні додатку (шкідливі програми, код Java і JavaScript).

Цілі:

- забезпечення доступу комп'ютерів локальної мережі до мережі Інтернет.
- Кешування даних: якщо часто відбуваються звернення до одних і тих же зовнішніх ресурсів, то можна тримати їх копію на проксі–сервері і видавати за запитом, знижуючи тим самим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації. З розвитком динамічного контенту кешування втратило актуальність.
- Стиснення даних: проксі–сервер завантажує інформацію з Інтернету і передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі–сервери використовуються в основному з метою економії зовнішнього мережевого трафіку клієнта або внутрішнього – компанії, в якій встановлений проксі–сервер.
- Захист локальної мережі від зовнішнього доступу: наприклад, можна налаштувати проксі–сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони «бачать» тільки проксі–сервер).
- Обмеження доступу з локальної мережі до зовнішньої: наприклад, можна заборонити доступ до певних веб–сайтів, обмежити використання інтернету якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу і шкідливі програми.
- Анонімізація доступу до різних ресурсів. Проксі–сервер може приховувати відомості про джерело запиту або користувача. В такому випадку цільової сервер бачить лише інформацію про проксі–сервер, наприклад, IP–адресу, але не має можливості визначити дійсне джерело запиту. Існують також спотворюючі проксі–сервери, які передають цільовому серверу неправдиву інформацію про справжнього користувача.

- VPN (віртуальна приватна мережа) дозволяє передавати секретну інформацію через мережі, в яких можливе прослуховування трафіку сторонніми людьми. Використовувані технології: PPTP, PPPoE, IPSec;
- засоби управління доступом. Засоби управління доступом дозволяють специфікувати і контролювати дії, які суб'єкти – користувачі і процеси можуть

виконувати над об'єктами – інформацією і іншими комп'ютерними ресурсами. Йдеться про логічне управлінні доступом, який реалізується програмними засобами. Логічне управління доступом – це основний механізм багатокористувацьких систем, покликаний забезпечити конфіденційність і цілісність об'єктів і, до певної міри, їх доступність шляхом заборони обслуговування неавторизованих користувачів. Завдання логічного управління доступом полягає в тому, щоб для кожної пари (суб'єкт, об'єкт) визначити безліч допустимих операцій, залежне від деяких додаткових умов, і контролювати виконання встановленого порядку. Простий приклад реалізації таких прав доступу – якийсь користувач (суб'єкт) увійшов в інформаційну систему отримав право доступу на читання інформації з якогось диска (об'єкт), право доступу на модифікацію даних в якомусь каталозі (об'єкт) і відсутність будь–яких прав доступу до решти ресурсів інформаційної системи [23].

Контроль прав доступу проводиться різними компонентами програмного середовища – ядром операційної системи, додатковими засобами безпеки, системою управління базами даних, посередницьким програмним забезпеченням (таким як монітор транзакцій) і т.д.;

- засоби ідентифікації та автентифікації. Ідентифікацію та автентифікацію можна вважати основою програмно–технічних засобів безпеки. Ідентифікація та автентифікація – це «прохідна» інформаційного простору організації.

Ідентифікація дозволяє суб'єкту – користувачеві або процесу, чинному від імені певного користувача, назвати себе, повідомивши своє ім'я. За допомогою автентифікації друга сторона переконується, що суб'єкт дійсно той, за кого себе видає. Як синонім слова «Автентифікація» іноді використовують поєднання «перевірка справжності».

Паролі давно вбудовані в операційні системи та інші сервіси. при правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх слід визнати найслабшим засобом перевірки автентичності. Надійність паролів ґрунтується на здатності пам'ятати їх і зберігати в таємниці. Паролі уразливі по відношенню до електронного перехоплення – це найбільш принциповий недолік, який не можна

компенсувати поліпшенням адміністрування або навчанням користувачів. Практично єдиний вихід – використання криптографії для шифрування паролів перед передачею по лініях зв'язку [24].

2.4 Апаратні засоби захисту

Апаратні (технічні) засоби захисту інформації – це різні за типом пристрою (механічні, електромеханічні, електронні і ін.), які апаратними засобами вирішують завдання захисту інформації. Вони перешкоджають доступу до інформації, в тому числі за допомогою її маскування. До апаратних засобів відносяться: генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, «перекривають» потенційні канали витоку інформації або дозволяють їх виявити.

До апаратних засобів захисту інформації відносяться самі різні за принципом дії, влаштування та можливостям технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидія несанкціонованому доступу до джерел конфіденційної інформації [25].

Апаратні засоби захисту інформації застосовуються для вирішення наступних завдань:

- проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;
- виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;
- локалізація каналів витоку інформації;
- пошук і виявлення засобів промислового шпигунства;
- протидія несанкціонованому доступу до джерел конфіденційної інформації та іншим діям.

За функціональним призначенням апаратні засоби можуть бути класифіковані на засоби виявлення, засоби пошуку та детальних вимірювань, засоби активного і пасивного протидії. При цьому за своїми технічними можливостями засоби захисту інформації можуть бути загального призначення, розраховані на використання непрофесіоналами з метою отримання попередніх (загальних) оцінок, і професійні

комплекси, що дозволяють проводити ретельний пошук, виявлення і прецизійні вимірювання всіх характеристик засобів промислового шпигунства.

Пошукову апаратуру можна поділити на апаратуру пошуку засобів знімання інформації і дослідження каналів її витоку. Апаратура першого типу спрямована на пошук і локалізацію вже впроваджених зловмисниками коштів несанкціонованого доступу. Апаратура другого типу призначається для виявлення каналів витоку інформації [26].

2.5 Комбіновані засоби захисту

Система виявлення вторгнення (IDS – Intrusion Detection System) є програмними або апаратними системами, які автоматизують процес перегляду подій, що виникають в комп'ютерній системі або мережі, і аналізують їх з точки зору безпеки. Так як кількість мережевих атак зростає, IDS стають необхідним доповненням інфраструктури безпеки.

Виявлення проникнення є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі, і аналізу їх проникнення визначаються як спроби компрометації конфіденційності, цілісності, доступності або обходу механізмів безпеки комп'ютера або мережі. Проникнення можуть здійснюватися як атакуючими, які отримують доступ до системам з Інтернету, так і авторизованими користувачами систем, намагаються отримати додаткові привілеї, яких у них немає. IDS є програмними або апаратними пристроями, які автоматизують процес моніторингу та аналізу подій, що відбуваються в мережі або системі, з метою виявлення проникнень.

IDS складаються з трьох функціональних компонентів: інформаційних джерел, аналізу та відповіді. Система отримує інформацію про подію з одного або більше джерел інформації, виконує визначається конфігурацією аналіз даних події і потім створює спеціальні відповіді – від найпростіших звітів до активного втручання при визначенні проникнень [27].

Основними комерційними IDS є Network–based. Ці IDS визначають атаки, захоплюючи і аналізуючи мережеві пакети, слухаючи мережевий сегмент, Network–based IDS може переглядати мережевий трафік від кількох хостів, які приєднані до мережевого сегменту, і таким чином захищати ці хости.

Network–based IDS часто складаються з безлічі сенсорів, розташованих в різних точках мережі. Ці пристрої переглядають мережевий трафік, виконуючи

локальний аналіз даного трафіку і створюючи звіти про атаки для центральної керуючої консолі. Багато з цих сенсорів розроблені для виконання в «Невидимому (stealth)» режимі, щоб зробити більш важким для атакуючого виявлення їх присутності і розташування.

Host–based IDS мають справу з інформацією, зібраною всередині єдиного комп'ютера. (Application–based IDS є підмножиною Host–based IDS.) Таке вигідне розташування дозволяє Host–based IDS аналізувати діяльність з великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають ставлення до конкретної атаці в ОС. Більш того, на відміну від Network–based IDS, Host–based IDS можуть «бачити» наслідки розпочатої атаки, так як вони можуть мати безпосередній доступ до системної інформації, файлів даних і системним процесам, що є метою атаки.

Host–based IDS зазвичай використовують інформаційні джерела двох типів: результати аудиту ОС і системні логи. Результати аудиту ОС зазвичай створюються на рівні ядра ОС і, отже, є більш детальними і краще захищеними, ніж системні логи. Однак системні логи набагато менше і не такі численні, як результати аудиту, і, отже, легше для розуміння. Деякі Host–based IDS розроблені для підтримки централізованої інфраструктури управління та отримання звітів IDS, що може допускати єдину консоль управління для відстеження багатьох хостів. Інші створюють повідомлення в форматі, який сумісний з системами мережевого управління [28].

2.6 Криптографічні засоби захисту

Криптографічні засоби захисту дозволяють захистити інформацію навіть після її перехоплення. Сучасна криптографія є областю знань, пов'язаної з рішенням таких проблем безпеки інформації, як конфіденційність, цілісність, автентифікація і неможливість відмови сторін від авторства. Досягнення цих вимог безпеки інформаційної взаємодії та становить основні цілі криптографії.

Сертифіковані шифрувальні засоби, призначені для захисту інформації, яка не містить відомості, що становлять державну таємницю, за функціональним призначенням забезпечують захист від прочитання і від несанкціонованого доступу до документальної інформації при її передачі по каналу зв'язку, обробці і зберіганні, а також захист інформації від безпосереднього прослуховування в телефонному каналі зв'язку. Основна категорія програмно–апаратних та програмних засобів захисту документальної інформації, як правило, поєднують в собі функцію шифрування з процедурами вироблення і перевірки електронного цифрового підпису (ЕЦП) [29].

Сучасна криптографія включає в себе чотири великих розділи:

1. Симетричні криптосистеми. У симетричних криптосистемах і для шифрування, і для дешифрування використовується один і той же ключ.

