

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий Інститут телекомунікаційних систем

Кафедра Електронних комунікацій та Інтернету речей

До захисту допущено:

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«___» _____ 2026 р.

Дипломна робота

на здобуття ступеня бакалавра

спеціальності 172 «Телекомунікації та радіотехніка»

**на тему: «Загрози і вразливості в мережах електронних
комунікацій та засоби їх усунення»**

Виконав:

Студент IV курсу, групи ТС-22

Картун Богдан Васильович

Керівник:

Доцент кафедри ЕКІР, к.т.н,

Григоренко Олена Григорівна

Рецензент:

Доцент, каф.Інформаційної безпеки НН ФТІ, доц., к.т.н

Федір РЕПА

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без
відповідних посилань.

Студент _____

Київ – 2026

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Електронних комунікацій та Інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«___» _____ 2026 р.

ЗАВДАННЯ

на дипломну роботу студенту

Картуну Богдану Васильовичу

1. Тема роботи «Загрози і вразливості в мережах електронних комунікацій та засоби їх усунення», керівник роботи Григоренко Олена Григорівна, доцент, затверджені наказом по університету від «26» травня 2026 р. № 1912 - С
2. Термін подання студентом роботи 9 червня 2026 року.
3. Вихідні дані до роботи: матеріали наукових видань з питань мережевої безпеки, нормативно-правова база України у сфері електронних комунікацій, статистичні дані та звіти про мережеві вразливості, навчально-методичні матеріали.
4. Зміст роботи: Обґрунтувати актуальність теми. Дослідити теоретичні основи безпеки мереж електронних комунікацій, їх структуру, основні принципи інформаційної безпеки та чинне нормативно-правове забезпечення. Виконати комплексний аналіз зовнішніх і внутрішніх загроз, специфіки поширених кібератак, а також технічних вразливостей обладнання та впливу людського фактора. Здійснити оцінювання ризиків та можливих наслідків реалізації цих загроз у телекомунікаційних системах. Провести аналіз існуючих методів та засобів захисту мереж, зокрема організаційних заходів і сучасних технічних рішень. Дослідити алгоритми виявлення та усунення вразливостей і на основі проведеного аналізу сформулювати обґрунтовані рекомендації щодо підвищення рівня загальної захищеності мереж електронних комунікацій.
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

- 1) Тема, мета, завдання, об'єкт та предмет дослідження.
- 2) Узагальнена багаторівнева структура мережі електронних комунікацій.
- 3) Основні складові елементи електронної комунікаційної мережі та їх функціональне призначення.
- 4) Нормативно-правове забезпечення України та міжнародні стандарти у сфері захисту електронних комунікацій.
- 5) Класифікація та порівняльна характеристика зовнішніх і внутрішніх загроз у мережах електронних комунікацій.
- 6) Статистичний аналіз та актуальні тенденції розвитку мережесих кіберінцидентів.
- 7) Технічні вразливості мережевого обладнання та програмного забезпечення.
- 8) Людський фактор як джерело вразливостей у телекомунікаційній інфраструктурі.
- 9) Методологія оцінювання ризиків та класифікація наслідків реалізації мережесих загроз.
- 10) Організаційна модель управління безпекою мереж електронних комунікацій.
- 11) Розподіл ключових функцій кібербезпеки відповідно до сучасної моделі NIST Cybersecurity Framework 2.0.
- 12) Комплекс технічних засобів захисту мережевої інфраструктури.
- 13) Методи та інструменти виявлення й усунення вразливостей.
- 14) Побудова та принципи функціонування системи управління інформаційною безпекою на основі безперервного циклу керування ризиками.
- 15) Комплексні рекомендації щодо підвищення рівня захищеності та нейтралізації вразливостей у реальних мережах.
- 16) Висновки за результатами дипломної роботи.

6. Дата видачі завдання: 03.02.2026 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз літератури за темою “Загрози і вразливості в мережах електронних комунікацій та засоби їх усунення”	05.03.2026	Виконано
2	Вступ	15.03.2026	Виконано
3	Дослідження теоретичних основ, структури та принципів безпеки мереж електронних комунікацій	10.04.2026	Виконано
4	Аналіз основних загроз і вразливостей у мережах електронних комунікацій	05.05.2026	Виконано

5	Розгляд методів та засобів захисту мереж електронних комунікацій	25.05.2026	Виконано
6	Висновки	04.06.2026	Виконано
7	Чистовий варіант дипломної роботи, плакати	08.06.2026	Виконано

Студент

Богдан КАРТУН

Керівник роботи

Олена ГРИГОРЕНКО

РЕФЕРАТ

Дипломну роботу виконано на 89 аркушах, вона містить перелік посилань на використані джерела з 36 найменувань. У роботі наведено 6 рисунків та 10 таблиць.

Дана дипломна робота присвячена розгляду актуальних загроз і технічних вразливостей у мережах електронних комунікацій, а також дослідженню та обґрунтуванню методів і засобів їх усунення для забезпечення інформаційної безпеки телекомунікаційної інфраструктури.

Об'єктом досліджень є забезпечення кібербезпеки в мережах електронних комунікацій відповідно до вимог національного законодавства України та міжнародних стандартів кіберзахисту.

Предметом досліджень є механізми виникнення мережових загроз, вектори реалізації кібератак, технічні й організаційні вразливості мережевого обладнання, а також характеристики ефективності організаційно-технічних засобів захисту.

Метою дипломної роботи є дослідження та класифікація загроз і вразливостей у мережах електронних комунікацій, проведення оцінки ризиків їх реалізації, а також обґрунтування оптимальних організаційно-технічних засобів для їх усунення.

КЛЮЧОВІ СЛОВА: мережі електронних комунікацій, інформаційна безпека, кіберзагрози, вразливості, кібератаки, оцінювання ризиків, засоби захисту

ABSTRACT

The diploma thesis consists of 89 pages and contains a list of references comprising 36 sources. The paper includes 6 figures and 10 tables.

This diploma thesis is devoted to the examination of current threats and technical vulnerabilities in electronic communication networks, as well as the research and justification of methods and tools for their elimination to ensure the information security of the telecommunication infrastructure.

The object of the research is the provision of cybersecurity in electronic communication networks in accordance with the requirements of the national legislation of Ukraine and international cybersecurity standards.

The subject of the research encompasses the mechanisms of network threat emergence, vectors of cyberattack execution, technical and organizational vulnerabilities of network equipment, as well as the effectiveness characteristics of organizational and technical security measures.

The aim of the diploma thesis is to research and classify threats and vulnerabilities in electronic communication networks, conduct a risk assessment of their implementation, and justify optimal organizational and technical security measures for their elimination.

KEYWORDS: electronic communication networks, information security, cyber threats, vulnerabilities, cyberattacks, risk assessment, security measures

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	9
ВСТУП.....	14
1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ	16
1.1 Поняття та структура мереж електронних комунікацій	16
1.2 Основні принципи інформаційної безпеки в телекомунікаційних системах ...	23
1.3 Класифікація загроз у мережах електронних комунікацій.....	28
1.4 Поняття вразливостей та їх роль у порушенні кібербезпеки мереж.....	32
1.5 Нормативно-правове забезпечення захисту електронних комунікацій в Україні та міжнародні стандарти.....	35
1.6 Висновки до розділу 1	37
2 АНАЛІЗ ОСНОВНИХ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ У МЕРЕЖАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ.....	39
2.1 Аналіз зовнішніх і внутрішніх загроз	39
2.2 Кібератаки на мережі електронних комунікацій DoS, DDoS, MITM, фішинг, spoofing.....	43
2.3 Технічні вразливості мережевого обладнання та програмного забезпечення..	50
2.4 Людський фактор як джерело вразливостей	55
2.5 Оцінка ризиків та наслідків реалізації загроз.....	58
2.6 Висновки до розділу 2	62
3 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ	64
3.1 Організаційні заходи забезпечення безпеки.....	64
3.2 Технічні засоби захисту: Firewall, IDS/IPS, VPN, SIEM	66
3.3 Методи виявлення та усунення вразливостей.....	71
3.4 Побудова системи управління інформаційною безпекою	74
3.5 Рекомендації щодо підвищення рівня захищеності мереж.....	79

3.6 Висновки до розділу 3	84
ВИСНОВКИ.....	85
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	87

ПЕРЕЛІК СКОРОЧЕНЬ

Скорочення	Розшифрування (англ.)	Пояснення (укр.)
ПЗ	—	Програмне забезпечення
ПК	—	Персональний комп'ютер
СУІБ	—	Система управління інформаційною безпекою
3G, 4G, 5G	3rd / 4th / 5th Generation	Третє, четверте та п'яте покоління мобільного зв'язку
API	Application Programming Interface	Інтерфейс програмування застосунків
ARP spoofing	Address Resolution Protocol spoofing	Підміна ARP-адрес
BGP	Border Gateway Protocol	Протокол граничного шлюзу
brute force-атаки	—	Атаки методом повного перебору (підбір паролів)
caller ID spoofing	ID —	Підробка ідентифікатора абонента
CISA	Cybersecurity and Infrastructure Security Agency	Агентство з кібербезпеки та безпеки інфраструктури США
DDoS	Distributed Denial of Service	Розподілена відмова в обслуговуванні
DHCP	Dynamic Host Configuration Protocol	Протокол динамічного налаштування вузла
DKIM	DomainKeys Identified Mail	Метод ідентифікації електронної пошти за доменними ключами
DMARC	Domain-based Message	Політика автентифікації

	Authentication, Reporting, and Conformance	електронної пошти
DMZ	Demilitarized Zone	Демілітаризована зона
DNS	Domain Name System	Система доменних імен
DNS-spoofing	—	Підміна записів системи доменних імен (DNS)
DNSSEC	Domain Name System Security Extensions	Розширення безпеки системи доменних імен
DoS	Denial of Service	Відмова в обслуговуванні
DWDM	Dense Wavelength Division Multiplexing	Щільне спектральне мультиплексування
email-spoofing	—	Підробка адреси відправника електронної пошти
ENISA Threat Landscape	—	Звіт Агентства Європейського Союзу з кібербезпеки щодо ландшафту загроз
Firewall	—	Міжмережевий екран
FTTx	Fiber To The X	Оптичне волокно до точки X
ICMP flooding	Internet Control Message Protocol flooding	Атака шляхом переповнення ICMP-пакетами
IDS/IPS	Intrusion Detection/Prevention System	Система виявлення та запобігання вторгненням
IP	Internet Protocol	Інтернет-протокол
IP-spoofing	—	Підробка IP-адреси
IP/MPLS	Internet Protocol / Multiprotocol Label Switching	Багатопротокольна комутація за мітками на базі IP
IPTV	Internet Protocol Television	Цифрове телебачення в мережах IP

ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія
LAN	Local Area Network	Локальна мережа
LoRaWAN	Long Range Wide Area Network	Протокол безпроводової мережі великого радіуса дії
LPWAN	Low-Power Wide-Area Network	Енергоефективна мережа дальнього радіуса дії
MAC-адреси	Media Access Control address	Унікальний ідентифікатор мережевого інтерфейсу / фізична адреса
MFA	Multi-Factor Authentication	Багатофакторна автентифікація
MITM	Man-in-the-Middle	Атака типу «людина посередині»
MPLS	Multiprotocol Label Switching	Багатопротокольна комутація за мітками
NB-IoT	NarrowBand Internet of Things	Вузькосмуговий Інтернет речей
NetFlow	—	Мережевий протокол для збору інформації про IP-трафік
NIST Cybersecurity Framework 2.0	—	Структура кібербезпеки від Національного інституту стандартів і технологій США
NMS	Network Management System	Система управління мережею
NVD	National Vulnerability Database	Національна база даних вразливостей
OSI	Open Systems Interconnection	Базова еталонна модель взаємодії відкритих систем

OSPF	Open Shortest Path First	Протокол динамічної маршрутизації
OSS/BSS	Operations Support System / Business Support System	Системи операційної та бізнес-підтримки
Palo Alto Networks	Alto —	Міжнародна компанія-розробник рішень з кібербезпеки
ransomware	—	Програма-вимагач (шкідливе програмне забезпечення)
SIEM	Security Information and Event Management	Система керування інформацією та подіями безпеки
SMS	Short Message Service	Служба коротких повідомлень
SNMP	Simple Network Management Protocol	Простий протокол управління мережею
SPF	Sender Policy Framework	Інфраструктура політики відправника для захисту від підробки пошти
SSH	Secure Shell	Мережевий протокол прикладного рівня для захищеного віддаленого доступу
SYN flood	—	Атака типу «SYN-повінь» (різновид DoS-атаки)
syslog-сервери	—	Сервери для збору та зберігання системних журналів повідомлень
TCP	Transmission Control Protocol	Протокол управління

		передаванням
TCP/IP	Transmission Control Protocol / Internet Protocol	Основний набір мережевих протоколів передавання даних
USB	Universal Serial Bus	Універсальна послідовна шина
VLAN hopping	—	Атака типу «перестрибування» між віртуальними локальними мережами
VoIP	Voice over IP	Технологія передавання голосу через інтернет-протокол
VPN	Virtual Private Network	Віртуальна приватна мережа
Wi-Fi	Wireless Fidelity	Технологія безпроводової локальної мережі
xDSL	Digital Subscriber Line	Сімейство технологій цифрової абонентської лінії

ВСТУП

Глобальна цифровізація суспільства та масовий перехід до хмарних сервісів, розподілених інфраструктур і технологій розумного дому перетворили мережі електронних комунікацій на головний фундамент сучасної економіки. Зі зростанням масштабів та складності цих мереж неминуче розширюється і поверхня для потенційних кібератак, що робить питання гарантування конфіденційності, цілісності та доступності даних критично важливим завданням. Актуальність теми зумовлена постійним зростанням кількості кіберінцидентів, необхідністю систематизації класифікації мережевих загроз та гострою потребою в розробці комплексних підходів до виявлення і нейтралізації технічних вразливостей телекомунікаційного обладнання.

Сучасне середовище загроз характеризується надзвичайною динамічністю. Зловмисники постійно вдосконалюють свої методи, активно застосовуючи такі вектори, як DoS та DDoS-атаки для порушення доступності сервісів, атаки типу Man-in-the-Middle (MITM) для перехоплення трафіку, а також витончені фішингові кампанії, спрямовані на експлуатацію людського фактора. В умовах, коли традиційні методи захисту периметра виявляються недостатніми, критичною стає потреба у переході до сучасних концепцій безпеки, зокрема впровадження архітектури нульової довіри (Zero Trust) та механізмів багатофакторної автентифікації (MFA).

Метою дипломної роботи є дослідження та класифікація загроз і вразливостей у мережах електронних комунікацій, проведення оцінки ризиків їх реалізації, а також обґрунтування оптимальних організаційно-технічних засобів для їх усунення.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

- Дослідити теоретичні основи безпеки мереж електронних комунікацій, їх структуру, базові принципи інформаційної безпеки та чинне нормативно-правове забезпечення.

- Виконати комплексну класифікацію загроз та вразливостей, притаманних телекомунікаційним системам.
- Проаналізувати основні зовнішні і внутрішні загрози, специфіку та вектори реалізації кібератак (DoS, DDoS, MITM, фішинг, spoofing), а також вплив людського фактора і технічних вразливостей обладнання.
- Провести оцінку ризиків та можливих наслідків від реалізації інцидентів інформаційної безпеки.
- Розглянути існуючі організаційні заходи та сучасні технічні засоби захисту (Firewall, IDS/IPS, VPN, SIEM).
- Дослідити методи виявлення і усунення вразливостей та сформулювати рекомендації щодо побудови системи управління інформаційною безпекою і підвищення загального рівня захищеності мереж.

Об'єктом дослідження є забезпечення кібербезпеки в мережах електронних комунікацій відповідно до вимог національного законодавства України та міжнародних стандартів кіберзахисту.

Предметом дослідження є механізми виникнення мережових загроз, вектори реалізації кібератак, технічні й організаційні вразливості мережевого обладнання, а також характеристики ефективності організаційно-технічних засобів захисту.

Методи дослідження: теоретичний аналіз нормативно-правової бази та міжнародних стандартів, системний аналіз для класифікації мережових загроз, а також методи ризик-орієнтованого моделювання для оцінки вразливостей телекомунікаційної інфраструктури.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

1.1 Поняття та структура мереж електронних комунікацій

Електронні комунікації є однією з ключових основ функціонування сучасного інформаційного суспільства. Саме через електронні комунікаційні мережі здійснюється передавання голосу, текстових повідомлень, мультимедійного контенту, службових даних, сигналів керування, інформації від сенсорів, пристроїв Інтернету речей, банківських систем, державних електронних сервісів та корпоративних інформаційних ресурсів.

Відповідно до Закону України «Про електронні комунікації», електронна комунікаційна мережа визначається як комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг. У цьому ж законі електронна комунікація розглядається як «передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.»[4]

Електронні комунікаційні мережі виконують важливу роль у забезпеченні доступу до інформаційних ресурсів, підтримці економічної діяльності, функціонуванні систем управління, освіти, медицини, транспорту, енергетики, фінансових установ та державного сектору. У повсякденному житті користувач взаємодіє з такими мережами під час здійснення телефонних дзвінків, використання мобільного Інтернету, роботи з електронною поштою, відеоконференціями, хмарними сервісами, месенджерами, системами онлайн-банкінгу, порталами державних послуг та іншими цифровими платформами. Для підприємств і організацій електронні комунікаційні мережі є основою обміну службовою інформацією, віддаленого адміністрування, роботи корпоративних систем, захисту інформаційних ресурсів та взаємодії з клієнтами.

З технічної точки зору електронна комунікаційна мережа складається з кінцевого обладнання, мереж доступу, транспортної або магістральної мережі,

вузлів комутації та маршрутизації, серверної інфраструктури, систем управління, засобів моніторингу, а також засобів захисту інформації (рис. 1.1). Кінцеве або термінальне обладнання — це обладнання, яке підключається до кінцевого пункту мережі для отримання електронних комунікаційних послуг.

