Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ___ інфокомунікації
(повна назва)
Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*
(позначення документа)

Порівняльний аналіз методів захисту інформації у мережах
(тема)

Виконав:
здобувач 2 року навчання,
групи *ІМІм-23-2*
Денис ЄВТУШЕНКО
(прізвище, ініціали)
Спеціальність
172 Електронні комунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник зав.*каф. Валерій БЕЗРУК*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри Валерій БЕЗРУК
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікації

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)
Спеціальність 172 Електронні комунікації та радіотехніка.
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма " Інформаційно-мережна інженерія"

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Євтушенку Денису Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи "Порівняльний аналіз методів захисту інформації у мережах"

затверджена наказом по університету від " *21* "*10* *2024 р. №* *1145 Ст*
2. Термін подання студентом роботи *22.01.2025 р.*
3. Вихідні дані до проекту (роботи)
1. Теоретичні основи методів захисту
2. Огляд методів захисту інформації
3. Порівняльний анлаз методів захисту
4. Приклади безпечної реалізації
5. Практична частина

4. Перелік питань, що потрібно опрацювати в роботі
ВСТУП
1. Теоретичні основи методів захисту
2. Огляд методів захисту інформації
3. Порівняльний анлаз методів захисту
4. Приклади безпечної реалізації
5. Практична частина

ВИСНОВКИ
ПЕРЕЛІК ПОСИЛАНЬ
ДОДАТКИ

5. Перелік графічного матеріалу із зазначенням обов'язкових креслеників, схем, плакатів, комп'ютерних ілюстрацій: *1. "Схема проведення DDoS атак" 2. "Топологія VPN на базі (MS Azure)" 3. " Перевірка встановлених правил" 4. "Стартова сторінка Nginx"*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термин виконання етапів роботи	Примітка
1.	Теоретичні основи методів захисту	28.10.24–28.11.24	
2.	Огляд методів захисту інформації	15.11.24–28.11.24	
3.	Порівняльний анлаз методів захисту	28.11.24–05.12.24	
4.	Приклади безпечної реалізації	28.12.24–-05.01.25	
5.	Практична частина	06.01.25–12.01.25	
6.	Перевірка керівником	13.01.25-16.01.25	
7.	Перевірка нормоконтроль	20.01.25-22.01.25	
8.	Перевірка на академічний плагіат	22.01.25-	
9.	Перевірка завідувачем кафедри, рецензування	22.01.25–	

Дата видачі завдання *21.10.2024 р.*

Здобувач _____ *Денис ЄВТУШЕНКО*
(підпис)

Керівник роботи _____ *зав.каф Валерії БЕЗРУК*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 53 стор., 4 рис., 3 табл., 2 додатки, 15 джерел.

У цій роботі розглядаються сучасні виклики інформаційної безпеки в мережах, а також пропонуються різноманітні методи та інструменти їх подолання — від криптографії й брандмауерів до IDS/IPS, VPN та антивірусних рішень. Детально аналізуються типи загроз (зовнішні й внутрішні, активні й пасивні) та їхній потенційний вплив на доступність, цілісність і конфіденційність даних. Окрему увагу приділено фішинговим атакам і технікам соціальної інженерії, що часто виявляються ефективними навіть у середовищі з передовими технічними засобами захисту.

Робота наголошує на важливості комплексного підходу: застосування лише одного методу (наприклад, шифрування або файрвола) не гарантує захисту в умовах стрімкої еволюції атак. У результаті проведеного порівняльного аналізу сформульовано рекомендації стосовно того, як краще поєднувати різні інструменти залежно від завдань і обмежень (ресурсних, організаційних, правових). Додатково наводяться приклади «лабораторних» налаштувань і реалізацій базових сценаріїв безпеки, які підтверджують здатність впроваджувати дієві рішення навіть без складної інфраструктури. У висновках підкреслюється, що безперервне вдосконалення захисних механізмів, навчання персоналу й уважне відстеження новітніх загроз є визначальними факторами успіху в контексті мережевої безпеки.

ABSTRACT

Explanatory note of the qualification work: 53 p., 4 fig., 3 table., 2 appendices, 15 sources.

This work examines contemporary challenges in network information security and proposes various methods and tools for tackling them—ranging from cryptography and firewalls to IDS/IPS, VPN, and antivirus solutions. A detailed analysis is provided on the types of threats (external and internal, active and passive) and their potential impact on the availability, integrity, and confidentiality of data. Special attention is paid to phishing attacks and social engineering techniques, which often prove effective even in environments equipped with advanced technical safeguards.

The paper emphasizes the importance of a comprehensive approach: relying on a single method (e.g., encryption or a firewall) does not guarantee protection in the context of rapidly evolving threats. As a result of the comparative analysis conducted, recommendations are formulated on how best to combine different tools depending on specific objectives and constraints (including resource, organizational, and legal factors). In addition, examples of “laboratory” configurations and implementations of basic security scenarios are provided, demonstrating the feasibility of deploying effective solutions even without complex infrastructure. The conclusion highlights that continuous improvement of defense mechanisms, staff training, and close monitoring of emerging threats are all crucial factors for success in the domain of network security.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ, І ТЕРМІНІВ

AES (Advanced Encryption Standard)

Симетричний блоковий алгоритм шифрування, що використовує 128-бітні блоки та різну довжину ключа (128, 192 чи 256 біт).

ACK (Acknowledge)

Службове повідомлення в TCP, яке підтверджує отримання пакета або завершення певного етапу «рукостискання».

API (Application Programming Interface)

Інтерфейс програмування додатків; не згадується детально в тексті, але є базовим терміном у мережевій взаємодії.

APWG (Anti-Phishing Working Group)

Організація, що досліджує й публікує дані про фішинг та інші кіберзагрози.

CA (Certificate Authority)

Центр сертифікації, що засвідчує автентичність криптографічних сертифікатів.

CBC (Cipher Block Chaining)

Режим шифрування, коли кожен блок XOR-иться з попереднім зашифрованим блоком, підвищуючи стійкість до повторів.

CFB (Cipher Feedback)

Режим потокового шифрування, який використовує вихід шифру для формування ключового потоку.

CVE (Common Vulnerabilities and Exposures)

Система ідентифікації відомих вразливостей; згадується у контексті «нульових днів».

DDoS (Distributed Denial of Service)

Розподілена атака відмови в обслуговуванні, метою якої є зробити ресурс недоступним шляхом перевантаження мережевого або обчислювального середовища.

DES (Data Encryption Standard)

Застарілий симетричний алгоритм шифрування, пізніше замінений AES.

DNS (Domain Name System)

Система доменних імен, яку зловмисники можуть використовувати в атаках Amplification.

ECC (Elliptic Curve Cryptography)

Асиметричний алгоритм, що базується на дискретних логарифмах на еліптичних кривих; забезпечує високу безпеку за менших ключів.

ECB (Electronic Codebook)

Режим шифрування блоків, у якому кожен блок обробляється незалежно (не рекомендовано для використання, бо дублікати блоків стають видимими).

FTP (File Transfer Protocol)

Протокол передачі файлів, згаданий як можливий вектор аналізу для IDS/IPS або брандмауерів.

HIDS (Host-based Intrusion Detection System)

Система виявлення вторгнень, що встановлюється безпосередньо на хості (сервері чи робочій станції).

HTTP (HyperText Transfer Protocol)

Протокол прикладного рівня, що використовується у вебі в незашифрованому вигляді.

HTTPS (HTTP Secure)

Розширення HTTP зі використанням TLS/SSL для шифрування.

ICMP (Internet Control Message Protocol)

Протокол керування та діагностики в IP-мережах. Зловмисники можуть використовувати ICMP-флуд (Ping-флуд) для DDoS-атак.

IDS (Intrusion Detection System)

Система моніторингу й аналізу подій без активного втручання в трафік.

IoT (Internet of Things)

Інтернет речей; згадується в контексті пристроїв із обмеженими ресурсами, для яких підходить ECC.

IPS (Intrusion Prevention System)

Система виявлення загроз із можливістю активного блокування чи перенаправлення трафіку.

IPsec (Internet Protocol Security)

Набір протоколів для VPN на мережевому рівні (рівень IP), застосовується для захищених тунелів.

MITM (Man in the Middle)

Атака «людина посередині», коли зловмисник знаходиться між двома вузлами й може «підслуховувати» чи змінювати трафік.

NAT (Network Address Translation)

Механізм трансляції мережевих адрес; не описано детально, але суміжний із темою фаєрволів.

NIDS (Network-based IDS)

Система виявлення вторгнень, що працює на мережевому сегменті, пасивно аналізуючи проходження пакетів.

NMap

Інструмент для сканування портів та виявлення служб на мережевих вузлах.

NTP (Network Time Protocol)

Протокол синхронізації часу; часто фігурує в атаках Amplification.

OSI (Open Systems Interconnection)

Еталонна модель взаємодії відкритих систем, згадувана у контексті 3–4 рівня (мережевий і транспортний).

RSA

Асиметричний алгоритм шифрування й підпису, базований на складності факторизації великих чисел.

RST (Reset)

Тип пакета TCP, що завершує з’єднання різко.

SHA (Secure Hash Algorithm)

Сімейство алгоритмів хешування, не обговорено детально, але є базовим у криптографії.

SIEM (Security Information and Event Management)

Система інтеграції та аналізу подій безпеки, журналів IDS, IPS, брандмауерів, антивірусів.

SYN (Synchronize)

Початковий пакет для встановлення з’єднання у TCP; часто застосовується в атаках SYN flood.

TLS (Transport Layer Security)

Криптографічний протокол, що забезпечує зашифроване передавання даних (заміна SSL).

UFW (Uncomplicated Firewall)

Спрощений інтерфейс налаштування iptables в Linux.

UDP (User Datagram Protocol)

Транспортний протокол без встановлення з’єднання; згадується у контексті UDP-флуду для DDoS.

VPN (Virtual Private Network)

Технологія створення зашифрованого тунелю (OpenVPN, IPSec, WireGuard), завдяки якому віддалені користувачі або мережі отримують доступ до внутрішніх ресурсів, імітуючи локальний зв’язок.

WAN (Wide Area Network)

Розгалужена мережа, зазвичай глобальна. Не згадано прямо, проте опосередковано через контекст зовнішніх загроз.