2. Криптосистеми з відкритим ключем. У системах з відкритим ключем використовуються два ключі – відкритий і закритий, які математично пов'язані один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення (ключ – інформація, необхідна для безперешкодного шифрування і дешифрування текстів.).

3. Електронний підпис. Системою електронного підпису називається приєднання до тексту його криптографічне перетворення, яке дозволяє при отриманні тексту іншим користувачем перевірити авторство і справжність повідомлення.

4. Управління ключами. Це процес системи обробки інформації, змістом яких є складання і розподіл ключів між користувачами.

Основні напрямки використання криптографічних методів – передача конфіденційної інформації з каналів зв'язку (наприклад, електронна пошта), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшої вартістю, проте їй притаманні і переваги: висока продуктивність, простота, захищеність і т.д. Програмна реалізація більш практична, допускає відому гнучкість у використанні для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги [30]:

- зашифроване повідомлення повинно піддаватися читання тільки при наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифрування інформації шляхом перебору всіляких ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);
- знання алгоритму шифрування не повинно впливати на надійність захисту;
- незначна зміна ключа повинно приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинен бути повністю та надійно сховані в зашифрованому тексті;
- довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

- не повинно бути простих і легко встановлюваних залежністю між ключами, послідовно використовуваними в процесі шифрування;
- будь–який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинно вести до якісного погіршення алгоритму шифрування.

2.7 Висновки за другим розділом

Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки – обмежена функціональність мережі, використання частини ресурсів файл–сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

РОЗДІЛ 3
ЗАХИСТ ІНФОРМАЦІЇ В ЛОКАЛЬНИЙ МЕРЕЖІ

3.1 Заходи, необхідні для захисту мереж за допомогою мережевих елементів керування

Необхідно встановити контроль доступу до мережі. Мережеві елементи управління засновані на програмному або апаратному забезпеченні та реалізовані у вигляді ієрархічної структури, що відбиває мережеву організацію. Ця ієрархія накладається на мережу від периметра мережі до рівня доступу кожного користувача до мережевих ресурсів. Функції мережевого управління полягають у виявленні несанкціонованого доступу, запобігання порушення безпеки мережі і, нарешті, в реагуванні на порушення: таким чином, існують три категорії виявлення, запобігання і реагування.

Роль превентивного контролю полягає в тому, щоб зупинити несанкціонований доступ до будь–якого ресурсу, доступному в мережі. Це може бути реалізовано так само просто, як пароль, необхідний для автентифікації користувача для доступу до ресурсу в мережі. Для авторизованого користувача цей пароль може надати вхід в мережу для доступу до служб бази даних, файлу, Інтернету, друку або сервера електронної пошти. Адміністратора пароль потрібен для доступу до комутатора або маршрутизатора. Профілактичний контроль в цьому випадку заснований на програмному забезпеченні. Аналогом апаратного управління може бути, наприклад, ситуація, коли такі ресурси, як серверні комп'ютери, комутатори і маршрутизатори, заблоковані в кімнаті управління доступом до мережі.

Роль контролю виявлення полягає в тому, щоб відстежувати дії в мережі та ідентифікувати подію або набір подій, які можуть негативно вплинути на безпеку мережі. Такою подією може бути атака вірусу, шпигунського або рекламного ПЗ. Крім реєстрації атаки, програмне забезпечення може генерувати або запускати

сигнал тривоги, щоб повідомити про незвичайну подію, щоб можна було негайно зробити коригувальні дії без шкоди для безпеки.

Роль управління реагуванням полягає в тому, щоб приймати коригувальні заходи щоразу, коли порушується безпека мережі, щоб виявляти такі ж порушення і запобігати подальшим пошкодження.

Проведення оцінки ризиків. На початковому етапі проектування мережі мережеві архітектори оцінюють типи ризиків для мережі, а також витрати на відновлення після атак для всіх ресурсів, які були скомпрометовані. Ці фактори витрат можуть бути реалізовані з використанням добре відпрацьованих процедур бухгалтерського обліку, таких як аналіз рентабельності, окупності інвестицій і загальної вартості володіння. Ці ризики можуть варіюватися від стихійного лиха до атаки хакера. Отже, необхідно розробити рівні ризиків для різних загроз для мережі. Необхідно розробити електронну таблицю, в якій перераховані ризики в порівнянні з загрозами, а також відповіді на ці виявлені загрози. Звичайно, електронна таблиця також відзначить розміщення елементів управління доступом до мережі для захисту мережі.

Перелік мережевих ресурсів. Необхідно визначити активи (ресурси), доступні в локальній мережі. Критично важливі компоненти будь–якої локальної мережі: маршрутизатор, сервер доменних імен, веб–сервер, сервер електронної пошти, основні комутатори, бази даних. Критично важливим компонентам необхідно встановити пріоритети, тому що не всі вони забезпечують однакові функції. Деякі ресурси надають контрольований доступ до мережі, інші несуть конфіденційні дані. Отже, загрози, які виходять від цих ресурсів, не несуть в собі таку ж ступінь уразливості мережі. Отже, контроль доступу до мережі повинен бути сформульований і застосований до кожного з перерахованих компонентів в різного ступеня. Наприклад, загрози сервера доменних імен створюють інший набір проблем, ніж загрози сервера бази даних.

Основні цілі політики безпеки – забезпечити безперервний доступ до мережевих ресурсів для автентифікованих користувачів і заборонити доступ нерозпізнаних користувачів. Звичайно, це завжди баланс між потребами

користувачів в мережевих ресурсах та еволюційним характером інформаційних технологій.

Політика мережевої безпеки може бути як простою, так і може бути роздільний доступ до ресурсів. Більшість користувачів локальної мережі повинні підписати політику використання мережі, і пам'ятати, що порушення безпеки є караним злочином. Найважливішими функціями хорошою політики безпеки є:

- Призначений адміністратор безпеки, який знайомий з вимогами користувачів і готовий постійно задовольняти потреби спільноти користувачів.
- Встановлена ієрархічна політика безпеки, яка відображатиме структуру.
- Визначені етичні можливості доступу в Інтернет.
- Розвиток політики віддаленого доступу.
- Забезпечений набір процедур обробки інцидентів.

Процес усунення інциденту. Процес обробки інцидентів – найважливіше завдання політики безпеки. Мета мережі – поділ ресурсів, тому необхідно розробити ефективну процедуру реагування на порушення.

Необхідний набір інструментів для моніторингу активності в мережі: система виявлення і запобігання вторгнень. Ці частини програмного забезпечення відстежуватимуть мережеву активність, реєструвати і повідомляти про дії, які не відповідають звичайним або прийнятним стандартам, визначеним програмним забезпеченням. Після виявлення і реєстрації активності активується відповідь. Недостатньо відреагувати на інцидент; мережевий адміністратор також повинен активувати інструменти, щоб відстежити джерело цього порушення. Це дуже важливо, так як мережевий адміністратор може оновити процедури безпеки, щоб переконатися, що цього конкретного інциденту не сталося.

Безпечний дизайн контроль доступу мережі. Для того щоб убезпечити мережу, потрібно визначити точки входу і виходу в мережу. Оскільки в більшості мереж передачі даних є обчислювальні вузли для обробки даних і вузли зберігання для зберігання даних, де дані можуть потребувати шифрування, щоб в разі порушення мережевої безпеки вкрадені дані могли залишатися конфіденційними, якщо не було порушено шифрування.

Точкою входу в будь–яку мережу є маршрутизатор, який знаходиться між зовнішнім фаєрволом і Інтернетом, ця модель може бути застосована до більшості локальних мереж. Отже, перший контроль доступу до мережі полягає у визначенні політики безпеки на маршрутизаторі периметра шляхом налаштування відповідних параметрів на маршрутизаторі. Маршрутизатор периметра буде фільтрувати трафік на основі діапазону IP–адрес.

Наступним по лінії захисту йде зовнішній брандмауер, який фільтрує трафік в залежності від стану мережевого підключення. Крім того, міжмережевий екран може перевіряти вміст пакета трафіку на предмет характеру запитаного з'єднання по протоколу управління передачею (TCP). Після брандмауера є так звана демілітаризована зона (DMZ), де розміщено наступні сервери: Інтернет, DNS і електронна пошта [31].

DMZ знаходиться між двома міжмережевими екранами, тому остання лінія захисту – це наступний міжмережевий екран, який буде перевіряти трафік і, можливо, фільтрувати потенційну загрозу. Вузли, розміщені в інтрамережі, можуть бути захищені комерційно доступним антивірусним програмним забезпеченням. І останнє: встановити в мережі систему виявлення і запобігання вторгнень, яка буде в режимі реального часу реагувати на загрозу.

Традиційний мережевий дизайн включає рівень доступу, рівень розподілу і базовий рівень. У разі LAN буде використано рівні доступу і розподілу, базовий рівень буде просто маршрутизатором периметра. Таким чином, LAN буде складатися з ряду сегментів, що відображають організаційну структуру.

Система виявлення вторгнень. Система виявлення вторгнень може бути як програмною, так і апаратною. IDS відстежує всі дії, що відбуваються як на комп'ютері (вузлі в мережі), так і в самій мережі. IDS збирає інформацію з різних системних і мережевих ресурсів, але насправді вона захоплює пакети даних, як це визначено стеком протоколів TCP / IP. У цьому сенсі IDS є одночасно програмним сніффером і аналізатором. У своїй ролі сніффер IDS буде або захоплювати все пакети даних, або вибирати ті, які вказані в сценарії конфігурації. Цей сценарій конфігурації являє собою набір правил, які повідомляють аналізатору, що шукати в

захопленому пакеті даних, а потім роблять обґрунтоване припущення за правилами і генерують попередження. Звичайно, це може привести до чотирьох можливих результатів щодо виявлення вторгнень: хибнопозитивний, псевдонегативний, істинно позитивний або істинно негативний. IDS виконує безліч функцій:

- контролювати і аналізувати дії користувачів і системи;
- перевіряти цілісність файлів даних, файли конфігурації системи аудиту;
- розпізнавати активність патернів, що відображають відомі атаки
- аналізувати статистику будь–якого невизначеного паттерна активності.