Мережа доступу забезпечує підключення кінцевого користувача або пристрою до інфраструктури оператора чи організації. Вона є першим рівнем взаємодії абонента з електронною комунікаційною мережею. Мережі доступу можуть використовувати різне фізичне середовище передавання: волоконно-оптичні кабелі, мідні лінії (вита пара), коаксіальні кабелі або радіоефір. Базуючись на цих середовищах, застосовуються відповідні технології зв'язку. До проводових технологій доступу належать сімейство стандартів Ethernet (IEEE 802.3), технології широкосмугового оптичного доступу FTTx (наприклад, xPON), технології цифрової абонентської лінії (xDSL) та стандарти передавання даних по коаксіальному кабелю (DOCSIS). До безпроводових технологій належать технології стільникового зв'язку (UMTS для 3G, LTE для 4G, NR для 5G), стандарти безпроводових локальних мереж Wi-Fi (IEEE 802.11), технології супутникового радіодоступу, технології мікрохвильового (радіорелейного) зв'язку, а також енергоефективні технології дальнього радіуса дії (LPWAN), зокрема LoRaWAN та NB-IoT. Вибір конкретної технології доступу залежить від призначення мережі, необхідної швидкості передавання даних, дальності зв'язку, вартості розгортання, рівня мобільності користувачів та вимог до надійності.

Важливими елементами мережі є вузли комутації та маршрутизації. Вони забезпечують вибір шляху передавання інформації, обробку пакетів, розподіл трафіку, взаємодію між різними сегментами мережі та підтримку заданого рівня якості обслуговування. До таких пристроїв належать маршрутизатори, комутатори, шлюзи, контролери безпроводових мереж, базові станції мобільного зв'язку, вузли агрегації, обладнання ядра мережі. У пакетних мережах, зокрема в мережі Інтернет, основою передавання даних є використання протоколів TCP/IP.



Рисунок 1.1 — Узагальнена структура мережі електронних комунікацій

Наведена схема (рис.1.1) демонструє, що електронна комунікаційна мережа є багаторівневою системою. Кожен рівень виконує окрему функцію, але всі вони працюють як єдиний механізм. Якщо на рівні доступу виникає пошкодження кабельної лінії або збій базової станції, користувач може втратити підключення до послуги. Якщо проблема виникає на транспортному рівні, наслідки можуть бути значно масштабнішими, оскільки порушується передавання трафіку між багатьма вузлами.

Окрему роль у структурі електронних комунікаційних мереж відіграє рівень сервісів. Він забезпечує надання конкретних послуг користувачам: доступ до Інтернету, голосовий зв'язок, передавання повідомлень, відеозв'язок, хмарні обчислення, IPTV, корпоративні VPN, послуги дата-центрів, послуги зберігання та обробки даних. Електронна комунікаційна послуга полягає у прийманні та/або передаванні інформації через електронні комунікаційні мережі. Тому мережа не є лише фізичним середовищем передавання сигналів, вона також включає

програмні платформи, протоколи, сервери, системи автентифікації, білінгу, керування доступом та обліку користувачів.

У сучасних умовах електронні комунікаційні мережі дедалі частіше будуються за принципом конвергенції. Якщо раніше телефонний зв'язок, телебачення і передавання даних часто функціонували як окремі мережі, то сьогодні вони можуть працювати на спільній основі з використанням пакетної комутації.

За призначенням електронні комунікаційні мережі можна поділити на мережі загального користування, корпоративні, відомчі, спеціальні, технологічні та приватні. Мережі загального користування призначені для надання послуг широкому колу користувачів. До них належать мережі операторів мобільного та фіксованого зв'язку, провайдерів доступу до Інтернету, операторів кабельного телебачення та інших постачальників електронних комунікаційних послуг. Корпоративні мережі використовуються підприємствами, установами та організаціями для внутрішнього обміну інформацією, доступу до службових ресурсів, роботи інформаційних систем і забезпечення взаємодії між філіями. Відомчі та спеціальні мережі застосовуються для потреб державних органів, критичної інфраструктури, оборони, безпеки, транспорту, енергетики та інших галузей, де особливо важливими є надійність, захищеність і контроль доступу.

Основні складові електронної комунікаційної мережі та їх призначення надані в табл.1.1.

Таблиця 1.1 — Основні складові електронної комунікаційної мережі та їх призначення

Складова мережі	Основне призначення	Приклади елементів
Кінцеве обладнання	Забезпечує доступ користувача або пристрою до мережі	Смартфон, ПК, модем, роутер, IP-телефон, IoT-датчик
Мережа доступу	Підключає користувача до мережі оператора або організації	Обладнання FTTx, Ethernet, Wi-Fi, 4G/5G, xDSL

Продовження таблиці 1.1

Рівень агрегації	Об'єднує трафік від багатьох користувачів або сегментів	Комутатори, маршрутизатори, вузли агрегації
Транспортна мережа	Передає великі обсяги даних між вузлами та регіонами	Оптичні лінії, обладнання DWDM, MPLS, IP/MPLS
Ядро мережі	Забезпечує високошвидкісну маршрутизацію та взаємодію основних сегментів	Магістральні маршрутизатори, шлюзи, дата-центри
Сервісна інфраструктура	Надає користувачам конкретні послуги	DNS, DHCP, VoIP, IPTV, хмарні платформи, білінг
Система управління	Забезпечує моніторинг, налаштування та контроль роботи мережі	NMS, OSS/BSS, системи журналювання
Засоби безпеки	Захищають мережу від несанкціонованого доступу та атак	Firewall, IDS/IPS, VPN, SIEM, системи автентифікації

Залежно від масштабу електронні комунікаційні мережі можуть бути локальними, міськими, регіональними, національними та глобальними. Локальні мережі, або LAN, функціонують у межах одного приміщення, будівлі чи організації. Вони забезпечують підключення робочих станцій, серверів, принтерів, IP-телефонів, камер відеоспостереження та іншого обладнання. Міські та регіональні мережі охоплюють більші території та можуть об'єднувати декілька локальних мереж, офісів або вузлів зв'язку.

За способом передавання даних електронні комунікаційні мережі можуть бути проводовими, безпроводовими та комбінованими. Проводові мережі характеризуються високою стабільністю, значною пропускнуою здатністю та відносно високим рівнем захищеності фізичного каналу, особливо якщо використовуються волоконно-оптичні лінії зв'язку. Безпроводові мережі забезпечують мобільність, гнучкість розгортання та зручність підключення, але вони більше залежать від радіочастотного середовища, перешкод, рівня сигналу та ризиків несанкціонованого доступу до радіоканалу.

Важливою характеристикою електронної комунікаційної мережі є топологія, тобто спосіб з'єднання її вузлів. Найпоширенішими є топології «зірка», «шина», «кільце», «дерево», «mesh» (рис.1.2) та гібридні структури [35]. Такий підхід простий в адмініструванні, але центральний вузол є критичною точкою відмови. У кільцевій топології вузли з'єднані послідовно, що може забезпечувати резервування, але потребує спеціальних механізмів відновлення зв'язку при пошкодженні кільця. Mesh-топологія передбачає наявність кількох альтернативних шляхів між вузлами, що підвищує стійкість мережі до відмов.

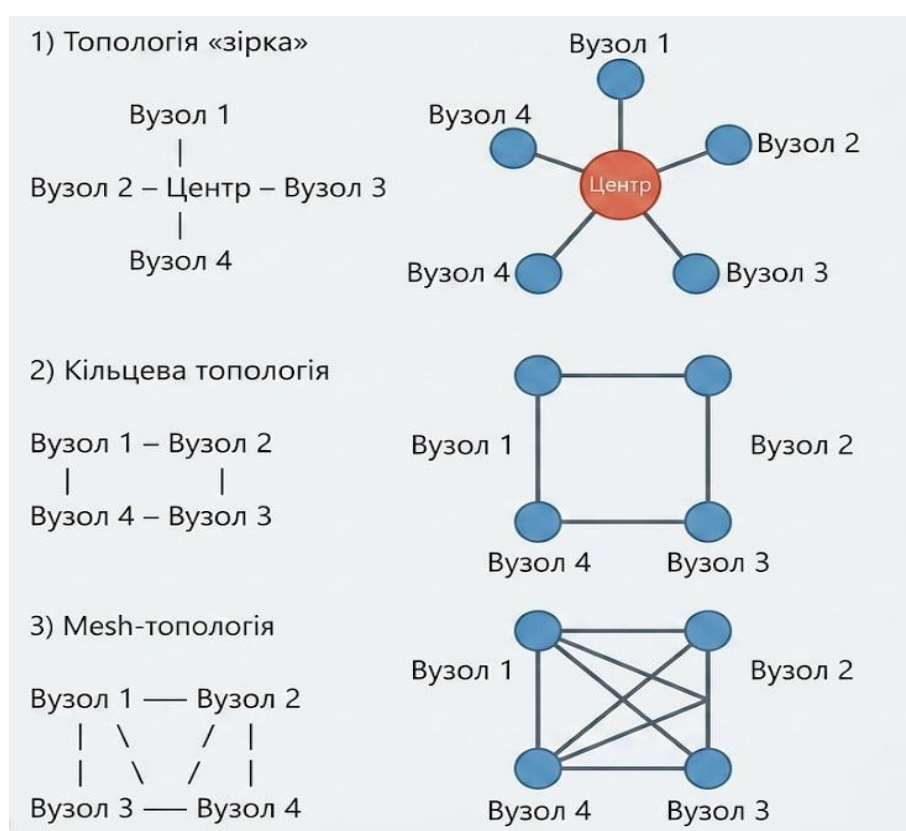


Рисунок 1.2 — Основні типи топологій електронних комунікаційних мереж

Одним із поширених підходів до побудови захищеної мережевої структури є сегментація. Її суть полягає у поділі мережі на окремі логічні або фізичні зони.

У такій структурі кожен сегмент має власне функціональне призначення та власний рівень доступу. Це дозволяє обмежити поширення атаки в разі компрометації одного з елементів мережі. Наприклад, якщо злоумисник отримає

доступ до гостьової Wi-Fi-мережі, він не повинен мати прямого доступу до серверів баз даних або систем адміністрування.

Управління електронною комунікаційною мережею здійснюється за допомогою спеціалізованих систем моніторингу, адміністрування та обліку. Такі системи дають змогу контролювати стан обладнання, завантаження каналів, доступність сервісів, якість обслуговування, події безпеки, аварії та спроби несанкціонованого доступу. До них належать системи управління мережею (NMS), системи операційної та бізнес-підтримки (OSS/BSS), системи керування інформацією та подіями безпеки (SIEM), сервери збору системних журналів (syslog-сервери), платформи керування конфігураціями, системи інвентаризації обладнання та засоби аналізу мережевого трафіку.

Особливу увагу в електронних комунікаційних мережах потрібно приділяти відмовостійкості. Відмовостійкість означає здатність мережі продовжувати роботу навіть у разі пошкодження окремих елементів. Для цього використовуються резервні канали, дублювання обладнання, альтернативні маршрути, резервні джерела живлення, географічно розподілені дата-центри, автоматичне перемикання трафіку та системи аварійного відновлення. Для критичної інфраструктури, державних сервісів, банківських систем, медичних установ і операторів зв'язку відмовостійкість є не менш важливою, ніж пропускна здатність або швидкість передавання даних.

Сучасні електронні комунікаційні мережі розвиваються під впливом цифровізації, зростання обсягів трафіку, поширення хмарних сервісів, мобільних технологій, Інтернету речей та систем штучного інтелекту. Кількість підключених пристроїв постійно збільшується, а разом з нею зростає складність мережевої інфраструктури.

1.2 Основні принципи інформаційної безпеки в телекомунікаційних системах

Інформаційна безпека в телекомунікаційних системах — це стан захищеності інформації, технічних засобів, програмного забезпечення, каналів зв'язку та процесів управління мережею від випадкових або навмисних впливів, які можуть призвести до порушення конфіденційності, цілісності, доступності або контрольованості інформаційних процесів. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» [5] визначено, що закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Це підкреслює, що телекомунікаційні мережі розглядаються не лише як технічна інфраструктура передавання сигналів, а і як об'єкти, що потребують комплексного правового, організаційного та технічного захисту.

Цілісність означає збереження правильності, повноти та незмінності інформації під час її передавання, зберігання або обробки. У телекомунікаційних мережах порушення цілісності може виникати внаслідок технічних збоїв, помилок програмного забезпечення, неправильної маршрутизації, атак типу Man-in-the-Middle, підміни DNS-записів, модифікації пакетів, пошкодження конфігураційного файлу мережевого обладнання або втручання зловмисника в роботу сервісу. Наслідком порушення цілісності може бути неправильне передавання даних, спотворення службової інформації, перенаправлення користувачів на фальшиві ресурси, відмова сервісів або некоректне функціонування мережі.

Для забезпечення цілісності застосовуються контрольні суми, хеш-функції, цифрові підписи, журнали подій, системи контролю змін конфігурацій, резервне копіювання, механізми перевірки автентичності повідомлень, захищені протоколи маршрутизації та системи моніторингу. Наприклад, цифровий підпис дає змогу підтвердити, що повідомлення або файл не були змінені після підписання. У мережевому адмініструванні контроль змін конфігурацій обладнання дозволяє

виявити несанкціоноване або помилкове внесення змін до маршрутизаторів, комутаторів чи міжмережових екранів.

Доступність означає можливість своєчасного доступу авторизованих користувачів до інформації, послуг і мережових ресурсів. Для телекомунікаційних систем цей принцип має особливо важливе значення, оскільки основне призначення мережі полягає саме в забезпеченні безперервного обміну інформацією. Порушення доступності може бути спричинене апаратною несправністю, перевантаженням каналів, аварією на лінії зв'язку, відмовою серверів, помилками конфігурації, відключенням живлення, DDoS-атакою або навмисним пошкодженням інфраструктури. У звіті ENISA Threat Landscape 2024 [12] загрози доступності були визначені серед основних кіберзагроз, а також окремо виділялися ransomware і загрози для даних.

Для забезпечення доступності використовуються резервування каналів, дублювання обладнання, балансування навантаження, системи аварійного відновлення, джерела безперебійного живлення, резервні дата-центри, системи захисту від DDoS-атак, моніторинг доступності сервісів і планування безперервності діяльності. Наприклад, якщо магістральний канал зв'язку виходить з ладу, трафік може бути автоматично перенаправлений через резервний маршрут. Якщо один сервер стає недоступним, навантаження може бути передане на інший сервер у кластері.

Окрім трьох базових принципів, у телекомунікаційних системах важливими є також автентичність, невідмовність, підзвітність, керованість, стійкість і відповідність нормативним вимогам. Автентичність означає можливість підтвердити справжність користувача, пристрою, сервера або повідомлення.

Невідмовність означає неможливість заперечення факту виконання певної дії. Наприклад, якщо користувач надіслав електронний документ або адміністратор змінив конфігурацію маршрутизатора, система повинна мати докази цієї дії: журнал подій, цифровий підпис, час виконання операції, ідентифікатор користувача. Підзвітність пов'язана з можливістю встановити, хто, коли і яку дію виконав у системі.

Основні принципи інформаційної безпеки та засоби їх реалізації наведено в табл. 1.2.

Таблиця 1.2 — Основні принципи інформаційної безпеки та засоби їх реалізації

Принцип	Зміст принципу	Приклади реалізації в телекомунікаційних системах
Конфіденційність	Захист інформації від несанкціонованого доступу	Шифрування, VPN, контроль доступу, сегментація мережі
Цілісність	Захист інформації від спотворення або несанкціонованої зміни	Хешування, цифровий підпис, контроль конфігурацій
Доступність	Забезпечення безперервного доступу до мережі та сервісів	Резервування, балансування навантаження, захист від DDoS

Комплексний підхід до інформаційної безпеки передбачає, що захист не може обмежуватися лише встановленням окремого технічного засобу, наприклад антивіруса або міжмережевого екрана. Безпека телекомунікаційної системи повинна будуватися як сукупність організаційних, технічних, програмних, криптографічних, фізичних і правових заходів. Такий підхід відповідає логіці міжнародних стандартів управління інформаційною безпекою. Зокрема, ISO/IEC 27001 [18] визначає вимоги до системи управління інформаційною безпекою, яка має створюватися, впроваджуватися, підтримуватися та постійно вдосконалюватися в організації.

У телекомунікаційній сфері система управління інформаційною безпекою повинна включати визначення активів, оцінювання ризиків, впровадження політик доступу, управління інцидентами, контроль постачальників, навчання персоналу, аудит, моніторинг і регулярний перегляд заходів захисту. Особливо

важливим є ризик-орієнтований підхід. Він передбачає, що організація спочатку визначає, які ресурси є найбільш важливими, які загрози можуть на них впливати, які вразливості існують, які наслідки може мати інцидент, і лише після цього обирає відповідні засоби захисту.

Ще одним важливим підходом є модель багаторівневого захисту, або *defense in depth* [19]. Її суть полягає в тому, що безпека забезпечується не одним бар'єром, а кількома взаємодоповнюючими рівнями захисту. Якщо зловмисник обходить один механізм, його дії повинні бути обмежені або виявлені на іншому рівні. Наприклад, навіть якщо користувач випадково відкрив шкідливий файл, антивірус, система контролю доступу, сегментація мережі, IDS/IPS і резервне копіювання можуть зменшити наслідки інциденту.

У телекомунікаційних системах багаторівневий захист (рис.1.3) охоплює фізичний рівень, каналний рівень, мережевий рівень, транспортний рівень, прикладний рівень, рівень користувачів і рівень управління.



Рисунок 1.3 — Багаторівнева модель захисту телекомунікаційної системи

На фізичному рівні захищаються приміщення, кабельні лінії, телекомунікаційні шафи, серверні, джерела живлення та обладнання. На каналному рівні застосовуються механізми контролю доступу до мережі, VLAN,

захист від атак на комутатори, безпечні налаштування Wi-Fi. На мережевому рівні використовуються міжмережеві екрани, маршрутизаційні політики, списки контролю доступу, VPN, захист від сканування та несанкціонованого підключення. На прикладному рівні забезпечується захист вебсервісів, поштових серверів, DNS, API, систем автентифікації та управління обліковими записами.