Wi-Fi

Безпровідна мережа, у якій часто ініціюють перехоплення (MitM) або проводять сканування через відкриті точки доступу.

Zero Trust

Концепція безпеки, за якою кожен запит або вузол слід перевіряти, незалежно від розташування, оскільки автоматично не довіряється жодному елементу мережі.

ЗМІСТ

ВСТУП

У сучасному середовищі інформаційні технології істотно спростили взаємодію між людьми та компаніями, проте водночас спричинили появу нових загроз. Дані, що циркулюють у мережевому просторі, часто стають привабливою ціллю для хакерів, недобросовісних конкурентів чи інших зловмисників, які прагнуть здобути несанкціонований доступ до чутливої інформації. Здійснення кібератак може завдати як фінансових збитків, так і репутаційної шкоди для установи, зумовивши витік конфіденційних відомостей. З огляду на це, забезпечення надійного захисту даних у мережах набуває першорядного значення.

Представлена робота спрямована на проведення порівняльного аналізу методів мережевої безпеки, виявлення їхніх переваг і вразливих моментів, а також формулювання рекомендацій стосовно їхнього ефективного застосування у практичних випадках

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Основні поняття інформаційної безпеки

У процесі проєктування будь-якої інформаційної системи на перший план виходять три ключові властивості безпеки: конфіденційність, цілісність і доступність. Конфіденційність передбачає захист даних від несанкціонованого доступу, коли сторонні особи не мають змоги переглянути чи використати інформацію. Цілісність зосереджена на запобіганні несхваленим змінам або руйнуванню даних, забезпечуючи, що вони зберігають первинний вигляд і точність. Доступність гарантує безперешкодний доступ користувачів до необхідних сервісів та ресурсів саме тоді, коли це потрібно. Порушення будь-якої з цих складових здатне спричинити суттєвий збій у роботі організації або призвести до витоку вкрай важливої інформації, наслідки чого можуть мати довгостроковий характер.

Загрози, що виникають у мережах, умовно поділяються на зовнішні та внутрішні; при цьому саме зовнішні атаки, спрямовані з глобальної мережі (Інтернету), залишаються одними з найпоширеніших. До них зазвичай зараховують розподілені атаки відмови в обслуговуванні (DDoS), фішинг, блокування трафіку та сканування портів. Усі вони можуть серйозно впливати на функціонування ресурсів та сервісів, адже зловмисники або перевантажують мережеві канали та сервери штучно згенерованим потоком запитів, або обманом виманюють у користувачів конфіденційні дані. Враховуючи швидкий розвиток та адаптивність згаданих способів проникнення, організаціям потрібно формувати належну стратегію захисту, що охоплюватиме не лише технічні, а й організаційні й освітні заходи.

1.2 DDoS

DDoS (Distributed Denial of Service) - це атака на доступність мережевих ресурсів і сервісів. Зловмисники використовують велику кількість комп'ютерів (часто об'єднаних у ботнет) для масового надсилання запитів або генерують такий обсяг мережевого трафіку, що легальні користувачі не можуть отримати доступ до сервісів (веб-сайтів, веб-додатків, ігрових серверів тощо). Основна мета DDoS-атаки - зробити послуги недоступними через надмірне використання пропускної здатності, обчислювальних та інших обмежених ресурсів (процесор, пам'ять, операції з дисками).

Атаки мережевого рівня (об'ємні/флуд-атаки). UDP-флуди спосіб яким зловмисники завалюють ціль великою кількістю UDP-пакетів з метою перевантаження каналу та обробки трафіку.

ICMP-флуди (Ping-флуди), коли зловмисники надсилають велику кількість ехо-запитів ICMP (Ping), які використовуються для перевантаження каналу та цільової системи, перевантаження каналу та цільової системи.

Усилювадьні атаки використовують протоколи (DNS, NTP, SSDP), які дають відповідь, що перевищує розмір запиту. Зловмисник підміняє IP-адресу жертви і надсилає запит на сервер, який повертає більшу відповідь на адресу жертви (наприклад, DNS Amplification, NTP Amplification). Протокольні атаки (SYN flood) - зловмисник надсилає велику кількість SYN-запитів «рукостискань», зловмисник не завершує рукостискання і тримає ресурси сервера в підвішеному стані. Це забиває таблицю з'єднань і не дозволяє сервісу відповідати на нові запити. ACK-флуд, RST-флуд тощо, типи запитів, які перевантажують сервер на рівні мережі/транспортного протоколу. Атаки на прикладному рівні HTTP GET/POST flood, надсилання великої кількості HTTP-запитів на веб-сервер, які потребують значних ресурсів (відповіді бази даних, обробка скриптів). Веб-сервер перевантажується під час обробки запитів.Slowloris: зловмисник встановлює велику кількість HTTP-з'єднань і надсилає заголовки вкрай повільно, змушуючи сервер підтримувати відкриті сесії протягом тривалого періоду часу.

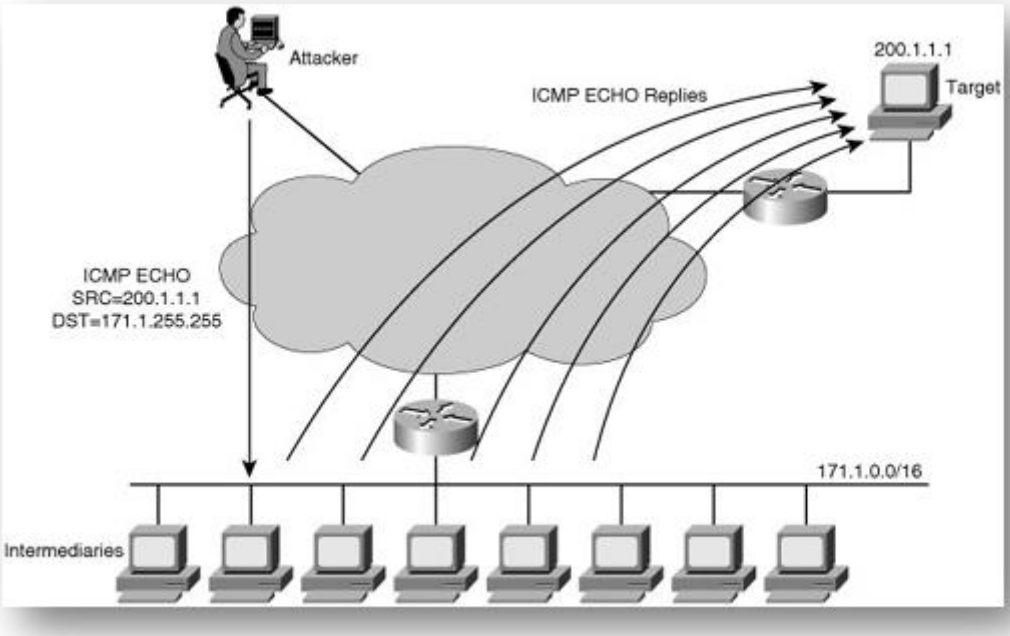

Рисунок 1.1 – Схема проведення DDoS атак

1.3 Фішинг

Фішингові практики можуть бути реалізовані в різних формах, але найчастіше до них належать обманні повідомлення електронної пошти, націлені фішингові атаки, а також маніпуляції через SMS і телефонні дзвінки. У випадку звичайного електронного листа, відправленого нібито від імені надійної організації (скажімо, банку чи популярного онлайн-сервісу), одержувача просять перейти на спеціально створену вебсторінку та «оновити» облікові дані або «підтвердити» акаунт. Насправді ж посилання веде на підроблений сайт, де користувач мимоволі розкриває свої паролі чи інші конфіденційні відомості. Цільова (Spear-фішинг) атака вимагає від шахраїв більш точного персонального підходу: вони заздалегідь збирають певні дані про посаду, контакти чи коло колег жертви, що підвищує ймовірність успішного обману. Прикладом може бути лист до бухгалтера, надісланий нібито від «генерального директора» з проханням здійснити невідкладний платіж.

Аналогічні методи використовують для SMS-фішингу (смішинг), коли на мобільний телефон надходить повідомлення, яке містить вигадану підставу для переходу за посиланням. Зловмисники, вказуючи себе за представників банку чи іншої авторитетної установи, просять «уточнити інформацію» чи «розблокувати рахунок». Голосовий фішинг (вішинг) ще простіший у сенсі комунікації, але не менш небезпечний: шахраї у розмові телефоном, презентуючи себе співробітниками фінансової або правоохоронної установи, примушують людину до передачі особистих даних, паролів чи інших секретних ключів.

Фішингові схеми постійно еволюціонують у відповідь на вдосконалення механізмів захисту користувачів. Окрім звичайної розсилки електронних листів від фальшивих «банків» чи «онлайн-сервісів», зловмисники все частіше застосовують елементи цільового аналізу аудиторії та використовують реальні відомості про потенційну жертву, отримані з відкритих джерел або соціальних мереж. Це підвищує переконливість повідомлень, оскільки шахрай додає до листа чи SMS-сповіщення такі деталі, як назва відділу, ім’я колеги чи конкретну подію, що мала місце у компанії.

Ключову роль у протидії фішинговим атакам відіграють заходи навчання персоналу: якщо співробітники усвідомлюють типові прийоми обману, вони набагато рідше «попадаються» на маніпулятивні пропозиції й переходять за небезпечними посиланнями. Технічні рішення, на зразок фільтрації підозрілих електронних листів, а також зашифровані канали зв’язку (HTTPS, VPN), дають змогу пом’якшити наслідки цих шахрайських дій, однак не виключають цілком можливості обману безпосередньо через людський фактор.

Також спостерігається зростання популярності векторів атаки через мобільні додатки або чати в месенджерах, де зловмисники можуть надсилати

офіційно виглядні посилання чи файли. Користувачі часто вважають спілкування у застосунках «безпечним» за замовчуванням, що створює додаткові можливості для шахраїв, особливо якщо адресат встановлює невідомі програми або ігнорує попередження системи.

Захист від фішингу передбачає як технічні (аналіз вхідних повідомлень, встановлення двофакторної аутентифікації), так і організаційні (введення політик безпеки, проведення регулярних тестових фішингових кампаній) заходи. Поєднання цих підходів підвищує стійкість до загроз, водночас зберігаючи базовий рівень зручності для користувачів.