IDS здатна розрізняти різні типи мережевого трафіку, такі як запит протоколу передачі гіпертексту (HTTP) через порт 80 від будь–якого іншого застосування, такого як SMTP, який запускається через порт 80. IDS розуміє, які програми TCP / IP працюють із заздалегідь призначеними номерами портів, і тому фальсифікація номерів портів може бути легко виявлена.

Завдання пакетів програмного забезпечення для виявлення вторгнень – уможливити складне, а іноді і практично нездійсненне завдання з управління безпекою системи. Програмне забезпечення IDS комерційного рівня розроблено з зручними інтерфейсами, які спрощують встановлення сценаріїв, що встановлюють правила виявлення вторгнень. Важливі функції IDS:

- надавати більшу ступінь гнучкості інфраструктурі безпеки мережі;
- контролювати функціональність маршрутизаторів, включаючи міжмережеві екрани, сервери і критично важливі комутатори;
- відстежувати активність користувачів від точки входу в мережу до точки виходу;
- повідомляти про перевірки цілісності файлів;
- визначати, чи була змінена конфігурація системи в результаті атаки;
- розпізнавати потенційну атаку і згенерувати попередження
- робити можливим управління безпекою мережі не маючи відповідної кваліфікації персоналу.

Датчики NIDS сканують мережні пакети на рівні маршрутизатора або хоста, перевіряють пакети даних і записують будь–які підозрілі пакети в файл журналу. Пакети даних захоплюються програмою–сніффером, яка є частиною програмного пакета IDS. Вузол, на якому включено програмне забезпечення IDS, працює в нерозбірливому режимі. У нерозбірливому режимі вузол NIDS захоплює всі пакети даних в мережі, як визначено сценарієм конфігурації. NIDS стали критично важливим компонентом управління мережевою безпекою, оскільки кількість вузлів в Інтернеті за останні кілька років зросла в геометричній прогресії. Ось деякі поширені шкідливі атаки на мережі:

- підміна IP–адреси;
- підміна адреси управління доступом до середовища (MAC);
- отруєння кеша протоколу дозволу адрес (ARP);
- пошкодження DNS–імені.

Деякі не дуже надійні функції системи виявлення мережевих вторгнень.

IDS не може компенсувати слабку ідентифікацію та автентифікацію. Отже, потрібно покладатися на інші засоби ідентифікації і автентифікації користувачів. Найкраще це реалізувати за допомогою токен–орієнтованих або біометричних схем і одноразових паролів.

IDS не може проводити розслідування атак без втручання людини. Тому, коли інцидент все–таки відбувається, необхідно визначити кроки щодо його усунення. Інцидент повинен бути відстежено для визначення відповідальної сторони, потім необхідно діагностувати і виправити уразливість, яка привела до виникнення проблеми. IDS не здатна ідентифікувати зловмисника, тільки по IP–адресі вузла, який служив точкою входу хакера.

IDS не може компенсувати недоліки мережевих протоколів. Підміна IP– і MAC–адрес – це поширена форма атаки, при якій вихідний IP або MAC–адреса не відповідає реальній вихідній IP або MAC–адресі хакера. Підроблені адреси можна імітувати для створення DDoS–атак [32].

IDS не може компенсувати проблеми з цілісністю інформації, що надається системою. Багато інструментів для атаки націлені на системні журнали, вибірково

стираючи записи, відповідні часу атаки, і таким чином приховують сліди хакера. Це вимагає надлишкових джерел інформації.

IDS не може аналізувати весь трафік в завантаженій мережі. Мережева IDS в безладному режимі може захоплювати всі пакети даних, в міру збільшення рівня трафіку NIDS може досягти точки насичення і почати втрачати пакети даних.

IDS не завжди може впоратися з проблемами, пов'язаними з атаками на рівні пакетів. Уразливості полягають в різниці між інтерпретацією IDS результату мережевої транзакції і фактичною обробкою транзакції вузлом призначення для даного мережевого сеансу. Отже, хакер може відправити серію фрагментованих мережевих транзакцій.

IDS має проблеми з обробкою фрагментованих пакетів даних. Хакери зазвичай використовують фрагментацію, щоб заплутати IDS і, таким чином, почати атаку.

Встановлення брандмауерів. Технологія брандмауера розвивалася для захисту локальної мережі від неавторизованих користувачів в Інтернеті. Так було в перші роки існування корпоративних мереж. З тих пір мережеві адміністратори усвідомили, що мережі можуть бути атаковані як довіреними користувачами, так і, наприклад, співробітниками компанії. Корпоративна мережа складається із сотень вузлів в кожному відділі і, таким чином, об'єднується до 1000 і більше, і тепер існує потреба в захисті даних в кожному відділі від інших відділів. Отже, виникла потреба у внутрішніх міжмережевих екранах для захисту даних від несанкціонованого доступу, навіть якщо вони є співробітниками корпорації. Згодом ця потреба призвела до розробки сегментованих IP–мереж, так що внутрішні міжмережеві екрани створювали бар'єри всередині бар'єрів, щоб обмежити потенційне проникнення в IP–сегмент, а не піддавати всю корпоративну мережу хакеру.

Майже кожна інтрамережа завжди підключена до Інтернету, і тому потенційна кількість хакерів чекають, щоб атакувати її. Таким чином, кожна інтрамережа є IP–мережею, в якій працюють додатки на основі TCP і UDP. Конструкція протоколів TCP і UDP вимагає, щоб кожен клієнт–серверний додаток взаємодіяв з іншими клієнт–серверними додатками через номери портів TCP і UDP. Як зазначалося

раніше, ці номери портів TCP і UDP добре відомі і, отже, призводять до необхідної слабкості в мережі. Номери портів TCP і UDP самі по собі створюють «дірки» в мережах. Кожна точка входу в Інтернет і інтрамережа повинна бути захищена, і потрібно відслідковувати трафік (пакети даних), який входить і залишає мережу.

Брандмауер – це комбінація апаратних і програмних технологій, який чекає в точках входу і виходу, щоб виявляти неавторизований пакет даних, який намагається отримати доступ до мережі. Адміністратор за допомогою іншого IT–персоналу повинен спочатку визначити ресурси і конфіденційні дані, які необхідно захистити від хакерів. Після виконання цього завдання наступне завдання – визначити, хто буде мати доступ до цих ідентифікованим ресурсів і даних.

Як тільки політика мережевої безпеки визначена і зрозуміла, можна визначити правильне розміщення міжмережевих екранів по відношенню до ресурсів в мережі. Отже, наступним кроком буде фактичне розміщення міжмережевих екранів в мережі в якості вузлів. Політика мережевої безпеки тепер визначає доступ до мережі, як це реалізовано в брандмауері. Ці права доступу до мережевих ресурсів засновані на характеристиках протоколів TCP / IP і номерів портів TCP / UDP.

Брандмауер дозволяє адміністратора централізувати контроль доступу до мережі. Брандмауер реєструє кожен пакет, який входить і залишає мережу. Політика безпеки мережі, реалізована в брандмауері, забезпечує кілька типів захисту, в тому числі:

- блокування небажаного трафіку;
- напрямок вхідного трафіку на більш надійні внутрішні вузли;
- приховування вразливих вузлів, які нелегко захистити від зовнішніх загроз;
- реєстрація трафіку в і з мережі.

Брандмауер прозорий для авторизованих користувачів (як внутрішніх, так і зовнішніх), тоді як він не прозорий для неавторизованих користувачів. Однак, якщо авторизований користувач намагається отримати доступ до послуги, яка не дозволена для цього користувача, буде відображений відмову в цій послузі, і ця спроба буде зареєстрована.

DMZ – це мережа периметра, в якій ресурси мають загальнодоступні IP–адреси, тому їх можна побачити в Інтернеті. Такі ресурси, як Інтернет (HTTP), електронна пошта (SMTP) і DNS, поміщаються в DMZ. Ресурси в демілітаризованій зоні можуть бути атаковані хакером, оскільки вони відкриті для користувачів в Інтернеті. Відповідні номери портів TCP і UDP на серверах в демілітаризованій зоні повинні бути відкриті для вхідного і вихідного трафіку.

Концептуально існує три типи міжмережевих екранів [33]:

- фільтрація пакетів: дозволяє пакетам входити в мережу або залишати її через інтерфейс на маршрутизаторі на основі протоколу, IP–адреси і номерів портів. Маршрутизатор з фільтрацією IP–пакетів дозволяє або забороняє пакету входити або виходити з мережі через інтерфейс (вхідний та вихідний) на основі протоколу, IP–адреси і номера порту. Протокол може бути TCP, UDP, HTTP, SMTP або протоколом передачі файлів (FTP). Розглянута IP–адреса буде як адресою джерела, так і адресою призначення вузлів. Міжмережевий екран з фільтрацією пакетів повинен перевіряти кожен пакет і приймати рішення на основі певного ACL, крім того, він буде реєструвати такі захищені атаки в мережі:

  - хакер, який намагається відправити підроблені IP–пакети з використанням сирих сокетів;
  - реєструвати спроби сканування мережі на предмет відкритих портів TCP і UDP, NIDS проведе цю детективну роботу більш детально;
  - SYN–атаки з використанням TCP connect () і напіввідкритого TCP;
  - фрагментарні атаки.