Сучасні підходи до кібербезпеки також враховують життєвий цикл управління безпекою. У NIST Cybersecurity Framework 2.0 [28] основні функції кібербезпеки згруповані у шість напрямів: Govern, Identify, Protect, Detect, Respond, Recover. Ці функції описують управління кіберризиками, визначення активів і загроз, впровадження захисту, виявлення інцидентів, реагування на них та відновлення після порушень. Для телекомунікаційної системи це означає, що безпека повинна бути безперервним процесом, а не одноразовим налаштуванням обладнання.

Принцип управління доступом є одним із найважливіших у телекомунікаційних системах. Він передбачає, що кожен користувач, адміністратор, пристрій або сервіс повинен мати лише ті права, які необхідні для виконання його функцій. Такий підхід називається принципом мінімальних привілеїв.

Важливим є також принцип розмежування повноважень. Він передбачає, що критичні дії не повинні залежати лише від однієї особи або одного облікового запису. Наприклад, зміна правил міжмережевого екрана, оновлення прошивки магістрального маршрутизатора або надання доступу до серверного сегмента повинні виконуватися за погодженою процедурою, із журналюванням і контролем. Це знижує ризик помилки, зловживання або несанкціонованої зміни.

Принцип безперервного моніторингу передбачає постійне спостереження за станом мережі, трафіком, подіями безпеки, доступністю сервісів і поведінкою користувачів. Для цього використовуються системи моніторингу мережі, SIEM-платформи, системи виявлення/запобігання вторгненням IDS/IPS, системи аналізу журналів, засоби виявлення аномалій, NetFlow-аналіз, SNMP-моніторинг та інші

інструменти. Без моніторингу організація може не помітити атаку або виявити її занадто пізно, коли зловмисник уже отримав доступ до критичних ресурсів.

Принцип резервування та відновлення є важливим для забезпечення стійкості телекомунікаційної системи. Навіть за наявності якісних засобів захисту повністю виключити ризик аварії або атаки неможливо. Тому необхідно заздалегідь планувати, як система буде відновлюватися після інциденту. Це включає резервне копіювання конфігурацій, дублювання критичного обладнання, резервні маршрути, аварійні канали зв'язку, плани реагування на інциденти, періодичне тестування відновлення та документування процедур.

1.3 Класифікація загроз у мережах електронних комунікацій.

Загроза в мережі електронних комунікацій — це потенційна можливість порушення нормального функціонування мережі, несанкціонованого доступу до інформації, зміни або знищення даних, блокування сервісів, втручання в роботу обладнання чи порушення прав користувачів. Загрози можуть бути навмисними або випадковими, внутрішніми або зовнішніми, технічними або організаційними, природними або антропогенними. Для ефективного захисту електронних комунікаційних мереж важливо не лише перелічити можливі загрози, а й правильно їх класифікувати. Класифікація дозволяє зрозуміти джерело загрози, механізм її реалізації, можливі наслідки та засоби протидії.

Мережі електронних комунікацій мають складну структуру, тому загрози можуть виникати на різних рівнях: фізичному, каналному, мережевому, транспортному, прикладному, організаційному та управлінському. Наприклад, на фізичному рівні загрозою може бути пошкодження кабельної лінії або відключення електроживлення.

За джерелом виникнення загрози поділяються на зовнішні та внутрішні. Зовнішні загрози надходять з-за меж організації або мережевого сегмента. Їх джерелами можуть бути кіберзлочинці, хакерські групи, конкуренти, ботнети, недобросовісні користувачі, автоматизовані сканери, шкідливі вебресурси або

інші зовнішні суб'єкти. До зовнішніх загроз належать DDoS-атаки, фішингові кампанії, спроби підбору паролів, експлуатація відкритих вразливостей, атаки на вебсервіси, підміна DNS, розповсюдження шкідливого програмного забезпечення, сканування мережі та несанкціоновані спроби доступу.

Внутрішні загрози виникають усередині організації або мережі. Їх джерелами можуть бути працівники, адміністратори, підрядники, користувачі корпоративної мережі, заражені внутрішні пристрої або неправильно налаштовані системи. Внутрішні загрози можуть бути як навмисними, так і ненавмисними. Наприклад, працівник може випадково відкрити шкідливе вкладення, використати слабкий пароль, підключити заражений USB-носій або надіслати конфіденційні дані не тому адресату. Водночас навмисний внутрішній порушник може копіювати службову інформацію, змінювати конфігурацію обладнання, створювати приховані облікові записи або передавати доступ стороннім особам.

За характером впливу загрози поділяються на навмисні та випадкові. Навмисні загрози реалізуються з певною метою: отримати доступ до інформації, порушити роботу сервісу, викрасти дані, завдати економічних збитків, отримати контроль над обладнанням або використати мережу для подальших атак. До навмисних загроз належать кібератаки, соціальна інженерія, шкідливе програмне забезпечення, атаки на маршрутизацію, саботаж, підміна трафіку, компрометація облікових записів. Випадкові загрози виникають без злого умислу. Це можуть бути помилки адміністраторів, збої обладнання, неправильне оновлення програмного забезпечення, відмова живлення, пошкодження кабелю, природні явища, помилки користувачів або недоліки в проєктуванні мережі.

Загрози програмному забезпеченню пов'язані з експлуатацією помилок у прошивках, операційних системах, мережевих сервісах, вебдодатках, системах управління або прикладних програмах. Особливо небезпечними є вразливості, для яких уже існують готові інструменти експлуатації. Загрози користувачам пов'язані з фішингом, соціальною інженерією, крадіжкою облікових даних, підміною сайтів, шкідливими вкладеннями, маніпуляціями та недостатнім рівнем обізнаності. Загрози системам управління можуть бути особливо критичними,

оскільки компрометація адміністративної платформи дає змогу змінювати конфігурацію великої кількості мережевих пристроїв.

За наслідками реалізації загрози поділяються на ті, що порушують конфіденційність, цілісність або доступність. Загрози конфіденційності спрямовані на отримання несанкціонованого доступу до інформації. Наприклад, перехоплення незашифрованого трафіку, викрадення бази даних, компрометація поштової скриньки або отримання доступу до журналів мережевого обладнання. Загрози цілісності змінюють інформацію або налаштування системи. Це може бути підміна маршруту, зміна DNS-записів, модифікація конфігурації маршрутизатора або внесення неправдивих даних у систему моніторингу. Загрози доступності спрямовані на блокування доступу до мережі або сервісів. Найтипівішим прикладом є DoS- або DDoS-атаки, які перевантажують сервери чи канали зв'язку.

Однією з найпоширеніших груп загроз у мережах електронних комунікацій є атаки на доступність. DoS-атака полягає у створенні умов, за яких сервіс, сервер або мережевий вузол не може обслуговувати легітимних користувачів. DDoS-атака відрізняється тим, що трафік надходить одночасно з великої кількості джерел, часто з заражених пристроїв, об'єднаних у ботнет. Для операторів зв'язку, провайдерів Інтернету, державних порталів, банківських систем і хмарних сервісів такі атаки можуть бути особливо небезпечними, оскільки навіть короточасна недоступність послуг призводить до фінансових, репутаційних і соціальних наслідків.

Шкідливе програмне забезпечення також є значною загрозою для електронних комунікаційних мереж. До нього належать віруси, трояни, шпигунські програми, програми-вимагачі, ботнет-клієнти, бекдори, руткіти та інші типи шкідливого коду. У телекомунікаційній інфраструктурі шкідливе ПЗ може використовуватися для викрадення облікових даних, створення прихованого доступу, участі пристрою в ботнеті, шифрування даних, порушення роботи системи моніторингу або поширення атаки на інші сегменти мережі. Особливу небезпеку становлять програми-вимагачі, оскільки вони можуть блокувати доступ

до важливих даних або сервісів. У звіті ENISA Threat Landscape 2024 [12] ransomware виділяється серед головних кіберзагроз після загроз доступності.

Окрему групу становлять загрози, пов'язані з маршрутизацією та мережевими протоколами. До них належать підміна маршрутів, помилкове оголошення префіксів, атаки на BGP, OSPF або інші протоколи маршрутизації, перенаправлення трафіку, петлі маршрутизації, несанкціонована зміна таблиць маршрутизації. Такі загрози можуть призвести до втрати доступності, перехоплення трафіку або його передавання через небажані вузли. У великих мережах операторів зв'язку атаки або помилки маршрутизації можуть мати масштабні наслідки, оскільки впливають на значну кількість користувачів.

Загрози безпроводовим мережам мають власну специфіку. Радіосередовище є відкритим, тому сигнал може бути перехоплений за межами приміщення або контрольованої території. До типових загроз Wi-Fi і мобільних мереж належать підбір паролів, використання слабких методів шифрування, створення фальшивої точки доступу, перехоплення автентифікаційних даних, атаки деавтентифікації, радіоперешкоди, підміна базової станції або несанкціонований доступ до гостьової мережі. Для IoT-пристроїв додатковими проблемами є слабкі паролі за замовчуванням, відсутність регулярних оновлень, обмежені ресурси пристроїв і недостатній рівень захисту протоколів.

Значну роль відіграють фізичні загрози. До них належать пошкодження кабельних ліній, крадіжка обладнання, несанкціонований доступ до серверних приміщень, відключення електроживлення, пожежі, затоплення, перегрів обладнання, пошкодження телекомунікаційних шаф або антенних споруд. Фізичні загрози часто недооцінюються, хоча їх наслідки можуть бути такими ж серйозними, як і наслідки кібератак. Наприклад, пошкодження магістральної оптичної лінії може призвести до втрати зв'язку для великої кількості користувачів.

Організаційні загрози пов'язані з недоліками в управлінні безпекою. До них належать відсутність політик безпеки, нерегулярне оновлення програмного забезпечення, використання однакових паролів, відсутність резервного

копіювання, неналежне документування мережі, відсутність плану реагування на інциденти, низький рівень навчання персоналу, недостатній контроль підрядників і постачальників.

Загрози також можна класифікувати за рівнем моделі OSI. На фізичному рівні це пошкодження кабелів, перешкоди, відмова живлення, фізичний доступ до обладнання. На канальному рівні — атаки на MAC-адреси, ARP spoofing, VLAN hopping, підключення неавторизованих пристроїв. На мережевому рівні — IP spoofing, атаки на маршрутизацію, ICMP flooding, сканування мережі. На транспортному рівні — SYN flood, TCP session hijacking, атаки на порти та сеанси. [22] [35]

Для України актуальність загроз у сфері електронних комунікацій є особливо високою через зростання залежності державних, освітніх, банківських, енергетичних, транспортних і комунальних сервісів від цифрової інфраструктури. Порушення роботи мереж зв'язку може вплинути не лише на приватних користувачів, а й на роботу підприємств, органів влади, систем оповіщення, медичних установ і об'єктів критичної інфраструктури. Тому класифікація загроз є необхідною основою для подальшого аналізу вразливостей, оцінювання ризиків і вибору ефективних засобів захисту.

1.4 Поняття вразливостей та їх роль у порушенні кібербезпеки мереж

Вразливості (табл.1.3) є однією з основних причин порушення безпеки мереж електронних комунікацій. Якщо загроза характеризує потенційну небезпеку для мережі, то вразливість є слабким місцем, через яке ця загроза може бути реалізована. У сфері електронних комунікацій вразливості можуть виникати в апаратному забезпеченні, програмному забезпеченні, мережевих протоколах, конфігураціях обладнання, організаційних процесах, системах управління доступом та діях користувачів. Наявність вразливості ще не означає автоматичного виникнення інциденту, але вона створює умови, за яких

зловмисник, технічний збій або помилка персоналу можуть призвести до порушення конфіденційності, цілісності чи доступності інформації.

У загальному вигляді вразливість можна визначити як недолік або слабе місце в системі, яке може бути використане для порушення її нормальної роботи. Для мереж електронних комунікацій це поняття має особливо широке значення, оскільки такі мережі складаються з багатьох взаємопов'язаних елементів: кінцевих пристроїв, маршрутизаторів, комутаторів, серверів, каналів зв'язку, систем автентифікації, програмного забезпечення, службових протоколів та засобів адміністрування. Через це вразливість одного елемента може вплинути на роботу всієї мережі або окремого її сегмента.

Таблиця 1.3 — Основні типи вразливостей у мережах електронних комунікацій

Тип вразливості	Приклади	Можливі наслідки
Технічні	Відсутність резервування, зношене обладнання, несправні порти	Відмова сервісів, зниження якості зв'язку
Програмні	Помилки в прошивках, ОС, вебсервісах, мережевих службах	Несанкціонований доступ, виконання шкідливого коду
Конфігураційні	Відкриті порти, стандартні паролі, неправильні ACL	Компрометація обладнання, витік даних
Організаційні	Відсутність політик, нерегулярні оновлення, слабкий контроль доступу	Підвищення ризику інцидентів
Фізичні	Незахищені серверні, доступ до кабелів, відсутність контролю входу	Пошкодження обладнання, переривання зв'язку
Людський фактор	Фішинг, слабкі паролі, помилки адміністраторів	Компрометація облікових записів, витік інформації

Особливо небезпечними є конфігураційні вразливості, оскільки вони часто виникають не через технічну несправність, а через помилку адміністратора або недостатній контроль змін. Наприклад, якщо на комутаторі неправильно налаштовано VLAN, користувач із гостьового сегмента може отримати доступ до внутрішньої мережі. Якщо на міжмережевому екрані створено надто широке правило доступу, зовнішній трафік може потрапляти до сервісів, які не повинні бути доступними з Інтернету. Якщо для віддаленого адміністрування використовується незахищений протокол або відкритий доступ без обмежень, ризик компрометації мережевого обладнання значно зростає (рис.1.4).



Рисунок 1.4 — Життєвий цикл управління вразливостями

Управління вразливостями повинно бути безперервним процесом. Недостатньо один раз перевірити мережу на наявність слабких місць, оскільки інфраструктура постійно змінюється: додаються нові пристрої, оновлюється програмне забезпечення, змінюються політики доступу, відкриваються нові сервіси, підключаються віддалені користувачі. Тому організація має регулярно проводити інвентаризацію активів, аналіз конфігурацій, тестування безпеки, встановлення оновлень, контроль журналів подій і перегляд прав доступу.

Роль вразливостей у порушенні безпеки мереж полягає в тому, що вони перетворюють потенційну загрозу на реальний інцидент. Наприклад, DDoS-атака буде більш результативною, якщо мережа не має захисту від перевантаження трафіком, резервного каналу або системи фільтрації. Фішингова атака буде успішнішою, якщо користувачі не проходять навчання, а доступ до службових систем не захищений багатофакторною автентифікацією. Атака на сервер буде небезпечнішою, якщо він працює із застарілим програмним забезпеченням і має надмірні права в мережі.

1.5 Нормативно-правове забезпечення захисту електронних комунікацій в Україні та міжнародні стандарти

Захист мереж електронних комунікацій не може розглядатися лише як технічне завдання. Він також має важливий правовий та організаційний вимір, оскільки функціонування електронних комунікаційних мереж пов'язане з обробкою інформації, захистом персональних даних, забезпеченням кібербезпеки, функціонуванням критичної інфраструктури, наданням послуг користувачам і виконанням вимог державного регулювання. В Україні нормативно-правове забезпечення захисту електронних комунікацій формується на основі законів, постанов Кабінету Міністрів України, нормативних документів Держспецзв'язку, національних стандартів, а також міжнародних стандартів і рекомендацій.

Базовим документом у сфері електронних комунікацій є Закон України «Про електронні комунікації» [4]. Він визначає правові та організаційні основи державної політики у сферах електронних комунікацій і радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами. Водночас ключовим нормативно-правовим актом, що визначає правові та організаційні основи захисту життєво важливих інтересів людини, суспільства і держави у кіберпросторі, є Закон України «Про основні засади забезпечення кібербезпеки України» [6]. Цей закон встановлює

національну систему кібербезпеки, визначає суб'єктів забезпечення кібербезпеки та вимоги до захисту об'єктів критичної інформаційної інфраструктури. У згаданих законах також передбачено застосування нормативних документів Міжнародного союзу електрозв'язку (ITU), СЕРТ, ЕСС та ETSI у сфері електронних комунікацій шляхом посилення на них у нормативно-правових актах України..

Окремим напрямом є захист інформації в інформаційно-комунікаційних системах. Закон України «Про захист інформації в інформаційно-комунікаційних системах» [5] регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Його положення важливі для телекомунікаційних систем, оскільки такі системи забезпечують не тільки передавання сигналів, а й обробку, зберігання, маршрутизацію та захист інформації.

Практичну роль у реагуванні на кіберінциденти відіграє CERT-UA [7] — урядова команда реагування на комп'ютерні надзвичайні події України. Вона функціонує у структурі Державного центру кіберзахисту Держспецзв'язку та займається питаннями реагування на комп'ютерні інциденти, поширенням попереджень і рекомендацій щодо кіберзагроз.

Для організацій, які експлуатують телекомунікаційні системи, ISO/IEC 27001 є корисним тим, що він орієнтує не лише на технічні засоби захисту, а й на створення повноцінної системи управління інформаційною безпекою. Така система включає визначення сфери застосування, оцінювання ризиків, вибір заходів контролю, розподіл ролей, управління документацією, внутрішній аудит, аналіз з боку керівництва і постійне вдосконалення. Це особливо важливо для операторів зв'язку, дата-центрів, провайдерів хмарних сервісів, державних установ і підприємств критичної інфраструктури.

Ще одним важливим міжнародним підходом є NIST Cybersecurity Framework 2.0. Цей документ надає рекомендації організаціям щодо управління кіберризиками. У версії 2.0 основні функції кібербезпеки подані як Govern, Identify, Protect, Detect, Respond і Recover. Для електронних комунікаційних

мереж це означає, що захист повинен охоплювати не лише попередження атак, а й управління ризиками, виявлення інцидентів, реагування на них та відновлення після порушень.

