Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ____Навчально-науковий центр заочної форми навчання_____
(повна назва)

Кафедра _____Інформаційно-мережної інженерії_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____перший (бакалаврський)_____
_____
_____ Дослідження методів захисту мережі від кібератак _____
(тема)

Виконала:
здобувачка _2025_____ року навчання,
групи ___ТРІМІз-21-1_____
_____Олександра Плужник_____
(власне ім'я, прізвище)

Спеціальність _172 Телекомунікації та_____
_____радіотехніка_____
(код і повна назва спеціальності)
Тип програми ____освітньо-професійна____
Освітня програма _Інформаційно-мережна інженерія_____
(повна назва освітньої програми)

Керівник _доц. Вадим Золотарьов_____
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ Валерій Безрук _____
(підпис) (власне ім'я, прізвище)
2025 р.

Не містить відомостей заборонених до відкритого публікування

Здобувачка  / Плужник О.І./

Керівник  / Золотарьов В.А./

Харківський національний університет радіоелектроніки

Факультет_Навчально-науковий центр заочної форми навчання_____

Кафедра__інформаційно-мережної інженерії_____

Рівень вищої освіти_____перший (бакалаврський)_____

Спеціальність__172 «Телекомунікації та радіотехніка»_____
(код і повна назва)

Тип програми _____освітньо-професійна_____

Освітня програма__інформаційно-мережна інженерія _____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

« 2» травня 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачці __Плужник Олександрі Ігорівні_____
(прізвище, ім'я, по батькові)

1. Тема роботи __Дослідження методів захисту мережі від кібератак_____
затверджена наказом університету від 2 травня 2025 р. № 63Стз_____
2. Термін подання здобувачем роботи до екзаменаційної комісії 18 червня 2025 р.
3. Вихідні дані до роботи Дослідити тенденції розвитку кібератак . Проаналізувати основні підходи до класифікації кібератак та створення системи захисту проти них. Виявити найнебезпечніші види кібератак на сьогодні для підприємств електронного бізнесу. Провести багатокритеріальний аналіз виявленого виду кібератаки. Запропонувати систему захисту на різних рівнях моделі OSI/ .
4. Перелік питань, що потрібно опрацювати в роботі _____

Вступ

1. Кібератака як цілеспрямоване втручання в мережеву інфраструктуру підприємства

2. Класифікація кібератак

3. Кібератаки на відмову в обслуговуванні

4. Багатокритеріальне оцінювання атак на відмову в обслуговуванні.

5. Методи захисту від атак на відмову в обслуговуванні на різних рівнях моделі OSI.

Висновки

Перелік посилань. Додаток А. Слайди презентації

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
_Слайди у форматі Power Point А.2 Актуальність теми А.3 Обгрунтування теми дослідження А.4.Кібератака:сутність та приклади А.5 Класифікація кібератак А.6 Класифікація кібератак А.7 DoS/DDos-атаки: типи виклики А.8 Протидія DDoS-атакам А.9 Моделювання успішності DDoS-атаки А.9 Метод AHP для оцінки DDoS-атак А.10 Результати оцінювання DDoS-атак А.11 OSI-модель, як основа побудови захисту А.12 Захист від DDoS за рівнями OSI_____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. .	03.05.25	виконано
2	Підбір джерел за темою роботи	09.05.25	виконано
3	Написання першого розділу	17.05.25	виконано
4	Написання другого розділу	22.05.25	виконано
5	Написання третього розділу	02.06.25	виконано
6	Написання четвертого розділу	09.06.25	виконано
7	Написання п'ятого розділу	16.06.25	виконано
8	Написання вступу та висновків	17.06.25	виконано
9	Оформлення пояснювальної записки	18.06.25	виконано
10	Подання пояснювальної записки на перевірку	18.06.25	виконано

Дата видачі завдання 2 травня 2025р.

Здобувачка _____ Олександра Плужник
(підпис)

Керівник роботи _____ доцент Вадим Золотарьов
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: – 54 с., 10 рис., 8 табл., 17 джерел.

Мета роботи – дослідити сучасні методи захисту комп’ютерних мереж від кібератак, зокрема атак типу відмови в обслуговуванні (DoS/DDoS), проаналізувати класифікацію кіберзагроз, розробити модель оцінки рівня небезпеки атак та визначити ефективні багаторівневі стратегії захисту мереж за моделлю OSI.

У вступі обґрунтовано актуальність теми в умовах цифрової трансформації. У першому розділі розглянуто поняття кібератак, приклади атак на об'єкти критичної інфраструктури України та модель кіберзлочинця. У другому – систематизовано типи атак за характером дії, засобами реалізації та джерелом походження, зокрема в банківській сфері.

Третій розділ присвячено DoS/DDoS-атакам, їх класифікації, способам реалізації та моделюванню ефективності захисту. У четвертому застосовано метод аналізу ієрархій (AHP) для багатокритеріальної оцінки загроз, що дозволило обґрунтувати рівень небезпеки різних типів атак.

П’ятий розділ описує багаторівневий захист за моделлю OSI, акцентуючи на ефективності інтегрованих заходів: маршрутизації, фільтрації, автентифікації та моніторингу.

КІБЕРАТАКА, DDOS, ЗАХИСТ МЕРЕЖІ, OSI, AHP, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, АНАЛІЗ РИЗИКІВ.

THE ABSTRACT

Explanatory Note: – 54 pages, 10 figures, 8 tables, 17 sources.

The purpose of this work is to explore modern methods of protecting computer networks from cyberattacks, particularly denial-of-service (DoS/DDoS) attacks, analyze the classification of cyber threats, develop a model for assessing the level of attack severity, and define effective multi-layered defense strategies based on the OSI model.

The introduction justifies the relevance of the topic in the context of digital transformation. The first chapter discusses the concept of cyberattacks, provides examples of attacks on critical infrastructure in Ukraine, and introduces a model of a cybercriminal. The second chapter systematizes types of attacks by nature, means of implementation, and source of origin, including those in the banking sector.

The third chapter focuses on DoS/DDoS attacks, their classification, implementation methods, and defense efficiency modeling. In the fourth chapter, the Analytic Hierarchy Process (AHP) is used for multi-criteria threat assessment, which allows for a justified evaluation of the danger posed by various types of attacks.

The fifth chapter presents a multi-level defense approach based on the OSI model, emphasizing the effectiveness of integrated measures such as routing, filtering, authentication, and monitoring.

CYBERATTACK, DDOS, NETWORK SECURITY, OSI, AHP, INFORMATION SECURITY, CYBER THREATS, RISK ANALYSIS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

EMI – елекромагнітний імпульс;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Anycast — метод маршрутизації в IP-мережах, за якого одна IP-адреса присвоюється кільком вузлам, і трафік до цієї адреси автоматично спрямовується до найближчого або найоптимальнішого за маршрутними критеріями вузла;

APT-групи (Advanced Persistent Threat) - висококваліфіковані хакерські угруповання, які проводять тривалі, цілеспрямовані кібератаки, зазвичай підтримувані державами або великими структурами;

CDN (Content Delivery Network) — мережа доставки контенту, що складається з розподілених серверів, розміщених у різних географічних локаціях;

CRM (Customer Relationship Management) – управління взаємовідносинами з клієнтами;

DoS (Denial of Service) - атака типу «відмова в обслуговуванні»;

DDoS (Distributed Denial Of Service) – розподілена атака типу «відмова в обслуговуванні», що здійснюється одночасно з багатьох пристроїв;

IEC-104 - мережевий протокол передачі телемеханічних даних, який широко використовується в енергетиці та промисловій автоматизації;

ICMP (Internet Control Message Protocol) — допоміжний мережевий протокол, що використовується для надсилання службових повідомлень, наприклад, помилок або перевірки доступності вузлів;

IP (Internet Protocol) –міжмережний протокол;

OSI (Open Systems Interconnection) — еталонна модель взаємодії відкритих систем, розроблена ISO, яка описує, як дані передаються через мережу;

SIEM (Security Information and Event Management) - керування інформацією та подіями безпеки;

TCP (Transmission Control Protocol) — протокол управління передаванням;

TCP SYN (Synchronize) — службовий пакет, що використовується на першому етапі встановлення TCP-з’єднання;

TCP PUSH + ACK — поєднання двох прапорців (flags) у заголовку TCP-пакета:

UDP (User Datagram Protocol) — протокол транспортного рівня без встановлення з’єднання, що робить його вразливим до подібних атак через відсутність перевірки цілісності чи підтверджень

VPN (Virtual Private Network) – віртуальна приватна захищена мережа;

WAF (Web Application Firewall) — фаєрвол для вебзастосунків, який контролює, фільтрує та блокує HTTP/HTTPS-трафік між користувачем і вебсервісом;

ВСТУП

У сучасних умовах стрімкої цифровізації всі сфери суспільного життя дедалі більше залежать від стабільного функціонування інформаційних систем. Проте зростання ролі цифрових технологій супроводжується підвищенням кіберзагроз, серед яких особливу небезпеку становлять атаки на відмову в обслуговуванні (DoS/DDoS). Ці атаки здатні паралізувати роботу цілих організацій, порушити функціонування державних сервісів і створити масштабні збитки для бізнесу. Саме тому питання ефективного захисту інформаційних систем набуває пріоритетного значення.

Впровадження сучасних інфокомунікаційних технологій у сферу кіберзахисту відкриває нові можливості для виявлення, запобігання та нейтралізації таких атак. Наприклад, використання поведінкової аналітики, мережевих фаєрволів нового покоління, а також автоматизованих систем виявлення загроз дозволяє не лише ідентифікувати шкідливу активність у режимі реального часу, а й адаптувати систему безпеки до нових сценаріїв атак. Особливо актуальним є застосування багаторівневого захисту за моделлю OSI, що забезпечує комплексну протидію на різних етапах обробки трафіку.

Водночас, нарощення технічного потенціалу кіберзлочинців — від аматорських дій до висококоординованих атак, організованих професійними групами — вимагає від фахівців системного підходу до оцінки загроз. Зокрема, важливо не лише ідентифікувати вид атаки, але й проаналізувати рівень її складності, масштаб потенційної шкоди, ресурси, необхідні для реалізації, а також здатність захисної системи адекватно реагувати.

Ключовим інструментом для такої оцінки є багатокритеріальний підхід, що дозволяє врахувати широкий спектр технічних та організаційних параметрів. Застосування аналітичних методів, таких як метод аналізу ієрархій (AHP), дає змогу не лише систематизувати дані про атаки, а й обґрунтовано визначити пріоритети у зміцненні захисту.

Отже, забезпечення кіберстійкості в умовах зростаючої цифрової загрози потребує інтегрованого підходу, що поєднує технологічні інструменти, глибокий аналіз загроз і адаптивні стратегії реагування. Ця робота спрямована на дослідження DoS/DDoS-атак з точки зору їх таксономії, моделювання, захисних механізмів та методів оцінювання, що в сукупності дозволяє сформувати ефективну систему протидії цим небезпекам.

1 КІБЕРАТАКА ЯК ЦІЛЕСПРЯМОВАНЕ ВТРУЧАННЯ В МЕРЕЖЕВУ ІНФРАСТРУКТУРУ

1.1 Визначення, цілі та класифікація кібератак

Кібератака - це цілеспрямоване втручання в роботу інфокомунікаційних систем, мереж або пристроїв з метою завдання шкоди, отримання несанкціонованого доступу до даних або порушення нормального функціонування цифрових інфраструктур.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України», «кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.» [1]

1.2 Приклади кібератак на Україну

Станом на квітень 2025 року, за час повномасштабної війни Україна зазнала більше ніж 600 кібератак. Це – п’ята частина від всіх кібератак у світі. [2]

Серед основних форм кібератак і дезінформації - клонування чи злам сайтів для поширення дезінформації, DDoS-атаки та глушіння супутникових сигналів для дестабілізації інформаційного простору України, різні методи фішингу з поширенням неправдивої інформації. [3]

Найвідомішими кібератаками з 2022 року стали:

Кібератака на урядові сайти. У переддень повномасштабного вторгнення росії в Україну, 23 лютого 2022 року, було здійснено масштабну кібератаку на державні сайти, включаючи портали Верховної Ради, Кабінету Міністрів, Міністерства зовнішніх справ та Служби безпеки України, що призвело до їх тимчасового відключення . [4]

Атака на Viasat. У лютому 2022 року, одночасно з початком повномасштабного вторгнення росії в Україну, було здійснено масштабну кібератаку на супутникову мережу KA-SAT компанії Viasat. Ця атака стала однією з наймасштабніших кібератак на супутникову інфраструктуру, спричинивши серйозні наслідки для цивільного та військового зв'язку. [4]

Атака на енергетичну інфраструктуру. У квітні 2022 року хакерська група Sandworm, пов’язана з ГРУ росії, здійснила спробу кібератаки на українську енергетичну інфраструктуру, використовуючи нову версію шкідливого програмного забезпечення Industroyer, відому як Industroyer2. [4]

Кібератака на «Київстар». 12 грудня 2023 року у роботі найбільшого в Україні оператора зв'язку «Київстар» стався масштабний збій. По всій країні у абонентів «Київстар» зник мобільний зв’язок та інтернет, при цьому користувачі не могли і приєднатися до мереж інших операторів у рамках внутрішньоукраїнського роумінгу. [4]