- брандмауер прикладного рівня: проксі–сервер, який діє як проміжний хост між вихідним і цільовим вузлами. Проксі–сервери, які діють як проміжний вузол між вихідним і цільовим вузлами. Кожен з джерел повинен буде встановити сеанс з проксі–сервером; потім проксі–сервер встановить сеанс з вузлом призначення. Пакети повинні проходити через проксі–сервер. В Інтернеті є приклади проксі–серверів Web і FTP. Проксі–сервери також повинні застосовувати внутрішні користувачами: тобто трафік від внутрішніх користувачів повинен проходити через проксі–сервер в зовнішню мережу;

- рівень перевірки стану: перевіряє пакет на основі його вмісту. У брандмауерах з перевіркою стану брандмауер перевіряє вміст пакетів, перш ніж дозволити їм вхід або вихід з мережі. Вміст пакетів має відповідати протоколу, заявленому в пакеті. Наприклад, якщо оголошений протокол HTTP, вміст пакету має відповідати визначенню пакета HTTP.

Система виявлення вторгнень в мережі (встановлення додаткового фаєрволу). Міжмережевий екран діє як бар'єр, якщо він так спроектований, між різними сегментами IP–мережі. Міжмережеві екрани можуть бути визначені серед IP–сегментів локальної мережі для захисту ресурсів. У будь–якої корпоративної мережі завжди буде кілька міжмережевих екранів, тому що зловмисник може бути одним з авторизованих користувачів мережі.

Оскільки брандмауер знаходиться на кордоні сегментів IP–мережі, він може тільки відслідковувати вхідний і вихідний трафік на інтерфейсі брандмауера, який підключається до мережі. Якщо зловмисник знаходиться всередині брандмауера, брандмауер не зможе виявити порушення безпеки. Як тільки зловмисникові вдасться пройти через інтерфейс брандмауера, зловмисник залишиться непоміченим, що може привести до крадіжки конфіденційної інформації, знищення інформації, залишивши після себе віруси, організувавши атаки на інші мережі та, що найбільш важливо, залишивши шпигунське ПЗ для відстеження дій в мережі на предмет майбутніх атак. Отже, NIDS буде грати вирішальну роль у моніторингу діяльності в мережі і постійному пошуку можливих аномальних моделей діяльності.

Нове покоління хакерів використовувало тунелювання як засіб обходу політики безпеки брандмауера. NIDS покращує інфраструктуру безпеки, відстежуючи дії системи на предмет ознак атаки, а потім, в залежності від налаштувань системи, реагує на атаку, а також генерує сигнал тривоги. Відповідь на потенційну атаку відомий як реакція на інцидент або обробка інциденту; він об'єднує фази дослідження і діагностики. Реагування на інциденти – це нова технологія, яка зараз є невід'ємною частиною технологій виявлення і запобігання вторгнень.

Що не менш важливо, захист мережевих систем – це безперервний процес, в якому постійно виникають нові загрози. Отже, міжмережеві екрани, NIDS і системи запобігання вторгнень є технологіями, які постійно розвиваються.

Моніторинг і аналіз діяльності системи. Наступне питання стосується термінів збору інформації, хоча це залежить від ступеня загрози, яка сприймається для мережі.

Якщо рівень передбачуваної загрози для мережі низький, негайна реакція на атаку не має вирішального значення. В такому випадку збір і аналіз даних з інтервалом є найбільш економічними з точки зору навантаження на NIDS і інші ресурси в мережі. Крім того, може не вистачити штатного персоналу з питань безпеки мережі, який міг би реагувати на сигнал тривоги, ініційований NIDS.

Якщо рівень передбачуваної загрози неминучий, а час і дані критично важливі для організації, збір і аналіз даних в реальному часі мають надзвичайно важливе значення. Звичайно, збір даних в реальному часі вплине на цикли в NIDS і призведе до величезного обсягу зберігання даних. Завдяки збору і аналізу даних в реальному часі відповідь на атаку в реальному часі може бути автоматизований за повідомленням. В такому випадку мережева діяльність може бути перервана, інцидент може бути ізольований, а відновлення системи і мережі може бути розпочато.

Захоплення і зберігання пакетів даних – одна з керованих функцій будь–якої IDS. Щоб проаналізувати пакети даних, які представляють потенційні або неминучі загрози для мережі, необхідно вивчити пакети даних і знайти докази, які можуть вказувати на загрозу. Звичайно, будь–який пакет майже інкапсулюється послідовними протоколами з Інтернет–моделі з даними в якості його ядра. Потенційні атаки можуть бути викликані спуфінгом IP або MAC, фрагментованими IP–пакетами, які ведуть до якогось DoS. Цей процес перевірки зводиться до алгоритму. Цей алгоритм повинен порівнювати пакети з відомим форматом пакета (сигнатури), який передбачає, що атака триває, або це може бути якась незвичайна активність в мережі. Повинен бути якийсь базовий рівень (статистичний), який

вказує на норму, і відхилення від нього буде показником відхилення від норми. Можна виділити два рівня аналізу: сигнатурний і статистичний.

Сигнатурний аналіз включає свого роду зіставлення зі зразком вмісту пакетів даних. Є шаблони, відповідні відомим атакам. Ці відомі атаки зберігаються в базі даних, і шаблон перевіряється на відповідність відомим шаблоном, який визначає аналіз сигнатур. Більшість комерційних продуктів NIDS виконують аналіз сигнатур бази даних відомих атак, яка є частиною програмного забезпечення NIDS. Хоча бази даних відомих атак можуть бути власністю постачальника, клієнт цього програмного забезпечення повинен мати можливість розширювати обсяг програмного забезпечення NIDS, додаючи сигнатури в базу даних.

Спочатку необхідно визначити, що становить нормальну структуру трафіку в мережі. Потім необхідно ідентифікувати відхилення від нормальних моделей як потенційні загрози. Ці відхилення повинні бути отримані шляхом статистичного аналізу схем руху. Хорошим прикладом може бути те, скільки разів записи записуються в базу даних за певний проміжок часу, а відхилення від звичайно прийнятих чисел вказують на те, що насувається атака. Звичайно, хакер може ввести детектор в оману, прийнявши атаку як нормальну, поступово міняючи поведінку з плином часу. Це був би приклад помилково негативного результату.

Сигнатурний аналіз заснований на наступних алгоритмах:

- зіставлення зі зразком;
- зіставлення зі зразком зі збереженням стану;
- аналіз протоколу на основі декодування;
- евристичний аналіз;
- аналіз на основі аномалій.

Відповідність шаблонам. Зіставлення зі зразком засноване на пошуку фіксованої послідовності байтів в одному пакеті. У більшості випадків шаблон порівнюється тільки з тим, чи пов'язаний підозрілий пакет з певною службою або, точніше, призначений для певного порту і від нього. Це допомагає зменшити кількість пакетів, які необхідно перевірити, і, таким чином, прискорює процес

виявлення. Однак це має тенденцію ускладнювати системам роботу з протоколами, які не існують на чітко визначених портах.

Переваги цього простого алгоритму полягають в наступному:

- Цей метод дозволяє безпосередньо співвідносити експлойт з шаблоном.
- Цей метод можна застосовувати до всіх протоколів.

Недоліки цього підходу полягають в наступному:

- Будь–яка модифікація атаки може привести до пропущених подій (псевдонегативним результатам).
- Цей метод може привести до високого рівня помилкових спрацьовувань, якщо шаблон не настільки унікальний, як припускав автор.
- Цей метод зазвичай обмежується перевіркою одного пакета і тому не підходить для потокової природи мережевого трафіку, такого як трафік HTTP.

Зіставлення зі зразком з відстеженням стану – цей метод доповнює концепцію зіставлення зі зразком, оскільки мережевий потік складається з більш ніж одного атомарного пакета. Відповідності повинні виконуватися в контексті стану потоку. Це означає, що системи, які виконують цей тип аналізу сигнатур, повинні враховувати порядок прибуття пакетів в потоці TCP. Це схоже на брандмауер з відстеженням стану.

Тепер замість того, щоб шукати шаблон в кожному пакеті, система повинна почати підтримувати інформацію про стан потоку TCP.

Переваги цієї техніки в тому, що:

- Цей метод дозволяє безпосередньо співвідносити експлойт з шаблоном.
- Цей метод можна застосовувати до всіх протоколів.
- Цей метод трохи ускладнює ухилення.
- Цей метод надійно попереджає про зазначене в шаблоні.

Недоліки аналізу на основі зіставлення зі зразком з відстеженням стану:

- Будь–яка модифікація атаки може привести до пропущених подій (псевдонегативним результатам).

- Цей метод може привести до високого рівня помилкових спрацьовувань, якщо шаблон не настільки унікальний, як припускав автор.

Аналіз на основі декодування протоколів. Багато в чому інтелектуальні розширення для зіставлення зі зразком з відстеженням стану являють собою сигнатури на основі декодування протоколів. Цей клас реалізується шляхом декодування різних елементів таким же чином, як це робив би клієнт або сервер в розмові. Коли елементи протоколу ідентифіковані, IDS застосовує правила, визначені запитом коментарів (RFC), для пошуку порушень. У деяких випадках ці порушення виявляються при зіставленні зі зразком в певному полі протоколу, а для деяких потрібні більш просунуті методи, що враховують такі змінні, як довжина поля або кількість аргументів.

Переваги аналізу на основі декодування протоколів полягають в наступному:

- Цей метод може дозволити пряму кореляцію експлойта.
- Цей метод може бути більш широким і загальним, щоб можна було вловити варіації.
- Цей метод зводить до мінімуму ймовірність помилкових спрацьовувань, якщо протокол чітко визначено і застосовується.
- Цей метод надійно попереджає про порушення правил протоколу, визначених у сценарії правил.