Для європейського простору важливою є Директива NIST [23]. Вона встановлює єдину правову основу для підтримання кібербезпеки в 18 критичних секторах Європейського Союзу та передбачає вимоги щодо національних стратегій кібербезпеки, співпраці між державами, реагування на інциденти та підвищення рівня захисту мережевих та інформаційних систем. Для України врахування європейських підходів є важливим через інтеграцію з європейським цифровим простором, розвиток електронних комунікацій і потребу в узгодженні національних підходів із міжнародною практикою.

Таким чином, нормативно-правове забезпечення захисту електронних комунікацій складається з кількох рівнів. Перший рівень — це національні закони, які визначають загальні правила функціонування електронних комунікацій, кібербезпеки та захисту інформації. Другий рівень — підзаконні акти, постанови та нормативні документи, які деталізують вимоги до критичної інфраструктури, кіберзахисту, реагування на інциденти та організації захисту. Третій рівень — національні та міжнародні стандарти, які надають практичні моделі управління безпекою, оцінювання ризиків і впровадження заходів контролю. У комплексі ці документи формують основу для побудови захищених телекомунікаційних систем.

1.6 Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи безпеки мереж електронних комунікацій. Встановлено, що електронні комунікаційні мережі є складними багаторівневими системами, які забезпечують передавання, обробку та маршрутизацію інформації між користувачами, пристроями, серверами та сервісними платформами. До їх складу входять кінцеве обладнання, мережі

доступу, транспортна інфраструктура, вузли комутації та маршрутизації, серверні ресурси, системи управління і засоби безпеки.

Було визначено, що інформаційна безпека в телекомунікаційних системах базується на принципах конфіденційності, цілісності та доступності. Крім того, важливими є автентичність, підзвітність, невідмовність, керованість, резервування, моніторинг, сегментація мережі та принцип мінімальних привілеїв. Дотримання цих принципів дозволяє знизити ризик несанкціонованого доступу, витоку даних, порушення роботи сервісів і компрометації мережевого обладнання.

У розділі також виконано базову класифікацію загроз у мережах електронних комунікацій. Загрози поділяються на зовнішні і внутрішні, навмисні і випадкові, технічні, організаційні, фізичні та пов'язані з людським фактором. Окрему і найбільш критичну групу становлять цілеспрямовані кібератаки (зокрема DDoS, перехоплення та підміна трафіку, фішинг, атаки на протоколи маршрутизації) та шкідливе програмне забезпечення (віруси, мережеві черв'яки, програми-вимагачі). Оскільки саме ці загрози є головними векторами компрометації телекомунікаційної інфраструктури, їх розширений технічний опис, механізми реалізації та експлуатовані вразливості детально досліджуються у наступному розділі роботи. Також було розглянуто нормативно-правове забезпечення захисту електронних комунікацій в Україні та міжнародні стандарти. Основу становлять закони України у сфері електронних комунікацій, кібербезпеки, захисту інформації та критичної інфраструктури, які визначають правові та організаційні засади державної політики, встановлюють вимоги до побудови системи кіберзахисту, регламентують порядок обробки даних у телекомунікаційних мережах та окреслюють механізми реагування на кіберінциденти.

2 АНАЛІЗ ОСНОВНИХ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ У МЕРЕЖАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

2.1 Аналіз зовнішніх і внутрішніх загроз

Інформаційна безпека в мережах електронних комунікацій базується на протидії загрозам, які за характером походження поділяються на зовнішні та внутрішні. Така класифікація є необхідною для визначення вектора атаки, оцінки рівня ризику та вибору адекватних організаційно-технічних засобів захисту. Згідно з методологією NIST [26], оцінювання ризику передбачає врахування джерел загроз, вразливостей, ймовірності їх реалізації та потенційного впливу на цілісність інфраструктури.

Зовнішні загрози походять із середовищ, що знаходяться поза межами контрольованого мережевого периметра організації. До основних джерел належать кіберзлочинні групи, ботнети, автоматизовані сканери та недобросовісні суб'єкти, що використовують методи соціальної інженерії, експлуатацію технічних вразливостей (у т.ч. вразливостей «нульового дня»), підбір паролів або перехоплення трафіку. Для зовнішніх загроз характерним є відсутність легального доступу зловмисника до ресурсів мережі, що змушує його використовувати вектори проникнення через публічні сервіси або прикладні інтерфейси.

Внутрішні загрози генеруються всередині мережевої інфраструктури та пов'язані з діяльністю персоналу, адміністраторів чи підрядників. Вони поділяються на ненавмисні (помилки під час конфігурації обладнання, нехтування політиками безпеки) та навмисні (зловживання наданими правами доступу, витік конфіденційної інформації).

Загроза інформаційній безпеці в мережах електронних комунікацій — це потенційна можливість реалізації дії або події, яка може призвести до порушення конфіденційності, цілісності, доступності або керованості інформаційних ресурсів. У контексті телекомунікаційних систем загрози можуть бути спрямовані як на інформацію, що передається мережею, так і на обладнання, програмне

забезпечення, канали зв'язку, мережеві протоколи, облікові записи користувачів та системи адміністрування.

До основних зовнішніх загроз для мереж електронних комунікацій належать несанкціоноване сканування мережі, спроби підбору паролів, атаки на відкриті порти, експлуатація вразливостей у маршрутизаторах, комутаторах, серверах, міжмережевих екранах, системах віддаленого доступу, а також фішингові повідомлення, шкідливі вкладення, DDoS-атаки та spoofing-атаки.

Особливо небезпечними є атаки, що поєднують технічні та соціальні методи. Наприклад, зловмисник може спочатку надіслати працівнику фішинговий лист, отримати його облікові дані, а потім використати ці дані для входу в корпоративну мережу.

Внутрішні загрози виникають усередині організації або мережевої інфраструктури. Їх джерелами можуть бути працівники, адміністратори, підрядники, користувачі корпоративної мережі, технічний персонал або будь-які особи, які мають легальний доступ до окремих ресурсів.

Зовнішні та внутрішні загрози не існують окремо одна від одної. У багатьох випадках реальна атака має комбінований характер. Наприклад, зовнішній зловмисник може отримати доступ до внутрішньої мережі через скомпрометований обліковий запис працівника.

Також можливий сценарій, коли внутрішній користувач випадково сприяє зовнішній атаці: відкриває фішингове посилання, підключає заражений носій інформації або використовує незахищене підключення до корпоративної мережі.

Як видно з табл.2.1, зовнішні загрози переважно пов'язані з проникненням до мережі або порушенням її доступності ззовні. Внутрішні загрози частіше пов'язані з помилками, недисциплінованістю користувачів або навмисним зловживанням доступом. При цьому обидва типи загроз можуть мати однаково серйозні наслідки для функціонування телекомунікаційної інфраструктури.

Таблиця 2.1 — Порівняльна характеристика зовнішніх і внутрішніх загроз у мережах електронних комунікацій

Ознака порівняння	Зовнішні загрози	Внутрішні загрози
Джерело виникнення	Сторонні особи, кіберзлочинці, ботнети, фішингові кампанії, шкідливе ПЗ	Працівники, адміністратори, підрядники, користувачі мережі
Наявність легального доступу	Зазвичай відсутній	Частково або повністю наявний
Основні методи реалізації	DDoS, фішинг, MITM, spoofing, експлуатація вразливостей, підбір паролів	Помилки конфігурації, зловживання правами, витік даних, порушення політик безпеки
Складність виявлення	Може виявлятися системами IDS/IPS, firewall, SIEM	Часто складніша через легітимний характер дій
Типові наслідки	Недоступність сервісів, компрометація даних, зараження систем, порушення роботи мережі	Витік конфіденційної інформації, зміна налаштувань, зниження надійності мережі
Основні засоби протидії	Фільтрація трафіку, міжмережеві екрани, DDoS-захист, оновлення ПЗ, моніторинг	Контроль доступу, журналювання, принцип мінімальних привілеїв, навчання персоналу

Узагальнену класифікацію загроз наведено на рис. 2.1.



Рисунок 2.1 — Класифікація загроз у мережах електронних комунікацій

Важливим елементом аналізу загроз є визначення їх впливу на базові властивості інформаційної безпеки: конфіденційність, цілісність і доступність.

Реалізація загроз у мережах електронних комунікацій безпосередньо впливає на базові властивості інформаційної безпеки: конфіденційність, цілісність та доступність. Механізми порушення цих властивостей варіюються від перехоплення даних до повного блокування інфраструктури, тому технічні аспекти експлуатації вразливостей і конкретні вектори атак потребують окремого детального аналізу..

Сучасні мережі електронних комунікацій також характеризуються високою взаємозалежністю. Порушення роботи одного елемента може вплинути на інші компоненти. Наприклад, атака на DNS-сервер може призвести до недоступності вебресурсів, навіть якщо самі сервери залишаються працездатними. Атака на систему автентифікації може заблокувати доступ користувачів до послуг. Компрометація маршрутизатора може змінити шляхи передавання трафіку або створити можливість його перехоплення.

2.2 Кібератаки на мережі електронних комунікацій DoS, DDoS, MITM, фішинг, spoofing.

Кібератаки на мережі електронних комунікацій є одним із найнебезпечніших проявів реалізації загроз інформаційній безпеці. На відміну від пасивних загроз, які лише створюють потенційну небезпеку, кібератака є активною дією, спрямованою на порушення роботи мережі, викрадення інформації, отримання несанкціонованого доступу або вплив на якість надання електронних комунікаційних послуг.

У телекомунікаційних мережах кібератаки можуть бути спрямовані на різні рівні інфраструктури: фізичний, каналний, мережевий, транспортний та рівень прикладних сервісів (до якого безпосередньо належать системи керування, сервери автентифікації, інфраструктура DNS, поштові сервіси та вебпортали). Окрім мережевих рівнів, мішенями злоумисників часто стають хмарні платформи та кінцеві абонентські пристрої. Особливістю таких атак є те, що вони здатні впливати не лише на окремого користувача, а й порушувати роботу великої кількості абонентів або виводити з ладу цілі сегменти мережі.

Найпоширенішими видами кібератак у мережах електронних комунікацій є DoS, DDoS, MITM, фішинг, spoofing, атаки з використанням шкідливого програмного забезпечення, атаки на протоколи маршрутизації, DNS-атаки, brute force-атаки та атаки на системи віддаленого адміністрування. Основні кібератаки та їх наслідки зведено у табл. 2.2

DoS-атаки

За визначенням Palo Alto Networks [31], DoS-атака полягає в перевантаженні системи, застосунок або мережі надмірним трафіком чи ресурсними запитами, що робить сервіс недоступним для легальних користувачів. Для мереж електронних комунікацій такі атаки особливо небезпечні, оскільки доступність є однією з ключових характеристик якості послуг.

DoS-атака може бути спрямована на вебсервер оператора, DNS-сервер, сервер автентифікації, поштовий сервер, VPN-шлюз або мережевий пристрій.

Наприклад, якщо атаковано сервер автентифікації користувачів, абоненти можуть не мати змоги підключитися до сервісів, навіть якщо основна мережа працює. Якщо перевантажено канал зв'язку, то знижується швидкість передавання даних, збільшується затримка, виникають втрати пакетів.

DoS-атаки можуть бути як простими, так і складними. Прості атаки створюють велику кількість однотипних запитів. Складніші атаки можуть імітувати легітимну поведінку користувачів, що ускладнює їх виявлення. Такі атаки можуть бути спрямовані не лише на пропускну здатність каналу, а й на конкретні ресурси сервера або прикладного сервісу.

DDoS-атаки

DDoS-атака є розподіленою формою DoS-атаки. Вона виконується не з одного джерела, а з великої кількості пристроїв, які можуть бути заражені шкідливим програмним забезпеченням і об'єднані в ботнет. Через це DDoS-атаки мають значно більший масштаб і складніші для блокування, ніж звичайні DoS-атаки.

IBM [17] визначає DDoS-атаку як атаку, під час якої онлайн-ресурс перевантажується фальшивими запитами або іншим шкідливим трафіком, зазвичай із використанням ботнету; у результаті ресурс сповільнюється або стає недоступним для легітимних користувачів. У телекомунікаційних мережах DDoS-атаки можуть спричиняти масові перебої в роботі сервісів, зниження якості зв'язку, недоступність сайтів, поштових систем, DNS та інших критичних компонентів.

DDoS-атаки можуть бути класифіковані за рівнем впливу. До основних типів належать об'ємні атаки, протокольні атаки та атаки прикладного рівня. Об'ємні атаки спрямовані на перевантаження каналу зв'язку великою кількістю трафіку. Протокольні атаки використовують особливості роботи мережових або транспортних протоколів. Атаки прикладного рівня спрямовані на конкретні сервіси, наприклад HTTP, DNS або API.

Захист від DDoS-атак зазвичай передбачає фільтрацію трафіку, використання спеціалізованих DDoS mitigation-сервісів, розподілення

навантаження, обмеження кількості запитів, моніторинг аномальної активності та співпрацю з провайдерами вищого рівня. Водночас повністю усунути ризик DDoS-атак складно, тому важливим є не лише запобігання, а й готовність до швидкого реагування.

MITM-атаки

MITM-атака (рис.2.2), або атака «людина посередині», полягає в тому, що зловмисник перехоплює або змінює комунікацію між двома сторонами, які вважають, що спілкуються напрямку. У мережах електронних комунікацій така атака може бути спрямована на перехоплення логінів, паролів, сесійних токенів, службових повідомлень, DNS-запитів або іншої конфіденційної інформації.

CISA (Cybersecurity and Infrastructure Security Agency) — Агентство з кібербезпеки та безпеки інфраструктури. [11] пояснює MITM-атаку як ситуацію, коли третя сторона вставляє себе між комунікацією клієнта і сервера. OWASP (Open Web Application Security Project) — Відкритий проєкт забезпечення безпеки вебдодатків. [29] також описує MITM як атаку, під час якої перехоплюється комунікація між двома системами, а початкове з'єднання фактично розділяється на два окремі з'єднання: між клієнтом і зловмисником та між зловмисником і сервером.

У телекомунікаційній інфраструктурі MITM-атаки можуть реалізовуватися у відкритих Wi-Fi-мережах, у неправильно налаштованих локальних мережах, при використанні незахищених протоколів, через підробку DNS-відповідей або шляхом компрометації мережевого обладнання. Особливо небезпечними є ситуації, коли користувачі передають облікові дані без належного шифрування або ігнорують попередження браузера про недійсний сертифікат.

Наслідки MITM-атак можуть бути серйозними. Зловмисник може отримати доступ до конфіденційної інформації, змінити передані дані, викрасти сесійні токени, перенаправити користувача на фальшивий сайт або зібрати службову інформацію для подальшої атаки. У корпоративних мережах така атака може стати початковим етапом більш масштабного інциденту.



Рисунок 2.2 — Принцип MITM-атаки

Основними засобами зменшення ризику MITM-атак є використання захищених протоколів, перевірка сертифікатів, застосування VPN, захищена автентифікація, сегментація мережі, контроль ARP/DNS-активності та заборона використання незахищених каналів для передавання службової інформації.

Фішинг

Фішинг є одним із найпоширеніших видів атак, що використовує соціальну інженерію. Його суть полягає в тому, що зловмисник намагається обманом змусити користувача передати конфіденційні дані, перейти за шкідливим посиланням, відкрити вкладення або виконати певну дію. Фішинг може здійснюватися через електронну пошту, SMS, месенджери, соціальні мережі, телефонні дзвінки або фальшиві вебсайти.

У мережах електронних комунікацій фішинг небезпечний тим, що він часто є початковим етапом більш складної атаки. Наприклад, після отримання пароля працівника зловмисник може увійти до корпоративної пошти, VPN, системи моніторингу або адміністративної панелі. Далі він може поширювати шкідливі листи від імені реального користувача, збирати службову інформацію або змінювати налаштування сервісів.

Фішингові атаки можуть бути масовими або цільовими. Масовий фішинг орієнтований на велику кількість користувачів і зазвичай має шаблонний характер. Цільовий фішинг, або spear phishing, спрямований на конкретну особу або організацію. У такому випадку повідомлення може містити реальні дані про

працівника, посаду, проєкт або внутрішні процеси, що робить атаку більш переконливою.

Наслідками фішингу можуть бути викрадення облікових даних, зараження комп'ютера шкідливим програмним забезпеченням, несанкціонований доступ до корпоративних ресурсів, витік персональних даних, фінансові втрати та репутаційні ризики. Тому протидія фішингу має включати не лише технічні засоби, а й навчання користувачів, перевірку повідомлень, багатофакторну автентифікацію, фільтрацію пошти та моніторинг підозрілих входів.

Spoofing-атаки

Spoofing — це тип атаки, за якого зловмисник підробляє певний ідентифікатор, щоб видати себе за довірене джерело. У мережах електронних комунікацій можуть зустрічатися IP-spoofing, DNS-spoofing, ARP-spoofing, email-spoofing, caller ID spoofing та інші різновиди. Основна ідея spoofing-атаки полягає в порушенні довіри до ідентифікаційної інформації.

IP-spoofing передбачає підробку IP-адреси джерела пакета. Це може використовуватися для обходу фільтрів, маскування джерела атаки або посилення DDoS-атак. DNS-spoofing полягає в підміні DNS-відповідей, унаслідок чого користувач може бути перенаправлений на фальшивий сайт. ARP-spoofing застосовується в локальних мережах і може бути використаний для перехоплення трафіку. Email-spoofing полягає в підробці адреси відправника електронного листа, що часто використовується у фішингових кампаніях.

Для захисту від spoofing-атак застосовують фільтрацію пакетів, перевірку джерел трафіку, DNSSEC, захищені протоколи, SPF/DKIM/DMARC для електронної пошти, статичні ARP-записи для критичних вузлів, сегментацію мережі та моніторинг аномальної активності.

Атаки на сервіси електронної пошти.