Фейкові версії застосунки «Дія». Під час повномасштабної війни росії проти України шахраї активно поширювали фейкові версії застосунку «Дія». Ці підроблені додатки імітували інтерфейс офіційного застосунку, але не мали доступу до державних реєстрів. Зловмисники використовували їх для створення фальшивих документів, таких як COVID-сертифікати та паспорти, а також для збору персональних даних користувачів. [4]

Кібератака на державні реєстри України. 19 грудня 2024 року російським хакерам вдалось вчинити кібератаку проти інформаційних систем служби Національних інформаційних систем України та Міністерства юстиції України. За атакою стоять російські спецслужби. Внаслідок атаки було закрито доступ до низки державних реєстрів України, що паралізувало значну частину господарської діяльності в країні, під загрозою опинились фінансові операції, перевірка контрагентів, державні закупівлі, припинили роботу деякі важливі державні послуги. [4]

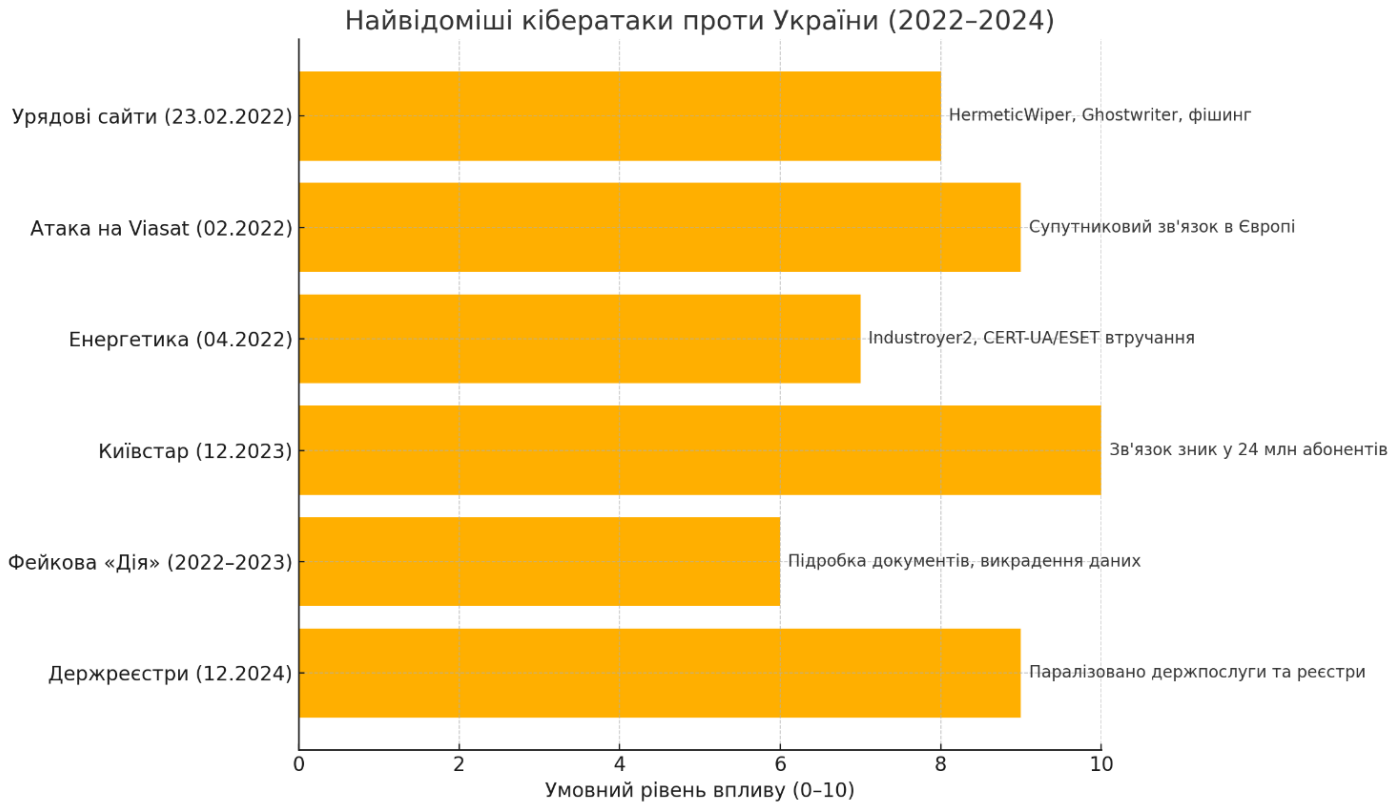

Рисунок 1.1 - Найвідоміші кібератаки в Україні протягом 2022-2024 років

На рисунку 1.1 наведено інфографіку найвідоміших кібератак в Україні протягом 2022-2024 років з зазначенням їх умовного впливу та описом наслідків.

Кібератака на акціонерне товариство «Укрзалізниця». У березні 2025 року «Укрзалізниця» зазнала масштабної кібератаки, яка суттєво вплинула на її онлайн-сервіси. 23 березня компанія повідомила про технічний збій, що призвів до припинення роботи мобільного застосунку та офіційного сайту, унеможлививши онлайн-продаж квитків. [5]

Кібератаки, як цілеспрямовані дії у кіберпросторі з метою порушення безпеки цифрових систем, стали одним із головних інструментів гібридної війни проти України. У період з 2022 по 2025 роки було зафіксовано понад 600 атак, спрямованих на державні органи, енергетичну, транспортну та інформаційну інфраструктуру. Наймасштабніші інциденти, зокрема атаки на урядові сайти, мережу Viasat, «Київстар» та державні реєстри, мали ознаки державного втручання з боку рф. Водночас, ефективна діяльність CERT-UA та міжнародна співпраця дозволили мінімізувати наслідки атак і посилили стійкість кіберпростору України. Зміцнення кібербезпеки є критично важливим елементом національної безпеки в умовах триваючої агресії. [8]

1.3 Модель кіберзлочинця

Оцінюючи загрози, пов’язані з кібератаками, важливо не лише аналізувати технічні аспекти, але й розуміти, хто саме стоїть за цими діями. У практиці інформаційної безпеки існує доцільна класифікація кіберзлочинців за рівнем підготовки та ресурсів: аматор, професіонал і суперпрофесіонал. Такий поділ дає змогу точніше оцінити потенційну складність і масштаб атаки, а також імовірність її реалізації в реальних умовах.[6]

Модель кіберзлочинця доцільно аналізувати за такими критеріями:

Обладнання: Аматор не потребує спеціалізованого обладнання, що робить атаку технічно доступною, а отже — більш ймовірною. Професіонал

використовує окремі сервери, маршрутизатори, хмарні ресурси. Суперпрофесіонал залучає унікальні технічні засоби: апаратні закладки, сегментовані бот-мережі, автономні пристрої. [6]

Програмне забезпечення: Аматор застосовує відкриті або скомпільовані з відкритих джерел утиліти. Професіонал працює з комерційним ПЗ, адаптованим під власні потреби. Суперпрофесіонал створює унікальне шкідливе ПЗ, обминаючи системи виявлення загроз. [6]

Кількість виконавців: Одинак — більш імовірна, маломасштабна атака. Невелика команда — координація, складніша реалізація. Велика група — характерно для масштабних та стратегічно спланованих атак. [7]

Наявність інсайдерів (зрадників): Аматору участь зрадників не потрібна. Професіонал може залучати співробітників для доступу до внутрішніх ресурсів. Суперпрофесіонал системно використовує зрадників або створює вразливості через них. [7]

Рівень підготовки атаки: Аматор діє спонтанно, часто без глибокого аналізу. Професіонал здійснює попередню розвідку, тестування та планування. Суперпрофесіонал проводить багаторівневе моделювання сценаріїв атаки, збирає детальну інформацію, готує середовище. [7]

Щоб глибше зрозуміти поведінкову модель кіберзлочинця, доцільно розглянути типову багатоступеневу структуру реалізації цілеспрямованої атаки. На рисунку 1.2 відображено поетапну схему кібератаки, починаючи від організації та зовнішньої розвідки до зараження цілі та досягнення результату. [7]

У кожній із фаз — зовнішній, внутрішній та фінальній (маніпуляції цілю) — залучаються ресурси відповідно до рівня підготовки зловмисника. Так, аматор, як правило, здатен виконати лише поверхневу розвідку та просте зараження. Професіонал — діє на етапі внутрішнього проникнення, здійснюючи ескалацію привілеїв, а суперпрофесіонал — координує всі фази, у тому числі етапи горизонтального просування, складного шкідливого впровадження та виведення даних. [8]

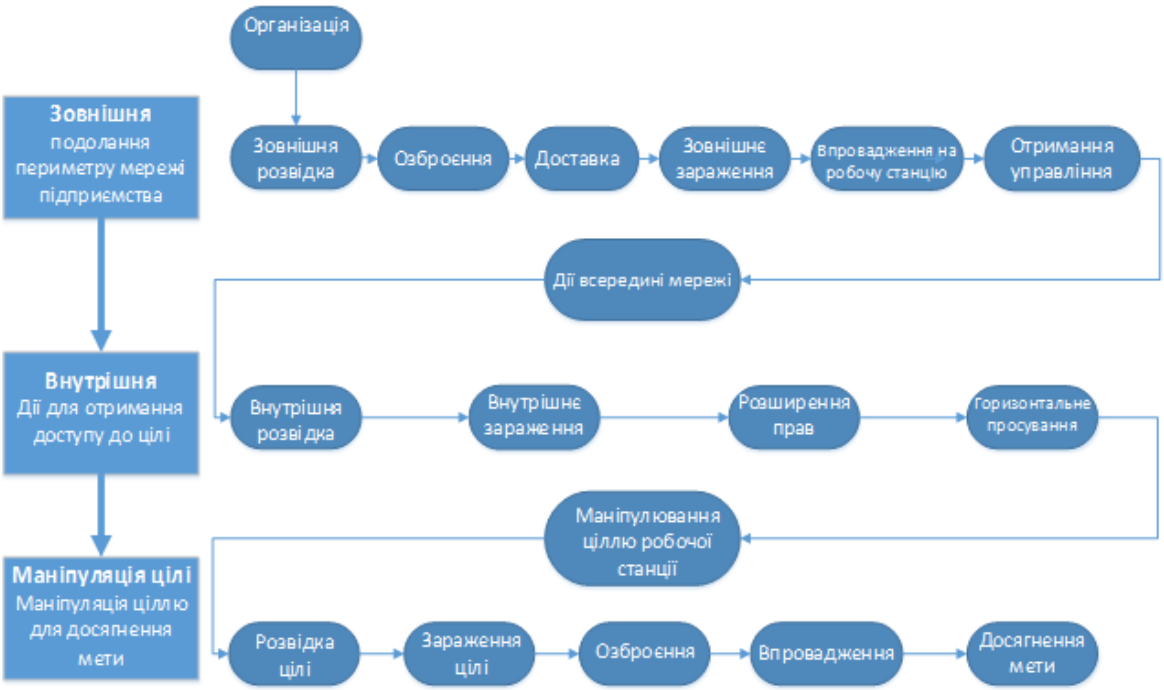

Рисунок 1.2 - Етапи реалізації цілеспрямованої кібератаки відповідно до рівня підготовки зловмисника

Кібератаки є невід’ємною складовою сучасних загроз в інформаційному просторі. Вони можуть мати серйозні наслідки як для окремих користувачів, так і для цілих держав, особливо в умовах воєнного конфлікту, де кіберпростір використовується як поле бою. Наведені приклади атак на українські об'єкти критичної інфраструктури демонструють високий рівень координації та складності з боку зловмисників. [8]

Водночас аналіз моделі кіберзлочинця дозволяє краще розуміти природу потенційного атакуючого, його можливості та ресурси. Це, у свою чергу, створює основу для більш точного прогнозування загроз та розробки ефективних методів захисту, які будуть розглядатися у наступних розділах. [8]

2 КЛАСИФІКАЦІЯ КІБЕРАТАК

Кібератаки можна здійснити за допомогою технічних та програмних засобів. Технічні засоби охоплюють фізичне обладнання, яке зловмисники використовують для несанкціонованого доступу, перехоплення даних або виведення з ладу інформаційних систем.

Програмні засоби, в свою чергу, використовуються для дистанційного проникнення в системи, порушення їхньої цілісності або викрадення даних.

Приклади технічних та програмних засобів наведені в таблиці 2.1

Кібератаки можна класифікувати за рядом ознак, які дають змогу оцінити їх природу, механізм реалізації, мету, джерело загрози, а також наслідки для об’єкта нападу. Такий підхід дозволяє створити більш повне уявлення про типи загрозі відповідні стратегії кіберзахисту. [9]

Окрім наведених вище типів кібератак, які можна класифікувати за засобами реалізації, також можна виділити ще декілька підходів у класифікації.