Окремим різновидом фішингу виступає так званий клон-фішинг, за якого зловмисник відтворює справжній електронний лист чи вебформу, але вбудовує у нібито автентичний зміст шкідливе посилання. У такій ситуації потенційна жертва отримує повідомлення, що зовні повністю відповідає офіційному листу зі знайомого сервісу, проте насправді воно спрямовує користувача на фальшивий вебсайт. Це робить підробку візуально переконливою і різко підвищує ризик того, що одержувач розкриє конфіденційні дані (паролі, фінансову інформацію тощо).

Загалом фішинг (phishing) належить до найпоширеніших форм соціальної інженерії: зловмисники імітують відомі бренди чи офіційні установи (банки, поштові сервіси, державні органи), аби ввести жертву в оману та примусити її добровільно надати чутливу інформацію. Серед найбільш небезпечних відомостей, які можуть бути викрадені внаслідок фішингу, фігурують паролі до електронних пошт і соціальних мереж, номери платіжних карток, CVV-коди, PIN-коди, а також персональні дані (адреси, номери телефонів, інші ідентифікаційні відомості). Як свідчить низка досліджень, масштаби фішингових атак зростають пропорційно до їхньої дедалі більшої складності та реалістичності.

Клон-фішинг вирізняється тим, що шахрай не просто видає себе за відоме джерело, а й послуговується оригінальним змістом колись дійсно отриманого або поширеного повідомлення, змінюючи лише посилання на те, яке веде на фальшиву вебсторінку чи інший шкідливий ресурс. Зазвичай такий лист виглядає цілком автентично, оскільки збігається з попереднім коректним текстом і форматом, через що одержувач часто не помічає підміни. Як наслідок, відкривши нібито надійний матеріал, користувач ризикує власноруч ввести конфіденційні дані у зовсім іншу форму, розміщену на сервері, контрольованому зловмисниками [1, 2].

Фішинг загалом залишається одним із ключових викликів у сфері соціальної інженерії, оскільки покладається не лише на технічні вразливості, а й на психологію користувача. Легітимні бренди, державні структури чи популярні сервіси часто стають «мішенню для клонування», аби викликати довіру у потенційних жертв. Це дозволяє успішно виманювати дані для авторизації, платіжні реквізити й усіляку чутливу інформацію, включно з персональними відомостями чи іншими ідентифікаційними деталями [3]. Кінцева мета таких дій полягає в одержанні доступу до чужих акаунтів чи банківських рахунків або ж перепродажу видобутих даних на чорному ринку.

1.4 Внутрішні загрози

Внутрішні загрози - це загрози інформаційній безпеці, які виникають безпосередньо від тих, хто має офіційний (хоча й обмежений) доступ до внутрішніх систем і даних, таких як працівники та підрядники. Загрози можуть бути навмисними або ненавмисними: Навмисні загрози Зловмисні дії працівників: навмисна крадіжка конфіденційної інформації, саботаж систем або внесення шкідливих змін (наприклад, введення неправдивих даних до баз даних). Економічні або ідеологічні загрози: дії через розчарування або з

метою отримання прибутку (наприклад, продаж комерційної таємниці конкурентам). Ненавмисні загрози Помилки або упущення: співробітники випадково видаляють важливі файли, надають доступ зовнішнім особам або вносять ненавмисні зміни, які призводять до витоку даних. Соціальна інженерія: Співробітників обманюють за допомогою фішингових електронних листів або телефонних дзвінків, змушуючи їх мимоволі розкрити свої паролі або конфіденційну інформацію.

Попри те, що внутрішні користувачі зазвичай проходять авторизацію, найчисленніші витоки або викривлення даних часто трапляються саме через їхні дії. Брак належного контролю версій та журнального аудиту робить непомітними як випадкові помилки, так і навмисні викрадення інформації. Особливо небезпечним стає саботаж у середовищах із браком деталізованого розмежування прав доступу: коли співробітники мають ширші привілеї, ніж потрібно для виконання службових обов'язків, вони можуть пошкодити базу даних чи знищити критичні файли без особливих перешкод. У корпоративному контексті загроза загострюється під час масштабування бізнесу або залучення віддалених підрядників, бо тоді важче забезпечити централізований нагляд та швидко відстежувати підозрілі дії. Іноді небажані події розпочинаються з буденних помилок: відправлення електронного листа із чутливими вкладеннями на неправильну адресу чи зберігання паролів у відкритому вигляді. Проте найпоширенішим каталізатором зростання внутрішніх ризиків залишаються техніки соціальної інженерії: якщо недбалі або необізнані працівники розкриють власні облікові записи, це дасть зловмисникам майже необмежені можливості зловживати довіреними ресурсами чи масштабувати атаку на інші частини системи.

1.5 Активні та пасивні загрози

Пасивні загрози передбачають приховане перехоплення та аналіз трафіку без внесення змін у його структуру. У такому разі зловмисник зазвичай використовує спеціалізовані інструменти (так звані «сніфери»), які дають змогу спостерігати за передаванням даних (логіни, паролі, номери карток), не залишаючи чітких слідів і не втручаючись у вміст пакетів. Хоча сучасні методи шифрування нерідко запобігають розкриттю справжньої інформації всередині повідомлень, атакувальна сторона все ж може дослідити метадані: частоту звернень, час активності, обсяги відправлених

пакетів. Це дозволяє визначити тип та інтенсивність взаємодії між вузлами й виявити закономірності, що прокладають шлях до складніших нападів, як-от атаки «людина посередині» (MitM). При цьому, на відміну від активних видів втручання, подібна діяльність залишається майже непомітною, оскільки не вносить жодних спотворень у середовище й не модифікує дані, унаслідок чого її важко виявити на етапі простого спостереження.

Пасивні загрози мають здебільшого непомітний характер, оскільки не змінюють ані змісту, ані структури даних, а також не спричиняють видимих порушень роботи системи. Зловмисник зазвичай покладається на спеціалізовані сніфери, щоби перехоплювати мережевий трафік, використовуючи при цьому як доступ до фізичного середовища передавання, так і вразливості у логічних сегментах. Хоча поширене шифрування (наприклад, TLS або VPN-тунелі) може закривати від сторонніх очей конкретний уміст пакетів, залишаються метадані, як-от обсяг, час і частота звернень, що розкривають модель діяльності користувача. Такі патерни здатні допомогти визначити особливо вразливі моменти взаємодії з мережею та уможливлюють підготовку складніших атак, наприклад «людина посередині» (MitM) [1, 2].

Головна риса пасивних загроз полягає в тому, що нападник залишає системі мінімальні ознаки своєї присутності: не відбувається модифікації даних чи збоїв у передаванні. Подібний «тихий» метод є особливо небезпечним, коли фахівці з безпеки покладаються переважно на моніторинг активності, очікуючи появи аномальних подій чи змін у журналах. За умов відсутності розширеного аналізу мережевого трафіку або метаданих (часто реалізованого у рамках SIEM або спеціалізованих IDS-рішень), перехоплення може тривати тривалий час, даючи змогу зловмисникам зібрати велику кількість відомостей про користувачів, структуру мережі та інші чутливі деталі

Активні загрози вирізняються тим, що зловмисник не обмежується простим переглядом чи пасивним збором даних, а безпосередньо втручається

в роботу системи. У такому разі відбувається несанкціонована модифікація або знищення інформації, а також вставлення шкідливих фрагментів коду. Прикладами можуть слугувати навмисне внесення хибних платіжних реквізитів у базу даних, фальсифікація контенту на вебсайтах або використання вразливостей (наприклад, SQL-ін’єкцій) для здобуття повного контролю над системою й подальшого поширення шкідливого ПЗ. В особливо критичних випадках зловмисник може застосовувати атаки на відмову в обслуговуванні (DDoS), блокуючи облікові записи чи ініціюючи масове видалення файлів, що позбавляє легітимних користувачів доступу до сервісів

Головна ознака активних загроз полягає в порушенні звичної роботи системи: дані піддаються спотворенню, ресурси стають недоступними, а у файловій системі або журналах подій з’являються аномальні записи. Хоча подібна діяльність залишає сліди (помітні зміни у функціонуванні або хибні дані в базах), вона здатна завдати прямої шкоди: викрасти конфіденційні відомості, завдати фінансових збитків чи знищити важливу інформацію. У разі відсутності дієвих систем моніторингу та оперативного реагування, зловмисник може тривалий час залишатися непоміченим, особливо якщо використовує методи приховування слідів або експлойти «нульового дня»

Активні загрози можуть реалізовуватися не лише шляхом безпосереднього втручання у файлову систему або створення шкідливих фрагментів коду, а й через поступове поширення впливу на суміжні вузли мережі. Якщо зловмисникові вдається здобути підвищені привілеї на одному сервері, він може поступово розширювати власні можливості, проникаючи у взаємопов’язані служби та бази даних. У такому сценарії навіть порівняно невелике виявлення вразливості призводить до ланцюгового ефекту, коли захоплення контрольного пункту дає змогу зламати весь контур безпеки. Це

особливо небезпечно у великих організаціях, де спільні ресурси (файлові сховища, поштові сервери) поєднані і мають спільні точки автентифікації.

До того ж сучасні методи атак можуть передбачати встановлення бекдорів або руткітів, що непомітно вбудовуються в операційну систему, приховуючи сліди втручання. Таким чином, навіть у разі поверхневої перевірки системні логи не свідчать про злам, а стандартні засоби захисту (антивірус, звичайний файрвол) не виявляють підозрілої активності. Така довготривала присутність (англ. *persistent threat*) забезпечує зловмиснику майже безперешкодний доступ до важливих процесів, дозволяючи викрадати дані, змінювати конфігурації або готувати додаткові «вхідні точки» для майбутніх вторгнень.

Водночас системи моніторингу та аналізу поведінки (евристичні IDS/IPS, SIEM-платформи) можуть визначати аномальні патерни, що не властиві штатній роботі: раптове збільшення обсягу вихідного трафіку, непритаманні операції з базами даних чи несумісні з розкладом резервування дії. Подібні сигнали вказують на факти зловмисного перезапису файлів або «зашумлення» журналів подій, які роблять картину атак складнішою, але все ще можуть бути розпізнані за допомогою досконалих механізмів виявлення.