Цей вид кібератак використовує електронну пошту як первинний вектор для проникнення в корпоративні мережі та компрометації користувачів. Подібно до фішингу та мережевого спуфінгу, такі атаки переважно спрямовані на порушення конфіденційності та цілісності інформаційного обміну. Зловмисники здійснюють

підробку адреси відправника (Email Spoofing) для обходу поштових фільтрів, видаючи себе за легітимного відправника або внутрішнього співробітника. Крім того, критичною загрозою є атаки типу бізнес-компрометації електронної пошти (BEC – Business Email Compromise), що призводять до викрадення службової інформації, перехоплення фінансових транзакцій або отримання несанкціонованого доступу до інших мережесих ресурсів. Технічною передумовою для успішної реалізації таких атак найчастіше є відсутність або некоректне конфігурування базових протоколів автентифікації поштових повідомлень, таких як SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та політик DMARC. Також скомпрометована електронна пошта активно застосовується для масового розповсюдження шкідливого програмного забезпечення через інфіковані вкладення, що в кінцевому підсумку може призвести до порушення доступності всієї інфраструктури через розгортання програм-вимагачів (Ransomware).

Інші види кібератак

Окрім DoS, DDoS, MITM, фішингу та spoofing, у мережах електронних комунікацій поширені й інші типи атак. До них належать атаки з використанням шкідливого програмного забезпечення, brute force-атаки, атаки на протоколи маршрутизації, експлуатація вразливостей програмного забезпечення, атаки на DNS, атаки на IoT-пристрої та компрометація систем віддаленого адміністрування.

Brute force-атаки полягають у багаторазових спробах підібрати пароль або ключ доступу. У телекомунікаційних мережах такі атаки можуть бути спрямовані на VPN, SSH, вебпанелі адміністрування, поштові сервіси або облікові записи користувачів. Їх успішність залежить від складності паролів, наявності обмежень на кількість спроб входу та використання багатофакторної автентифікації.

Атаки на протоколи маршрутизації можуть призводити до зміни маршрутів передавання даних, перехоплення трафіку, створення петель маршрутизації або недоступності окремих сегментів мережі. Для операторських і корпоративних

мереж це особливо критично, оскільки маршрутизація визначає шлях проходження трафіку та стабільність зв'язку між вузлами.

Атаки на DNS можуть призводити до перенаправлення користувачів на фальшиві ресурси або недоступності доменних імен. DNS є одним із ключових сервісів мережі, тому його компрометація може впливати на велику кількість інших сервісів. Саме тому DNS-інфраструктура потребує особливого захисту, резервування та моніторингу.

Таблиця 2.2 — Основні кібератаки на мережі електронних комунікацій

Вид атаки	Основна мета	Об'єкт впливу	Можливі наслідки
DoS	Порушення доступності сервісу	Сервер, канал зв'язку, мережевий пристрій	Недоступність послуг, затримки, втрати пакетів
DDoS	Масове перевантаження ресурсу	Вебсервери, DNS, канали зв'язку, хмарні сервіси	Масові перебої, фінансові та репутаційні втрати
MITM	Перехоплення або зміна трафіку	Канал зв'язку між клієнтом і сервером	Викрадення даних, підміна інформації, компрометація сесій
Фішинг	Отримання конфіденційних даних шляхом обману	Користувачі, працівники, облікові записи	Викрадення паролів, зараження пристроїв, несанкціонований доступ
Spoofing	Підrobка ідентифікатора або джерела	IP, DNS, ARP, email, телефонний номер	Перенаправлення трафіку, обман користувачів, MITM
Brute force	Підбір облікових даних	VPN, SSH, пошта, адмін-панелі	Несанкціонований доступ
Malware	Компрометація пристроїв або систем	ПК, сервери, IoT-пристрої	Витік даних, ботнет, шифрування файлів
DNS-атаки	Порушення роботи доменних сервісів	DNS-сервери та DNS-запити	Перенаправлення користувачів, недоступність ресурсів

Таким чином, кібератаки на мережі електронних комунікацій можуть бути спрямовані на різні компоненти інфраструктури та мати різні цілі. Одні атаки порушують доступність, інші — конфіденційність або цілісність інформації. Найнебезпечнішими є комбіновані атаки, які поєднують технічні методи з соціальною інженерією. Наприклад, фішинг може використовувати email-spoofing, після чого викрадені облікові дані застосовуються для входу до внутрішньої мережі, а далі зловмисник може виконати MITM-атаку або встановити шкідливе програмне забезпечення.

2.3 Технічні вразливості мережевого обладнання та програмного забезпечення

Технічні вразливості мережевого обладнання та програмного забезпечення є однією з основних причин виникнення інцидентів інформаційної безпеки в мережах електронних комунікацій. Вони створюють умови, за яких зовнішні або внутрішні загрози можуть бути реалізовані на практиці. Якщо загроза є потенційною небезпекою, то вразливість є слабким місцем у системі, через яке ця небезпека може перетворитися на реальний інцидент.

Відповідно до визначення NIST [24], вразливість — це слабкість в інформаційній системі, процедурах безпеки, внутрішньому контролі або реалізації, яка може бути використана або активована джерелом загрози. У контексті мереж електронних комунікацій такими слабкими місцями можуть бути помилки в програмному коді, неправильні налаштування обладнання, застарілі версії прошивок, відкриті службові порти, слабкі механізми автентифікації, незахищені протоколи передавання даних, відсутність сегментації мережі або недостатній контроль доступу.

Технічні вразливості можуть виникати як у фізичному обладнанні, так і в програмному забезпеченні. До мережевого обладнання належать маршрутизатори, комутатори, точки доступу Wi-Fi, міжмережеві екрани, сервери, контролери, базові станції, оптичні термінали, шлюзи, системи балансування навантаження та

інші пристрої, що забезпечують передавання, обробку або маршрутизацію трафіку. Програмне забезпечення включає операційні системи, мережеві служби, системи керування обладнанням, вебінтерфейси адміністрування, серверні застосунки, бази даних, системи моніторингу, засоби автентифікації та хмарні сервіси.

Однією з найпоширеніших технічних вразливостей є використання застарілого програмного забезпечення або прошивки. Мережеве обладнання часто працює протягом багатьох років, і якщо його не оновлювати, воно може містити вже відомі вразливості. Зловмисники активно використовують інформацію про такі недоліки, оскільки після публікації вразливості з'являються готові інструменти для її експлуатації. Саме тому CISA веде каталог Known Exploited Vulnerabilities [10], який містить відомості про вразливості, що вже використовувалися зловмисниками в реальних атаках.

Особливо небезпечними є вразливості в обладнанні, яке має доступ до Інтернету. До таких пристроїв можуть належати VPN-шлюзи, маршрутизатори, поштові сервери, вебсервери, системи віддаленого адміністрування та обладнання операторського рівня. Якщо такий пристрій має не виправлену вразливість, він може стати початковою точкою проникнення в мережу. ENISA у звіті Threat Landscape 2025 [13] зазначає, що сучасні загрозливі групи активно використовують вразливості та нові моделі атак, спрямовані на цифрову інфраструктуру.

До важливої групи технічних вразливостей належать помилки конфігурації. Навіть надійне обладнання може стати небезпечним, якщо воно налаштоване неправильно. Наприклад, використання стандартних паролів, відкриття зайвих портів, відсутність обмежень на доступ до адміністративного інтерфейсу, неправильне налаштування VLAN, слабка політика доступу або відсутність шифрування створюють додаткові ризики. У телекомунікаційних мережах помилки конфігурації можуть вплинути не лише на один пристрій, а й на цілий сегмент мережі.

Поширеною проблемою є використання стандартних або слабких облікових даних. Багато мережових пристроїв постачаються із типовими логінами та паролями, які необхідно змінювати під час первинного налаштування. Якщо цього не зробити, зловмисник може отримати доступ до обладнання без складної технічної атаки. Особливо це стосується недорогих маршрутизаторів, точок доступу, IoT-пристроїв, камер відеоспостереження та іншого обладнання, яке часто встановлюється без належного адміністрування.

Технічні вразливості програмного забезпечення часто пов'язані з помилками в коді. Це можуть бути помилки перевірки введених даних, неправильна робота з пам'яттю, недостатня автентифікація, помилки керування сесіями, некоректна обробка запитів або недоліки в логіці застосунку. NVD [25] визначає вразливість як слабкість у логіці програмного або апаратного компонента, яка при експлуатації може негативно вплинути на конфіденційність, цілісність або доступність.

У мережах електронних комунікацій програмні вразливості можуть бути присутніми в операційних системах серверів, вебінтерфейсах керування обладнанням, білінгових системах, системах моніторингу, базах даних, DNS-серверах, поштових серверах, VPN-сервісах і хмарних платформах. Їх експлуатація може призвести до несанкціонованого доступу, зміни налаштувань, викрадення даних, встановлення шкідливого програмного забезпечення або повного порушення роботи сервісу.

Окрему небезпеку становлять вразливості в системах віддаленого доступу. Для адміністрування мережевого обладнання часто використовуються VPN, SSH, вебпанелі або спеціальні системи керування. Якщо доступ до таких систем недостатньо захищений, зловмисник може отримати широкі можливості для впливу на мережу. Саме тому для віддаленого адміністрування необхідно застосовувати багатофакторну автентифікацію, обмеження доступу за IP-адресами, журналювання подій, регулярне оновлення програмного забезпечення та контроль привілеїв (табл. 2.3).

Таблиця 2.3 — Основні технічні вразливості мережевого обладнання та програмного забезпечення

Вид вразливості	Приклад прояву	Можливі наслідки
Застаріле програмне забезпечення	Неоновлена прошивка маршрутизатора або сервера	Експлуатація відомої вразливості, несанкціонований доступ
Стандартні паролі	Використання типових admin/admin	Компрометація обладнання
Помилки конфігурації	Відкриті зайві порти, неправильні ACL	Доступ до службових сервісів, витік даних
Не захищені протоколи	Telnet, FTP, HTTP без шифрування	Перехоплення логінів, паролів і службового трафіку
Вразливості вебінтерфейсів	Помилки автентифікації або перевірки запитів	Захоплення панелі керування
Недостатня сегментація	Відсутність поділу на VLAN або зони безпеки	Поширення атаки всередині мережі
Слабкий контроль доступу	Надмірні привілеї користувачів	Зловживання правами, зміна налаштувань
Відсутність моніторингу	Немає журналювання або SIEM	Пізнє виявлення інциденту
Неправильна робота резервування	Відсутність резервних каналів або копій	Тривала недоступність сервісів
Уразливі IoT-пристрої	Камери, датчики, шлюзи зі слабким захистом	Ботнети, DDoS, проникнення в мережу

Окремої уваги потребують вразливості IoT-пристроїв, які дедалі частіше підключаються до мереж електронних комунікацій. До таких пристроїв належать датчики, контролери, камери, розумні лічильники, шлюзи, системи моніторингу та промислові пристрої. Часто вони мають обмежені обчислювальні ресурси, слабкі механізми захисту, рідко оновлюються та можуть використовувати стандартні облікові дані. У разі компрометації такі пристрої можуть бути використані для створення ботнетів, проведення DDoS-атак або прихованого доступу до внутрішньої мережі.

Технічні вразливості можуть мати різний рівень критичності. Деякі з них створюють лише локальний ризик, наприклад доступ до одного пристрою. Інші можуть мати системний характер і впливати на всю інфраструктуру. Наприклад, вразливість у сервері автентифікації може заблокувати доступ користувачів до послуг, а вразливість у маршрутизаторі ядра мережі може порушити маршрутизацію великого обсягу трафіку.

Оцінювання технічних вразливостей має здійснюватися системно. Для цього використовують інвентаризацію активів, сканування вразливостей, аналіз конфігурацій, тестування оновлень, аудит прав доступу, перевірку журналів подій та аналіз мережевого трафіку. Також важливо визначати пріоритетність усунення вразливостей. Найперше необхідно усувати ті, які вже активно експлуатуються, мають високий рівень критичності або стосуються обладнання, доступного з Інтернету.

Таким чином, технічні вразливості мережевого обладнання та програмного забезпечення є важливою складовою загального ризику для мереж електронних комунікацій. Вони можуть виникати через помилки виробника, недоліки програмного коду, неправильні налаштування, відсутність оновлень або недостатній контроль з боку адміністраторів. Для зменшення таких ризиків необхідно впроваджувати регулярне оновлення систем, контроль конфігурацій, сегментацію мережі, захищене адміністрування, моніторинг подій і системне управління вразливостями.

2.4 Людський фактор як джерело вразливостей

Людський фактор є одним із найважливіших джерел вразливостей у мережах електронних комунікацій. Навіть за наявності сучасних технічних засобів захисту безпека мережі значною мірою залежить від дій користувачів, адміністраторів, технічного персоналу та керівництва організації. Людина може як забезпечувати належний рівень безпеки, так і ненавмисно або навмисно створювати умови для реалізації загроз.

Під людським фактором у сфері кібербезпеки слід розуміти сукупність дій, помилок, рішень, звичок, рівня обізнаності та поведінкових особливостей людей, які впливають на захищеність інформаційних систем і мереж. У телекомунікаційних мережах людський фактор проявляється під час налаштування обладнання, керування обліковими записами, використання паролів, обробки електронної пошти, роботи з конфіденційною інформацією, реагування на інциденти та дотримання політик безпеки.

Найпоширенішою формою людського фактора є помилки користувачів. Користувач може випадково перейти за фішинговим посиланням, відкрити шкідливе вкладення, використати слабкий пароль, передати облікові дані сторонній особі або підключити до комп'ютера невідомий носій інформації. Такі дії часто не мають зловмисного характеру, однак їх наслідки можуть бути дуже серйозними.

Однією з найбільш небезпечних людських вразливостей є використання слабких або повторюваних паролів. Користувачі часто обирають прості паролі, які легко запам'ятати, або використовують один і той самий пароль для різних сервісів. Якщо пароль буде викрадений на одному ресурсі, зловмисник може спробувати використати його для доступу до інших систем. У мережах електронних комунікацій це може стосуватися поштових скриньок, VPN, особистих кабінетів, систем адміністрування або службових порталів.

Людський фактор проявляється не лише серед звичайних користувачів, а й серед адміністраторів. Помилки адміністрування можуть мати значно більші

наслідки, оскільки адміністратори мають розширені права доступу. До таких помилок належать неправильне налаштування маршрутизаторів і комутаторів, відкриття зайвих портів, надання надмірних привілеїв, несвоєчасне встановлення оновлень, відсутність резервного копіювання, неправильне налаштування firewall або некоректне ведення журналів подій.

Особливо небезпечним є порушення принципу мінімальних привілеїв. Цей принцип передбачає, що користувач або система повинні мати лише ті права, які необхідні для виконання конкретних завдань. Якщо користувач має надмірні привілеї, компрометація його облікового запису створює більший ризик для всієї мережі.

Окрему групу становлять навмисні внутрішні порушення. Працівник або підрядник може свідомо передати конфіденційну інформацію стороннім особам, скопіювати службові дані, змінити налаштування обладнання, створити прихований обліковий запис або пошкодити систему. Причинами таких дій можуть бути конфлікти, фінансова мотивація, недобросовісність, тиск з боку сторонніх осіб або бажання отримати особисту вигоду.

Важливим джерелом вразливостей є недотримання політик безпеки. Організація може мати формально затверджені правила, але якщо працівники їх не виконують, реальний рівень захисту залишається низьким. Наприклад, політика може забороняти передавання паролів у месенджерах, використання особистих пристроїв для службових завдань або підключення невідомих USB-носіїв. Однак без навчання, контролю та відповідальності такі правила можуть ігноруватися.

У сучасних умовах значний ризик створює використання особистих пристроїв і віддаленої роботи. Працівники можуть підключатися до корпоративних сервісів із домашніх мереж, особистих ноутбуків або смартфонів. Якщо такі пристрої не мають належного захисту, вони можуть стати слабкою ланкою. Ризик підвищується, якщо використовується незахищений Wi-Fi, відсутнє оновлення операційної системи, не встановлений антивірус або один пристрій використовується кількома членами сім'ї.

Людський фактор також впливає на реагування на інциденти. Якщо працівник помітив підозрілу активність, але не повідомив про неї відповідальним особам, інцидент може розвиватися далі. Якщо адміністратор неправильно оцінив серйозність події або несвоєчасно виконав оновлення, наслідки можуть бути значно більшими. Тому організація повинна мати зрозумілі процедури повідомлення про інциденти, відповідальних осіб і порядок дій у разі підозри на компрометацію.

Особливістю людського фактора є те, що його неможливо повністю усунути лише технічними засобами. Навіть найсучасніші системи захисту не гарантують безпеки, якщо користувачі не дотримуються правил або адміністратори неправильно налаштовують обладнання. Тому захист від людських помилок має бути комплексним і поєднувати технічні, організаційні та навчальні заходи.

До технічних заходів зменшення впливу людського фактора належать багатофакторна автентифікація, політики складності паролів, автоматичне блокування підозрілих входів, обмеження прав доступу, централізоване керування пристроями, фільтрація пошти, захист від шкідливих вкладень, резервне копіювання та моніторинг подій. Такі заходи не усувають людські помилки повністю, але зменшують ймовірність того, що одна помилка призведе до серйозного інциденту.

Для адміністраторів і технічного персоналу необхідні окремі програми підготовки. Вони повинні охоплювати безпечне налаштування мережевого обладнання, керування оновленнями, роботу з журналами подій, сегментацію мережі, захист від DDoS, контроль доступу, безпечне резервне копіювання та реагування на інциденти. Помилки адміністратора можуть бути значно небезпечнішими за помилки звичайного користувача, тому рівень підготовки технічного персоналу має бути високим.

Таким чином, людський фактор є одним із ключових джерел вразливостей у мережах електронних комунікацій. Він проявляється через помилки користувачів, необережність, недостатню обізнаність, неправильне адміністрування, надмірні привілеї, порушення політик безпеки та навмисні дії внутрішніх порушників. Для

зменшення таких ризиків необхідно поєднувати технічні засоби захисту, організаційні правила, регулярне навчання персоналу, контроль доступу та постійний моніторинг подій.