2.1 Основні підходи до класифікації кібератак

2.1.1 Пасивні та активні

Активні атаки - це несанкціоновані дії, які змінюють систему або дані. Під час активної атаки зловмисник безпосередньо втручається в роботу цілі, щоб пошкодити або отримати несанкціонований доступ до комп'ютерних систем і мереж. Це відбувається шляхом впровадження ворожого коду в комунікації, маскування під іншого користувача або зміни даних для отримання несанкціонованого доступу. За джерелом атаки – внутрішні (інсайдерські); зовнішні (APT-групи, хакери) та автоматизовані. [10]

Пасивні атаки — це тип кібератак, під час яких зловмисник не втручається у функціонування системи, а натомість спостерігає за обміном даними з метою

їх перехоплення чи аналізу. Вони не змінюють і не знищують інформацію або ресурси, що робить їх важчими для виявлення в порівнянні з активними атаками. Основна мета таких атак — несанкціоноване отримання доступу до конфіденційної інформації, яка передається каналами зв'язку. Пасивні дії можуть здійснюватися як у реальному часі, так і через подальший аналіз перехоплених даних. Типовими прикладами пасивних атак є підслуховування (eavesdropping) та винюхування (sniffing) — застосування спеціалізованих програм або пристроїв для перехоплення, збереження та подальшого аналізу мережевих пакетів. [10]

Таблиця 2.1 - Технічні та програмні засоби для здійснення кібератак

Технічні засоби	Програмні засоби
Шпигунське устаткування (key-логери, аналізатори бездротових пакетів)	Бот-мережі (bothers) – сукупність заражених пристроїв, що керуються зловмисником
Апаратні закладки, які встановлюються в мережеве чи комп'ютерне обладнання для прихованого збору інформації	Трояни – програми, які маскуються під легітимні, але дають контроль над системою
Генератори та боєприпаси електромагнітного імпульсу (EMI), які здатні виводити з ладу електронні пристрої через вплив потужного імпульсу	Віруси і хробаки, що самостійно розмножуються і поширюються
	Експлойти – програмні модулі, які використовують вразливість ПЗ для несанкціонованого доступу
	Руткіти і бекдори, що забезпечують прихований контроль над системою
	Програми підбору паролів
	Шпигунські програми для відстеження дій користувача
	Сніфери, які перехоплюють мережевий трафік для збору важливої інформації

2.1.2 Маскарадні атаки.

Маскарадні атаки - вважаються одним з видів кібератак, в яких зловмисник маскується під іншу особу і отримує доступ до систем або даних. Це може бути видавання себе за законного користувача або систему і вимога до інших користувачів або систем надати інформацію з конфіденційним вмістом або доступ до областей, до яких не передбачається звичайний доступ. Це може навіть включати поведінку як реального користувача або навіть певного компонента системи з наміром маніпулювати людьми, щоб змусити їх розкрити свою приватну інформацію або допустити їх до захищених місць. [10] Існує кілька типів маскувальних атак, зокрема:

2.1.2.1 Маскування імені користувача та пароля: в цій атаці людина використовує викрадені або навіть підроблені облікові дані, щоб ідентифікувати себе як дійсного користувача, отримуючи доступ до системи або додатку.

2.1.2.2 Маскарад IP-адрес: це атака, в якій IP-адреса зловмисника підміняється або підробляється таким чином, щоб джерело, з якого здійснюється доступ до системи або програми, виглядало надійним.

2.1.2.3 Маскарад веб-сайту: Хакер створює фальшивий веб-сайт, схожий на легітимний, щоб отримати інформацію про користувача або навіть завантажити шкідливе програмне забезпечення.

2.1.2.4 Маскарад електронної пошти: це атака-маскарад електронної пошти, за допомогою якої зловмисник надсилає електронний лист з нібито надійного джерела, щоб одержувач міг помилково поділитися конфіденційною інформацією або завантажити шкідливе програмне забезпечення.

2.1.2.5 Модифікація повідомлень - коли хтось змінює частини повідомлення без дозволу або змінює порядок повідомлень, щоб спричинити неприємності. Наприклад, хтось таємно змінив надісланий

лист, зробивши в ньому заміну тексту на інший. Такий вид атаки підриває довіру до інформації, що надсилається. [10]

2.1.2 Відмова від авторства

Відмова від авторства (заперечення) - це тип кібератаки, коли зловмисник навмисно робить певну дію в мережі (наприклад, проводить фінансову транзакцію або надсилає повідомлення), а згодом заперечує свою причетність до неї. Подібні атаки ускладнюють встановлення справжнього джерела дії та особи, відповідальної за інцидент, що істотно перешкоджає притягненню зловмисника до відповідальності. Існує кілька типів атак із відмовою від авторства, зокрема:

2.1.2.1 Атаки із запереченням повідомлення. Цей тип кібератаки полягає у тому, що зловмисник надсилає певне повідомлення, однак згодом відмовляється від факту його надсилання. Для цього можуть застосовуватись методи фальсифікації або модифікації заголовків повідомлень, а також експлуатація вразливостей у системах обміну інформацією. Метою атаки є унеможливлення доведення авторства.

2.1.2.2 Атаки із запереченням трансакції. У цьому випадку зловмисник здійснює трансакцію (наприклад, фінансову операцію), але пізніше заперечує свою участь у ній. Атака реалізується шляхом використання вразливостей у системах обробки трансакцій або через підроблені чи викрадені облікові дані, що створює перешкоди для встановлення відповідальності.

2.1.2.3 Атаки із запереченням зміни даних. Зловмисник навмисно змінює або видаляє дані в системі, а потім заперечує свою причетність до цього. Для реалізації таких дій використовуються вразливості в системах зберігання даних або несанкціонований доступ, отриманий через викрадені або підроблені облікові записи. Такі атаки можуть мати серйозні наслідки для цілісності та достовірності даних. [10]

2.1.3 Атака повторного відтворення

Атака повторного відтворення - це пасивне перехоплення повідомлення з метою його передачі для досягнення певного ефекту. Таким чином, в цьому типі атаки основною метою зловмисника є збереження копії даних, які спочатку були присутні в цій конкретній мережі, і подальше використання їх в особистих цілях. Після пошкодження або витоку даних вони стають незахищеним і небезпечним інструментом для користувачів. [9]

2.1.4 Атака на відмову в обслуговуванні

Атака на відмову в обслуговуванні (DoS) - це форма атаки на кібербезпеку, яка передбачає відмову в доступі до системи або мережі цільовим користувачам шляхом переповнення трафіку або запитів. У DoS-атаці зловмисник переповнює цільову систему або мережу трафіком або запитами, щоб поглинути доступні ресурси, такі як пропускна здатність, цикли процесора або пам'ять, і перешкодити законним користувачам отримати до них доступ. Існує кілька типів DoS-атак, зокрема:

2.1.4.1 Флуд-атаки: Тут зловмисник надсилає таку велику кількість пакетів або запитів до системи чи мережі, що вона не може їх обробити, і система виходить з ладу.

2.1.4.2 Атаки посилення: У цій категорії зловмисник збільшує потужність атаки, використовуючи іншу систему або мережу для збільшення трафіку, а потім спрямовує його на ціль, щоб підвищити потужність атаки. [10]

2.1.5 Оприлюднення вмісту повідомлення

Оприлюднення вмісту повідомлення - є серйозною загрозою для конфіденційності інформації в інформаційно-комунікаційних системах. Передача даних через відкриті канали зв’язку — наприклад, телефонні розмови, електронна пошта чи передача файлів — може містити важливу або

конфіденційну інформацію, яка повинна залишатися недоступною для сторонніх осіб. [9]

2.1.6 Аналіз трафіку

Аналіз трафіку — це вид пасивної кібератаки, при якому зловмисник, не змінюючи передані дані, спостерігає за параметрами мережевих комунікацій, такими як обсяг, частота, час відправлення та отримання повідомлень, а також ідентифікаційні дані учасників обміну.
Навіть за умови використання шифрування для захисту вмісту повідомлень, аналіз трафіку дозволяє опоненту отримати цінну інформацію про структуру взаємодії, імовірний зміст комунікації або визначити критичні елементи інфраструктури. [10]

Крім поділу за технічними і програмними засобами реалізації атак, доцільним є також моделювання типів вразливостей на основі інфраструктурного підходу. Така класифікація дозволяє виділити основні області, де можуть виникати уразливості, що використовуються зловмисниками.

На рисунку 2.1 наведено класифікацію моделей кібератак за принципом організаційної архітектури — від мережної інфраструктури до прикладного програмного забезпечення.

Представлена класифікація дозволяє системно аналізувати ризики на кожному з рівнів архітектури IT-системи та використовувати її як орієнтир при побудові моделі загроз.

Для складніших об’єктів, таких як підприємства електронного бізнесу, застосовується більш комплексний підхід до аналізу — так званий синергетичний підхід, який буде розглянуто нижче.

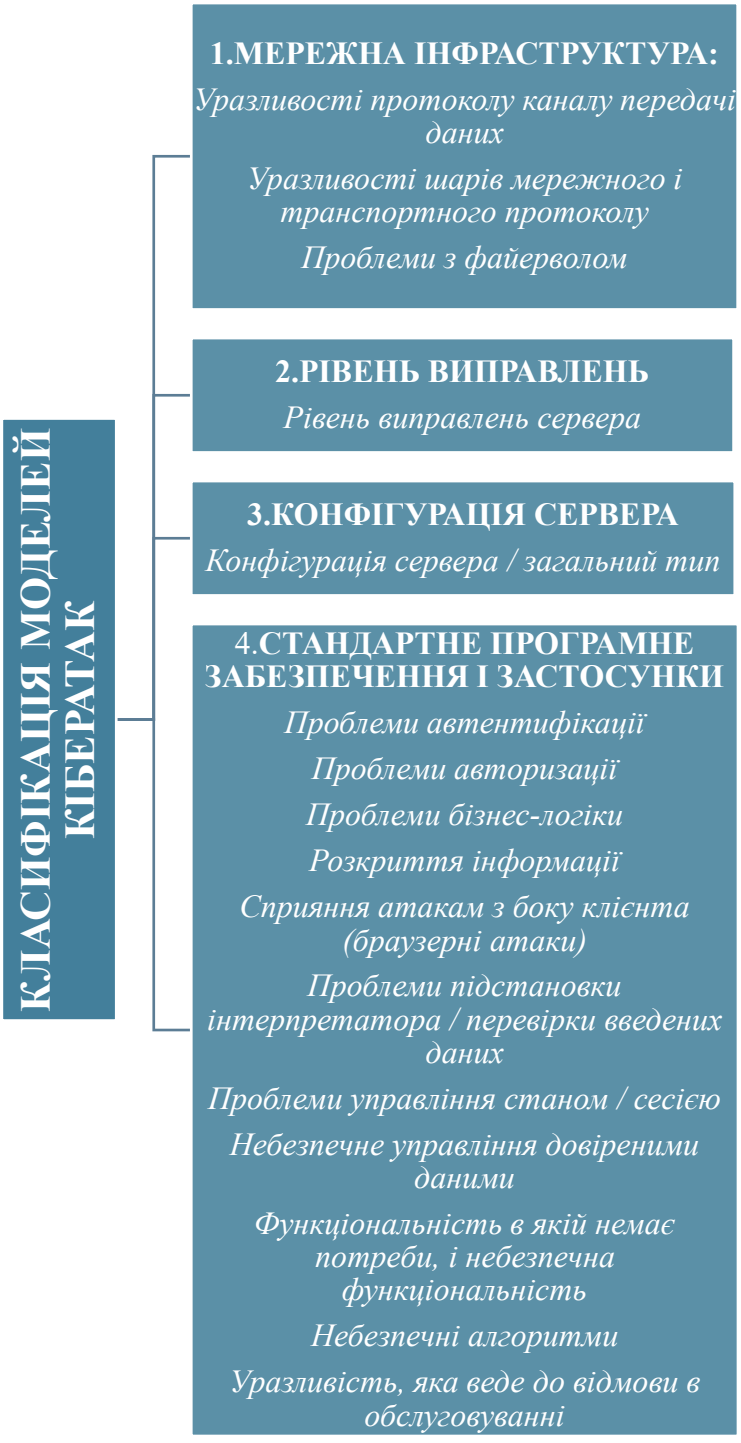

Рисунок 2.1 - Класифікація моделей кібератак

2.2 Синергетичний підхід до класифікації кіберзагроз у підприємствах електронного бізнесу

Класифікуючи кібератаки, важливо враховувати не лише інструменти, за допомогою яких вони здійснюються (технічні чи програмні засоби), або характер впливу (активний чи пасивний), а й ширший контекст, у якому ці атаки відбуваються. Особливої актуальності це набуває у підприємствах електронного бізнесу, де інформаційні ресурси є критичними як для внутрішньої діяльності установи, так і для клієнтських сервісів.