Недоліки цієї методики в тому, що:

- Цей метод може привести до високого рівня помилкових спрацьовувань, якщо RFC неоднозначний і дозволяє розробникам на свій розсуд інтерпретувати і реалізовувати їх так, як вони вважають за потрібне.
- Цей метод вимагає більш тривалого часу на розробку для правильної реалізації аналізатора протоколу.

Евристичний аналіз. Хорошим прикладом цього типу сигнатури є сигнатура, яка буде використовуватися для виявлення розгортки порту. Ця сигнатура перевіряє наявність потрібної кількості унікальних портів, задіяних на конкретній машині. Сигнатура може додатково обмежувати себе, вказуючи типи пакетів, в яких вона

зацікавлена (тобто пакети SYN). Крім того, може бути вимога, щоб всі зонди походили з одного джерела. Підписи цього типу вимагають деяких маніпуляцій. Цей тип може використовуватися для пошуку складних взаємозв'язків.

Перевага евристичного сигнатурного аналізу полягає в тому, що деякі типи підозрілої / або шкідливої активності неможливо виявити ніякими іншими засобами. Недоліком є те, що алгоритми можуть зажадати налаштувань або модифікації для кращої відповідності мережевого трафіку і обмеження помилкових спрацьовувань.

Аналіз на основі аномалій. Сигнатури на основі аномалій зазвичай призначені для пошуку відкритого мережевого трафіку. Сама велика проблема з цією методологією – почала визначати, що таке нормально. У деяких системах є жорстко запрограмовані визначення нормального, у цьому випадку вони можуть розглядатися як системи, основані на евристиці. Деякі системи, створені для навчання нормальним перетворенням, але завдання цих систем не є в тому, щоб виключити можливість неправильної класифікації ненормального введення як нормального. Крім того, якщо передбачається, що вивчений шаблон трафіку є звичайним, система повинна боротися з тим, як відмінити допустимі викладки від недозволених або представлених трафіків, заснованих на атаках. Підкатегорія цього типу виявлення – це методи виявлення на основі профілю. Ці системи базуються на попередженні змін у способах взаємодії користувачів або системи в мережі.

Статистичні аномалії також можуть бути ідентифіковані в мережі за допомогою вивчення або навчання статистичним нормам для певних типів трафіку: наприклад, система, яка виявляє потоки трафіку, такі як UDP, TCP або ICMP– потоки. Ці алгоритми порівнюють поточну швидкість вступу трафіка з історичною довідкою. На основі цього алгоритму попереджатимуть про статистично значущі відхилення від середнього значення. Часто користувач може вказати статистичний поріг для попередження. Переваги виявлення аномалій укладаються в наступному:

- Якщо цей метод реалізований правильно, він може виявити невідомі атаки.
- Цей метод пропонує низькі накладні результати, оскільки не потрібно розробляти нові підписи.

- Як правило, ці системи не можуть надавати детальні дані про введення. Може надати дані про те, що щось трапилось, щось негативне, але не можна сказати однозначно.
- Цей метод сильно залежить від середовища, в якій системи дізнаються, що таке нормально.

Шифрування каналів та кінцеве шифрування. Шифрування, що застосовується між кожною парою хостів, з'єднаних каналом, називається міжканальним шифруванням. Шифрування каналу краще, коли всі вузли в мережі безпечні, але середовище зв'язку використовується спільно кількома користувачами і не є безпечною. Майже всі компоненти кадру даних (за винятком апаратних адрес джерела і одержувача в заголовку кадру) зашифровані до того, як кадр буде вставлений в фізичний канал зв'язку. Коли кадр досягає одержувача наступного переходу (може бути маршрутизатор або кінцевий хост), кадр дешифрується на нижньому рівні протоколу і відправляється на більш високі рівні для подальшої обробки та пересилання. Оскільки шифрування знаходиться на нижньому рівні протоколу, повідомлення відображається у вигляді відкритого тексту на всіх інших рівнях відправника і одержувача, а також на канальному та Інтернет–рівнях проміжних вузлів для апаратної адресації і маршрутизації. Таким чином, шифрування каналу захищає повідомлення, передане між двома комп'ютерами, але повідомлення знаходиться у відкритому вигляді всередині кінцевих і проміжних вузлів. Один або кілька проміжних хостів можуть не викликати довіри.

Шифрування, що застосовується між двома прикладними програмами, що працюють на кінцевих вузлах зв'язку, називається наскрізним шифруванням. Тут тільки частина даних пакета зашифрована на найвищому рівні (тобто на рівні додатку), і пакет передається з даними в зашифрованому вигляді по всьому Інтернету. Таким чином, наскрізне шифрування захищає дані від розкриття під час передачі, але пакет даних може пройти через потенційно небезпечні проміжні вузли. У таблиці 1 порівнюються плюси і мінуси шифрування каналів і наскрізного шифрування.

Таблиця 3.1 – Шифрування посилання та кінцеве шифрування.

Шифрування каналів	Наскрізне шифрування
Кінцеві хости кожного посилання повинні мати спільний ключ і мати можливість виконувати шифрування та дешифрування	Проміжні хости шляху передачі не повинні мати криптографічних засобів.

продовження табл.3.1

Шифрування каналів	Наскрізне шифрування
Якщо в мережі N хостів і n користувачів (N << n), кількість потрібних ключів буде N (N –1) / 2	Кількість ключів, необхідних для симетричного шифрування та шифрування відкритим ключем, буде n (n –1) / 2 та 2n відповідно.
Усі передачі повідомлень мають бути зашифровані та розшифровані за кожним посиланням.	Шифрування залежить від програми та повідомлення, і його не потрібно виконувати для всіх повідомлень.
Один алгоритм шифрування може бути використаний для всіх користувачів у всіх посиланнях	Кожен користувач програми може розгорнути вибраний алгоритм шифрування.
Дані відображаються у кінцевих хостів та проміжних хостів	За винятком прикладного рівня, дані шифруються як на кінцевих хостах, так і на проміжних хостах

Безпечна електронна пошта. Електронна пошта (e–mail) стала звичайним способом спілкування як для ділових, так і для звичайних користувачів. Електронний лист, хоча і поширюється по мережевих каналах, є загальнодоступним і відображається у вигляді відкритого тексту на кожному етапі від системи відправника до екрану одержувача.

Основні вимоги до захищеної електронної пошти. Будь–яка конструкція захищеної електронної пошти повинна враховувати, що заходи захисту повинні

застосовуватися в тексті листа, оскільки існуюча мережа електронної пошти в Інтернеті не повинна бути змінена для забезпечення безпеки електронної пошти. Ключові вимоги для безпечної електронної пошти полягають в наступному:

- Конфіденційність: вміст електронної пошти не повинно бути відкрито на шляху від відправника до одержувача.
- Цілісність: одержувач повинен бачити в електронному листі той же зміст, що і відправник.
- Дійсність: одержувач повинен мати можливість перевірити, чи дійсно повідомлення електронної пошти прийшло від відправника.
- Фіксація авторства: відправник електронного листа не може заперечувати відправку повідомлення.

Безпечний дизайн електронної пошти для забезпечення конфіденційності, запобігання відмови від авторства і автентичності відправника

Можна забезпечити конфіденційність, зашифрувавши повідомлення (перед передачею), щоб повідомлення передавалося в зашифрованому вигляді по мережевих каналах і могло бути переглянуто відкритим текстом тільки в одержувача, після успішної розшифровки. Крім забезпечення конфіденційності під час передачі, для одержувача важливо перевірити справжність відправника, а також використовувати електронну пошту як доказ того, що відправник дійсно відправив повідомлення і не може заперечувати відправку такого повідомлення.

Частина корисного навантаження електронного листа містить зашифровану версію сертифіката відкритого ключа відправника і зашифровану версію вихідного заголовка електронного листа і повідомлення електронної пошти. Сертифікат відкритого ключа відправника зашифрований відкритим ключем одержувача і включений в корисне навантаження. Первісне повідомлення і заголовок електронного листа спочатку шифруються за допомогою закритого ключа відправника (забезпечує неспростовності і справжність відправника), а зашифрований текст, отриманий в результаті цього шифрування, додатково шифрується відкритим ключем одержувача (забезпечує конфіденційність), а результуючий зашифрований текст включається в корисну частину електронної

пошти, переданої по мережевих каналах. Тема цього електронного листа являє собою текстову копію заголовка електронного листа, укладену в зашифрованому форматі в частині корисного навантаження.

Безпечний дизайн електронної пошти для S / MIME. S / MIME (безпечні / багатоцільові розширення електронної пошти) – це стандарт захищеної електронної пошти, що часто використовується в Інтернеті. Він задовольняє всім чотирьом вимогам до безпечного дизайну електронної пошти.

Корисне навантаження електронного листа, що відправляється відправником одержувачу, складається з чотирьох компонентів:

- Зашифрована версія вихідного відкритого тексту (заголовок і тіло повідомлення електронної пошти): на стороні відправника генерується випадковий сеансовий ключ, який використовується в якості секретного ключа для цього симетричного шифрування. Цей компонент задовольняє вимогу забезпечення конфіденційності.
- Зашифрована версія випадкового сеансового ключа, використовуваного для симетричного шифрування вихідного заголовка і тіла повідомлення: сеансовий ключ зашифрований відкритим ключем одержувача. Такий підхід генерації випадкового сеансового ключа для шифрування кожного відправленого повідомлення, а також відправка сеансового ключа разом з повідомленням дозволяє уникнути автономного використання алгоритму розподілу ключів між відправником і отримувачем. Цей компонент задовольняє вимогу забезпечення конфіденційності.
- Зашифрована версія хеша заголовка і тіла вихідного повідомлення електронної пошти: хеш–значення заголовка і тіла вихідного повідомлення електронної пошти обчислюється з використанням стандартного алгоритму хешування (наприклад, SHA1). Це хеш–значення зашифровано закритим ключем відправника. Цей компонент задовольняє вимогу забезпечення цілісності повідомлення.
- Зашифрована версія сертифікату відкритого ключа відправника: сертифікат відкритого ключа відправника зашифрований відкритим ключем одержувача, так що він може бути розшифрований тільки одержувачем і

використаний для отримання хеш–значення заголовок і тіло повідомлення у вигляді відкритого тексту. Цей компонент задовольняє вимогу забезпечення дійсності відправника і запобігання відмови від авторства.