2 ОГЛЯД МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Криптографія

Розглядаючи криптографічні механізми, варто виокремити симетричне шифрування, що передбачає використання спільного ключа для процесів шифрування й розшифрування. Одним із найвідоміших стандартів цієї групи вважають Advanced Encryption Standard (AES), розроблений як більш надійна заміна для Data Encryption Standard (DES) і затверджений Національним інститутом стандартів і технологій США (NIST) на початку 2000-х років [1]. Його безпеку та широку підтримку обумовлює низка переваг:

- Розмір блоку: 128 біт, що дає змогу стабільно обробляти великі обсяги даних.
- Довжина ключа: зазвичай 128, 192 або 256 біт (залежно від вимог до безпеки і швидкості).
- Продуктивність: AES ефективно реалізується як програмно, так і апаратно, завдяки чому часто застосовується в реальному часі для шифрування чи дешифрування великих потоків (VPN-тунелі, Wi-Fi з WPA2/WPA3, файлові системи BitLocker або FileVault).
- Режими шифрування: окремо можна згадати ECB (шифрування блоків незалежно), CBC (ланцюгування блоків), CFB/OFB (зворотний зв’язок за шифротекстом або виводом) та CTR (лічильник). Обрання відповідного режиму допомагає усувати дублювання та забезпечує додаткову випадковість у зашифрованих даних [2, 3].

Загальна ідея роботи алгоритму полягає в тому, що дані поділяються на 128-бітні блоки, які піддають низці раундів (10, 12 або 14, залежно від довжини ключа). На кожному етапі виконуються операції перестановок, заміщень та накладання ключа, аби перетворення стало незворотним з

погляду нескінченно малого перебору. Такий підхід поєднує високу стійкість до зломів із продуктивністю, що робить AES універсальним рішенням для захисту даних як у проводових чи безпровідних мережах, так і в локальних системах зберігання [4].

У низці сучасних обчислювальних платформ реалізовано апаратні інструкції (AES-NI), що прискорюють обчислення, пов’язані з AES. Завдяки цьому, навіть за довжини ключа в 256 біт досягається висока пропускна здатність при шифруванні потокових даних. До того ж архітектура AES передбачає використання S-box (таблиць заміщення), побудованих на основі операцій у скінчених полях (Galois Field), які значно ускладнюють криптоаналіз. Такий підхід, у поєднанні з повторюваними раундами й операціями перестановки, робить відновлення початкових даних неможливим без знання відповідного симетричного ключа, навіть якщо зловмисник перехоплює велику кількість зашифрованих блоків.

Важливо враховувати, що безпека AES значною мірою залежить від коректного управління ключами. Якщо ключ зберігається без належного захисту або передається незашифрованим каналом, криптостійкість алгоритму втрачає сенс, оскільки ключ може опинитися в руках сторонніх. На додаток, вибір режиму шифрування має відповідати конкретній задачі: у випадку потокового передавання в реальному часі зазвичай перевагу надають CFB або CTR, натомість CBC часто використовують у сховищах даних з обмеженим доступом, де відсутні вимоги до інтерактивної обробки. У кожному разі AES залишається базовим стандартом для захисту чутливої інформації в низці застосувань — від захищеного мережевого трафіку до підсистем шифрування дисків.

2.1.1 Асиметричні алгоритми

Асиметрична криптографія (криптографія з відкритим ключем) використовує пари приватних і публічних ключів. Відкритий ключ може вільно розповсюджуватися для шифрування та перевірки підпису, тоді як закритий ключ зберігається в таємниці і використовується для дешифрування та підпису. Існує два найпоширеніші підходи: (RSA, ECC).

2.1.2 RSA

Безпека RSA залежить від складності факторізації (розкладання) великих чисел, які є добутком двох (або більше) великих простих чисел. Користувач вибирає два великих простих числа, *pp* і *qq*, обчислює добуток (*n=p×qn=p×q)*. Відповідна функція використовується для генерації ключа (модуль *nn*, відкрита експонента, закрита експонента) довжина ключа 1024 біт не вважається достатньо безпечною тому треба використовувати ключ від 2048 біт, що є мінімально прийнятним Стандартом є ключ розміром 3072 біт, рекомендується використання ключа від 4096 біт і більше - для більш високої безпеки. Використовується під час обміну ключами (сеансові ключі, відкриті ключі) при встановленні захищеного з'єднання (TLS/SSL). Цифрових підписів (перевірка авторства та цілісності документів). Цифрових сертифікатів (X.509) для перевірки автентичності веб-сайтів і користувачів. Особливості RSA є повільніша за симетричні алгоритми робота, тому великі обсяги даних зазвичай не шифруються безпосередньо за допомогою RSA. Зазвичай використовується «гібридна схема»: RSA використовується тільки для обміну секретними ключами (симетричними ключами), а потім застосовується швидший симетричний алгоритм (AES).

2.1.3 ECC

Замість вичерпної факторизації, ECC базується на складності дискретних логарифмів на еліптичній кривій. Відправник і одержувач отримують пару ключів (відкритий і закритий), якщо відомий лише відкритий ключ, то відновити закритий ключ майже неможливо через математичні властивості еліптичної кривої. ECC має коротші ключі з 256-бітними ключами забезпечує майже такий самий рівень безпеки, як і RSA з

3072-бітними ключами при цьому обробка проходить швидше, менше навантаження на процесор (особливо важливо для пристроїв з обмеженими ресурсами (смартфони, IoT)). Менше даних для передачі (важливо для мережевих протоколів). ECC широко використовується в областях, де потрібна висока ефективність і безпека, таких як цифрові підписи (ECDSA), протоколи обміну ключами (ECDH), TLS/SSL, VPN, блокчейни (Bitcoin, Ethereum). Реалізація ECC повинна бути коректною (помилки в параметрах кривої або випадкових змінних знижують безпеку). У випадку з квантовими комп'ютерами, якщо з'явиться достатньо потужний квантовий комп'ютер, ECC буде настільки ж вразливим, як і RSA (однак, в даний час ECC вважається дуже надійним в класичних обчисленнях).

Таблиця 3.1 - Порівняння RSA та ECC

Критерій	RSA	ECC
Безпека (класична)	Висока за умови достатньої довжини ключа	Аналогічна або вища за менших ключів
Довжина ключа	Зазвичай 2048–4096 біт	224–521 біт (рекомендовано ~256–384 біт)
Швидкість	Повільніший, великі числа	Швидший, менша обчислювальна складність
Використання	Обмін ключами, цифрові підписи, сертифікати	Цифрові підписи (ECDSA), обмін ключами (ECDH)
Стійкість	Сильна, та потребує довших ключів	Сильна, але з коротшими ключами

Із вишенаданої таблиці RSA залишається класичним і широко розповсюдженим завдяки своїй історії та підтримці в багатьох системах, але вимагає великих ключів для забезпечення високого рівня безпеки.

ECC пропонує такий самий (або кращий) рівень безпеки з меншими ключами і кращою продуктивністю, що робить його привабливим для мобільних пристроїв, IoT і високонавантажених серверів. У реальних системах часто використовуються «гібридні» протоколи, де RSA/ECC використовується для створення сеансу шифрування, а потім симетричний алгоритм (AES) використовується для швидкого шифрування великих обсягів даних.

2.2 Міжмережеві екрани (фаєрволи)

Фаєрвол слугує засобом первинного аналізу мережевого трафіку відповідно до визначених правил безпеки. Одним із найпростіших його різновидів є пакетні фільтри, котрі зосереджені виключно на аналізі заголовків (IP-адрес, портів, протоколів) і не вдаються до розгляду вмісту (даних) пакета [15]. Здебільшого вони працюють на мережевому та транспортному рівнях (3-4-й рівні моделі OSI), орієнтуючись на попередньо задані політики (ALLOW, DENY) або політику за замовчуванням (Allow All чи Deny All).

Принцип дії ґрунтується на порівнянні атрибутів пакета (IP-адреса джерела й призначення, номер порту, тип протоколу) із визначеним набором правил, створеним адміністратором системи. Якщо під час перевірки пакет не відповідає жодному з них, застосовується політика за замовчуванням. До переваг такого підходу належать відносна простота налаштування та висока швидкість обробки, оскільки фільтр розглядає лише поля заголовка, не аналізуючи вміст даних.[10]

Водночас пакетні фільтри мають низку обмежень. По-перше, вони не враховують стан з’єднання (на відміну від брандмауерів зі Stateful Inspection), отже не «розуміють» типового поведінкового патерну різних протоколів (HTTP, FTP тощо). По-друге, у разі відсутності додаткових механізмів автентифікації чи перевірки цілісності зростає ризик IP-підроблення, оскільки зловмисник може видавати трафік за легітимний, використовуючи фальшиві заголовки. І нарешті, у великих розподілених мережах, де правила часто набувають значного обсягу, адміністрування ускладнюється, що підвищує ймовірність помилок або конфліктів.

Попри ці недоліки, пакетні фільтри широко застосовують на базових маршрутизаторах, формуючи першу лінію оборони. Поєднання з більш розвинутими системами (Stateful Firewall, IDS/IPS) забезпечує глибшу перевірку трафіку й аналіз його вмісту, зокрема виявляючи шкідливі або нетипові пакети у вищих шарах мережевої взаємодії.[7]

2.2.1 Stateful Inspection

Stateful Inspection є підходом до фільтрації мережевого трафіку, що дає змогу брандмауеру відстежувати контекст сесій, а не лише аналізувати окремі пакети ізольовано [15]. На відміну від базових пакетних фільтрів, цей метод дає змогу визначити, до якого з'єднання належить кожен пакет, та ухвалити рішення, виходячи з дійсного стану (установлено з'єднання чи ні, який етап TCP-«рукостискання» тощо).

В основі Stateful Inspection лежить динамічна таблиця станів, де реєструються відомості про з'єднання (IP-адреси, порти джерела й призначення, параметри TCP або UDP, обсяг переданих байтів та ін.). Наприклад, коли встановлюється TCP-сеанс, брандмауер відслідковує етапи SYN/ACK, а згодом очікує завершення (FIN або RST). Якщо новий пакет не відповідає жодному з відкритих або очікуваних з'єднань, він блокується [10]. Так само система забороняє спроби надсилання трафіку, що декларує себе «внутрішнім», проте не відповідає активній сесії у таблиці станів, що утруднює IP-підміну.