Спираючись на розробки С.П. Євсєєва, сучасні кіберзагрози у підприємствах електронного бізнесу мають багаторівневу і багатовимірну структуру. [11] Вони можуть одночасно впливати на кілька елементів системи, порушувати декілька властивостей інформації, а також бути результатом як зовнішнього втручання, так і внутрішніх зловживань. Саме тому дослідники, зокрема С.П. Євсеєв з колегами запропонували синергетичний підхід до класифікації кіберзагроз, який дозволяє оцінити загрози у взаємозв’язку та взаємопідсиленні. [11]

У цьому підході пропонується виокремлювати кібератаки:

За складовими безпеки інформаційних ресурсів, що включають: інформаційну безпеку як середовище функціонування, кібербезпеку як технічний захист інфраструктури, безпеку інформації як змісту даних (у тому числі трансакцій, фінансових документів, персональних записів клієнтів). [11]

За напрямом реалізації загроз, зокрема: нормативно-правові загрози (недотримання регламентів), організаційні загрози (людський фактор, помилки персоналу, інсайдерські дії), інженерно-технічні загрози (збої обладнання, слабкі точки інфраструктури, фізичне втручання). [11]

За порушеними властивостями інформації: конфіденційність (витік інформації), цілісність (фальсифікація трансакцій або звітності), доступність (відмова в обслуговуванні або блокування систем), автентичність (підробка облікових даних, маніпуляції з цифровими підписами). [11]

За джерелом загрози, що особливо важливо для підприємств електронного бізнесу: зовнішні атаки (APT-групи, хакерські угруповання), внутрішні атаки (інсайдери, недобросовісні співробітники), автоматизовані загрози (ботнети, шкідливе ПЗ, скриптові атаки). [11]

За рівнем реалізації в інфраструктурі підприємств електронного бізнесу: фізичний рівень (сервери, обладнання, точки доступу), мережевий рівень (канали зв'язку між офісами/філіями), рівень операційних систем (Windows/Linux-сервери), рівень баз даних (клієнтські бази, реєстри трансакцій), прикладний рівень (CRM-системи, мобільні застосунки). [11]

На рисунку 2.1 наведена схема, яка показує, за якими напрямками відбувається класифікація загроз в наведеній моделі.

Кожна з вищенаведених загроз може існувати окремо, проте на практиці часто відбувається накладання кількох типів загроз одночасно, що значно підвищує рівень ризику. Наприклад, зовнішня атака на прикладний рівень через уразливість в онлайн-банкінгу може одночасно порушити конфіденційність (витік даних), доступність (DoS-атака) та автентичність (використання підроблених токенів доступу). [11]

Такий багатофакторний аналіз загроз дозволяє не лише краще зрозуміти логіку кібератак у банківській сфері, а й сформувати цілісну систему їх оцінювання та протидії. Застосування синергетичної моделі класифікації загроз також створює підґрунтя для розробки адаптивних систем кіберзахисту — зокрема, з використанням платформ моніторингу безпеки (SIEM) та алгоритмів прогнозування ризиків. [11]

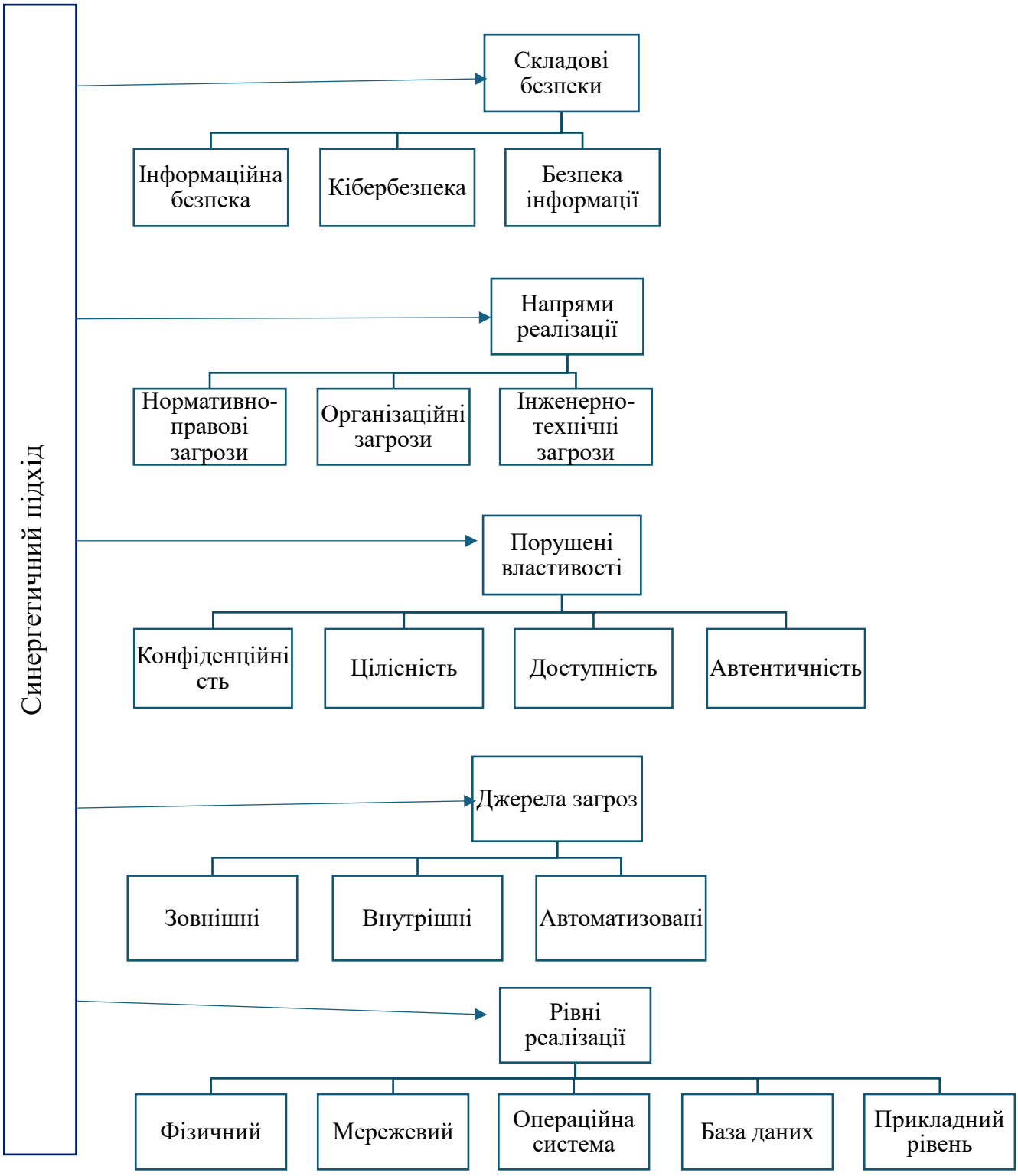

Рисунок 2.1 - Синергетичний підхід до класифікації кіберзагроз у банківській системі

У вищезазначеній інформації наведено комплексний аналіз особливостей здійснення та класифікації кібератак, що дає змогу сформувати цілісне уявлення про природу сучасних кіберзагроз. Розглянуто технічні та програмні засоби, за допомогою яких можуть здійснюватися атаки, наведено приклади їх практичного застосування. Акцентовано увагу на класифікації кібератак за характером впливу (активні та пасивні) із детальним описом основних видів атак, зокрема маскарадних атак, модифікації повідомлень, атак із відмовою від авторства, атак повторного відтворення та атак на відмову в обслуговуванні.

Також розкрито синергетичний підхід до класифікації кіберзагроз у підприємствах електронного бізнесу, що передбачає врахування впливу атак на різні складові безпеки, напрями реалізації загроз, порушення властивостей інформації, джерела походження та рівні інфраструктури. Такий підхід дозволяє забезпечити комплексну оцінку ризиків та сприяє побудові ефективних стратегій кіберзахисту в умовах зростання складності інформаційних систем, зокрема у фінансовому секторі.

Отже, проведений аналіз класифікації кібератак створює основу для подальшого вивчення механізмів захисту інформаційних ресурсів та удосконалення систем протидії кіберзагрозам.

3 КІБЕРАТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ

3.1. Таксономії DoS та DDoS-атак

В умовах стрімкого розвитку інформаційних технологій та зростання цифровізації усіх сфер суспільного життя, питання кібербезпеки набуває особливої актуальності. Одним із найбільш поширених і небезпечних видів кібератак є атаки типу відмови в обслуговуванні.

DoS-атака (Denial of Service) — це навмисне перевантаження інформаційної системи великою кількістю запитів з одного джерела, що призводить до неможливості обробки легітимного трафіку та тимчасового або повного порушення роботи сервісу.

DDoS-атака (Distributed Denial of Service) — це розподілений варіант DoS-атаки, який здійснюється з багатьох пристроїв одночасно (часто об’єднаних у ботнет), що значно ускладнює виявлення джерел атаки та забезпечує вищу ефективність порушення роботи цільових систем.[10]

Особливу загрозу в сучасних умовах становлять низькошвидкісні HTTP DDoS-атаки, які є складними для виявлення через свою приховану природу. На відміну від традиційних атак, що спричиняють різке зростання обсягу трафіку, низькошвидкісні атаки імітують звичайну поведінку користувачів, надсилаючи невелику кількість HTTP-запитів, що поступово виснажують ресурси сервера. Такий підхід дозволяє атакам залишатися непоміченими для стандартних засобів моніторингу, орієнтованих переважно на фіксацію аномально високої активності.

Таким чином, DDoS-атаки, зокрема їх низькошвидкісні варіанти, становлять серйозний виклик для систем кіберзахисту та вимагають впровадження нових моделей виявлення та запобігання.

Цей підхід детально розглядається у науковій статті Поночовного Петра Михайловича, аспіранта Державного університету інформаційно-

комунікаційних технологій (м. Київ), під назвою «Модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача», опублікованій у журналі «Кібербезпека», де обґрунтовано потребу в спеціалізованих алгоритмах для протидії цим видам атак.[12]

Не існує єдиного стандарту у класифікації атак DDoS. При класифікації таких атак науковці можуть використовувати різні параметри.

Наприклад, з огляду на місце, де відбувається атака, може існувати п’ять категорій: рівень мережевого пристрою; рівень операційної системи; рівень програми; потік даних; атака на особливості протоколу.

За іншим підходом, для визначення класифікації може використовуватися кількість комп’ютерів, які використовуються на виконання однієї атаки : атаки з одного джерела та атаки з кількох джерел. Атаки з одного джерела класифікуються на атаки використання протоколу та атаки програмних помилок. Водночас атаки з кількох джерел класифікуються на хаотичні і структуровані (розподілена відмова від джерела та розподілена відображена відмова в обслуговуванні). [12]

Нижче розглянемо таксономію, яка була запропонована C. Douligeris, де не розрізняються цілі DDoS-атаки, але зосереджуються на описі атаки відповідно до різних підходів:

- ступінь автоматизації;
- використання вразливості;
- динаміка швидкості атаки;
- вплив.

З точки зору ступіню автоматизації атаки розрізняються на такі, що можуть бути ручними (виконаними за інструкцією), напівавтоматичними або повністю автоматизованими. Цей параметр визначає рівень залучення зловмисника в процес атаки та складність її реалізації. [12]

За використанням вразливостей, класифікація охоплює широкий спектр технічних механізмів, зокрема атаки типу нападу повенів (UDP-флуд, ICMP-флуд), атаки посилення (наприклад, смурф-атака чи фрагментована атака), а

також складніші варіанти, що експлуатують протокольні недоліки або некоректну обробку специфічного мережевого трафіку (атаки використання протоколу та атаки неправильного пакету). [12]

Третім критерієм є динаміка швидкості атаки. Атака може здійснюватися постійно або змінюватися в часі — поступово зростати, коливатися чи мати імпульсний характер. Цей параметр важливий для виявлення аномалій, оскільки дозволяє відрізняти типові атаки від прихованих сценаріїв із низькою швидкістю. [12]

Четвертий підхід стосується впливу атаки на цільову систему. У цьому контексті атаки поділяються на підривні, які повністю виводять систему з ладу, та принизливі — ті, що не зупиняють її роботу, але значно знижують продуктивність і стабільність. [12]

Згідно з цією моделлю, кожна атака, описується за всіма чотирма параметрами одночасно. Такий комплексний опис дозволяє не лише глибше аналізувати характеристики атаки, а й обґрунтовано обирати відповідні методи протидії. Універсальність таксономії полягає в тому, що вона дає змогу приймати єдине рішення щодо реагування, незалежно від специфіки атаки, оскільки всі її критичні риси вже враховано в межах запропонованих підходів. [12]

Більш орієнтованою на практичне та миттєве визначення характеристик атаки є таксономія DDoS-атак, запропонована S. Specht і R. Lee. На відміну від підходу C. Douligeris, ця модель зосереджується переважно на тому, яким чином виконується атака та на які вразливі місця об’єкту атаки вони направлені, тобто що саме є ціллю атаки — пропускна здатність мережі або обчислювальні ресурси системи. В даній класифікації атаки поділяються всього на дві групи.

Перша група – це атаки на вичерпання пропускної здатності. До них належать атаки повені, що можуть реалізовуватись через UDP або ICMP-протоколи. У разі UDP-флуду трафік може надходити як на випадкові порти, так і на конкретно визначений порт. Другий підтип – це атаки посилання, серед яких виділяються смурф-атака (використання підробленої IP-адреси для створення

масових ICMP-відповідей), фраггл атаки та інші, які реалізуються шляхом прямого надсилання трафіку або через створення замкнених маршрутів (петель).

Друга група атак в даній класифікації – це атаки на виснаження ресурсів. У цьому випадку метою є споживання обчислювальних або логічних ресурсів сервера. До них належать атаки використаного протоколу, зокрема TCP SYN-флуд (створення великої кількості незавершених з'єднань), а також атаки із застосуванням комбінацій прапорців TCP, такі як PUSH + ACK. [12]

Різновид атаки неправильного пакету є атаками, які спрямовані на IP-адреси або використовують специфічні параметри IP-пакетів для викликання помилок у обробці трафіку.