3.2 Контрольний список заходів безпеки LAN

Організації, що використовують локальні мережі, повинні знати про обмежені і слабких засобах управління безпекою, доступних для захисту зв'язку. Успадковані локальні мережі особливо схильні до втрати конфіденційності, цілісності та доступності. Неавторизовані користувачі мають доступ до добре задокументованим вразливостям безпеки, які можуть легко поставити під загрозу системи і інформацію організації, пошкодити дані організації, використовувати пропускну здатність мережі, знизити продуктивність мережі, запустити атаки, які не дозволяють авторизованим користувачам отримати доступ до мережі, або використовувати ресурси організації. ресурси для запуску атак на інші мережі. Організації повинні знижувати ризики для своїх локальних мереж, застосовуючи контрзаходи для усунення конкретних загроз і вразливостей. Отже, враховуючи все вищесказане, можна розглянути контрольний список заходів безпеки LAN, в якому описані заходи управління, експлуатації та технічні заходи, які можуть бути ефективними для зниження ризиків, в основному пов'язаних із застарілими LAN.

Програма дій щодо забезпечення безпеки локальної мережі. Заходи по реалізації контрзаходів:

Ролі та обов'язки:

1. Необхідно вказати, які користувачі або групи користувачів мають право використовувати локальні мережі організації, а які ні.

2. Вказати, які сторони мають повноваження та несуть відповідальність за встановлення та налаштування точок доступу та іншого обладнання LAN.

Безпека інфраструктури LAN:

3. Вимоги до фізичної безпеки для LAN і пристроїв , включаючи обмеження на зони обслуговування.

4. Типи інформації, яка може і не може бути відправлена по локальній мережі, включаючи правила допустимого використання.

5. Необхідно зазначити, як слід захищати передачі по локальній мережі, включаючи вимоги до використання шифрування і управління криптографічними ключами.

Безпека клієнтського пристрою LAN:

6. Умови, при яких клієнтські пристрої LAN дозволені і не можуть використовуватися і експлуатуватися.

7. Стандартні конфігурації обладнання та програмного забезпечення, які повинні бути реалізовані на клієнтських пристроях в локальній мережі, щоб забезпечити відповідний рівень безпеки.

8. Обмеження на те, як і коли можуть використовуватися клієнтські пристрої LAN, наприклад, в певних місцях.

9. Рекомендації по звітності про втрати клієнтських пристроїв в локальній мережі і про інциденти, пов'язані з безпекою локальної мережі.

10. Рекомендації щодо захисту клієнтських пристроїв LAN від крадіжки.

Оцінка безпеки LAN:

11. Частота і об'єм оцінок безпеки LAN.

12. Дії, які необхідно вжити для усунення виявлених несанкціонованих або неправильно налаштованих пристроїв.

Інші рекомендації з управлінських контрзаходів:

13. Розглянути можливість призначення людини для відстеження прогресу в області стандартів безпеки, функцій, загроз і вразливостей. Це допомагає забезпечити безперервне безпечне впровадження технології LAN.

14. Розглянути введення інвентаризації застарілих точок доступу і пристроїв, що підключаються. Ця інвентаризація корисна при проведенні аудитів технологій, особливо при виявленні несанкціонованих пристроїв.

За допомогою цього контрольного списку ці контрзаходи не гарантують безпечного середовища локальної мережі та не можуть запобігти проникненню всіх противників. Крім того, безпека має свої витрати: фінансові витрати, пов'язані з обладнанням безпеки, незручності, обслуговування та експлуатація. Кожна організація повинна оцінити допустимий рівень ризику, виходячи з численних факторів, які впливатимуть на рівень безпеки, що реалізується цією організацією. Щоб бути ефективною, безпека локальної мережі повинна бути включена у весь життєвий цикл рішень локальної мережі. Організації повинні створити мережеву політику безпеки.

Локальні мережі суттєво впливають на спосіб ведення бізнесу організаціями. Оскільки все більше і більше критичної роботи переходить від мейнфреймів до локальних мереж, стає очевидною потреба у кращому контролі. Вище були описані питання безпеки та контролю, пов'язані з локальними мережами; типи критичних та конфіденційних даних, які зараз перебувають у локальних мережах; вплив втрати, зміни чи розголошення; та реалістичні засоби усунення виявлених вразливих місць. Також було висвітлено, як перехідні технології, топології та архітектури створюють складні проблеми безпеки, відновлення та цілісності. Крім того, були визначені особливості безпеки популярного програмного забезпечення для систем локальної мережі та додаткових пакетів. Потім була висвітлена потреба у політиці, процедурах та адміністративному контролі.

Були визначені основи того, як і де впроваджувати ефективні засоби контролю в локальній мережі. Були виявлені підводні камні, що існують як в апаратному, так і в програмному компонентах, що входять до мережі. Значні проблеми, спричинені швидким зростанням локальних мереж на робочому місці, були вирішені безпосередньо вказівками щодо зменшення небезпеки.

3.3 Висновки до третього розділу

Суть захисту інформації в локальній мережі – забезпечити доступ до мережі і її даними для авторизованих хостів / користувачів і заборонити доступ

неавторизованих хостам / користувачам. Безпечна мережа повинна мати захищені від несанкціонованого доступу засоби зв'язку і стійкі механізми протоколу, які можуть уникнути або знизити ймовірність атаки. За успіхом більшості атак лежить спуфінг IP. Отже, крім аутентифікації користувачів додатка також важливо аутентифікувати мережі і хости, з яких користувачі програми спілкуються в Інтернеті. Механізми протоколу, такі як SSH, TLS, IPSec, забезпечують дотримання вищевказаного вимоги і знижують ймовірність атак на основі спуфінга. Єдиний механізм контролю безпеки не може протистояти всім видам мережевих атак. Механізми управління безпекою, обраний для мережі, повинен бути заснований на конкретні загрози, які в даний час існують для мережі. Завжди існує компроміс між використанням механізмів контролю безпеки в якості простих модулів і їх більшої інтеграції з основними функціями протоколів в стеку TCP / IP. Для механізму управління безпекою було б краще вимагати внесення змін тільки на одному конкретному рівні стека Інтернет–протоколу, а не на всіх рівнях.

ВИСНОВКИ

Отже, основним завданням дипломної роботи була розробка рекомендацій щодо захисту інформації в локальній мережі.

В першому розділі було визначено, що собою представляє локальна мережа, які існують схеми локальних мереж, які є методи доступу до мережі, технології мереж та були розглянуті атаки на мережу та їх методи.

В другому розділі були охарактеризовані основні проблеми безпеки локальних мереж та основні принципи та засоби захисту інформації в локальній мережі.

В третьому розділі були надані заходи, необхідні для захисту мереж за допомогою мережевих елементів керування та був наданий контрольний список заходів безпеки LAN.

На основі проведеної роботи можна зробити такі висновки, як: кожна локальна мережа має вразливості, які без негайного усунення стають великою загрозою для безпеки мережі. Такими вразливостями є: використання відкритих протоколів передачі даних, вразливі версії програмного забезпечення, інтерфейси віддаленого доступу, управління обладнанням, зберігання важливих даних у відкритому вигляді або відкритому доступі, словникові паролі, завантаження довільних файлів.

Були визначені основні принципи забезпечення інформаційної безпеки: системність підходу (для захисту інформації необхідно враховувати всі взаємопов'язані елементи, умови і чинники, які є вагомими для розуміння і вирішення проблеми забезпечення інформаційної безпеки); комплексні рішення (комплексне використання різних засобів захисту, а також методів і засобів захисту

інформаційних систем); розумна достатність засобів захисту (важливо правильно вибрати той правильний рівень захисту, при якому витрати, ризик злому і розмір можливих збитків були б прийнятні); розумна надмірність засобів захисту (на етапі розробки системи захисту в неї повинна закладатися якась надмірність, яка б дозволила збільшити термін її життєздатності); гнучкість управління та застосування (реалізовані принципи гнучкості управління для забезпечення можливості налаштування механізмів в процесі функціонування системи); відкритість алгоритмів і механізмів захисту (захист не повинен забезпечуватися тільки за рахунок секретності, структурної безпеки і алгоритмів функціонування її підсистем); простота застосування захисту, засобів і заходів; уніфікація засобів захисту (сучасні системи захисту відрізняються високим рівнем складності, що вимагає високої кваліфікації обслуговуючого персоналу).

В роботі було проаналізовано існуючі атаки в локальних мережах та механізми захисту і були надані певні рекомендації щодо захисту інформації в локальних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nataliia Lukova–Chuiko, Victoriia Klochko Collective defense of corporate networks against computer attacks // Information Technology and Interactions (IT&I–2020) – Київ, 2020, – с.83.

2. Лукова–Чуйко Н.В., Клочко В.Є. Забезпечення безпеки локальних мереж на підприємстві // IV Міжнародна науково–практична конференція “Проблеми кібербезпеки інформаційно–телекомунікаційних систем” (PCSITS). – Київ, 2021. – с. 65–66.