При цьому Stateful Inspection забезпечує більш гнучкі правила безпеки, адже дозволяє не лише перевіряти IP та порти, а й перевіряти легітимність поточного етапу з'єднання. Якщо ініціаторами сеансу виступають внутрішні хости, то брандмауер пропускає зворотний трафік із зовнішньої мережі, оскільки у таблиці станів уже зафіксовано легітимне встановлення [3]. Водночас такий підхід потребує додаткових ресурсів: системі потрібно зберігати й оновлювати записи про кожну активну сесію, що збільшує навантаження на процесор і пам'ять. Утім, сучасні апаратні та програмні реалізації (наприклад, у продуктах Cisco ASA, Check Point, Fortinet) здатні ефективно впоратися з великою кількістю паралельних з'єднань [11].

Таким чином, порівняно з фільтруванням окремих пакетів на рівні заголовків, Stateful Inspection підвищує точність ухвалення рішень і суттєво ускладнює атаки підміни IP або зловживання нестандартними послідовностями пакетів. Цим пояснюється, чому SPI є поширеною технологією в як корпоративних брандмауерах, так і у звичайних домашніх маршрутизаторах, які дозволяють з'єднання лише тоді, коли вони дійсно ініційовані зсередини.

2.2.2 NGFW (Next-Generation Firewall)

Це новітній тип брандмауерів, який поєднує в собі класичний підхід перевірки стану з розширеними функціями безпеки на прикладному рівні. Основне призначення NGFW - надавати більш детальну інформацію про мережевий трафік, не обмежуючись IP-адресами, портами і протоколами. Контроль і аналіз мережевого трафіку, включаючи, але не обмежуючись IP-адресами, портами і протоколами.

Ключові особливості глибокої перевірки пакетів NGFW (DPI): Перевірка даних у пакетах на рівні прикладних протоколів (наприклад, HTTP, FTP, DNS). Ідентифікація конкретних додатків і сервісів (Facebook, YouTube, BitTorrent), навіть, якщо вони використовують нестандартні порти ідентифікація та контроль додатків NGFW можуть розрізняти різні типи трафіку (наприклад, завантаження файлів з Google Drive або перегляд відео на YouTube). Можна створювати правила для дозволу/заборони певних сервісів або певних дій (наприклад, блокувати передачу файлів в Instant Messenger). Інтегрована система виявлення та запобігання вторгненням (IDS/IPS) NGFW зазвичай включають IDS/IPS для виявлення відомих шаблонів атак, сигнатур і незвичайної активності. Вони автоматично блокують або повідомляють про підозрілий трафік без необхідності встановлювати окремий продукт IPS. Антивірусні/антишкідливі модулі (іноді їх називають «пісочниця») Деякі NGFW надають можливість аналізувати файли і контент, що проходять через брандмауер, і миттєво виявляти шкідливе програмне забезпечення. Також можлива інтеграція з хмарними сервісами «пісочниці», за допомогою яких підозрілі файли запускаються у

віртуальному середовищі і перевіряється їх поведінка. Контроль і автентифікація користувачів NGFW можна інтегрувати з корпоративними системами (Active Directory, LDAP), щоб ідентифікувати конкретного користувача, який ініціює з'єднання. Правила безпеки можуть бути визначені за ролями та групами (наприклад, дозволити доступ до певних сайтів у відділі кадрів і заблокувати інші). Більшість рішень NGFW надають веб-інтерфейс або спеціальну інформаційну панель для управління політиками безпеки, перегляду журналів, генерації звітів тощо. перевагами NGFW є комплексний захист «з коробки» Інтеграція перевірки стану, IDS/IPS, фільтрації на рівні додатків та механізмів захисту від шкідливого програмного забезпечення в одному пристрої спрощує інфраструктуру та управління. Спрощення інфраструктури та управління. Більш тонкий контроль Можна точно налаштувати політики, наприклад, дозволити тільки текстові повідомлення з певних додатків, а не передачу файлів. Удосконалене виявлення загроз Вбудований евристичний аналіз і механізми сигнатур, що працюють в режимі реального часу, можуть виявляти шкідливий трафік, який може бути пропущений традиційними брандмауерами. Гнучка масштабованість Постачальники NGFW (Cisco, Palo Alto, Fortinet, Check Point) пропонують різноманітні моделі - від невеликих для середнього бізнесу до високопродуктивних для центрів обробки даних.

У порівнянні з традиційними брандмауерами, рішення NGFW зазвичай дорожчі (включаючи ліцензії на додаткові модулі IDS/IPS, фільтрацію веб-додатків, антивірус тощо). Ресурсоємність Глибоке сканування на рівні додатків вимагає більше ресурсів процесора та пам'яті для аналізу великих обсягів трафіку. Складніша конфігурація Для детального контролю протоколів і додатків потрібні більш спеціалізовані знання (розуміння бізнес-процесів, додатків і потреб користувачів). Потенційні конфлікти з окремими додатками Якщо NGFW неправильно визначають трафік, легітимні сервіси можуть бути заблоковані або пропускна здатність може бути зменшена 4. Застосування Корпоративна мережа Цільові атаки, інсайдерські загрози, фільтрація веб-трафіку, захист від відомчого контролю доступу. Державні установи Підвищення безпеки, контроль над даними, які можуть бути завантажені або передані, інтеграція з оперативними центрами кібербезпеки. Центри обробки даних і хмарні середовища Висока пропускна здатність, масштабованість, захист розподілених додатків і віртуальних машин. Постачальники послуг (ISP) Захист інфраструктури та надання послуг безпеки клієнтам (наприклад, керовані рішення NGFW).

2.3 Системи виявлення та запобігання вторгнень (IDS/IPS)

2.3.1 IDS

Системи виявлення вторгнень (IDS) здійснюють моніторинг мереж і систем для виявлення активності, яка може свідчити про спроби несанкціонованого доступу, порушення політик або зловмисну поведінку (наприклад, вірусні атаки, сканування портів, програмні експлойти). Основна функція IDS - сповіщення адміністратора безпеки або відповідної системи про підозрілу активність, зазвичай без блокування (це вже робить IPS) .

HIDS (Host Based IDS) Встановлюється безпосередньо на хості (сервері, робочій станції). Відстежує локальні події, зміни файлів, системні журнали, транзакції та інші метрики для виявлення аномалій і відомих шаблонів атак: OSSEC, Tripwire (моніторинг змін файлів).

Антивірусне програмне забезпечення з розширеними функціями моніторингу NIDS (Network Based IDS) Розгортається в мережі і пасивно прослуховує трафік, що проходить через певні сегменти або порти. Аналізує пакети (заголовки і, можливо, вміст) на наявність підозрілих сигнатур, відомих векторів атак і аномалій трафіку. Приклади: Snort, Suricata, Zeek (раніше Bro).

Сигнатурний метод порівнює трафік і активність з базою даних відомих шаблонів атак (сигнатур) (наприклад, SQL-ін'єкції, переповнення буфера, шкідливі пакети). Перевага це висока точність проти відомих загроз, а недоліком є неефективний проти нових або модифікованих атак, не включених до бази даних сигнатур.

Аномальні (евристичні) методи - Система вивчає, які показники трафіку або активності є «нормальними», і виявляє відхилення від цієї норми (аномальні обсяги, аномальний час доступу, підозрілі операції з файловою системою). Переваги: може виявляти нові або рідкісні загрози, яких немає в сигнатурах. Недоліки: «норма» може динамічно змінюватися і призводити до хибних спрацьовувань.

Сучасні IDS часто поєднують методи сигнатур і виявлення аномалій для підвищення загальної ефективності. Збір трафіку NIDS отримує копії

пакетів з мережевого середовища (через SPAN-порти комутатора або мережеві точки доступу). Аналіз заголовків і вмісту коли система перевіряє IP-адреси, порти і протоколи, можливо, на більш глибокому рівні.

2.3.2 IPS

Система запобігання вторгненням (IPS) - це програмно-апаратний комплекс, який виконує функції системи виявлення вторгнень (IDS), але з додатковими механізмами активного блокування. Це означає, що коли IPS виявляє аномальну або небезпечну активність (наприклад, відомі атаки або експлойти), він може відмовити в обслуговуванні пакетів або з'єднань. Перенаправлення трафіку для подальшого аналізу. Скинути існуючі з'єднання. Мета IPS - захист мереж і хостів від атак в режимі реального часу Хост-орієнтована IPS (HIPS) Безпосередньо на кінцевому комп'ютері (сервері, робочій станції) Встановлення. Аналізує системні процеси (процеси, файли, реєстр, мережеві з'єднання) і може блокувати потенційно небезпечні дії (наприклад, виконання шкідливого коду) на хості NIPS (Network-based IPS) Працює в мережі і перевіряє пакети на льоту, якщо виявлено атаку (наприклад, відомий підпис експлойта або аномальний трафік), шкідливе з'єднання може бути негайно заблоковано або перервано.

2.4 Порівняння IDS та IPS

Перевагами IDS можна вважати раннє виявлення атак, IDS може попередити про потенційну зловмисну активність до того, як вона завдасть масштабної шкоди. Додатковий аналіз: журнали, статистика та інформація про події можуть бути зібрані для подальшого аналізу. Захист від внутрішніх загроз (особливо HIDS), може захистити від внутрішніх загроз у разі аномальної поведінки співробітників або зловмисних операцій на вузлах. Недоліки Немає автоматичного блокування: IDS переважно повідомляє, але не блокує загрози (для блокування використовуйте СПП). Хибні спрацьовування: неповні правила та аномальні шаблони можуть призвести до хибних спрацьовувань, що ускладнює роботу аналітиків. Обмежена ефективність проти зашифрованого трафіку та дуже спеціалізованого трафіку, який IDS не може або не хоче розшифровувати; відсутність 100%

гарантії виявлення: якщо зловмисники обережні або використовують нові методи, IDS може пропустити атаку.

Переваги IPS це активний захист: “негайне блокування атак ускладнює проникнення в мережу”. Зменшення навантаження на адміністраторів, адміністратори відстежують тривоги 24/7 і не повинні вручну блокувати загрози (як у випадку з IDS). Комбінована функціональність Багато систем IPS мають вбудовану функціональність NGFW, модулі захисту від шкідливого програмного забезпечення та інтеграцію з хмарними сервісами аналізу загроз.