Дана класифікація є досить зручною для оперативного аналізу та реагування на атаку, проте вона не враховує додаткових характеристик, таких як динаміка трафіку, ступінь автоматизації чи рівень впливу. Перевагою є те, що її практична спрямованість дозволяє ефективно ідентифікувати тип атаки та джерело навантаження та зосередити увагу на конкретних точках вразливості інформаційної системи. [12]

3.2. Таксономія засобів протидії атак DDoS

Через те, що атаки типу DDoS відрізняються значною варіативністю — як за способами реалізації, так і за напрямками впливу — для обробки кожного конкретного типу атаки може бути застосовано цілу низку заходів з протидії ним. Саме тому надзвичайно важливою є також і класифікація наявних засобів протидії DDoS-атакам , оскільки вона дозволяє сформувати цілісне уявлення про наявні механізми захисту, а також обрати найбільш ефективний та актуальний інструмент серед усіх можливих. [12]

Одну з найбільш структурованих і прикладних моделей класифікації запропонував Д. Кагір. Його таксономія заходів протидії віддаленим атакам на відмову в обслуговуванні базується на поділі контрзаходів за рівнем їх реалізації

в системі, що дозволяє враховувати специфіку об'єкта атаки. Кагір виділяє п’ять ключових рівнів протидії, орієнтованих на тип цільового ресурсу. [12]

Першим є рівень мережевого пристрою, який охоплює базові технічні заходи захисту на рівні маршрутизаторів, комутаторів, міжмережевих екранів тощо. Основними засобами є встановлення патчів і оновлень, які закривають відомі вразливості, а також фільтрація пакетів, що дозволяє блокувати підозрілий трафік на ранній стадії.

Другий — рівень операційної системи, де захист реалізується шляхом оновлення системного програмного забезпечення, а також модифікації реалізації протоколів, наприклад, зміни параметрів обробки з’єднань, тайм-аутів і обмежень кількості активних сесій, що дозволяє зменшити ризик перевантаження.

Рівень застосування стосується механізмів безпеки, вбудованих у прикладні сервіси та програми. Він передбачає регулярне оновлення програмного забезпечення для усунення логічних вразливостей, а також використання систем сканування та виявлення вторгнень, здатних ідентифікувати ознаки атак на основі поведінкового аналізу.

Четвертий рівень — реплікація та балансування навантаження, орієнтований не стільки на блокування трафіку, скільки на перерозподіл навантаження між декількома вузлами або серверами, що дозволяє підтримувати працездатність навіть у разі великомасштабної DDoS-атаки. [12]

На рисунку 3.1 наведена таксономія протидії атак DDoS, запропонована Д. Кагіром, яка виокремлює п’ять груп протидії DDoS-атакам, орієнтованих на тип жертви.

П’ятий, стандартний рівень протоколу включає заходи зі зміни стандартів мережевих протоколів або впровадження додаткових захисних рівнів, які унеможливлюють або значно ускладнюють використання слабких місць протоколів для здійснення атак. [12]

Кожен із цих рівнів може реалізовувати захист через дві основні підкатегорії: ітераційне обслуговування (тобто динамічна реакція на зміну умов

— наприклад, адаптивна фільтрація) та використання додаткових захисних систем, таких як проксі-сервери, хмарні платформи безпеки або шлюзи DDoS-захисту.

Таким чином, модель Кагіра забезпечує багаторівневу та адаптивну основу для побудови стійкої архітектури протидії DDoS-атакам, дозволяючи системно поєднувати різні засоби захисту залежно від характеру загроз, інфраструктури та доступних ресурсів. [12]

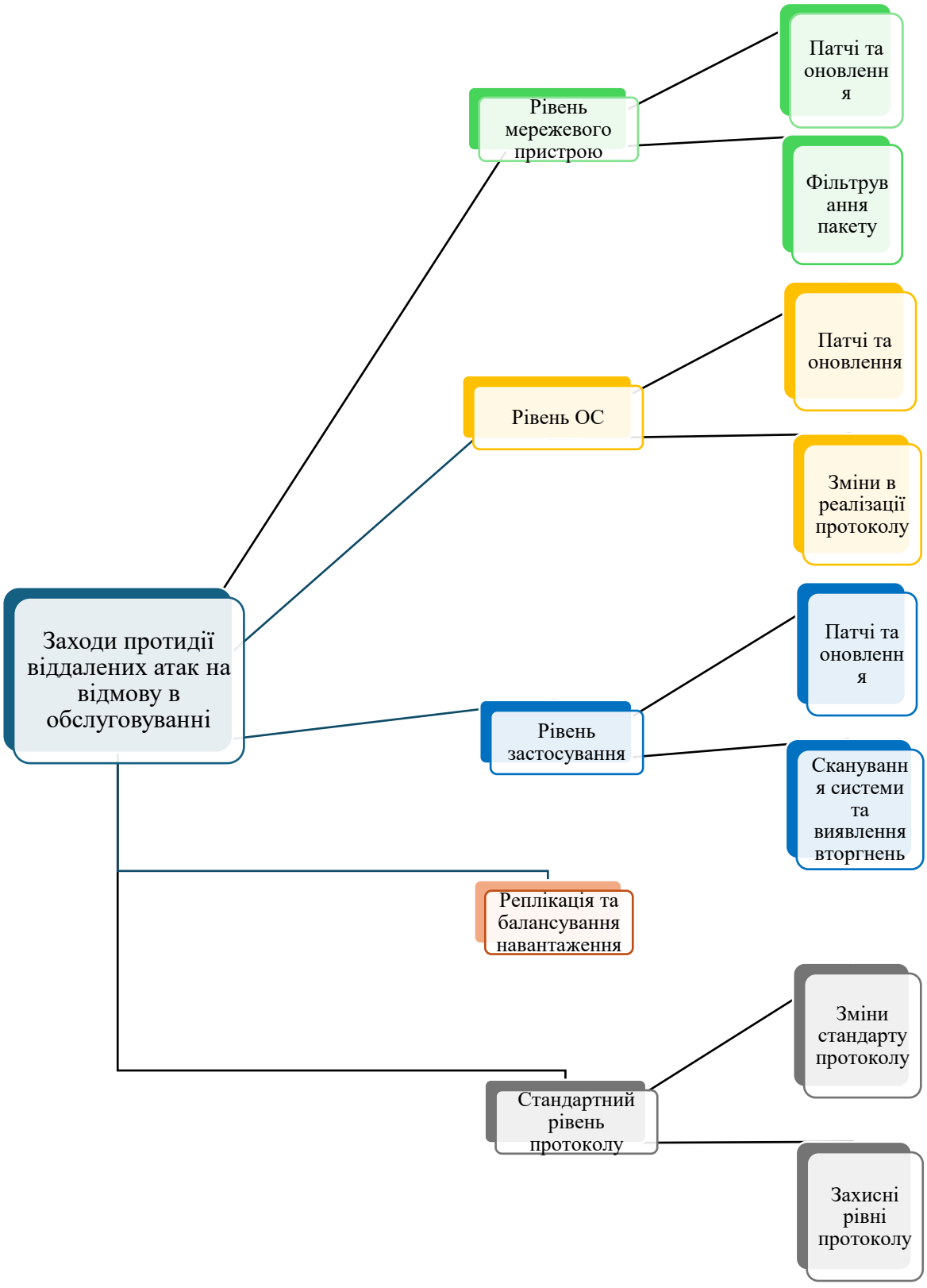

Рисунок 3.1 - Таксономія протидії атак DDoS, запропонована Д. Кагіром

3.3 Розрахунок впливу різних властивостей атаки на успіх атаки DDoS

На підставі зазначених вище класифікацій можна розрізнити всі можливі комбінації DDoS-атак і властивості їх протидії. Проте для того, щоб отримати кількісний вираз аналізованих властивостей, DDoS-атаку або її протидію необхідно оцінити на практиці або змоделювати відповідними інструментами.

Візьмемо для прикладу модель атаки DDoS, коли трафік атаки вичерпує як пропускну здатність, так і ресурси пам’яті. На рисунку 3.2 представлено концептуальну модель комбінованої DDoS-атаки з пропускною здатністю та вичерпанням пам’яті. [13]

Для представлення повної ймовірності атаки використаємо формулу

$$P=1 - \overline{P_B} * \overline{P_M} * \overline{P_C} , \qquad (3.1)$$

де P – ймовірність P_{Fn}:з виснаженням ресурсу,

P_B – зниження пропускної здатності,

P_C – виснаження процесів,

P_M – вичерпання пам’яті, щоб додати ймовірність фільтрації законного трафіку

$$P = 1 – (1 - P_B) * (1 - P_{Fn}) * (1 - P_M) \qquad (3.2)$$

де P_{Fn} – ймовірність фільтрації законного трафіку.

Використовуючи дану модель DDoS-атаки, проведемо дослідження.

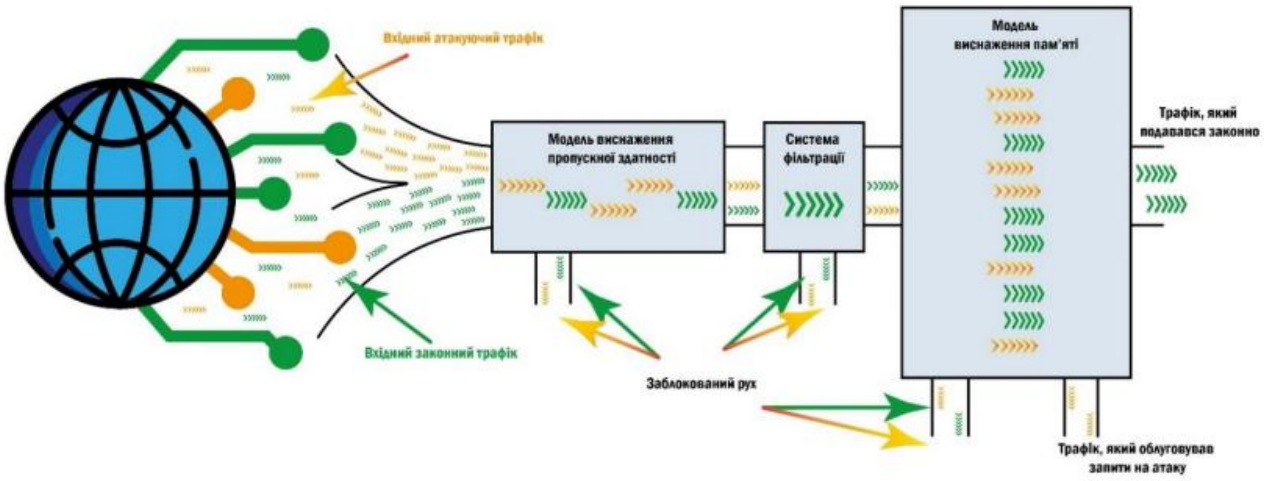

Рисунок 3.2 Концептуальна модель комбінованої DDoS-атаки з пропускною здатністю та вичерпанням пам’яті

Для аналізу оберемо параметри ситуації, наведені у таблиці 3.1. Ці параметри атаки та інфраструктури жертви призводять до 41,3% виснаження пропускної здатності, 5% законних запитів було відфільтровано, а ймовірність виснаження пам’яті досягла 100% через перевантаження активними з’єднаннями. Композитна ймовірність успіху DDoS-атаки склала 100%, що свідчить про повну втрату доступності сервісу за заданих умов.

З аналізу видно, що навіть за часткової фільтрації атакувального трафіку й незначного блокування легітимних запитів, перевантаження пам’яті залишається ключовим фактором успішної реалізації DDoS-атаки. Зміна фільтраційних параметрів демонструє, що ймовірність блокування законного трафіку лінійно впливає на загальну ефективність атаки, тоді як фільтрація трафіку атаки має складніший, нелінійний характер впливу, особливо у випадках високого навантаження на буферну пам’ять.

На рисунку 3.3 наведено графік залежності успіху атаки від відсотка фільтрації запитів атаки.

У таблиці 3.2 наведено вихідні параметри для побудови графіка залежності успіху DDoS-атаки від рівня фільтрації запитів атаки.

Проведене моделювання комбінованої DDoS-атаки дало можливість провести оцінку впливу різних параметрів системи захисту на загальну ймовірність успішної атаки. Було встановлено, що при недостатній пропускній здатності каналу та обмеженій буферній пам’яті навіть помірний обсяг атакувального трафіку здатен повністю вивести з ладу систему обробки запитів.

Найбільш критичним фактором виявилося виснаження пам’яті, що напряму залежить від кількості активних з’єднань та часу їх обробки. Збільшення рівня фільтрації атакувального трафіку призводить до істотного зменшення навантаження на буфер, що у свою чергу знижує загальну ймовірність успіху атаки. Водночас було виявлено, що навіть незначна фільтрація легітимного трафіку (5%) лінійно підвищує ризик відмови обслуговування для законних користувачів.

Результати демонструють, що ефективна протидія DDoS-атакам вимагає збалансованого підходу — з одного боку, потужних фільтрів для обмеження шкідливого трафіку, а з іншого — мінімізації впливу цих фільтрів на легітимні запити. Оптимізація параметрів фільтрації є ключовим елементом зменшення вразливості системи до комбінованих DDoS-атак.