3. Биячуев Т.А. Безопасность корпоративных сетей / Т. А. Биячуев. – М.: Государственный университет ИТМО, 2004. – 38 с.

4. Маркина Т.А. Средства защиты вычислительных систем и сетей / Т.А. Маркина – М.: Университет ИТМО, 2016. – 13 с.

5. Сергій Євдокимов, Сергій Устенко Розробка системи захисту інформації в локальній мережі підприємства. – Миколаїв, 2019.

6. Абраров, Г. Д. Информационная безопасность в компьютерных сетях / Р. Д. Абраров, Д. А. Курязов. – Текст: непосредственный // Молодой ученый. – 2016. – № 9.5 (113.5). – С. 10–12.

7. LOCAL AREA NETWORKS [Electronic resource] – Access: http://www.univasf.edu.br/~joseamerico.moura/pag_autom_arquivos/LOCAL_AREA_NETWORK.pdf

8. Introduction to Networking Technologies [Electronic resource] – 1994. – Access:https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.7540&rep=rep1&type=pdf

9. Бормотов, В. Е. Проблемы защиты информации в компьютерной сети / В. Е. Бормотов. – Текст: непосредственный // Молодой ученый. – 2016. – № 11 (115). – С. 148–150.

10. Software protection Article [Electronic resource] – March 2011. – Access: https://ieee–sw–2011–GE–intro.pdf

11. Cheng Hu Intranet Security – Mikkelin University of Applied Sciences, December 2013.

12. Pandya, P. Local Area Network Security [Electronic resource] – 2013. – Access: https://sci–hub.se/https://doi.org/10.1016/B978–0–12–803843–7.00016–8

13. Components and means of communication within the Local Area Network: An analytical study [Electronic resource] – March 2018. – Access: http://paper.ijcsns.org/07_book/201803/20180310.pdf

14. Куранов А. И. Основи інформаційної безпеки. – К.: Ріпол – 2005. –38–41с.

15. Самарский П. А. Основы структурированных кабельных систем. Из–во: ДМК — АйТи, 2005.

16. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards, 2002. — С. 432.

17. Таненбаум Э, Уэзеролл Д.Компьютерные сети. — Питер, 2012. — 960 с.

18. Asaf Shabtai, Yuval Elovici, Lior Rokach, A Survey of Data Leakage Detection and Prevention Solutions, Springer–Verlag New York Incorporated, 2012.

19. Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS)Archived 2006–08–27 at the Wayback Machine, University of Washington.

20. Graves, Michael W. (2004). The Complete Guide to Networking And Network +. Cengage Learning.

21. INDUSTRIAL COMPANIESATTACK VECTORS [Electronic resource]. – Access: https://www.ptsecurity.com/upload/corporate/ww–en/analytics/ICS–attacks–2018–eng.pdf

22. John Pescatore (October 2, 2008). “This Week in Network Security History: The Firewall Toolkit”. Retrieved 2018–12–28.

23. Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7.

24. Scott, W. Ross; Cavedo, Robert F. (1984–09–01), “Local Area Network Demonstration Procedures.”

25. Security information and event management (SIEM) implementation. — New York: McGraw–Hill, 2011.

26. “Virtual Private Networking: An Overview.” Microsoft Technet. 4 September 2001.

27. VPN and Firewalls (Windows Server). Resources and Tools for IT Professionals | TechNet.

28. What is Group Policy, GPO and Why it Matters for Data Security By Jeff Petters [Electronic resource]. – Access: https://www.varonis.com/blog/group–policy/

29. 3 Levels of Corporate Network Security By Uladzislau Murashka [Electronic resource]. – Access: https://www.scnsoft.com/blog/3–levels–corporate–network–security

30. 7 Tactics To Prevent DDoS Attacks & Keep Your Website Safe By Bojana Dobran [Electronic resource]. – Access: https://phoenixnap.com/blog/prevent–ddos–attacks

31. 17 Types of Cyber Attacks To Secure Your Company From in 2019 By Bojana Dobran [Electronic resource]. – Access: https://phoenixnap.com/blog/cyber–security attack–types

32. Applied Network Security Monitoring: Collection, Detection, and Analysis / Chris Sanders, Jason Smith. – Syngress, 2013. – 496 p.

33. Network Security: A Decision and Game–Theoretic Approach / Tansu Alpcan, Tamer Başar. – Cambridge University Press, 2010. – 334 p.

ДОДАТОК А

Doctor of Technical Science, Professor of the Department of Cybersecurity and Information Protection Nataliia Lukova–Chuiko, student Victoriia Klochko

Taras Shevchenko National University of Kyiv

COLLECTIVE DEFENSE OF CORPORATE NETWORKS AGAINST COMPUTER ATTACKS

Abstract

These days, content analysis of text information is used to prevent threats, along with the analysis of the network traffic characteristics, the behavior of corporate networks and their security policy. Existing systems of text analysis and modeling include different kinds of search engines and information–analytical systems. They are capable of solving such tasks as classification of documents by its subject matter, author identification, detection of plagiarism, modeling representations of the knowledge about the subject area and the content of text, classification and filtering of documents by specified queries, and much more.

Keywords

Corporate network, attacks, SDA, System Monitoring Unit, cybersecurity, collective protection.

Introduction

In the modern world, problems related to the use and spread of malicious software, information attacks and other types of cyber threats, which have received the general name “cybercrime” are becoming more and more relevant. Sophisticated threats require an innovative approach. Sophisticated threats require an innovative approach. Collective defense empowers organization to stay ahead of evolving threats to better defend network through real–time sharing and collaboration across industries and sectors.

Main text

A number of freely distributed and commercial systems of defense from attacks (SDA) was developed and became widely accepted in the field of corporate computer networks building [1].

The analysis of the structure of circulating packages in the corporate network is the essence of the analysis at the network layer of protection in SDA. As a rule, the package flags, the port addresses for network nodes, the time intervals between specific events and so on are analyzed here.

The package contains the information about the sender, which is often represented as a DNS–address. This information is definitely of a great value as it can clearly point at the source of the attack. However, the truth of address information about the source of the attack is often questionable, since it can be easily corrected by the sender of the package. For some protocols, such as mail, the address of the attacker may also be obviously stated. However, as in the previous case, the address of the sender can easily be changed.

As a result, there is a need to allocate one more level of realization of the protective methods – the level of the global network.

At this level the information, which is contained in the text documents on web–sites, global network portals, social networks or other legitimate objects of the information space can be analyzed and both the sources of attacks and their information characteristics can be indirectly identified.

The concept of a text document here is multivalued: it is text information from websites and portals, and emails, and program codes that are entered into the computing environment of the victim's computer. In any case, this level is characterized by, on the one hand, methods used in intelligence activities, including business or competitive intelligence, and, on the other hand, methods of text processing.

IT professionals very often have problems with viruses and other malware. Actual threats include spreading spam, phishing, network attacks on enterprise infrastructure, including tar– get and DDoS attacks, where use potentially dangerous software vulnerabilities.

These and other similar examples show a close relationship between cybersecurity systems and word processing systems: when detecting spam, data loss, detecting and tracking potentially dangerous messages, etc.

This field of the research is actively evolving lately. From one side, it is connected with intellectual property protection, from another, it is connected with the necessity of cyber threats prevention, which arises because of the malware usage. In the latter case, it is hard to overestimate the possible damage, which can be caused to control systems by the key infrastructure, including to the military targets. Because there are new kinds of malware being created all over the globe, there is a necessity of the identification of the malicious code creators and bringing them to justice.

Processing, careful analysis and synthesis of information collected from Internet resources is made using content and/or rapid analysis methods, bibliometric and/or cluster analysis, as well as expert and/or situational methods.

However, a tight time limit for the search, collection, extraction and processing of information circulating in the global information space of the Internet, its accumulation, classification by certain attributes, further analysis, synthesis, compilation and making it accessible to the concerned users, as well as transformation into synthesized conclusions and recommendations necessitates some arrangements. First, the automation of all measures in the complex of risks monitoring system associated with these processes. Second, the configuration of SDAs subordinate to the System Monitoring Units of corporate networks according to their risk vectors.

The development of a corporate networks protection model with a collective System Monitoring Unit defense module, methods for detecting and identifying computer attacks with help of content analysis of the global information space and the architecture of SDA, related to it, will provide a basis for the synthesis of a reliable and high–performance adaptive cyber threats detection systems and will shorten the detection time of the computer attacks of the new generation.

Further improvement of the security and stability in functioning of the information and telecommunication systems of corporate networks in the conditions of massive influence of computer attacks requires an increase in the probability of detection of new computer attacks and a decrease in the recognition time for the signs of known attacks.

To solve this problem, it is not enough to use only traditional methods that utilize identification characteristics of network traffic and information about the work of corporate networks and security devices. The processing of data sets of the body of network packages, content of Internet pages, information from social networks is very valuable in this area.

Conclusion

Calculations of risks from various attacks require the identification of sources of attacks on indirect grounds, determining their inclinations to attacks or undesirable influences of one kind or another, determining the characteristics of attack activity, calculating predictive activity indicators based on time series analysis, and the like [2].

This protection becomes possible or by configuring the corporate network SDA to prepare the activation of attack detection algorithms. Given the temporary limitations of the attack detection process, such actions should be performed based on predictions of the activity of potential attack sources, the detection of which is the task of the global network security level of the corporate network.

References

[1] Chi, S.–D., Park, J. S., Jung, K.–C. & Lee, J.–S., Network security modeling and cyber– attack simulation methodology. Lecture Notes in Computer Science. Springer–Verlag 2001 .

[2] Shannon, C. E., A mathematical theory of communication. Bell System Technical (1948), Vols. 27.