Недоліки IDS ризик хибних спрацьовувань: “хибні спрацьовування СПП можуть призвести до переривання роботи легітимних сервісів або блокування критично важливого трафіку". Високі вимоги до продуктивності Безперервний аналіз трафіку і фільтрація «на льоту» вимагають швидких процесорів і достатнього обсягу пам'яті, особливо у великих мережах. Більш складна конфігурація Правильна конфігурація IPS вимагає детальних знань мережевої архітектури, протоколів і сервісів, щоб запобігти випадковим блокуванням.

Таблиця 2.2 - Порівняння IDS та IPS

Основна ідея	Виявлення загроз (пасивний режим)	Запобігання загрозам (активний режим)
Реакція на атаку	Аналізує та сповіщає про підозрілу активність	Може блокувати, перенаправляти або скидати підозрілий трафі
Втручання в трафік	Зазвичай не втручається в проходження пакетів	Активно змінює або блокує трафік у разі виявлення загрози
Ризик помилкового спрацювання	Високий ризик хибних тривог (False Positives), але не блокує	При помилковому спрацюванні може порушити роботу легітимних сервісів

Продуктивність	Менший вплив на мережеву продуктивність (пасивна обробка)	Часто вимагає більшої обчислювальної потужності (активна обробка)
Переважний рівень застосування	Контроль та аудит подій, аналіз інцидентів, дослідження безпеки	Оперативний захист від атак, блокування інцидентів у реальному часі
Приклад використання	Збір логів, сигнатурний/аномалійний моніторинг, сповіщення аналітиків	Апаратний або програмний блок трафіку в корпоративних мережах, дата-центрах
Сумісність з іншими системами	Легко інтегрується з SIEM для централізованого аналізу	Може доповнювати фаєрвол (NGFW), складніше інтегрується з іншими рішеннями

Ця порівняльна таблиця демонструє, що IDS і IPS мають різні підходи до забезпечення безпеки мереж. IDS є пасивною системою, основне завдання якої — виявлення загроз і сповіщення про підозрілу активність без прямого втручання. Це робить її менш ресурсоємною та ефективною для аналізу й аудиту подій, але водночас залишає можливість для хибних тривог без негайної реакції.

IPS, у свою чергу, працює в активному режимі, не лише виявляючи загрози, але й запобігаючи їм шляхом блокування або перенаправлення шкідливого трафіку. Однак така функціональність потребує більше обчислювальних ресурсів і може викликати перебої у роботі легітимних сервісів у разі хибного спрацювання.

Вибір між IDS і IPS залежить від конкретних потреб організації: IDS підходить для моніторингу та аналізу, тоді як IPS забезпечує активний захист і є ефективним для оперативного реагування на загрози. У багатьох випадках

найкращим рішенням є їхнє поєднання для досягнення балансу між точністю виявлення й активною протидією атакам.

2.5 VPN (Virtual Private Network)

Віртуальні приватні мережі (VPN) формують захищений тунель передавання даних у відкритих або ненадійних мережах на кшталт Інтернету. Серед поширених протоколів для цього можна виокремити *OpenVPN, IPSec* чи *WireGuard.* Вони надають змогу встановлювати віддалені підключення до ресурсів, цілковито шифруючи трафік між клієнтом і сервером. Унаслідок цього, навіть якщо нападник перехоплює пакети, їхній зміст залишається недоступним — у тому числі й для потенційних спроб «підглядання» чи модифікації.[13, 3]

Суть полягає в тому, що обидві сторони (клієнт і сервер) домовляються про криптографічні параметри, аби захистити весь обмін: кожний пакет інкапсулюється у зашифрований контейнер, перш ніж вийти у глобальну мережу. Це ускладнює як пасивні загрози (спостереження), так і активні (підміна пакетів), оскільки зловмисник не здатний розшифрувати або коректно підробити трафік без відповідних ключів. Такий підхід є надзвичайно актуальним для корпоративного сектору, де співробітники працюють з дому або під час поїздок, а також для приватних користувачів, які не бажають відкривати власний трафік у публічних Wi-Fi чи інших небезпечних точках доступу.[12]

2.5.1 Типи і протоколи

Типи й протоколи VPN можуть істотно відрізнятися залежно від цілей і масштабів використання. Одним із найбільш популярних і гнучких рішень є

OpenVPN з відкритим вихідним кодом, який базується на TLS/SSL і забезпечує багатий набір конфігураційних можливостей (зокрема гнучке налаштування ключів і методів автентифікації).[14] Іншим прикладом слугує IPSec, тобто набір протоколів, які працюють на мережевому рівні й часто застосовуються в корпоративному середовищі, коли потрібно прозоро об’єднати філії в єдиний віртуальний простір.[3] Новіший за них WireGuard вирізняється спрощеною конфігурацією, сучасними криптопримітивами й високою швидкістю, тоді як L2TP/IPSec чи SSTP зазвичай вбудовані в операційні системи Windows або macOS, хоч можуть пропонувати менше гнучкості.

Застосування VPN-технологій дає змогу вирішувати кілька завдань: забезпечення безпечного віддаленого доступу користувачів (remote access) до корпоративної мережі, створення наскрізних тунелів між географічно розподіленими офісами (site-to-site VPN), а також надання послуг приховування IP-адреси чи обходу регіональних обмежень (особливо затребувано серед індивідуальних користувачів) [14]. Серед найбільших переваг можна назвати суттєве підвищення конфіденційності, адже кожен пакет передається у зашифрованому вигляді, що унеможливлює читання або втручання зловмисників у відкритих мережах, а також імітацію локальної мережі, коли віддалені працівники можуть взаємодіяти з внутрішніми ресурсами так, ніби вони фізично перебувають в офісі. Крім того, за наявності різноманітних протоколів з’являється змога адаптуватися до конкретних вимог і будувати складні топології з використанням маршрутизаторів чи шлюзів.

Незважаючи на очевидні переваги, VPN вимагає врахування низки обмежень і викликів. Шифрування й дешифрування можуть знижувати пропускну здатність з’єднання, якщо обчислювальні ресурси обмежені. Надійність системи залежить від правильності конфігурації й захисту ключів,

оскільки витік цих ключових даних або помилки в налаштуваннях часто спричиняють повний компроміс безпеки, хай навіть алгоритми шифрування самі по собі є надійними. У великих інфраструктурах із багатьма віддаленими клієнтами й офісами адміністрування ключів, сертифікатів та правил доступу вимагає додаткового планування та ресурсів, а також постійного моніторингу й оновлень [7].

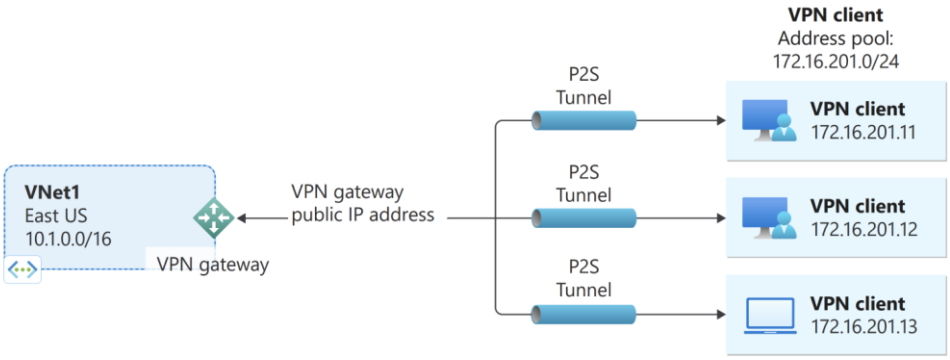

Рисунок 2.1 - Топологія VPN на базі (MS Azure)

2.6 Антивірусні системи та моніторинг мережі

Антивірус, визначає та усуває шкідливі програми (віруси, трояни). Потребує регулярного оновлення сигнатур. Регулярне оновлення сигнатур потрібно тому що творці вірусів постійно демонструють та роблять нові загрози, тому наявність актуальної бази сигнатур дає змогу миттєво розпізнавати шкідливі файли. Без оновлень антивірус може пропустити нові типи вірусів, які невідомі старим версіям бази сигнатур. Антивірусне ПО використовує декілька мтодів виявлення. Сигнатурний аналіз - порівнює файли з базою даних відомих загроз.

Евристичний/поведінковий аналіз - відстежує підозрілі дії (наприклад, модифікацію системних файлів, запуск нетипових процесів) для виявлення невідомих або поліморфних шкідливих програм. У більшості випадків антивіруси містять антишпигунські та брандмауерні модулі, а також можуть сканувати електронну пошту та інші протоколи (HTTP, FTP), підвищуючи таким чином загальний рівень безпеки системи.

Моніторинг мережі (SIEM), аналітика подій мережі у реальному часі, виявлення аномалій у логах системи.

SIEM (Security Information and Event Management) це дані з системних журналів, мережевих журналів та інших інструментів безпеки (брандмауерів, IDS, антивірусів) інтегруються в єдину інформаційну панель для централізованого аналізу. Якщо IDS виявляє підозрілий пакет, а брандмауер блокує невідомий IP, SIEM «зіставляє факти» і генерує оповіщення про потенційну атаку або вторгнення. SIEM може надсилати сповіщення в режимі реального часу (інтегровані з електронною поштою, SMS та месенджерами), якщо правила кореляції показують підозрілу поведінку. У більшості випадків впроваджується модуль SOAR (Security Orchestration, Automation and Response), який може автоматично реагувати на певні типи подій (наприклад, блокувати IP-адреси або відключати користувачів).

3 ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ

3.1 Критерії порівняння

1. Рівень безпеки - наскільки метод може захистити від найпоширеніших загроз.
2. Продуктивність - як змінюється пропускна здатність мережі та використання ресурсів.
3. Зручність впровадження - чи потрібне складне обладнання або спеціальні навички.
4. Масштабованість - можливість розширення при збільшенні кількості користувачів.
5. Вартість - закупівля, ліцензії, навчання персоналу, супровід.