Таблиця 3.1 – Параметри ситуації

Звичайний трафік	18 Мбіт/с (90 запитів на секунду по 200 біт у кожному)
Трафік атаки	15 Мбіт/с (60000 запитів на секунду по 200 біт у кожному)
Пропускна здатність каналу	80 Мбіт/с
Фільтри, які використовує жертва	Фільтрують 15% атак і 5 % легітимного трафіку
Час на виконання законного запиту	150 мс
Час на виконання запиту атаки	2500 мс
Здатність буфера	інформація про 40 з’єднань

Таблиця 3.2 - Вихідні параметри для побудови графіка залежності успіху DDoS-атаки від рівня фільтрації запитів атаки

Фільтрація атак (%)	Виснаження пропуску (%)	Фільтрація легітимного трафіку (%)	Виснаження пам’яті (%)	Композитна ймовірність (%)
1	2	3	4	5
0	41,3	5	100	100
10	41,3	5	85	91,9
20	41,3	5	70	82,5
30	41,3	5	55	70,9
40	41,3	5	40	56,4
50	41,3	5	25	39,5
60	41,3	5	10	20,2
70	41,3	5	5	12,0
80	41,3	5	2	6,7
90	41,3	5	1	3,2
100	41,3	5	0,5	1,6

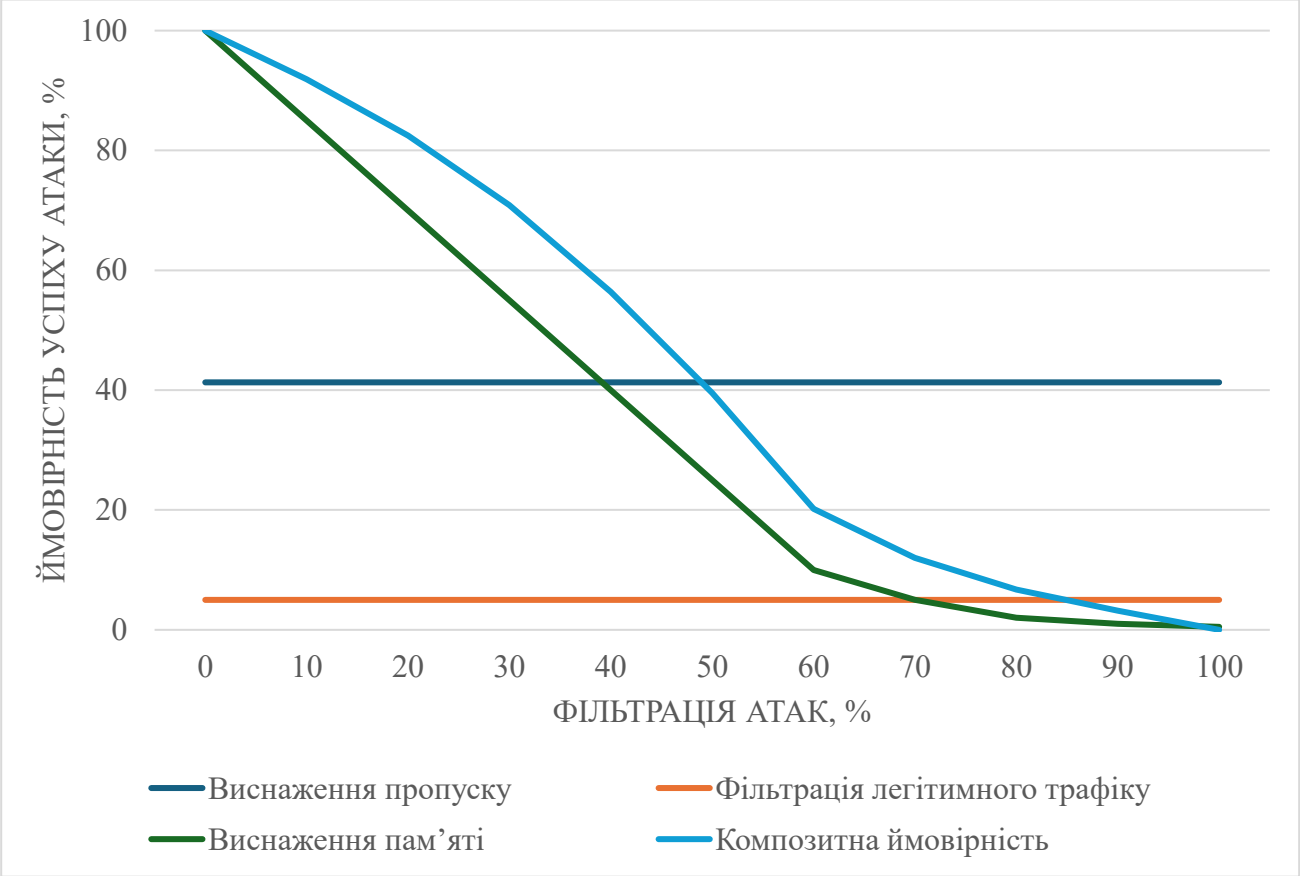

Рисунок 3.3 - Залежність успіху атаки від відсотка фільтрації запитів атаки

3.4 Можливі методи протидії та запобігання DDoS-атакам

Запобігання DDoS-атакам може бути складним завданням, особливо під час великого трафіку або в масштабній розподіленій мережевій архітектурі. По-справжньому активний захист від DDoS-загроз залежить від кількох ключових факторів, серед яких зменшення поверхні атаки, моніторинг загроз і масштабовані інструменти пом'якшення DDoS-атак. [13]

Одним з поширених методів протидії та запобігання DDoS-атакам є зменшення поверхні атаки**:** обмеження впливу, яке може допомогти мінімізувати ефект DDoS-атаки. Кілька методів зменшення цього ризику включають обмеження трафіку в певних місцях, впровадження банлансувальника навантаження та блокування зв'язку від застарілих або невикористовуваних портів, протоколів і програм.

Ще один з методів - дифузія мережі Anycast**.** Мережа допомагає збільшити площу поверхні мережі організації, щоб вона могла легше поглинати об'ємні стрибки трафіку (і запобігати збоям), розподіляючи трафік між кількома розподіленими серверами. [13]

Адаптивний моніторинг загроз у режимі реального часу. Моніторинг журналів може допомогти точно визначити потенційні загрози, аналізуючи моделі мережевого трафіку, відстежуючи стрибки трафіку або іншу незвичайну активність, а також адаптуючись для захисту від аномальних або зловмисних запитів, протоколів та IP-блоків.

Кешування зберігає копії запитуваного вмісту, щоб менше запитів обслуговувалося вихідними серверами. Використання мережі доставки контенту (CDN) для кешування ресурсів може зменшити навантаження на сервери організації та ускладнити їх перевантаження як законними, так і зловмисними запитами.

Обмеження швидкості обмежує обсяг мережевого трафіку протягом певного періоду часу, по суті, запобігаючи перевантаженню веб-серверів запитами з певних IP-адрес. Обмеження швидкості може використовуватися для

запобігання DDoS-атакам, які використовують боти для спаму кінцевої точки з аномальною кількістю запитів одночасно.

Інструментами запобігання DDoS-атакам можуть бути брандмауер веб-додатків (WAF**),** який допомагає блокувати атаки, використовуючи настроювані політики для фільтрації, перевірки та блокування шкідливого трафіку HTTP між вебпрограмами та інтернетом. За допомогою WAF організації можуть застосовувати позитивну та негативну модель безпеки, яка контролює вхідний трафік із певних місць та IP-адрес.

Завжди ввімкнене запобігання DDoS-атакам, в якому постачальник засобів захисту від DDoS-атак може допомогти запобігти DDoS-атакам, постійно аналізуючи мережевий трафік, впроваджуючи зміни в політику у відповідь на нові моделі атак і надаючи розгалужену та надійну мережу центрів обробки даних. Оцінюючи хмарні послуги захисту від DDoS-атак, необхідно шукати постачальника, який пропонує адаптивний, масштабований і постійно ввімкнений захист від загроз від складних і об'ємних атак.

Одним із ефективних прикладів реалізації захисту від DDoS-атак на практиці є сервісна платформа компанії Cloudflare, яка забезпечує багаторівневу систему протидії атакам на рівнях L3–L7 моделі OSI. Рішення Cloudflare дозволяє організаціям своєчасно виявляти, ізолювати та блокувати шкідливий трафік до того, як він досягне критичних компонентів інфраструктури або додатків. [13]

Ключовою перевагою системи є використання глобальної мережі Anycast, яка охоплює понад 330 міст у 125 країнах світу. Це дає змогу ефективно розподіляти та поглинати надлишковий трафік, включно з масштабними DDoS-атаками, ще на периферії мережі. Завдяки механізмам оптимізованої маршрутизації та прискорення трафіку, Cloudflare знижує ризик перевантаження каналів зв’язку та мінімізує затримки.

Особливо важливою є система постійно активного захисту, яка функціонує в режимі реального часу і здатна виявити та заблокувати шкідливу активність менш ніж за три секунди. Крім того, платформа інтегрує веб-аплікаційний

фаєрвол нового покоління (WAF), що дозволяє гнучко налаштовувати правила обробки запитів, застосовувати розширене обмеження швидкості та адаптувати систему до актуальних загроз.

Таким чином, платформа Cloudflare ілюструє сучасний підхід до захисту від DDoS-атак, заснований на поєднанні широкомасштабної інфраструктури, високої швидкості реакції та інтелектуальних засобів аналізу трафіку. [13]

4 БАГАТОКРИТЕРІАЛЬНЕ ОЦІНЮВАННЯ КІБЕРАТАК НА ВІДМОВУ У ОБЛУГОВУВАННІ

Проведений у попередніх розділах аналіз дозволив зрозуміти природу атак на відмову в обслуговуванні, методи їх класифікації, шляхи реалізації та методи захисту від них. В той самий час протидія таким атакам вимагає не лише розуміння вищезазначених питань, а й системного підходу до їх оцінювання на основі декількох параметрів – від характеристик атаки до здатності системи реагувати на подібні загрози. З цією метою може бути використано багатокритеріальний метод оцінювання атак на відмову в обслуговуванні, який враховує багато параметрів і дозволяє оцінити ймовірність успіху атаки та ефективність засобів протидії.

Метод багатокритеріального оцінювання заснований на підході аналізу ієрархій, який був розроблений математиком Т.Сааті у 1970 році. Його суть полягає у розбитті загальної задачі на підзадачі (в нашому випадку – на критерії), які потім оцінюються попарно за шкалою важливості (наприклад, від 1 до 9, де 1 означає рівну важливість, а 9 — абсолютну перевагу одного над іншим). Такий підхід дає можливість врахувати як кількісні, так і якісні характеристики, отримати вагу критерія на основі аналізу, вивести узагальнену оцінку для кожного предмету оцінювання. [14]

Однією з суттєвих переваг способу є змога обґрунтованого ранжування об'єктів, навіть якщо критерії не є незалежними чи виражені у різних одиницях виміру. У нашому випадку, це дає змогу порівнювати атаки на відмову в обслуговуванні (DoS/DDoS) за параметрами, що не мають спільної шкали — наприклад, ефективність виявлення (у відсотках), час реагування (в секундах) та тип зловмисника (якісна характеристика).

Оцінювання проводиться на основі дев'яти критеріїв, сформованих з урахуванням аналізу нормативних документів, практичних рекомендацій з кібербезпеки та сучасних досліджень у сфері інформаційного захисту.

Ці критерії забезпечують комплексний підхід до аналізу загроз, охоплюючи технічні аспекти атак (зокрема, рівень складності їх здійснення чи ефективність виявлення), організаційно-ресурсні фактори (витрати на впровадження заходів безпеки, навантаження на інфраструктуру) та характеристику самої загрози (тип зловмисника, масштаби потенційної шкоди, готовність системи до захисту).

Зазначений підхід спрямований на оцінку не лише потужності та небезпеки атак, але й складності їх реалізації для зловмисників, ймовірності успішного реагування на загрози, а також адаптованості стандартних систем захисту до певних типів атак. Детальний опис критеріїв наведено в Таблиці 4.1 із коротким поясненням кожного параметра. [15]

Для проведення багатокритеріального аналізу було обрано чотири найбільш поширені та показові типи DDoS-атак, які суттєво відрізняються за характером реалізації, рівнем технічної складності, навантаженням на інфраструктуру і способом впливу на сервіси.[16]

Обрані типи атак:

UDP-флуд є класичною об’ємною атакою, що спрямована на переповнення каналу великою кількістю непотрібного UDP-трафіку. Легко здійснюється та має високу швидкість, часто застосовується новачками. Виявляється системами захисту, але може бути ефективною при недостатньому налаштуванні безпеки.

TCP SYN-флуд атакує на рівні сеансового з’єднання, імітуючи створення великої кількості з'єднань без їх завершення. Це призводить до вичерпання ресурсів сервера. Хоча є відносно простою, вона більш витончена, ніж UDP-флуд, і потребує базових технічних знань.

HTTP Low&Slow діє на прикладному рівні, використовуючи легальні HTTP-запити, які надсилаються повільно, заважаючи серверу обробляти інші запити. Небезпечна тим, що важко помітна і важко виявляється традиційними засобами захисту. Її реалізація складніша і потребує досвіду.