2.5 Оцінка ризиків та наслідків реалізації загроз

Оцінка ризиків є важливим етапом аналізу безпеки мереж електронних комунікацій, оскільки дає змогу не лише виявити потенційні загрози та вразливості, а й визначити, наскільки небезпечними вони є для конкретної телекомунікаційної інфраструктури. Якщо на попередніх етапах розглядаються джерела загроз, типи кібератак, технічні вразливості та людський фактор, то оцінка ризиків дозволяє встановити пріоритетність їх усунення та визначити можливі наслідки для мережі, користувачів і організації загалом.

У сфері інформаційної безпеки ризик зазвичай розглядається як поєднання ймовірності реалізації певної загрози та величини можливих наслідків. Згідно з підходом NIST SP 800-30 [26], оцінювання ризику є частиною загального процесу управління ризиками та допомагає керівництву визначати доцільні дії щодо реагування на виявлені ризики. У цьому підході враховуються такі фактори, як загроза, вразливість, імовірність, вплив та умови, що сприяють реалізації ризику.

Оцінка ризиків у мережах електронних комунікацій є критично важливою, оскільки вони забезпечують функціонування базових інформаційних ресурсів та інфраструктури IoT. Будь-яке порушення їхньої безперервної роботи неминуче призводить до комплексних технічних збоїв, компрометації даних та зупинки бізнес-процесів.

Оцінювання ризиків доцільно проводити за чітко регламентованою послідовністю: ідентифікація критичних активів інфраструктури, визначення актуальних загроз та наявних вразливостей, після чого оцінюється ймовірність реалізації кіберінциденту та його потенційний вплив. На основі цих показників формується загальний рівень ризику.

Таблиця 2.4 — Приклад якісної шкали оцінки ймовірності та впливу ризику

Рівень	Ймовірність реалізації загрози	Можливий вплив на мережу
Низький	Загроза малоімовірна або потребує специфічних умов	Незначне погіршення роботи окремого сервісу
Середній	Загроза може бути реалізована за наявності вразливостей	Часткове порушення роботи мережі або витік обмеженого обсягу даних
Високий	Загроза є реальною, поширеною або вже активно використовується	Значна недоступність сервісів, компрометація даних або порушення роботи інфраструктури

Для визначення загального рівня ризику можна використовувати якісну шкалу (табл. 2.4) та матрицю ризиків, у якій поєднуються два показники: ймовірність реалізації загрози та рівень наслідків. Наприклад, якщо ймовірність атаки висока, а наслідки також значні, такий ризик вважається критичним або високим і потребує першочергового реагування. Якщо ж ймовірність низька, а наслідки незначні, ризик може бути прийнятий або контрольований базовими заходами захисту.

У мережах електронних комунікацій до високих і критичних ризиків зазвичай належать ті, що можуть вплинути на доступність сервісів, компрометувати службову або персональну інформацію, порушити маршрутизацію трафіку, надати зловмиснику адміністративний доступ або спричинити масштабне поширення атаки. Саме тому особливу увагу слід приділяти DDoS-атакам, компрометації облікових записів адміністраторів, експлуатації відомих вразливостей у мережевому обладнанні, помилкам конфігурації, фішингу та атакам на системи віддаленого доступу.

Важливо враховувати, що один і той самий тип загрози може мати різний рівень ризику залежно від умов конкретної мережі. Наприклад, DDoS-атака для

невеликої локальної мережі може мати середній рівень ризику, якщо мережа не надає публічних сервісів. Водночас для інтернет-провайдера або організації, що обслуговує велику кількість користувачів, така атака може мати критичний рівень ризику. Аналогічно, вразливість у внутрішньому сервері може бути менш небезпечною, якщо він ізольований, але дуже небезпечною, якщо сервер доступний з Інтернету або містить конфіденційні дані.

Оцінка ризику повинна враховувати не лише технічні аспекти, а й організаційні умови. Наприклад, наявність політик безпеки, регулярного оновлення програмного забезпечення, резервного копіювання, журналювання подій, систем моніторингу, навчання персоналу та плану реагування на інциденти знижує рівень ризику. Водночас відсутність цих заходів підвищує ймовірність реалізації загроз і збільшує масштаб можливих наслідків.

Наслідки реалізації загроз у мережах електронних комунікацій можна поділити на технічні, інформаційні, фінансові, організаційні, правові та репутаційні. Такий поділ дозволяє ширше оцінити вплив інцидентів, оскільки наслідки кібератак не обмежуються лише тимчасовим збоєм обладнання.

До технічних наслідків належать недоступність сервісів, перевантаження каналів зв'язку, порушення маршрутизації, втрата пакетів, збільшення затримок, відмова серверів, збої в роботі DNS, VPN, поштових або вебсервісів, пошкодження конфігурацій обладнання та порушення роботи систем моніторингу. Наприклад, DDoS-атака може перевантажити канал зв'язку або сервер, унаслідок чого користувачі не зможуть отримати доступ до послуг. Помилка конфігурації маршрутизатора може призвести до неправильного передавання трафіку або повного відключення окремого сегмента мережі.

Під час оцінки наслідків важливо враховувати взаємозв'язок між різними видами впливу. Наприклад, технічний збій може спричинити фінансові втрати, а витік інформації — правові та репутаційні наслідки. Компрометація облікового запису адміністратора може одночасно призвести до зміни конфігурації обладнання, витоку службової інформації, недоступності сервісів і втрати довіри

користувачів. Тому оцінка ризиків повинна бути комплексною, а не обмежуватися лише технічними параметрами.

У сучасних підходах до кібербезпеки оцінка ризиків є безперервним процесом. NIST Cybersecurity Framework 2.0 [28] підкреслює необхідність визначати, організовувати та пріоритезувати дії з управління ризиками відповідно до цілей організації, вимог законодавства та очікувань щодо управління ризиками. Це означає, що ризики потрібно переглядати регулярно, особливо після змін у мережевій інфраструктурі, появи нових сервісів, оновлення обладнання, виявлення нових вразливостей або після інцидентів.

Після визначення рівня ризику організація повинна обрати спосіб реагування. Основними варіантами є зниження ризику, уникнення ризику, передавання ризику або прийняття ризику. Зниження ризику передбачає впровадження технічних і організаційних заходів захисту. Уникнення ризику означає відмову від певної небезпечної дії або сервісу. Передавання ризику може здійснюватися через страхування, договори або використання зовнішніх сервісів захисту. Прийняття ризику можливе тоді, коли його рівень є допустимим і витрати на усунення перевищують потенційні наслідки.

Для мереж електронних комунікацій найбільш доцільним є поєднання різних заходів реагування. Наприклад, ризик DDoS-атаки можна зменшити завдяки фільтрації трафіку, резервуванню каналів і використанню спеціалізованих сервісів захисту. Ризик фішингу можна знизити через навчання персоналу, багатофакторну автентифікацію та фільтрацію пошти. Ризик експлуатації технічних вразливостей зменшується завдяки регулярному оновленню програмного забезпечення, інвентаризації активів і скануванню вразливостей. Ризик внутрішніх порушень знижується завдяки контролю доступу, журналюванню дій і принципу мінімальних привілеїв.

Окремо слід зазначити поняття залишкового ризику. Навіть після впровадження засобів захисту повністю усунути ризики неможливо. Завжди залишається певна ймовірність інциденту, пов'язана з новими вразливостями, людськими помилками, невідомими методами атак або непередбачуваними

обставинами. Тому метою кібербезпеки є не абсолютне усунення всіх ризиків, а зниження їх до прийнятного рівня.

Для ефективної оцінки ризиків у мережах електронних комунікацій необхідно враховувати такі принципи: регулярність оцінювання, актуальність даних про загрози, повноту інвентаризації активів, урахування людського фактора, аналіз технічних вразливостей, документування результатів, визначення відповідальних осіб і постійний моніторинг.

2.6 Висновки до розділу 2

У другому розділі було проаналізовано основні загрози і вразливості в мережах електронних комунікацій. Встановлено, що небезпеки можуть мати як зовнішнє, так і внутрішнє походження. Зовнішні загрози найчастіше пов'язані з кібератаками, шкідливим програмним забезпеченням, фішингом, DDoS-атаками та спробами несанкціонованого доступу.

Розглянуто основні типи кібератак на мережі електронних комунікацій, зокрема DoS, DDoS, MITM, фішинг і spoofing. Визначено, що такі атаки можуть призводити до порушення доступності сервісів, перехоплення або підміни інформації, викрадення облікових даних і зниження якості надання послуг.

Окрему увагу приділено технічним вразливостям мережевого обладнання та програмного забезпечення. До них належать застарілі прошивки, слабкі або стандартні паролі, неправильні конфігурації, відкриті порти, незахищені протоколи, недостатня сегментація мережі та відсутність належного моніторингу.

Також визначено, що людський фактор є одним із важливих джерел вразливостей. Помилки користувачів і адміністраторів, низька обізнаність з питань кібербезпеки, використання слабких паролів, відкриття фішингових повідомлень або несвоєчасне реагування на інциденти можуть суттєво знижувати рівень захищеності мережі.

При виконанні оцінки ризиків найбільш небезпечними є загрози з високою ймовірністю реалізації та значним впливом на конфіденційність, цілісність і

доступність інформації. Наслідки реалізації загроз можуть бути технічними, інформаційними, фінансовими, організаційними, правовими та репутаційними.

3 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

3.1 Організаційні заходи забезпечення безпеки

Захист мереж електронних комунікацій не може базуватися лише на технічних засобах, оскільки значна частина загроз виникає через неправильну організацію процесів, недостатній контроль доступу, відсутність регламентів, помилки персоналу або несвоєчасне реагування на інциденти. Тому організаційні заходи є основою системи кіберзахисту та визначають порядок управління інформаційною безпекою на рівні підприємства, установи або оператора електронних комунікацій.

Організаційні заходи забезпечення безпеки — це комплекс правил, процедур, політик, розподілу відповідальності та управлінських рішень, спрямованих на зменшення ризиків порушення конфіденційності, цілісності та доступності інформації. У сфері електронних комунікацій такі заходи особливо важливі, оскільки мережі забезпечують передавання даних, голосового трафіку, службової інформації, сигналізації, даних користувачів і керувальних команд. Порушення роботи таких мереж може спричинити не лише втрату інформації, а й зупинку сервісів, фінансові втрати, витік персональних даних або порушення роботи критичної інфраструктури.

В Україні питання захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах регулюється Законом України «Про захист інформації в інформаційно-комунікаційних системах» [5]. Цей закон визначає загальні правові засади захисту інформації в системах, де вона обробляється, передається або зберігається. Також важливим є Закон України «Про основні засади забезпечення кібербезпеки України» [6], який визначає основні напрями державної політики у сфері кібербезпеки та роль суб'єктів, відповідальних за кіберзахист. Зокрема, Державна служба спеціального зв'язку та захисту інформації України здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту.

Організаційна система захисту має будуватися на принципі безперервного управління ризиками. Цей підхід формалізовано в актуальній моделі NIST Cybersecurity Framework 2.0 [28], де життєвий цикл кібербезпеки визначається шістьма ключовими функціями: Govern (Управління), Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування) та Recover (Відновлення). До основних організаційних заходів забезпечення безпеки мереж електронних комунікацій належать: розроблення політики інформаційної безпеки, визначення правил доступу до мережевих ресурсів, призначення відповідальних осіб, навчання персоналу, ведення журналів подій, організація резервного копіювання, проведення аудитів, контроль змін у конфігураціях обладнання, регламентація роботи з інцидентами та періодична оцінка ризиків.

Політика інформаційної безпеки є базовим документом, який визначає правила використання інформаційних ресурсів, порядок доступу до мережі, вимоги до паролів, правила роботи з електронною поштою, хмарними сервісами, віддаленим доступом, мобільними пристроями та зовнішніми носіями.

Важливим елементом організаційного захисту є розмежування прав доступу. Кожен користувач або адміністратор повинен мати лише ті права, які необхідні для виконання його функцій. Такий підхід називається принципом мінімальних привілеїв. Наприклад, звичайний користувач не повинен мати доступу до налаштувань маршрутизаторів або серверів, а системний адміністратор не повинен використовувати обліковий запис із максимальними правами для щоденної роботи. Для критичних дій доцільно застосовувати багатофакторну автентифікацію, журнали аудиту та погодження змін.

Не менш важливим є навчання персоналу. Людський фактор залишається одним із найпоширеніших джерел вразливостей, оскільки користувачі можуть відкривати фішингові листи, переходити за небезпечними посиланнями, використовувати слабкі паролі, передавати службову інформацію стороннім особам або неправильно працювати з конфіденційними даними.

Основні організаційні заходи захисту наведено в табл. 3.1.

Таблиця 3.1 — Основні організаційні заходи захисту мереж електронних комунікацій

Організаційний захід	Призначення	Очікуваний результат
Політика інформаційної безпеки	Визначення правил захисту інформації та мережевих ресурсів	Єдині вимоги до користувачів і адміністраторів
Розмежування прав доступу	Надання користувачам лише необхідних повноважень	Зменшення ризику несанкціонованого доступу
Навчання персоналу	Формування навичок безпечної роботи	Зменшення впливу людського фактора
Управління інцидентами	Регламентація дій у разі атаки або збою	Швидке реагування та мінімізація наслідків
Резервне копіювання	Збереження критичних даних і конфігурацій	Можливість відновлення після інциденту
Аудит безпеки	Перевірка відповідності політикам і стандартам	Виявлення слабких місць у системі захисту
Контроль змін	Облік змін у конфігураціях обладнання	Запобігання помилкам адміністрування

3.2 Технічні засоби захисту: Firewall, IDS/IPS, VPN, SIEM

Технічні засоби захисту є практичним інструментом реалізації політики кібербезпеки. Якщо організаційні заходи визначають правила та відповідальність, то технічні засоби забезпечують фактичне обмеження доступу, фільтрацію трафіку, виявлення атак, шифрування передавання даних, моніторинг подій і

реагування на інциденти. У мережах електронних комунікацій технічний захист повинен бути багаторівневим, оскільки атака може бути спрямована на різні компоненти: кінцеві пристрої, сервери, маршрутизатори, бездротові сегменти, канали зв'язку, хмарні сервіси або системи адміністрування.

Сучасний підхід до захисту мереж базується на принципі *defense in depth*, тобто багаторівневого захисту. Його суть полягає в тому, що навіть у разі обходу одного механізму безпеки інші рівні повинні продовжувати захищати систему. Наприклад, якщо зломисник отримав пароль користувача, його дії можуть бути обмежені багатофакторною автентифікацією, сегментацією мережі, журналюванням, SIEM-кореляцією подій і правилами доступу на міжмережевому екрані.

Одним із базових технічних засобів є міжмережевий екран, або Firewall. Його основне призначення — фільтрація мережевого трафіку між різними сегментами мережі відповідно до заданих правил. Firewall може обмежувати доступ за IP-адресами, портами, протоколами, напрямом з'єднання, типом додатка або станом сесії. У телекомунікаційних мережах міжмережеві екрани застосовуються для захисту периметра, ізоляції внутрішніх сегментів, контролю доступу до серверів, захисту DMZ-зони та обмеження несанкціонованого трафіку.

Системи виявлення та запобігання вторгненням (IDS/IPS)

Для забезпечення глибокого аналізу трафіку (Deep Packet Inspection) у мережах електронних комунікацій застосовуються системи виявлення (IDS) та запобігання (IPS) вторгненням. Незважаючи на спільну мету — ідентифікацію шкідливої активності на основі сигнатур, аномалій або евристичного аналізу — ці системи мають принципові архітектурні та функціональні відмінності.

Система виявлення вторгнень (Intrusion Detection System — IDS) є пасивним компонентом безпеки. Вона отримує копію мережевого трафіку (наприклад, через SPAN-порт комутатора або апаратний Network TAP), аналізує його та генерує сповіщення для адміністратора. Основна перевага IDS полягає в тому, що вона працює паралельно (*out-of-band*), не створює затримок у передачі даних і не

впливає на доступність мережі в разі власного збою. Проте IDS не здатна самостійно заблокувати атаку.

Система запобігання вторгненням (Intrusion Prevention System — IPS) працює в активному режимі (inline) і пропускає весь трафік безпосередньо через себе. У разі виявлення аномалії (спроби експлуатації вразливостей, сканування портів, DDoS-атаки) IPS автоматично скидає шкідливі пакети та розриває з'єднання. Головним недоліком такого підходу є ризик блокування легітимного трафіку (False Positives) та те, що IPS може стати точкою відмови (Single Point of Failure), тому вимагає налаштування механізмів апаратного обходу (Bypass).

Топологія розміщення цих систем залежить від їхнього режиму роботи. IPS зазвичай розгортається на периметрі мережі безпосередньо за міжмережевим екраном (Firewall) або перед демілітаризованою зоною (DMZ) із критично важливими сервісами. IDS доцільно розташовувати глибше у внутрішній мережі біля рівня ядра (Core layer) для моніторингу внутрішнього трафіку (East-West traffic) і виявлення активності шкідливого ПЗ, яке вже пододало периметр.

Детальна порівняльна характеристика рішень наведена в табл. 3.2

Таблиця 3.2 — Основні організаційні заходи захисту мереж електронних комунікацій

Характеристика	IDS (Система виявлення)	IPS (Система запобігання)
Режим роботи	Пасивний (Out-of-band)	Активний (Inline)
Реакція на загрозу	Аналіз копії трафіку, генерація сповіщень	Аналіз «на льоту», автоматичне блокування
Вплив на мережу	Не створює затримок (Zero latency)	Вносить затримку обробки; є точкою відмови
Переваги	Безпека при апаратних збоях самої системи; відсутність впливу на пропускну здатність	Миттєве реагування на інциденти; зниження навантаження на адміністраторів
Недоліки	Не зупиняє атаку в реальному часі	Ризик блокування легітимного трафіку; складність розгортання

Важливим технічним засобом захисту є VPN, тобто віртуальна приватна мережа. VPN забезпечує захищений канал передавання даних через незахищене середовище, наприклад Інтернет. У такому каналі дані шифруються, а користувачі або пристрої проходять автентифікацію. VPN широко використовується для віддаленої роботи, підключення філій, адміністрування мережевого обладнання, захищеного доступу до внутрішніх сервісів і передавання службової інформації.