Таблиця 3.1 - Порівняльна таблиця методів

Метод	Рівень безпеки	Продуктивність	Зручність впровадження	Масштабованість	Вартість
Криптографія	Високий (шифрування	Помірний вплив	Потребує керування ключами	Висока	Середня (залежно від PKI)
Фаєрволи	Середній–Високий	Зазвичай мінімальний	Відносно просте	Висока (гнучкі налаштування)	Від середньої до високої
Аутентифікація, контроль доступу	Високий (особливо 2FA)	Низький	Середня складність	Висока	Середня
IDS/IPS	Високий (реагування в реальному часі)	Може бути великим при великому трафіку	Складне (оновлення, налаштування)	Висока	Від середньої до високої

VPN	Високий (шифрований тунель)	Може знизити швидкість	Залежить від вибраного протоколу	Висока	Середня
Антивірус	Середній	Низький	Потребує	Висока	Середня

4 ПРИКЛАДИ БЕЗПЕЧНОЇ РЕАЛІЗАЦІЇ

Для початку треба вибрати операційну систему та встановити основні інструменти: брандмауер (мережевий екран) для перевірки портів. Антивірус для виявлення та видалення шкідливого програмного забезпечення. Моніторинг/журнали (наприклад, стандартні системні журнали та інструменти аналізу подій). Далі треба налагтувати брандмауер для базового захисту За замовчуванням усі вхідні з'єднання блокуються. Дозвояємо лише ті порти та протоколи, які дійсно необхідні (80/443 для веб-серверів). Така «мінімізація відкритих портів» запобігає багатьом атакам. Далі треба встановити та активувати антивірус. Рішення треба приймати ісходячи з того на скільки регулярно здійснюється оновлення сигнатур (онлайн-оновлення або через окремий файл). Робити регулярну перевірку папок та файлів, щоб запобігти поширенню вірусів і троянів. Постійно слідкуйте за журналами антивірусу, щоб переконатися, що підозрілі об'єкти не будуть знайдені.

Наступний крок це розгортння HTTPS (сшифрування з'єднання), якщо використовується локальний веб-сервер тоді для тестування або локальних проектів треба увімкнути шифрування (TLS). Це захистить паролі, форми та конфіденційні дані від перехоплення навіть на локальному рівні. Сертифікати можуть бути самопідписаними (для внутрішнього використання) або виданими офіційним центром сертифікації, якщо вони є у відкритому доступі. Використовуйте вбудовані журнали подій (системні журнали, журнали безпеки) для запису блокування брандмауером, виявлення шкідливого програмного забезпечення антивірусом та нетипових спроб доступу. Рекомендується аналізувати ці журнали вручну або за допомогою простих інструментів. Додаємо «мінімальні» елементи SIEM. Якщо потрібні централізовані інформаційні панелі або кореляція подій, можна встановити

інструменти для збору журналів і генерування сповіщень у режимі реального часу.

Для зменшення «поверхні атаки» брандмауери відкривають лише потрібні їм порти і блокують доступ до випадкових або службових портів. Антивірус виявляє відомі віруси, трояни та руткіти, знижуючи ризик компрометації. HTTPS запобігає перехопленню конфіденційного трафіку (логінів, паролів та іншої важливої інформації). Моніторинг та швидке реагування: ведення журналів та (мінімальний) моніторинг дозволяють розпізнавати підозрілі події (наприклад, численні спроби підключення з невідомих IP-адрес, виявлення шкідливих файлів тощо) та реагувати на них до того, як вони стануть серйозними інцидентами.

.

5 ПРАКТИЧНА ЧАСТИНА

5.1 Середовище та інструменти виконання.

Після ознайомлення з теоретичними засадами і ключовими методами захисту даних у мережах логічним продовженням є демонстрація практичної реалізації, що дає змогу перевірити дієвість відповідних технологій у реальному контексті. Метою практичної частини є показати, як можна налаштувати елементи мережевої безпеки на одній-єдиній машині, не вдаючись до масштабної інфраструктури чи кількох серверів. Такий підхід дає змогу моделювати мережеві взаємодії локально через інтерфейси localhost або внутрішні мережеві адаптери, налаштовувати та випробовувати базові механізми захисту (фаєрвол, шифрування з'єднання, сканування портів), а також порівнювати рівень безпеки «до» і «після» впровадження конкретних рішень на кшталт фільтрації портів чи використання протоколу TLS.

У результаті отримано емпіричні дані, що підтверджують ефективність низки методів, розглянутих у теоретичному розділі, і створюють цілісне уявлення про базові принципи мережевої безпеки. Це, своєю чергою, демонструє на практиці здатність застосувати описані підходи й технології навіть за умов обмежених ресурсів і без складної інфраструктури

Ідея полягає в тому, що на одному комп'ютері ви одночасно розгортатимете веб-сервер (Nginx або Apache), налаштовуватимете фаєрвол для регулювання відкритих/закритих портів і запускатимете інструменти на кшталт nmap, аби перевірити, які сервіси лишаються видимими «з середини» (через localhost). Також слід увімкнути HTTPS з самопідписаним сертифікатом, щоби перевірити, як браузер і мережеві сканери реагують на зашифрований канал.

5.2 Підготовка середовища

5.2.1 Передумови

На машину буде встановлено ОС Linux (Debian 12) з налаштованими правами адміністратора (sudo), щоб встановлювати й налаштовувати компоненти безпеки та мережеві інструменти.

5.2.2 Установка потрібних утиліт

1. Веб-сервер (Nginx) — достатньо виконати sudo apt-get update і sudo apt-get install nginx. Далі перевіряють, чи служба запущена: sudo systemctl status nginx. За умовчанням Nginx слухає порт 80.
2. nmap — sudo apt-get install nmap, використовується для сканування та аудиту відкритих портів.
3. ufw (або iptables) — sudo apt-get install ufw, дає змогу керувати тим, які порти лишаються відкритими.
4. OpenSSL для створення самопідписаного TLS-сертифіката.

5.3 Кроки експерименту

5.3.1 Перевірка портів до увімкнення фаєрвола

Насамперед слід запустити (*sudo nmap -sS localhost;*) щоб зрозуміти, які порти машини «відкриті». Це допомагає усвідомити, які служби працюють за замовчуванням.

5.3.2 Налаштування фаєрволу

За допомогою UFW налаштовують політику за умовчанням:

sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw enable

Далі потрібно явно «дозволити» потрібні порти, наприклад 80 (для Nginx) та 22 (для SSH):

sudo ufw allow 80/tcp

sudo ufw allow 22/tcp

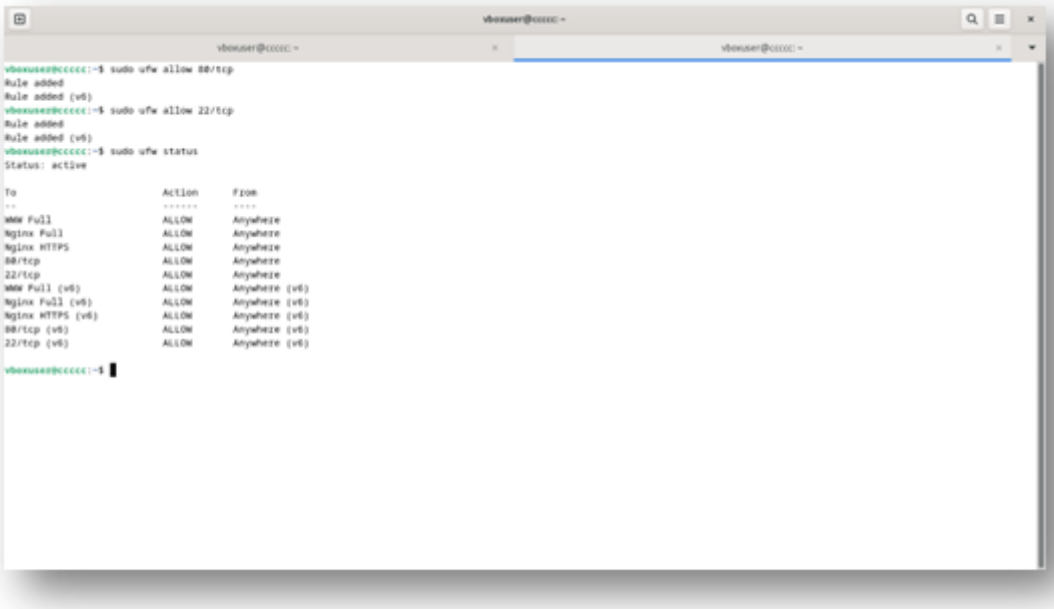

Рисунок 5.1 - перевірка встановлених правил

Повторне сканування sudo nmap -sS localhost покаже зміни: ті порти, які не дозволені, перейдуть у стан «closed» або «filtered».

5.3.3 Перевірка HTTP на локальній машині

Заходимо до браузеру на IP-Адресу пристороюю, скориставшись командою ip addr або на сторінку http://localhost/ і побачимо стартову сторінку Nginx (“Welcome to nginx!”).

Рисунок 5.2 - Стартова сторінка Nginx

5.4 Ручне налаштування HTTPS із самопідписаним сертифікатом

5.4.1 Створення сертифіката

У каталозі /etc/ssl/ виконують:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \ -keyout server.key -out server.crt

У полі Common Name (CN) доцільно вказати localhost, щоб отримати меньше попереджень у браузері.

5.4.2 Налаштування Nginx (порт 443)

У файлі /etc/nginx/sites-available/default створюють або редагують блок:

server {

listen 443 ssl;

server_name localhost;

ssl_certificate /etc/ssl/server.crt;

ssl_certificate_key /etc/ssl/server.key;

root /var/www/html; index index.html;

}

Після sudo nginx -t і перезапуску (sudo systemctl reload nginx), можна за потребою дозволити порт 443 у файрволі: (*sudo ufw allow 443/tcp)*

5.4.2 Перевірка HTTPS

Відкривають (https://localhost/) Браузер попередить про «недовірений сертифікат», але після підтвердження «Advanced → Proceed» сторінка завантажиться зашифрованим каналом.

5.5 Середовища використання

Нижче буде наведено середовища де використання подібної структури буде доцільним.

5.5.1 Тимчасовий або польовий офіс

Уявімо, що волонтерська або благодійна організація, яка регулярно переміщується між різними пунктами (гуманітарні центри, кризові зони), стикається з відсутністю розвиненої мережевої інфраструктури та стабільного інтернету (часто використовуються мобільні точки доступу чи чужий Wi-Fi). У таких умовах залишається потреба працювати з конфіденційними відомостями (заявками, персональними даними бенефіціарів), і водночас слід гарантувати захист від несанкціонованого доступу чи перехоплення трафіку.