Комбінована атака поєднує різні типи DDoS-навантажень (наприклад, SYN + UDP + HTTP Flood), які виконуються одночасно чи послідовно. Це найбільш продуманий і небезпечний варіант, який вимагає координації дій зловмисника,

використання ботнетів і ретельного планування. Зазвичай здійснюється професійними кіберзлочинцями або в контексті цільових атак.

Обрані типи атак дозволяють охопити різні рівні моделі OSI (від мережевого до прикладного) та різні сценарії атак — від простих і масових до точкових і цільових. Це дає можливість порівняти DDoS-загрози не тільки з технічної сторони, але й оцінити ризики з точки зору захисту, потреб реагування та потенційної шкоди. Всі оцінки у таблиці 4.2 базуються на узагальнених експертних даних, результатах моделювання, практиці реагування CERT-груп та матеріалах технічної документації провідних рішень з мережевої безпеки.

З метою отримання інтегральної оцінки кожного типу атаки було визначено вагові коефіцієнти для кожного критерію оцінювання. Це дозволяє відобразити відносну значущість кожного критерію в загальній структурі оцінки загрози.

Призначення ваг здійснюється в рамках методу аналізу ієрархій за допомогою експертного порівняння важливості критеріїв між собою. Зокрема, критерії, які мають безпосередній вплив на ризик функціонального порушення системи (наприклад, ефективність виявлення чи рівень захищеності), отримують вищу вагу. Натомість критерії, що стосуються непрямих або допоміжних аспектів (наприклад, складність реалізації атаки), мають нижчий вплив.

Ваги використовуються для нормалізованого зважування критеріїв перед підсумковим обчисленням інтегральної оцінки загрози. Це дозволяє враховувати не лише значення кожного параметру, але й його внесок у загальний ризик для інформаційної інфраструктури.

В Таблиці 4.3 наведено вагові коефіцієнти, які було використано для багатокритеріального оцінювання. Сума всіх ваг дорівнює 1, що забезпечує подальші коректні розрахунки.

Таблиця 4.1 – Критерії оцінювання атак на відмову в обслуговуванні

№	Критерій	Опис
1	2	3
1	Ефективність виявлення (%)	Ключова мета будь-якої системи захисту — швидке та точне виявлення загрози. Висока ефективність дозволяє зменшити ризик переривання сервісу.
2	Середній час реагування (сек)	Час реагування безпосередньо впливає на тривалість простою сервісу, втрати прибутку і довіри користувачів.
3	Стійкість до хибнопозитивів (від 1 до 5)	Висока точність виявлення дозволяє уникнути блокування легітимного трафіку, що критично для комерційних систем.
4	Споживання ресурсів (від 1 до 5)	Захисні системи можуть створювати навантаження на інфраструктуру. Параметр важливий для малих і середніх компаній.
5	Складність впровадження захисту (від 1 до 5)	Враховується необхідність технічної експертизи, витрати часу та ресурсів на інтеграцію рішень
6	Складність реалізації атаки (від 1 до 5)	Чим складніша атака для реалізації, тим менш імовірно, що вона буде здійснена, особливо аматорами.
7	Тип зловмисника (Аматор/ Професіонал/Суперпрофесіонал)	Дає уявлення про рівень загрози (від аматорських до організованих атак
8	Рівень шкоди (Незначна/Значна/Критична)	Оцінка масштабу негативного впливу на функціонування системи.
9	Ступінь захищеності системи (від 1 до 5)	Показує, наскільки типова IT-система готова до цього типу атаки.

Таблиця 4.2 – Багатокритеріальне оцінювання атак на відмову в обслуговуванні

Критерій/Атака	UDP-флуд	TCP SYN-флуд	HTTP Low&Slow	Комбінована
Ефективність виявлення (%)	90	85	60	80
Середній час реагування (сек)	3	4	12	6
Стійкість до хибнопозитивів (1-5)	5	4	3	4
Споживання ресурсів (1-5)	2	3	4	5
Складність впровадження захисту (1-5)	2	3	4	5
Складність реалізації (1-5)	1	2	3	5
Тип зловмисника	Аматор	Професіонал	Професіонал	Суперпрофесіонал
Рівень шкоди	Незначна	Значна	Критична	Критична
Ступінь захищеності системи (1-5)	3	3	2	1

Таблиця 4.3 – Вагові коефіцієнти, визначені для багатокритеріального оцінювання

Критерій	Позначка	Вага
Ефективність виявлення	ω_1	0,25
Середній час реагування	ω_2	0,15
Стійкість до хибнопозитивів	ω_3	0,10
Споживання ресурсів	ω_4	0,10
Складність впровадження захисту	ω_5	0,10
Складність реалізації	ω_6	0,10
Тип зловмисника	ω_7	0,10
Рівень шкоди	ω_8	0,10
Ступінь захищеності системи	ω_9	0,20

У процесі побудови системи оцінювання було сформовано дев’ять критеріїв, які охоплюють як технічні, так і загрозові аспекти атак. Однак для кількісного обчислення інтегральної оцінки було використано сім критеріїв, що наведені у таблиці вагових коефіцієнтів.

Це пояснюється тим, що два з дев’яти критеріїв — а саме: тип зловмисника та рівень потенційної шкоди мають якісний характер і не піддаються прямій нормалізації у межах шкали [0;1] без втрати інтерпретованості. У зв’язку з цим вони були виключені з формального обчислення, але відіграють аналітичну роль у висновках, де враховуються як додаткові фактори ризику. Зокрема, комбіновані атаки реалізуються здебільшого професійними групами, що підвищує їхню цілеспрямованість; HTTP Low&Slow при невеликому навантаженні здатні завдати непропорційно великої шкоди через труднощі виявлення.

Після призначення ваг та нормалізації оцінок усіх критеріїв до уніфікованого діапазону розрахунок інтегральної оцінки загрози кожного типу DDoS-атаки здійснюється за наступною формулою:

$$I = \sum_{i=2}^{n} \omega_i \cdot K_i^{'} \quad (4.1)$$

де:

- I — інтегральна оцінка загального рівня загрози;
- ω_i — ваговий коефіцієнт і-го критерію;
- $K_i^{'}$ — нормалізоване значення і-го критерію для конкретного типу атаки;
- n — кількість критеріїв (у цьому випадку — 7).

Ця формула дозволяє поєднати різнотипні характеристики в єдину кількісну метрику, що дозволяє об’єктивно порівняти альтернативи між собою.

На основі обчислень було сформовано узагальнену Таблицю 4.4 з оцінкою кожної атаки. Для спрощення сприйняття таблиця містить лише основні показники: назву типу атаки, інтегральну оцінку та рівень загрози.

Таблиця 4.4 – Оцінка атак на відмову в облуговуванні відповідно до обчислень.

Тип атаки	Інтегральна оцінка	Рівень загрози
UDP-флуд	0,862	Високий
TCP SYN-флуд	0,756	Помірно високий
Комбінована атака	0,444	Середній
HTTP Low&Slow	0,440	Середній/прихований

Рисунок 4.1 - Порівняння типів атак на відмову в облуговуванні за інтегральною оцінкою

Порогові значення інтерпретації:

- 0.80 — високий рівень загрози;
- 0.60 – 0.79 — помірно високий;
- 0.40 – 0.59 — середній;
- < 0.40 — низький.

На рисунку 4.1 наведено діаграму результатів обчислення. UDP флуд — найбільш небезпечна в умовах відсутності фільтрації та базового захисту. Висока швидкість атаки та низька вартість реалізації. TCP SYN флуд — дещо складніша, але все ще поширена атака на рівні транспортного протоколу.

Комбінована атака — технічно найскладніша, проте її складність реалізації компенсується меншою поширеністю. HTTP Low&Slow — "тиха" атака прикладного рівня, що вимагає поведінкового аналізу. Виявляється важко, але має нижчу ефективність масового ураження.

У цьому розділі було здійснено багатокритеріальне оцінювання основних типів атак на відмову в обслуговуванні (DoS/DDoS) із застосуванням методу аналізу ієрархій (AHP). На основі дев’яти критеріїв, які охоплюють технічні, організаційні та загрозові аспекти, було проведено порівняння чотирьох типів атак: UDP-флуд, TCP SYN-флуд, HTTP Low&Slow та комбінованої атаки.

Запропонований підхід дозволив не лише порівняти атаки за окремими характеристиками, а й отримати інтегральні оцінки, що відображають загальний рівень загрози. За результатами розрахунків найбільш небезпечною виявилася UDP-флуд атака (0,862), що пояснюється її високою ефективністю, швидкістю реалізації та широким розповсюдженням. TCP SYN-флуд (0,756) також продемонструвала високий рівень загрози. Натомість HTTP Low&Slow (0,440) та комбінована атака (0,444), хоч і технічно складніші, мають нижчі інтегральні показники через кращу підготовленість захисних систем до подібних сценаріїв або меншу ймовірність їх широкого використання.

Багатокритеріальний аналіз дозволяє глибше оцінити ризики від кіберзагроз, оскільки враховує як можливості зловмисників, так і слабкі місця захисної інфраструктури. Отримані результати можуть бути використані як

основа для пріоритезації заходів з кіберзахисту, вибору технологій та формування політик реагування. Крім того, адаптивність методики дозволяє її подальше використання для аналізу інших типів загроз або порівняння ефективності засобів захисту.

5 ЗАХИСТ ВІД КІБЕРАТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ НА РІЗНИХ РІВНЯХ МОДЕЛІ OSI

5.1 Аналіз механізмів захисту за рівнями моделі OSI

Дієвий захист інформаційних систем в умовах зростаючих кіберзагроз вимагає реалізації багаторівневої системи безпеки. Однією з ключових концептуальних моделей, яка дозволяє класифікувати та впорядковувати методи безпеки, є модель взаємодії відкритих систем OSI. Вона поділяє процес обміну даними на сім логічних рівнів, кожен з яких може бути ціллю для атак і відповідно – точкою для впровадження захисту.

У таблиці 5.1 наведено узагальнені дані щодо рівня надійності основних механізмів безпеки, згрупованих за рівнями моделі OSI. До цих механізмів належать шифрування, цифрові підписи, автентифікація, контроль доступу, контроль цілісності даних, управління маршрутами та інші. Відповідно до кожного з механізмів було визначено рівень їх ефективності, що дозволяє оцінити дієвість конкретного способу захисту в межах того чи іншого рівня OSI. Зокрема, найбільш ефективними були визнані методи автентифікації та маршрутизації, які забезпечують найбільшу надійність при належному впровадженні.

Ці дані наведено на основі дослідження М. Ю. Толкачова [17]

У контексті даного дослідження особливу увагу привертають механізми, які дозволяють ефективно протидіяти атакам на відмову в обслуговуванні (DDoS-атакам).

Таблиця 5.1 - Узагальнені дані щодо рівня надійності основних механізмів безпеки, згрупованих за рівнями моделі OSI

	Шифрування	Цифровий підпис	Керування доступом	Контроль цілісності даних	Автентифікаційний обмін	Заповнення трафіку	Керування маршрутом
	1	2	3	4	5	6	7
Фізичний рівень	Використовується мінімально (наприклад фізичні пристрої шифрування для маршрутизаторів).	Використовується для захисту доступу до фізичних пристроїв (наприклад, на рівні вхідного контролю).	Забезпечує фізичний контроль доступу до обладнання, що знижує фізичний ризик зламів і крадіжок.	Захищає цілісність даних на фізичних пристроях, хоча реалізація може бути складною.	Використовується для автентифікації фізичних пристроїв, забезпечуючи початковий рівень безпеки.	Допомагає зменшити ризик перехоплення даних на фізичному рівні шляхом генерації додаткових пакетів.	Забезпечує безпечне направлення трафіку, що знижує ризики перехоплення на фізичному рівні.
Емпіричний рівень	Необхідне для захисту передачі емпіричних даних (наприклад, HTTPS для веб з'єднань)	Важливий для підтвердження автентичності емпіричних даних (наприклад, документи).	Забезпечує контроль доступу до емпіричних даних у системах (наприклад, обмеження на доступ до документів).	Ефективний для перевірки цілісності емпіричних даних (наприклад, для збереження логів).	Корисний для автентифікації передавачів емпіричних даних, зменшує ризик підробки даних	Використовується для приховання емпіричних даних під час передачі, знижує ймовірність виявлення трафіку.	Важливий для контролю маршрутів емпіричних даних, забезпечуючи оптимальне передавання через безпечні вузли.
Синтаксичний рівень	Високий захист від атак на синтаксичному рівні, особливо для мережевих пакетів і формату даних.	Часто використовується для підтвердження автентичності пакетів даних, але не завжди ефективний проти атак.	Захищає від несанкціонованого доступу до даних, але іноді є вразливим до соціальної інженерії.	Ефективно застосовується до даних на рівні протоколу, захищає від змін у форматі або структурі пакетів.	Забезпечує захист на рівні протоколів мережі (наприклад, SSL/TLS), але може мати обхідні шляхи.	Зменшує ризик атак на синтаксичному рівні, приховуючи реальні дані у великому обсязі "заповненого" трафіку.	Дозволяє зменшити ризики на рівні протоколу, обираючи безпечні маршрути для передачі даних.