Для організацій електронних комунікацій VPN має особливе значення, оскільки адміністрування обладнання часто здійснюється віддалено. Без захищеного каналу існує ризик перехоплення облікових даних, несанкціонованого доступу до інтерфейсів керування або втручання в конфігурацію мережі. Тому доступ до маршрутизаторів, комутаторів, серверів і систем моніторингу повинен здійснюватися лише через захищені канали, бажано з багатофакторною автентифікацією та журналюванням усіх дій адміністратора.

Ще одним важливим компонентом є SIEM — система керування інформацією та подіями безпеки, що застосовується в операційних центрах кібербезпеки SOC (Security Operations Center) організацій і підприємств. SIEM збирає журнали подій із різних джерел: серверів, робочих станцій, мережевого обладнання, Firewall, IDS/IPS, VPN, антивірусів, систем автентифікації та хмарних сервісів. Потім система виконує нормалізацію, кореляцію та аналіз подій. Основна перевага SIEM полягає в тому, що вона дозволяє бачити загальну картину безпеки, а не окремі ізольовані повідомлення.

Наприклад, окрема невдала спроба входу може не бути критичною. Але якщо SIEM виявляє десятки невдалих спроб входу з різних IP-адрес, потім успішний вхід, після цього підключення до внутрішнього сервера та завантаження великого обсягу даних, така послідовність може свідчити про компрометацію облікового запису. Саме тому SIEM є важливим інструментом для центрів моніторингу безпеки та служб реагування на інциденти.

Особливу увагу при проектуванні захищеної інфраструктури слід приділяти сегментації мережі. Її суть полягає у фізичному або логічному поділі єдиного адресного простору на ізольовані зони безпеки (користувацькі підмережі, DMZ,

сегмент управління, IoT). Технічно логічна сегментація на каналному рівні (L2) реалізується за допомогою віртуальних локальних мереж (VLAN) згідно зі стандартом IEEE 802.1Q, а на мережевому (L3) — шляхом розподілу IP-підмереж та використання технологій віртуальної маршрутизації (VRF). Такий підхід мінімізує поверхню атаки та унеможливорює безперешкодний горизонтальний рух (lateral movement) зломисника: компрометація користувацького комп'ютера не дасть йому прямого доступу до серверного сегмента.

Для контролю взаємодії між створеними сегментами критично важливим засобом забезпечення кібербезпеки є фільтрація трафіку. Базовим інструментом такої фільтрації на маршрутизаторах та комутаторах рівня ядра (L3) є списки контролю доступу (ACL — Access Control Lists). Застосування розширених ACL дозволяє адміністраторам гнучко керувати потоками даних, блокуючи (deny) або дозволяючи (permit) пакети на основі IP-адрес джерела і призначення, транспортних протоколів (TCP/UDP) та номерів портів. Наприклад, саме за допомогою ACL реалізується політика, за якої з користувацької мережі дозволено лише HTTP/HTTPS-трафік до вебсерверів, а доступ до інтерфейсів адміністрування (SSH) заблоковано для всіх, крім виділеного сегмента управління.

Технічні засоби захисту мають працювати узгоджено. Firewall блокує небажаний трафік, IDS/IPS аналізує підозрілі дії, VPN забезпечує захищене з'єднання, SIEM збирає події та формує сповіщення, EDR (Endpoint Detection and Response) — система виявлення та реагування на загрози на кінцевих точках (тобто на комп'ютерах, серверах, мобільних пристроях) контролює кінцеві пристрої, а резервне копіювання забезпечує відновлення після інциденту. Саме поєднання цих засобів дозволяє створити комплексну систему захисту, яка відповідає сучасним вимогам кібербезпеки.

3.3 Методи виявлення та усунення вразливостей

У контексті телекомунікаційної інфраструктури вразливості розглядаються як комплексні архітектурні та конфігураційні недоліки, що дозволяють зловмисникам реалізувати описані раніше вектори атак. Для уніфікованої класифікації та оцінки таких недоліків доцільно використовувати відкритий стандарт CVSS (Common Vulnerability Scoring System). Згідно з цією метрикою, найбільш критичними для мереж електронних комунікацій є вразливості, що мають віддалений вектор експлуатації (Network Vector) і не вимагають попередньої автентифікації. Переважно вони зумовлені використанням застарілих мережових протоколів без нативної підтримки криптографічного захисту, а також недоліками в конфігурації активного мережевого обладнання. Методи виявлення та усунення вразливостей є одним із ключових напрямів забезпечення безпеки мережі. Вони дозволяють не чекати фактичної атаки, а заздалегідь знаходити слабкі місця та зменшувати ймовірність їх використання. Сучасні звіти ENISA [13] підкреслюють, що загрозові групи активно використовують вразливості, повторно застосовують інструменти атак і адаптують нові моделі атак проти цифрової інфраструктури. Це підтверджує необхідність регулярного виявлення, оцінювання та усунення вразливостей у мережах електронних комунікацій.

Процес роботи з вразливостями доцільно розглядати як життєвий цикл. Він починається з інвентаризації активів, тобто визначення всіх пристроїв, серверів, сервісів, програм, користувачів і мережових сегментів. Неможливо захистити те, що не обліковано. Тому організація повинна мати актуальний перелік обладнання, IP-адрес, версій програмного забезпечення, відповідальних осіб і критичності кожного ресурсу.

Першим практичним методом є сканування вразливостей. Воно виконується за допомогою спеціалізованих інструментів, які перевіряють мережеві вузли, відкриті порти, версії сервісів, відомі вразливості, слабкі конфігурації та наявність оновлень. Сканування може бути зовнішнім і внутрішнім. Зовнішнє сканування показує, які ресурси доступні з Інтернету, а внутрішнє — які ризики існують

усередині мережі. Для телекомунікаційної інфраструктури важливо проводити обидва типи перевірок, оскільки атаки можуть починатися як ззовні, так і з внутрішнього скомпрометованого пристрою.

Другим методом є аналіз конфігурацій мережевого обладнання. Неправильні налаштування часто є не менш небезпечними, ніж програмні помилки. Наприклад, небезпечними є відкритий доступ до адміністративних інтерфейсів із зовнішньої мережі, використання стандартних паролів, відсутність обмеження доступу за IP-адресами, незашифровані протоколи адміністрування, зайві VLAN, неправильні ACL, відсутність журналювання або використання застарілих протоколів. Тому конфігурації маршрутизаторів, комутаторів, Firewall і VPN-шлюзів повинні регулярно перевірятися.

Третім методом є аналіз журналів подій. Лог-файли дозволяють виявити підозрілу активність, навіть якщо вона не була заблокована автоматично. До таких ознак належать багаторазові невдалі спроби входу, підключення з нетипових IP-адрес, зміна конфігурації обладнання, створення нових облікових записів, нетипова передача даних, помилки автентифікації, сканування портів, зміни в правилах Firewall або відключення служб моніторингу. Найефективніше такий аналіз виконувати через SIEM, оскільки вручну обробляти велику кількість журналів складно.

Четвертим методом є тестування на проникнення, або penetration testing. На відміну від автоматичного сканування, тестування на проникнення передбачає імітацію дій зловмисника з метою перевірки реального рівня захищеності системи. Воно може включати перевірку зовнішнього периметра, вебдодатків, бездротової мережі, внутрішніх сегментів, облікових записів і процедур реагування. Результатом такого тестування є звіт із виявленими вразливостями, рівнем критичності та рекомендаціями щодо усунення.

П'ятим методом є аудит безпеки. Він може бути внутрішнім або зовнішнім. Внутрішній аудит проводиться силами організації, а зовнішній — незалежними спеціалістами. Аудит дозволяє перевірити відповідність системи захисту політикам, стандартам, законодавчим вимогам і найкращим практикам. Для

систем управління інформаційною безпекою часто використовується підхід ISO/IEC 27001 [18]. В Україні національна версія стандарту ДСТУ ISO/IEC 27001:2023 [2] стосується систем керування інформаційною безпекою та встановлює вимоги до їх побудови.

Після виявлення вразливостей необхідно виконати їх оцінку. Не всі вразливості мають однаковий рівень небезпеки. Наприклад, критична вразливість на сервері, доступному з Інтернету, має вищий пріоритет, ніж низькоризикова помилка на ізольованому тестовому пристрої. Для визначення пріоритетів враховують критичність активу, можливість експлуатації, наявність публічного експлойта, доступність системи з Інтернету, потенційні наслідки та наявність компенсуючих заходів захисту.

Іншим способом усунення є зміна конфігурації. Наприклад, можна закрити зайві порти, вимкнути небезпечні протоколи, обмежити доступ до адміністративних інтерфейсів, змінити стандартні паролі, увімкнути шифрування, налаштувати ACL, сегментувати мережу або посилити правила Firewall. У деяких випадках повністю усунути вразливість неможливо одразу, тому застосовуються компенсуючі заходи: обмеження доступу, посилений моніторинг, ізоляція системи, використання IPS-сигнатур або тимчасове відключення небезпечної функції.

Окремим напрямом є документування процесу усунення. Для кожної виявленої вразливості доцільно фіксувати дату виявлення, джерело інформації, уражений актив, рівень критичності, відповідального виконавця, заплановані дії, дату усунення та результат повторної перевірки. Такий підхід дозволяє контролювати стан безпеки та демонструвати виконання вимог під час аудиту.

Після усунення вразливості обов'язково проводиться повторна перевірка. Вона підтверджує, що проблема справді усунена, а зміни не створили нових ризиків. Наприклад, після оновлення VPN-сервера потрібно перевірити, чи збереглися правила доступу, чи працює автентифікація, чи не відкрилися зайві порти та чи фіксуються події в журналах.

Таким чином, методи виявлення та усунення вразливостей повинні застосовуватися системно. Найкращий результат досягається тоді, коли організація поєднує інвентаризацію активів, регулярне сканування, аудит конфігурацій, аналіз журналів, тестування на проникнення, пріоритезацію ризиків, своєчасне оновлення та повторну перевірку. Для мереж електронних комунікацій це особливо важливо, оскільки їх стабільність і безпека безпосередньо впливають на доступність цифрових сервісів, передавання даних і безперервність роботи користувачів.

3.4 Побудова системи управління інформаційною безпекою

Побудова системи управління інформаційною безпекою є одним із ключових етапів захисту мереж електронних комунікацій. Якщо окремі технічні засоби, такі як Firewall, IDS/IPS, VPN або SIEM, виконують конкретні функції захисту, то система управління інформаційною безпекою забезпечує цілісний підхід до організації, контролю, оцінювання та постійного вдосконалення безпеки. Така система дозволяє не лише реагувати на вже виявлені інциденти, а й попереджати їх виникнення шляхом управління ризиками, розподілу відповідальності, документування процедур і регулярного моніторингу стану захищеності.

Система управління інформаційною безпекою, або СУІБ, — це сукупність політик, процедур, організаційних рішень, технічних засобів, ролей персоналу та механізмів контролю, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. У міжнародній практиці основою для побудови СУІБ є стандарт ISO/IEC 27001 [18]. Він визначає вимоги до системи управління інформаційною безпекою та може застосовуватися організаціями різного розміру й сфери діяльності.

Для мереж електронних комунікацій побудова СУІБ має особливе значення, оскільки такі мережі забезпечують передавання великого обсягу даних, роботу сервісів зв'язку, доступ до Інтернету, функціонування корпоративних і державних

інформаційних систем. Порушення безпеки такої інфраструктури може призвести до витоку даних, відмови сервісів, несанкціонованого доступу, поширення шкідливого програмного забезпечення, фінансових втрат і зниження довіри користувачів.

Основною метою побудови СУІБ є створення керованої системи захисту, у межах якої всі процеси інформаційної безпеки мають чітке призначення, відповідальних осіб, порядок виконання та критерії оцінювання ефективності. Приклад класифікації активів для такої системи наведено в табл. 3.2.

Таблиця 3.2 — Приклад класифікації активів мережі електронних комунікацій

Група активів	Приклади	Рівень критичності	Основні ризики
Мережеве обладнання	Маршрутизатори, комутатори, Firewall	Високий	Зміна конфігурації, відмова мережі, перехоплення трафіку
Сервери	DNS, DHCP, VPN, SIEM, сервери автентифікації	Високий	Несанкціонований доступ, витік даних, зупинка сервісів
Кінцеві пристрої	ПК користувачів, ноутбуки адміністраторів	Середній/високий	Шкідливе ПЗ, фішинг, компрометація акаунтів
Дані та конфігурації	Бази даних, резервні копії, конфігурації обладнання	Високий	Втрата, зміна або несанкціоноване копіювання
Облікові записи	Користувацькі та адміністративні акаунти	Високий	Підбір паролів, крадіжка облікових даних
Документація	Схеми мережі, регламенти, інструкції	Середній	Розкриття внутрішньої структури мережі

Після інвентаризації активів виконується оцінювання ризиків. Ризик у сфері інформаційної безпеки можна розглядати як імовірність реалізації певної загрози

через наявну вразливість із подальшими негативними наслідками для організації. Наприклад, якщо VPN-сервер має застарілу версію програмного забезпечення, а доступ до нього відкритий з Інтернету, існує ризик його компрометації. Якщо цей VPN-сервер використовується адміністраторами для доступу до критичної інфраструктури, наслідки такого ризику можуть бути значними.

Оцінка ризиків може здійснюватися якісним або кількісним способом. У якісному підході рівень ризику визначається як низький, середній, високий або критичний. У кількісному підході можуть використовуватися числові показники ймовірності та можливих втрат.

Для оцінювання ризиків інформаційної безпеки в мережах електронних комунікацій застосовуються якісний та кількісний підходи. Кожен із них має свою специфіку та обирається залежно від наявності статистичних даних і вимог до точності.

Якісний підхід базується на експертній оцінці та використанні відносних шкал (наприклад, «Низький», «Середній», «Високий», «Критичний»). Він є зручним для швидкого ранжування загроз.

Приклад оцінки: Розглядається ризик компрометації облікових даних адміністратора мережі через фішинг. Ймовірність реалізації загрози експертно оцінюється як «Висока» (через часті спроби атак), а рівень впливу на інфраструктуру — як «Критичний» (зловмисник отримає повний доступ до маршрутизаторів ядра). За матрицею ризиків загальний рівень загрози, який визначається як комбінація ймовірності та наслідків, класифікується як «Критичний». Це вказує на необхідність негайного впровадження багатофакторної автентифікації (MFA).

Кількісний підхід оперує точними фінансовими показниками. Базовими метриками тут є очікувані втрати від одного інциденту та статистика його виникнення протягом року. Завдяки цьому можна спрогнозувати сумарні потенційні збитки в річному вимірі.

Після оцінювання ризиків формується план їх обробки. Для кожного ризику організація може обрати один із варіантів: зменшити ризик шляхом впровадження

захисних заходів, прийняти ризик, уникнути ризику або передати його. У сфері електронних комунікацій найчастіше використовується саме зменшення ризику, тобто впровадження технічних, організаційних і процедурних контролів. Наприклад, ризик несанкціонованого доступу до адміністративного інтерфейсу маршрутизатора можна зменшити через VPN, ACL, багатофакторну автентифікацію, зміну стандартних портів, журналювання та обмеження доступу лише з визначених IP-адрес.

Важливою частиною СУІБ є розроблення документації. До основних документів належать політика інформаційної безпеки, політика управління доступом, політика резервного копіювання, політика використання паролів, регламент реагування на інциденти, інструкція для адміністраторів, інструкція для користувачів, план відновлення після аварій, порядок управління змінами, порядок проведення аудиту та порядок роботи з вразливостями.

Документація повинна бути не лише формальною, а й реально застосовуваною. Наприклад, якщо в політиці зазначено, що резервне копіювання виконується щоденно, то має бути визначено, хто це контролює, де зберігаються копії, як перевіряється їх цілісність, як часто проводиться тестове відновлення та хто відповідає за відновлення у разі інциденту.

Для ефективного реагування на інциденти необхідно визначити рівні критичності подій. Наприклад, невдала спроба входу одного користувача може бути подією низького рівня, тоді як масові спроби входу до VPN із різних країн, виявлення шкідливого ПЗ на сервері або зміна правил Firewall без погодження можуть мати високий або критичний рівень. У методичних рекомендаціях щодо реагування на події в кіберпросторі [7] зазначено, що за потреби суб'єкти забезпечення кібербезпеки можуть звертатися за допомогою до CERT-UA, команд реагування або організацій, які надають послуги у сфері кіберзахисту.

Функція Govern відповідає за управління ризиками, політики, відповідальність і контроль на рівні організації. Identify передбачає визначення активів, загроз, залежностей і ризиків. Protect охоплює заходи захисту, зокрема контроль доступу, навчання персоналу, шифрування, резервне копіювання та

технічні засоби безпеки. Detect зосереджується на виявленні аномалій, моніторингу подій і роботі SIEM. Respond визначає порядок реагування на інциденти, а Recover — процеси відновлення сервісів після порушення.

Для мереж електронних комунікацій така модель є практичною, оскільки дозволяє пов'язати організаційні й технічні заходи в єдину структуру. Наприклад, інвентаризація маршрутизаторів і серверів належить до Identify, налаштування Firewall і VPN — до Protect, аналіз журналів SIEM — до Detect, ізоляція скомпрометованого сегмента — до Respond, а відновлення конфігурації з резервної копії — до Recover.

Побудова СУІБ повинна передбачати постійне вдосконалення. Загрози змінюються, з'являються нові вразливості, оновлюється програмне забезпечення, змінюється склад персоналу та структура мережі. Тому система безпеки не може залишатися незмінною. Потрібно регулярно переглядати політики, проводити аудит, оновлювати правила Firewall, перевіряти резервні копії, проводити навчання персоналу, аналізувати інциденти та впроваджувати нові засоби захисту.