Ноутбук або малопотужний десктоп, налаштований як «міні-сервер» і робоча станція одночасно, пропонує просте вирішення цієї задачі. Адміністратор установлює брандмауер (UFW чи iptables) і закриває всі порти, крім тих, що потрібні для веб-сервера — зазвичай 443, якщо передбачено використання HTTPS. Таке налаштування зменшує можливість легкого сканування у випадкових публічних мережах. Далі, локально розгортається веб-сервер (наприклад, Nginx) з мінімальним веб-застосунком

(це можуть бути прості форми для фіксації даних про отримувачів допомоги, реалізовані як HTML-сторінки, що зберігають записи у файлах чи невеликій базі SQLite).

Щоб унеможливити відкриту передачу логінів і конфіденційних полів, на веб-сервері генерують самопідписаний сертифікат (OpenSSL) і вмикають HTTPS. Хоча браузер і попереджає про «недовірений» центр сертифікації, увесь локальний трафік буде зашифрованим, позбавляючи зловмисника шансу прочитати чи підробити пакети. Перевірка за допомогою nmap демонструє помітну різницю «до» і «після» налаштування: раніше потенційно видно SSH, принт-сервіс або інші небажані послуги, тоді як тепер відкрито лише 443, а весь інший трафік блокується.

У результаті волонтери зберігають високий рівень мобільності: достатньо підключитися до чергового Wi-Fi, при цьому шифрування й файрволові політики зберігаються на ноутбуці, тож конфіденційні відомості захищені. Таке рішення не вимагає розгортання складних VPN-тунелів чи придбання офіційних сертифікатів, маючи мінімальні вимоги до компетентності в керуванні базовими інструментами (OpenSSL, UFW). При цьому локальний характер сховища означає, що дані не потрапляють у хмару чи на сторонні сервери, а налаштування безпеки можна розгорнути приблизно за годину-дві без доступу до стаціонарної інфраструктури. Цей приклад засвідчує, що навіть за частих переїздів і перебування у відкритих мережах можна забезпечити фундаментальний захист від більшості загроз — від сканування портів до несанкціонованого перехоплення [1].

5.5.2 Система для віддаленного навчання

Уявімо, що викладач чи студент у галузі комп’ютерних наук, кібербезпеки або системного адміністрування постає перед завданням

ознайомити новачків із базовими принципами мережевої безпеки. Виникає проблема відсутності великої лабораторії чи окремих серверів, де можна було б продемонструвати налаштування фаєрвола, шифрування з'єднання чи використання інструментів на кшталт nmap. У такому разі підхід «одна машина» стає практичним розв'язанням: кожен учасник (чи то викладач, чи студент) може, маючи лише ноутбук з ОС Linux (або через WSL2 у Windows), розгорнути потрібні сервіси й продемонструвати найважливіші аспекти безпеки.

Замість використання кількох фізичних пристроїв, достатньо інсталювати веб-сервер (Nginx чи Apache) і відкрити кілька портів (зокрема 80 для HTTP і 443 для HTTPS). Спочатку залишають увесь трафік дозволеним, аби nmap чітко виявляв типові відкриті порти (на кшталт SSH чи служб принтера). Згодом за допомогою файрвола (UFW або iptables) більшість портів закривають, залишаючи лише той, що справді потрібен для веб-сервера, і повторюють сканування nmap, аби пересвідчитись у змінах у мережевому профілі машини.

Для ілюстрації шифрування з'єднання студенти генерують самопідписаний сертифікат (OpenSSL) і налаштовують веб-сервер на застосування протоколу HTTPS. У браузері на "https://localhost" вони побачать попередження про «недовіреного» постачальника сертифікатів, однак зможуть оцінити різницю між відкритим HTTP (який легко читається у Wireshark чи tcpdump) і зашифрованим трафіком, що вже виглядає як набір зашифрованих пакетів. Отже, мінімальне налаштування дає змогу зрозуміти принципи TLS без розгортання повноцінного центру сертифікації.

Подібний «лабораторний» сценарій має кілька переваг. По-перше, студенти одразу бачать, які порти «світяться» в системі після встановлення певного ПЗ (приміром, принт-сервер чи база даних). По-друге, завдяки

HTTPS зменшується ризик перехоплення незашифрованого трафіку у локальній мережі, що було б імовірним у разі використання звичайного HTTP. По-третє, відпадає потреба створювати складну інфраструктуру або орендувати сервер у хмарі.

Результат для учасників очевидний: кожен здобуває реальний досвід налаштування і взаємодії з фаєрволом, HTTPS та інструментами на кшталт nmap у безпечному середовищі «однієї машини», не ризикуючи пошкодженням чи перенавантаженням загальної мережі. Такий метод не тільки розкриває ключові поняття (на кшталт «відкритий»/«закритий»/«фільтрований» порт) і дозволяє збагнути різницю між “http://” і “https://”, а й уможливлює безболісні експерименти: у разі помилки не страждає реальна інфраструктура навчального закладу.

Таким чином, навіть відсутність потужних серверів чи розгалуженої мережевої архітектури не перешкоджає демонструванню засад мережевої безпеки. Достатньо одного ноутбука та кількох базових інструментів, щоби ознайомитися з налаштуванням фаєрвола, шифруванням з’єднання і принципами сканування портів, що є необхідними знаннями для будь-якого майбутнього фахівця з кібербезпеки чи системного адміністрування.

5.6 Підсумок практичной частини

У ході практичной частини було продемонстровано, як за допомогою одного комп'ютера можна реалізувати базові заходи інформаційної безпеки в мережевому середовищі. Зокрема, було встановлено брандмауер для обмеження доступу до портів, просканово порти для виявлення відкритих сервісів та встановлено веб-сервер з шифруванням HTTPS на одному пристрої. Незважаючи на простоту експерименту, результати підтвердили, що навіть початкові заходи безпеки були ефективними: обмеження відкритих портів за допомогою брандмауера (UFW) швидко мінімізувало можливі

вектори атаки. Порівняння стану мережі «до» і «після» з увімкненим брандмауером показало, що кількість доступних сервісів зменшилася, що ускладнило несанкціонований доступ для зловмисників.

Самопідписані сертифікати (TLS/SSL) дозволили шифрувати веб-трафік навіть у локальних мережах, що унеможливлює перехоплення або читання відкритих текстових HTTP-запитів. Те, що браузер показує попередження про «ненадійний» центр сертифікації, не змінює факту шифрування і доводить ефективність таких рішень для захисту від простих загроз. Сканування портів (nmap) у поєднанні з системними журналами показало, як проста діагностика може надати важливу інформацію про потенційні ризики. Результати допомагають адміністраторам швидко реагувати на порти і сервіси, які відкриваються ненавмисно або випадково

ВИСНОВКИ

Проведений аналіз засвідчує, що застосування поодиноких підходів не забезпечує всеосяжного захисту від усієї різноманітності загроз. Максимальний рівень надійності досягається виключно за умови комплексного впровадження технічних і процедурних засобів. Зокрема, потрібно використовувати криптографічні інструменти для зашифрування транзитних даних, аби запобігти їх перехопленню; налаштовувати фаєрволи й системи виявлення/запобігання вторгненням (IDS/IPS), що слугують основою мережевої безпеки; застосовувати потужні механізми автентифікації (на кшталт дво- чи трифакторного підтвердження) та жорсткий контроль доступу; а також розгортати антивірусні рішення й постійні системи моніторингу, які сприятимуть швидкому виявленню та реагуванню на інциденти.

Враховуючи стрімку еволюцію атак, організаціям потрібно регулярно оновлювати захисні стратегії, приділяти увагу навчанню співробітників і впроваджувати сучасні технології (штучний інтелект, концепцію «нульової довіри» або елементи блокчейну). Лише такий комплексний і динамічний підхід дає змогу зберігати стійкість до сьогоднішніх та майбутніх загроз

Проведений аналіз підтверджує, що ізольовані заходи безпеки не здатні надійно протидіяти повному спектру сучасних кібератак. Вищий рівень захисту можливий лише за умови одночасного застосування кількох інструментів і процедур, зокрема криптографії (для запобігання перехопленню даних), фаєрволів і систем IDS/IPS (як першого рівня фільтрації та виявлення загроз), а також надійних технологій автентифікації і засобів контролю доступу. Важливим елементом лишається антивірус, доповнений системами моніторингу мережі, що можуть оперативно реєструвати й повідомляти про аномалії або несанкціоновані дії.

Варто також враховувати, що атакувальні техніки еволюціонують надзвичайно швидко, тому знання й підготовка персоналу мають оновлюватися у тому ж ритмі. Інвестиції в навчальні програми, упровадження концепції нульової довіри (Zero Trust), а також експерименти з інструментами штучного інтелекту та децентралізованими підходами (скажімо, на базі блокчейну) стають усе більш релевантними. Це не лише віддзеркалює динаміку загроз, а й робить кібербезпеку гнучкою, дозволяючи передбачати ймовірні вектори атак та реагувати на нетипові інциденти. [1]

Таким чином, ефективна безпека є радше процесом, аніж статичним комплексом інструментів: вона передбачає адаптацію, регулярні огляди застосованих політик і корекцію тактик захисту відповідно до актуальних викликів у середовищі швидко мінливих технологій і зловмисних практик.

.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard (AES). 2001. [Онлайн].
2. Daemen, J. і Rijmen, V. *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer, 2002.
3. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd ed., Wiley, 1996.
4. SANS Institute. *Intrusion Detection & Threat Hunting Whitepaper*. [Онлайн].
5. Cisco. *Cisco ASA Series Firewall CLI Configuration Guide*. [Онлайн].
6. IETF. *RFC 4949: Internet Security Glossary*. [Онлайн].
7. OpenVPN. *OpenVPN Community Documentation*. [Онлайн].
8. WireGuard. *WireGuard Protocol and Cryptography*. [Онлайн].
9. Anti-Phishing Working Group (APWG). *Phishing Activity Trends Reports*. [Онлайн].
10. Check Point. *Stateful Inspection Technology Whitepaper*. [Онлайн].
11. Ferguson, P., & Senie, D. *Network Ingress Filtering (RFC 2827)*. [Онлайн].
12. NIST. *SP 800-77: Guide to IPsec VPNs*. [Онлайн].
13. Ferguson, N., & Schneier, B. *Practical Cryptography*. Wiley, 2003.
14. Proofpoint. *State of the Phish*. [Онлайн].
15. Cheswick, W., Bellovin, S., & Rubin, A. *Firewalls and Internet Security: Repelling the Wily Hacker*. 2nd ed., Addison-Wesley, 2003.