Продовження таблиці 5.1

Семантичний рівень	Обмежене використання : частковий захист значень даних, але не їх контексту.	Ефективний для захисту автентичності інформації, проте не захищає змістовний контекст даних.	Контролює доступ до певних даних, проте може бути обійдений при витоку інформації.	Забезпечує базову цілісність значень даних, проте не завжди ефективний для запобігання їх витоку	Часто не застосовується для семантичного рівня, проте важливий для автентифікації користувачів.	Рідко застосовується, оскільки мало впливає на значення даних.	Рідко використовується для цього рівня, оскільки не забезпечує контекстуального захисту даних.
Прагматичний рівень	Використовується для захисту даних користувачів у месенджерах та електронній пошті, але не завжди захищає метадані.	Дозволяє перевірку достовірності повідомлень, що корисно для збереження довіри.	Часто використовується для захисту конфіденційних даних, але вразливий до фішингових атак.	Важливий для збереження цілісності особистих повідомлень і файлів, але уразливий до складних атак.	Дозволяє автентифікацію користувачів для захисту доступу до конфіденційних даних, але уразливий до атак.	Низький рівень застосування, оскільки практично не використовується для приховання контексту повідомлень.	Практично не застосовується, оскільки управління маршрутом не впливає на практичне використання даних.
Соціальний рівень	Низький рівень застосування, оскільки соціальні взаємодії часто не шифруються, особливо в соцмережах.	Використовується рідко, оскільки часто обмежений соцмережами та особистими контактами.	Захищає взаємодії користувачів, але може бути вразливим, якщо політика доступу слабка або не оновлена.	Часто недостатньо ефективний для захисту цілісності взаємодій користувачів, особливо у відкритих соцмережах	Часто вимагає посилення, оскільки багато взаємодій користувачів у соцмережах мають слабку автентифікацію.	Практично не застосовується для соціального рівня, де важливий зміст, а не обсяг трафіку.	Мало застосовується, оскільки соціальні взаємодії часто проходять через стандартні мережі, без налаштування маршрутів.

<table>
<tr><th>1.РОЗВІДКА</th><th>2.ПОЧАТКОВЕ ВТРУЧАННЯ</th><th>3.РОЗШИРЕННЯ ПОВНОВАЖЕНЬ</th><th>4.ПОДАЛЬША ЕКСПЛУАТАЦІЯ</th></tr>
<tr><td colspan="2">Організація периметра захисту</td><td colspan="2">Розмежування повноважень та управління обліковими записами при доступі до програмних та технічних ресурсів організації</td></tr>
<tr><td colspan="2">Захищеність серверного забезпечення</td><td colspan="2">Мінімальні повноваження для облікових записів</td></tr>
<tr><td colspan="4">Збирання та аудит журнальних файлів активного мережного та серверного обладнання</td></tr>
<tr><td></td><td colspan="2">Антивірусне програмне забезпечення</td><td>Контроль та запис сесій (особливо – адміністративних)</td></tr>
<tr><td>Антивірусне програмне забезпечення</td><td>Захист від фішингу</td><td>Контроль та запис сесій (особливо –адміністративних)</td><td>Реалізація безпеки систем та середовищ віртуалізації</td></tr>
<tr><td></td><td colspan="2">Навчання та тренування персоналу</td><td>Управління ідентифікацією та авторизацією (багатофакторна автентифікація)</td></tr>
<tr><td></td><td></td><td colspan="2">Реалізація політики безпеки у форсмажорних/нестандартних ситуаціях та політики безпеки при реагуванні на зовнішні для організації загрози</td></tr>
<tr><td></td><td></td><td></td><td>Впровадження елементів/політики управління</td></tr>
</table>

Рисунок 5.1 - Етапи побудови багаторівневої системи захисту від кібератак

5.2 Захист від DDoS-атак за рівнями моделі OSI

Як уже згадувалося раніше, напади на відмову в службі (DDoS) є однією з найнебезпечніших форм кіберзагроз у сучасних цифрових умовах.

Характерною особливістю атак на відхилення є те, що вони реалізуються з декількох джерел одночасно, що імітує нормальну активність, при цьому значно ускладнюючи ідентифікацію загроз та захисту.

Модель OSI розділена на сім логічних рівнів, але в деяких випадках може бути реалізований захист DDoS.

На мережевому рівні основними методами протидії є фільтрація IP-адрес, блокування небажаних підмереж, контроль ICMP-трафіку та маршрутизація через безпечні вузли. Це дозволяє зупиняти ворожий трафік ще до того, як він надходить до серверних систем. На транспортному рівні доцільним є застосування механізмів підтвердження TCP-з'єднання без резервування ресурсів (SYN cookies), налаштування таймаутів, обмеження кількості відкритих з'єднань, використання міжмережевих екранів та балансувальників навантаження. Ці заходи допомагають зменшити ризик перевантаження серверних портів і запобігають надмірному використанню ресурсів.

Сеансовий рівень встановлює обмеження на кількість одночасних сесій, адаптивне управління таймаутами та виявлення аномальної активності, забезпечуючи додатковий бар'єр. На прикладному рівні реалізуються найскладніші форми захисту — виикористання механізмів верифікації користувача (CAPTCHA), поведінкова аналітика, обмеження частоти запитів та використання веб-аплікаційних фаєрволів. Ці інструменти дозволяють ідентифікувати автоматизовану активність зловмисника, яка маскується під справжніх користувачів.

Організаційний рівень не є частиною класичної моделі OSI, але він забезпечує моніторинг, управління інцидентами, а також своєчасну реакцію на аномальні активності в трафіку. Саме тут реалізуються системи виявлення та

попередження атак, централізоване логування, SIEM-платформи та автоматизовані сценарії реагування.

Таким чином, ефективна протидія DDoS-атакам можлива лише за умови реалізації комплексного, багаторівневого підходу до безпеки. Використання інструментів захисту на кількох рівнях одночасно дозволяє зменшити вразливість системи, своєчасно виявити загрозу та мінімізувати її наслідки.

Найвищу ефективність демонструють поєднання механізмів автентифікації, маршрутизації, шифрування і контролю доступу, які розподіляються між різними рівнями моделі OSI. Це підтверджує актуальність багаторівневої архітектури безпеки як основи для захисту сучасних інфокомунікаційних систем від атак типу DDoS.

5.3 Етапи побудови багаторівневої системи захисту від кібератак

Результатом проведеного дослідження стало формування узагальненої моделі захисту, яка охоплює ключові етапи реагування на загрози у цифровому середовищі. На рисунку 5.1 представлена запропонована система захисту, яка складається з чотирьох логічно послідовних етапів, що охоплюють повний цикл протидії кібератакам – від виявлення потенційних ризиків до управління наслідками та відновлення. Розвідка – це початковий етап, на якому критично важливо забезпечити захист периметра мережі, виявлення зовнішніх сканувань та контроль доступу до інфраструктури. Початкове втручання – передбачає виявлення та блокування перших спроб порушення безпеки за допомогою базових інструментів (антивіруси, фільтрація фішингових повідомлень, аудит журналів подій). Розширення повноважень – включає заходи з контролю облікових записів, мінімізації привілеїв користувачів, управління адміністративними сесіями та багатофакторної аутентифікації, що дозволяє уникнути захоплення критичних ресурсів. Подальша експлуатація – це етап реалізації стратегічних політик безпеки, включаючи реагування на інциденти,

моніторинг у віртуалізованих середовищах, підготовку персоналу, а також впровадження елементів управління ризиками.

Таким чином, запропоновані заходи захисту формують цілісну, багаторівневу систему кібербезпеки, що поєднує технічні, процедурні та організаційні компоненти. Ця модель може бути адаптована до різних типів організацій і вважається ефективним інструментом для підвищення стійкості до складних атак, зокрема DDoS. Вона доповнює технічні рекомендації за рівнями OSI, розширюючи їх у напрямку управління повним циклом захисту.

ВИСНОВКИ

У результаті дослідження методів захисту мережі від кібератак зроблено низку важливих висновків. Аналіз сучасного стану кіберзагроз показав, що кібератаки, зокрема атаки типу відмови в обслуговуванні (DoS/DDoS), залишаються однією з найбільш небезпечних форм цифрового втручання, здатною виводити з ладу критичну інфраструктуру.

Значна увага була приділена класифікації атак, що дозволило систематизувати їх за джерелом, способом реалізації, рівнем впливу та типом застосованих інструментів. Розгляд моделі кіберзлочинця допоміг краще зрозуміти логіку дій зловмисників і адаптувати захисні заходи відповідно до рівня загрози.

Дослідження DDoS-атак показало необхідність впровадження комплексної системи протидії, яка включає не лише технічні засоби, а й моделювання ризиків. Проведене моделювання комбінованої атаки засвідчило критичну важливість параметрів, пов’язаних із буферною пам’яттю та пропускною здатністю мережі.

Особливу цінність має застосування багатокритеріального методу оцінювання на основі аналізу ієрархій (AHP), що дозволяє врахувати широкий спектр факторів — від технічної складності атаки до ефективності реагування системи. Це дає можливість обґрунтовано пріоритезувати загрози.

Нарешті, реалізація захисту за рівнями моделі OSI підтвердила ефективність багаторівневої архітектури безпеки. Лише поєднання засобів фільтрації, автентифікації, маршрутизації, обмеження сесій та поведінкової аналітики забезпечує стійкість системи до атак.

Отже, протидія кібератакам вимагає інтегрованого підходу — поєднання аналітики, технологій і стратегії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України Про основні засади забезпечення кібербезпеки України : Верхова Рада України від 05.10.2017, № № 2163-VIII : станом на 27.03.2025. URL: Про основні засади забезпе... | від 05.10.2017 № 2163-VIII (дата звернення: 30.04.2025).
2. За час повномасштабної війни Україна зазнала більш як 600 кібератак - це п’ята частина від усіх кібератак у світі. *Укрінформ*. 30.04.2025. URL: Україна під час повномасштабної війни зазнала більш як 600 кібератак (дата звернення: 30.04.2025).
3. Державна Служба Спеціального Зв’язку Та Захисту Інформації України. Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії. *Державна служба спеціального зв’язку та захисту інформації України*. 21.01.2023. URL: КІБЕРАТАКИ, АРТИЛЕРІЯ, ПРОПАГАНДА. ЗАГАЛЬНИЙ ОГЛЯД ВИМІРІВ РОСІЙСЬКОЇ АГРЕСІЇ (дата звернення: 30.04.2025).
4. Російсько-українська кібервійна. *Вікіпедія*. URL: Російсько-українська кібервійна — Вікіпедія (дата звернення: 30.04.2025).
5. Глава УЗ спрогнозував, скільки триватиме повне відновлення IT-сервісів після кібератаки. *Слово і діло*. 01.04.2025. URL: Кібератака на Укрзалізницю – повне відновлення всіх сервісів займе щонайменше кілька тижнів » Слово і Діло (дата звернення: 01.05.2025).
6. Types of Cybersecurity Attacks. *Rapid7*. URL: Types of Cyber Attacks | Hacking Attacks & Techniques - Rapid7 (дата звернення: 30.04.2025).
7. Active and Passive attacks in Information Security. *Https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/*. URL: Active and Passive attacks in Information Security - GeeksforGeeks (дата звернення: 29.04.2025).

8. Threat Actors Explained. *Crowdstrike.com*. *Cyber Threat Intelligence Explained*. 04.03.2025. URL: What is a Cyber Threat Actor? | CrowdStrike (дата звернення: 29.05.2025).
9. Understanding Cyber Threat Actors: Types, Motivations, and Damage. *Redlegg.com*. *Cyber Threat*. 09.04.2023. URL: 7 Types of Cyber Threat Actors And Their Damage (дата звернення: 29.05.2025).
10. Advanced Persistent Threats (APT) Explained. *Crowdstrike.com*. *Cyber Threat Intelligence Explained*. 04.03.2025. URL: What is an Advanced Persistent Threat (APT)? | CrowdStrike (дата звернення: 29.05.2025).
11. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем / С. П. Євсєєв та ін. *Кібербезпека: освіта, наука,техніка*. 2018. Т. 2 : Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. С. 47–67.
12. Поночовний П. М. Модель упередження низькошвидкісних http ddos атак на кінцевого користувача. *Кібербезпека: освіта, наука,техніка*. 2024. Т. 2, вип. 26 : Модель упередження низькошвидкісних http ddos атак на кінцевого користувача. С. 291–304.
13. How to prevent DDoS attacks | Methods and tools. *Https://www.cloudflare.com/*. URL: How to prevent DDoS attacks | Methods and tools | Cloudflare (дата звернення: 17.05.2025).
14. Saati T. L., Vagras L. G. Models, Methods, Concepts & Applications of the Analytic Hierarchy Process / ред. F. Hillier ; Stanford University, CA, USA. London : Springer New York Heidelberg Dordrecht, 1980. 343 с.
15. Щодо невідкладних заходів кіберзахисту. *Cert.gov.ua*. *Рекомендації*. 12.09.2022. URL: CERT-UA (дата звернення: 13.06.2025).
16. What is a DDoS attack?. *Cloudflare.com*. URL: What is a distributed denial-of-service (DDoS) attack? | Cloudflare (дата звернення: 13.06.2025).
17. Толкачов М. Механізми захисту трафіку в кіберпросторі. *Сучасний захист інформації*. 2024. Т. 4, вип. 60 : Механізми захисту трафіку в кіберпросторі. С. 85–99.