Планування реагування на інциденти та відновлення

Невіддільним організаційним заходом забезпечення кібербезпеки в мережах електронних комунікацій є розробка та впровадження регламентованих процедур дій в умовах реалізації кібератак. Відповідно до базових принципів управління інцидентами, політика безпеки організації повинна обов'язково включати два ключові документи:

План реагування на інциденти кібербезпеки (IRP — Incident Response Plan). Цей документ визначає алгоритм дій технічного персоналу під час активної фази атаки. Він регламентує процеси локалізації загрози (наприклад, ізоляція скомпрометованого VLAN-сегмента на комутаторах), нейтралізації шкідливого впливу та збирання цифрових доказів (Forensics). Наявність IRP дозволяє мінімізувати час перебування зловмисника в інфраструктурі (Dwell Time) та уникнути хаотичних дій адміністраторів під час стресової ситуації.

План відновлення після катастроф (DRP — Disaster Recovery Plan). На відміну від IRP, який фокусується на зупинці атаки, DRP спрямований на

забезпечення безперервності бізнес-процесів і відновлення працездатності критичних мережевих сервісів після їхньої зупинки. Розробка DRP базується на двох критичних метриках: цільовому часі відновлення (RTO — Recovery Time Objective, тобто максимально допустимий час простою мережі) та цільовій точці відновлення (RPO — Recovery Point Objective, максимально допустимий обсяг втрачених даних).

3.5 Рекомендації щодо підвищення рівня захищеності мереж

Підвищення рівня захищеності мереж електронних комунікацій має здійснюватися комплексно, з урахуванням організаційних, технічних, кадрових і процедурних аспектів. Недостатньо встановити лише міжмережевий екран або антивірусне програмне забезпечення, оскільки сучасні кібератаки часто поєднують технічні методи, соціальну інженерію, використання вразливостей, викрадення облікових даних і приховане переміщення всередині мережі. Тому рекомендації мають бути спрямовані на створення багаторівневої системи захисту.

1-ю рекомендацією є впровадження ризик-орієнтованого підходу до кібербезпеки. Організація повинна визначити найбільш критичні активи, оцінити можливі загрози та встановити пріоритети захисту. Наприклад, сервери автентифікації, VPN-шлюзи, SIEM, маршрутизатори ядра мережі та системи резервного копіювання мають вищу критичність, ніж звичайні робочі станції. Саме тому їхній захист повинен бути посиленним.

2-ю рекомендацією є впровадження суворої сегментації мережі з використанням механізмів ізоляції на каналному (L2) та мережевому (L3) рівнях моделі OSI. Технічно внутрішню інфраструктуру доцільно розділити на ізольовані широкомовні домени — віртуальні локальні мережі (VLAN) відповідно до стандарту IEEE 802.1Q, кожній з яких виділяється окрема IP-підмережа. Відповідно до цього підходу формуються такі логічні зони: користувацька мережа, серверний сегмент, гостьова мережа, DMZ, ізольована мережа

адміністрування (Out-of-Band Management), сегменти IoT-пристроїв і відеоспостереження, а також резервна інфраструктура.

Для контролю взаємодії між цими зонами механізмом фільтрації виступають списки контролю доступу (ACL) на маршрутизаторах рівня ядра або політики безпеки на міжмережевих екранах наступного покоління (NGFW). Налаштування цих правил має базуватися на принципі «заборонити все за замовчуванням» (Implicit Deny), дозволяючи виключно той трафік (на рівні конкретних IP-адрес та TCP/UDP портів), який є критично необхідним для функціонування сервісів. Такий бар'єрний підхід унеможливорює несанкціонований горизонтальний рух (lateral movement) у мережі та локалізує загрозу в межах одного сегмента у разі компрометації кінцевого пристрою.

3-ю рекомендацією є посилення контролю доступу. Для всіх користувачів необхідно застосовувати унікальні облікові записи, складні паролі або парольні фрази, політику блокування після багаторазових невдалих спроб входу та регулярний перегляд прав доступу.

4-ю рекомендацією є оновлення програмного забезпечення та керування вразливостями. Необхідно регулярно перевіряти наявність оновлень для операційних систем, серверів, мережевого обладнання, Firewall, VPN, IDS/IPS, SIEM, вебдодатків і систем керування. Вразливості потрібно пріоритизувати за критичністю, доступністю активу з Інтернету та можливими наслідками. Особливу увагу слід приділяти обладнанню, яке має відкриті мережеві сервіси або використовується для віддаленого доступу.

5-ю рекомендацією є впровадження централізованого моніторингу. Події з маршрутизаторів, комутаторів, серверів, Firewall, VPN, IDS/IPS, антивірусних систем і контролерів домену потрібно передавати до SIEM або іншої системи аналізу журналів. Це дозволяє швидко виявляти підозрілу активність, наприклад масові невдалі спроби входу, зміну конфігурацій, появу нових облікових записів, підозрілий трафік або нетипову активність користувачів.

6-ю рекомендацією є захист віддаленого доступу. У сучасних умовах віддалене адміністрування та дистанційна робота стали звичними, однак саме

віддалений доступ часто є ціллю атак. Тому підключення до внутрішньої мережі має здійснюватися лише через захищені VPN-канали з багатофакторною автентифікацією. Доступ до адміністративних інтерфейсів мережевого обладнання не повинен бути відкритим безпосередньо з Інтернету. Усі дії адміністраторів мають журналюватися.

7-ю рекомендацією є впровадження комплексної стратегії резервного копіювання та забезпечення безперервності роботи інфраструктури. З метою нівелювання загроз втрати даних (зокрема через деструктивні дії програм-вимагачів або апаратні збої), резервні копії повинні охоплювати не лише файли користувачів, а й повні конфігурації мережевого обладнання, бази даних, журнали подій (logs), налаштування серверів та політики безпеки. Організація зберігання даних має суворо спиратися на архітектурний принцип «3-2-1»: створення трьох копій даних, використання двох різних типів носіїв, при цьому щонайменше одна копія повинна зберігатися фізично або логічно ізольовано від основної мережі (Air-Gapped Backup). Крім того, критично важливим є регламентоване проведення тестового відновлення (Disaster Recovery Testing), оскільки лише верифікована копія здатна гарантувати відновлення працездатності мережі.

8-ю рекомендацією є впровадження безперервної програми підвищення обізнаності персоналу з питань інформаційної безпеки (Security Awareness Program). Людський фактор залишається однією з найкритичніших вразливостей мережевої інфраструктури: ефективність найсучасніших апаратних засобів захисту нівелюється, якщо користувачі порушують парольні політики, ігнорують регламенти безпеки або стають жертвами методів соціальної інженерії.

З огляду на постійну еволюцію кіберзагроз, навчання має проводитися на регулярній основі (наприклад, у форматі обов'язкових щорічних курсів та щоквартальних інструктажів). Програма повинна роз'яснювати алгоритми розпізнавання цілеспрямованого фішингу, правила безпечної обробки вкладень та процедури оперативного інформування про підозрілі інциденти. Окрім теоретичної підготовки, обов'язковим елементом є систематичне тестування практичних знань працівників. Технічно це реалізується шляхом запуску

контрольованих імітованих фішингових атак (Phishing Simulations) та проведення автоматизованого зрізу знань. Такий підхід дозволяє об'єктивно оцінити рівень кібергігієни в організації та своєчасно виявляти співробітників, які потребують додаткового навчання.

9-ю рекомендацією є проведення періодичного аудиту безпеки. Аудит має охоплювати перевірку правил Firewall, налаштувань VPN, актуальності облікових записів, відкритих портів, версій програмного забезпечення, конфігурацій маршрутизаторів і комутаторів, стану резервного копіювання, наявності журналів подій і виконання політик безпеки. Результати аудиту потрібно оформлювати у вигляді звіту з переліком недоліків, рівнем критичності та строками усунення.

10-ю рекомендацією є розроблення та перевірка плану реагування на інциденти. CERT-UA у своїх рекомендаціях [8] звертає увагу на важливість плану реагування, зокрема на випадок необхідності ізоляції сегментів мережі, а також на необхідність налагодженої оперативної взаємодії під час кібератак. Тому в організації має бути визначено, хто приймає рішення про ізоляцію сегмента, хто відповідає за технічне відновлення, хто повідомляє керівництво, хто контактує із зовнішніми фахівцями та як документуються дії під час інциденту.

11-ю рекомендацією є впровадження принципу Zero Trust для критичних ресурсів. Його сутність полягає в тому, що жоден користувач, пристрій або сервіс не вважається довіреним автоматично, навіть якщо він знаходиться всередині корпоративної мережі. Кожен доступ повинен перевірятися, автентифікуватися та обмежуватися відповідно до ролі користувача, стану пристрою й рівня ризику. Для мереж електронних комунікацій цей підхід є особливо корисним, оскільки дозволяє зменшити ризик внутрішнього переміщення зловмисника після компрометації одного вузла.

12-ю рекомендацією є захист IoT-пристроїв та допоміжного обладнання. У багатьох мережах електронних комунікацій використовуються камери відеоспостереження, датчики, контролери доступу, системи моніторингу, бездротові точки доступу та інші пристрої, які часто мають обмежені можливості захисту. Такі пристрої потрібно розміщувати в окремому сегменті мережі,

змінювати стандартні паролі, регулярно оновлювати прошивки, обмежувати доступ до них і контролювати їхню активність.

13-ю рекомендацією є захист DNS (Domain Name System) — система доменних імен, електронної пошти та вебресурсів. DNS є критичним сервісом для роботи мережі, тому його потрібно захищати від несанкціонованих змін, підміни записів і DDoS-атак. Електронна пошта повинна мати фільтрацію спаму, антивірусну перевірку вкладень, захист від фішингу та налаштування SPF (Sender Policy Framework) — інфраструктура політик відправника, DKIM (DomainKeys Identified Mail) — пошта, ідентифікована доменними ключами і DMARC (Domain-based Message Authentication, Reporting, and Conformance) — доменна автентифікація повідомлень, звітування та відповідність. Вебресурси доцільно захищати за допомогою WAF (Web Application Firewall) — міжмережевий екран для вебдодатків, регулярного оновлення CMS (Content Management System) — система управління контентом., контролю доступу та сканування вразливостей.

14-ю рекомендацією є контроль змін у мережевій інфраструктурі. Будь-які зміни в конфігураціях маршрутизаторів, комутаторів, Firewall — міжмережевий екран, VPN (Virtual Private Network) — віртуальна приватна мережа, серверів або систем моніторингу повинні погоджуватися, документуватися та перевірятися. Це дозволяє уникнути ситуацій, коли помилка адміністратора відкриває небезпечний порт, вимикає журналювання або порушує роботу критичного сервісу.

15-ю рекомендацією є оцінювання ефективності впроваджених заходів. Для цього можна використовувати показники: кількість виявлених і усунених вразливостей, середній час реагування на інцидент, кількість невдалих спроб входу, кількість фішингових листів, відсоток пристроїв з актуальними оновленнями, успішність резервного відновлення, кількість незакритих критичних ризиків. Такі показники дозволяють не лише контролювати стан безпеки, а й обґрунтовувати необхідність додаткових ресурсів.

Таким чином, підвищення рівня захищеності мереж електронних комунікацій повинно базуватися на поєднанні технічних рішень, організаційних правил, постійного моніторингу та регулярного вдосконалення.

3.6 Висновки до розділу 3

У третьому розділі було розглянуто основні методи та засоби захисту мереж електронних комунікацій. Визначено, що ефективна система безпеки має поєднувати організаційні, технічні та процедурні заходи.

Організаційні заходи забезпечують розроблення політик безпеки, розподіл відповідальності, управління доступом, навчання персоналу та планування реагування на інциденти. Технічні засоби, зокрема Firewall, IDS/IPS, VPN, SIEM, EDR, WAF і системи резервного копіювання, дозволяють контролювати трафік, виявляти атаки, захищати віддалений доступ і забезпечувати відновлення після збоїв.

Окрему увагу приділено методам виявлення та усунення вразливостей, серед яких інвентаризація активів, сканування, аудит конфігурацій, аналіз журналів подій, тестування на проникнення та регулярне оновлення систем. Також розглянуто побудову системи управління інформаційною безпекою, яка дозволяє комплексно керувати ризиками, інцидентами та процесами захисту.

За результатами проведеного аналізу сформовано комплекс практичних рекомендацій щодо підвищення рівня захищеності мереж електронних комунікацій. Серед ключових заходів доцільно виокремити такі:

Логічна сегментація мережевої інфраструктури (із застосуванням VLAN та списків контролю доступу ACL) для локалізації загроз та обмеження горизонтального переміщення злоумисників.

Ешелонований захист периметра та кінцевих точок шляхом інтеграції систем виявлення/запобігання вторгненням (IDS/IPS) та рішень класу EDR.

Захист критичних мережевих сервісів, що включає налаштування криптографічних політик автентифікації електронної пошти (SPF, DKIM, DMARC) та захист системи DNS.

ВИСНОВКИ

Загальний висновок дипломної роботи полягає в тому, що стрімкий розвиток та ускладнення мереж електронних комунікацій роблять їх критичним елементом сучасної інфраструктури, захист якої вимагає відмови від фрагментарних рішень на користь комплексних стратегій. Дослідження доводить, що сучасний ландшафт загроз характеризується надзвичайною динамічністю та поєднує в собі як зовнішні кібератаки (наприклад, DDoS, MITM, фішинг та spoofing), так і серйозні внутрішні ризики. Серед останніх ключову небезпеку становлять технічні вразливості застарілого обладнання, помилки в конфігурації мереж та людський фактор, який залишається однією з найслабших ланок у системі кібербезпеки.

Для ефективної протидії цим викликам застосування виключно технічних засобів, таких як міжмережеві екрани (Firewall), системи виявлення вторгнень (IDS/IPS) або VPN, є недостатнім, якщо вони не інтегровані в єдину керовану структуру. У роботі обґрунтовано необхідність застосування концепції багаторівневого захисту (Defense-in-Depth), яка гармонійно поєднує технічні інструменти із суворими організаційними політиками, контролем доступу на основі мінімальних привілеїв та постійним навчанням персоналу.

Вирішальним етапом у забезпеченні надійності телекомунікаційної інфраструктури є впровадження повноцінної системи управління інформаційною безпекою (СУІБ), що базується на ризик-орієнтованому підході та міжнародних стандартах, зокрема ISO/IEC 27001 [18] та NIST [28]. Тільки завдяки безперервному циклу виявлення вразливостей, централізованому моніторингу подій (за допомогою SIEM), застосуванню принципів сегментації мережі та архітектури нульової довіри (Zero Trust), організації здатні звести потенційні ризики до прийнятного рівня. Це дозволяє не лише успішно відбивати атаки, а й гарантувати стабільне функціонування мереж, зберігаючи конфіденційність, цілісність і доступність інформації в умовах постійного зростання кіберзагроз.

На основі проведеного аналізу в дипломній роботі сформульовано комплекс практичних рекомендацій щодо усунення виявлених вразливостей. Ключові з них включають: логічну сегментацію інфраструктури із застосуванням VLAN та списків контролю доступу (ACL); ешелонований захист вузлів за допомогою систем IDS/IPS та EDR; налаштування криптографічних протоколів автентифікації електронної пошти (SPF, DKIM, DMARC) та захист DNS; впровадження ізольованого резервного копіювання за правилом «3-2-1» із підтримкою планів відновлення (DRP); а також регулярне тестування персоналу (Security Awareness) та регламентований контроль змін у конфігураціях мережевого обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Базові рекомендації щодо кіберзахисту інформаційних систем організацій / Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/>
2. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023. URL: <http://uas.gov.ua/>
3. Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України / Державна служба спеціального зв'язку та захисту інформації України.
4. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20>
5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
7. CERT-UA. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. URL: <https://cert.gov.ua/>
8. CERT-UA. Рекомендації щодо протидії кіберзагрозам та реагування на кіберінциденти. URL: <https://cert.gov.ua/>
9. CISA. Cybersecurity Best Practices and Vulnerability Management Guidance. URL:
10. CISA. Known Exploited Vulnerabilities Catalog. URL: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
11. CISA. Securing End-to-End Communications. URL: <https://www.cisa.gov/>

12. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
13. ENISA. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
14. ENISA. Official information page of the European Union. URL: <https://www.enisa.europa.eu/>
15. Federal Bureau of Investigation. Spoofing and Phishing. URL: <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing>
16. Federal Trade Commission. How To Recognize and Avoid Phishing Scams. URL: <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
17. IBM. What is a Distributed Denial-of-Service Attack? URL: <https://www.ibm.com/topics/ddos>
18. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/27001>
19. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. URL: <https://www.iso.org/standard/27002>
20. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. URL: <https://www.iso.org/standard/27005>
21. ITU-T Recommendation Y.101. Global Information Infrastructure terminology. International Telecommunication Union, 2000. URL: <https://www.itu.int/rec/T-REC-Y.101/en>
22. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. Pearson Education. URL: <https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000003336/9780136681557>

23. NIS2 Directive: securing network and information systems. European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
24. NIST Computer Security Resource Center. Vulnerability — Glossary. URL: <https://csrc.nist.gov/glossary/term/vulnerability>
25. NIST National Vulnerability Database. Vulnerabilities. URL: <https://nvd.nist.gov/vuln>
26. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012. URL: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
27. NIST Special Publication 800-41 Revision 1. Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology, 2009. URL: <https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final>
28. NIST. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. URL: <https://www.nist.gov/cyberframework>
29. OWASP Foundation. Manipulator-in-the-Middle Attack. URL: https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack
30. OWASP Foundation. Web Security Testing Guide and Application Security Risks. URL: <https://owasp.org/www-project-web-security-testing-guide/>
31. Palo Alto Networks. What Is a Denial of Service Attack? URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>
32. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education.
33. Stallings W. Data and Computer Communications. Pearson Education.
34. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education.
35. Tanenbaum A. S., Wetherall D. J. Computer Networks. Pearson Education.
36. Verizon. Data Breach Investigations Report 2026. URL: <https://www.verizon.com/business/resources/reports/dbir/>