[3] Martovitsky V., Ruban I., Lukova–Chuiko N., Kortyak E., Kruglikov Y., Model monitoring network infrastructure based on standard FIPA, 2020.

[4] Ruban I., Martovitsky V., Lukova–Chuiko N., Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System (2018), 302–309.

Забезпечення безпеки локальних мереж на підприємстві

Вікторія Клочко[1], Наталія Лукова–Чуйко[2]

1. Кафедра кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, УКРАЇНА, м.Київ, вул.Богдана Гаврилишина, 24, E–mail: klviktoriya1310@gmail.com

2. Кафедра кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, УКРАЇНА, м.Київ, вул.Богдана Гаврилишина, 24, E–mail: lukova@ukr.net

Abstract – We analysed and classified primary threat types concerning information security in local area networks, including those of businesses. We discuss techniques and methods for information protection in computer networks.

Ключові слова – Безпека, локальна мережа, користувач, атака.

Вступ

Внаслідок інтенсивного розвитку комп'ютерної техніки і систем передачі інформації, все більш актуальною стає проблема забезпечення безпеки інформації. Під загрозою безпеки інформації розуміють дію або подію, яка може привести до руйнування, спотворення чи несанкціонованого (недозволеного) використання інформаційних ресурсів [1].

Проблеми інформаційної безпеки посилюються в міру проникнення в усі сфери діяльності технічних засобів обробки і передачі даних, і перш за все обчислювальних систем. Об'єктами посягань можуть бути самі технічні засоби (комп'ютери і периферія) як матеріальні об'єкти, програмне забезпечення (ПЗ) і бази даних, для яких технічні засоби є оточенням.

Не випадково, захист даних в комп'ютерних мережах стає однією з найгостріших проблем в сучасному світі. В даний час сформульовані базові принципи інформаційної безпеки, які повинні забезпечити:

– цілісність даних;

– захист від збоїв, що ведуть до втрати інформації, а також неавторизованого створення або знищення даних;

– конфіденційність інформації і, одночасно, її доступність для всіх авторизованих користувачів.

Слід також зазначити, що окремі сфери діяльності (банківські та фінансові інститути, інформаційні мережі, системи державного управління, оборонні та спеціальні структури) вимагають спеціальних заходів безпеки даних і пред'являють підвищені вимоги до надійності функціонування інформаційних систем, відповідно до характеру і важливістю вирішуваних ними завдань.

Загрози безпеці інформації можуть бути випадковими (ненавмисними) – це загрози, джерелом яких є помилки в ПЗ, вихід з ладу апаратних засобів, неправильні дії користувачів і інші, і навмисними, мета яких нанесення шкоди (наприклад, отримання інформації, що циркулює в каналах зв'язку, за допомогою їх прослуховування, виведення з ладу комп'ютерної техніки, спотворення інформації в базах даних і ін.).

Забезпечення безпеки необхідно для будь–яких організацій незалежно від розмірів і форм їх діяльності, але вразливими частіше є малі підприємства, пов'язані локальними інформаційними мережами. Тому захист і контроль необхідно забезпечити на всіх рівнях: фізичному, програмному, призначеному для користувача і зовнішньому.

I. Основні технічні загрози безпеки ЛОМ на підприємстві

1. Помилки в ПЗ. Джерелами помилок в ПЗ є робота конкретних людей, з їх індивідуальними особливостями, кваліфікацією і т. п. Більшість помилок не представляє ніякої небезпеки, однак деякі можуть привести до серйозних наслідків таким, як отримання зловмисником контроля над сервером, несанкціоноване використання ресурсів. Такі «уразливості» усувають за допомогою пакетів оновлень. Своєчасне установлення оновлень є необхідною умовою безпеки мережі.

2. DoS і DDoS–атаки. Атаки відмови в обслуговуванні DoS направляються зазвичай на інформаційні сервери підприємства, функціонування яких є критично важливою умовою для працездатності всього підприємства. Для проведення таких атак зловмисники координують роботу декількох робочих станцій, в цьому випадку можлива і DDoS атака. Зловмисник захоплює управління над групою ввіддалених комп'ютерів, посилає потужний сумарний потік пакетів в атакуючий комп'ютер, викликаючи його перевантаження, в результаті чого відбувається вичерпування ресурсів операційної системи або процесора комп'ютера [2].

3. Шкідливі програми («троянський кінь», комп'ютерні віруси). Збиток, нанесений шкідливими програмами, може виражатися в розкраданні, спотворенні, знищення інформації, а також приведення в непрацездатний стан ПЗ. Мережеві «черв'яки» здатні самостійно поширюватися по локальній мережі і глобальних мереж шляхом поширення своїх копій [3].

З метою забезпечення безпеки окремих комп'ютерів і локальної мережі застосовують: антивірусний захист, в основі роботи якої три групи методів:

–методи аналізу вмісту файлів – сканування сигнатур (унікальна послідовність байтів, яка завжди присутня в певному виді вірусів і по якій цей вид вірусу можна з великою ймовірністю впізнати) вірусів, а також перевірка цілісності і сканування підозрілих них команд. Для кожного вірусу фахівець виконує аналіз

коду, на основі якого потрібно сигнатура. Отриманий кодовий фрагмент поміщають в базу даних вірусних сигнатур. Далі працює антивірусна програма, яка буде сканувати файли на наявність вірусів і, в разі виявлення небезпеки, заблокує файл (тимчасово зашифрує заражений файл);

–методи, які відстежують проведення програм при їх виконанні – протоколювання всіх подій, які загрожують безпеці системи регламентація порядку роботи з файлами і програмами – в системі корпоративної мережі виконуються тільки ті програми, запис про які є в списку програм, дозволених до виконання в даній системі [4].

II. Загальні принципи забезпечення безпеки

1.Мережеве обладнання, яке виконує маршрутизацію трафіку в мережу Інтернет має бути оснащений системою фільтрації трафіку з заборонами за замовчуванням.

2.Локальна мережа повинна мати мінімальну кількість глобальних адрес.

3.На проксі–сервері має бути встановлене антивірусне ПЗ, яке забороняє доступ до потенційно небезпечних джерел.

4.Весь трафік повинен бути отриманий з використанням кешування інформації за допомогою проксі–серверів.

5.Прямий доступ до мережі Інтернет з використанням механізму трансляції мережевих адрес (NAT) може бути включений тільки для обмеженого числа користувачів, щоб запобігти звернення ззовні до внутрішніх хостів. ПЗ для перегляду інформації по http–протоколу має використовувати максимальний рівень безпеки.

6.У мережі, що має вихід в Інтернет, повинна бути розроблена політика автоматичної установки всіх доповнень і виправлень, що випускаються постачальниками операційної системи. Установка оновлень і доповнень повинна виконуватися для всіх комп'ютерів мережі, незалежно від прав користувача комп'ютера на отримання доступу до мережі Інтернет.

III. Загрози через людський фактор

1. Промислове шпигунство. Форма недобросовісної конкуренції, при якої здійснюється незаконне отримання, використання, розголошення інформації, що становить комерційну, службову або іншу таємницю з метою отримання переваг при здійсненні підприємницької діяльності, а так само отримання матеріальної вигоди. В основному захист здійснюється за допомогою охоронної системи.

2. Недостатня кваліфікація працівника при роботі з локальною мережею може привести до ряду помилок.

Для запобігання позначених загроз необхідно:

–передбачити наявність єдиної системи автентифікації користувачів, на основі дерева каталогів;

–забезпечити зберігання облікової інформації користувачів в зашифрованому вигляді;

–відмовитися від протоколів передачі пароля в незашифрованому вигляді;

–розробити політику періодичної заміни паролів користувачами;

–виробити вимоги до обов'язкового складу паролів користувачів;

–вести облік входів в мережу користувачами;

–розробити систему надання прав використання ресурсів мережі користувачам на основі груп безпеки;

–заборонити використання користувачами комп'ютерів з правами адміністратора;

–розробити заходи безпеки, що запобігають використання змінних носіїв користувачами.

Таким чином, щоб мінімізувати ризик перерахованих вище факторів, необхідно провести ряд заходів при проектуванні і введенні в експлуатацію ЛОМ.

1.Розробити систему періодичного резервного копіювання інформації серверів на змінні носії.

2.Передбачити наявність в мережі виділеного сервера, що виконує резервування інформації. На ньому повинна бути встановлена серверна частина ПЗ резервного копіювання.

3.Забезпечити автоматичне виконання резервного копіювання по розкладом.

4.Розробити систему моніторингу стану ключових елементів мережі і оповіщення адміністратора мережі про потенційні проблеми. У великих мережах цю функцію необхідно покласти на окремий сервер, оскільки обсяг інформації моніторингу може досягати значних значень.

5. Передбачити використання клієнт–серверного режиму для роботи з корпоративними додатками там, де це можливо. Це позбавить від необхідності підтримки цілісності даних на безлічі комп'ютерів, зменшить обсяги резервного копіювання інформації.

Висновок

Забезпечення безпеки інформації локальних мереж на підприємстві – це комплекс заходів, спрямованих на запобігання несанкціонованого отримання інформації, її знищення, а також модифікації (видозміни), що захищається. Використання цих заходів допоможе різним підприємствам розвиватися, бути конкурентоспроможними і фінансово стабільними.

Література

[1] Applied Network Security Monitoring: Collection, Detection, and Analysis / Chris Sanders, Jason Smith. – Syngress, 2013. – 496 p.

[2] Барабаш О.В., Лукова–Чуйко Н.В., Мусієнко А.П., Собчук В.В., Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDOS атакам, 2018.

[3] Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. – Санкт–Петербург, 2010. – 918 с.

[4] Network Security: A Decision and Game–Theoretic Approach / Tansu Alpcan, Tamer Başar. – Cambridge University Press, 2010. – 334 p.