УДК 004.056:004.7 **doi: 10.26906/SUNZ.2026.2.073**

Т. М. Деркач[1], Г. В. Головко[1], А. О. Дмитренко[1], Л. А. Клочко[2]

[1] Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
[2] Геологічне бюро BEG SA, Швейцарія

АНАЛІЗ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ОБҐРУНТУВАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ЇХ КІБЕРБЕЗПЕКИ

Анотація. У статті здійснено комплексний аналіз сучасних загроз та вразливостей комп'ютерних мереж, що виникають у процесі функціонування мережевої інфраструктури в умовах стрімкого розвитку цифрових технологій та зростання кількості кіберзагроз. Особливу увагу приділено дослідженню архітектурних і протокольних вразливостей мережі, зокрема на канальному та транспортному рівнях моделі взаємодії відкритих систем (OSI), які часто стають початковим етапом реалізації складних кібернетичних атак. У роботі проведено систематизацію та класифікацію основних типів мережевих атак за характером впливу, джерелом походження та рівнем мережевої моделі, на якому вони реалізуються. Розглянуто особливості пасивних і активних атак, внутрішніх та зовнішніх загроз, а також їхній вплив на конфіденційність, цілісність і доступність інформаційних ресурсів. Значну увагу приділено аналізу сучасних методів мережевої розвідки та сканування, які використовуються як фахівцями з кібербезпеки для проведення аудиту інформаційних систем, так і потенційними зловмисниками для виявлення вразливостей мережевої інфраструктури. Досліджено механізми пасивної та активної мережевої розвідки, включаючи методи збору інформації з відкритих джерел, сканування хостів, аналіз мережевих портів, ідентифікацію мережевих сервісів, визначення операційних систем та виявлення відомих вразливостей. Встановлено, що використання таких методів дозволяє формувати детальну карту мережевої інфраструктури, що може бути використано для підготовки подальших етапів кібернападу. Окремий розділ дослідження присвячено аналізу архітектурних вразливостей канального рівня, які виникають через відсутність механізмів автентифікації в базових протоколах сімейства IEEE 802. Розглянуто особливості реалізації атак, пов'язаних із маніпуляцією кадрами Ethernet, зокрема атак на таблиці комутації, ARP-спуфінг, VLAN hopping, а також атаки на інфраструктуру DHCP та протокол Spanning Tree. Показано, що експлуатація таких вразливостей може призводити до перехоплення мережевого трафіку, порушення сегментації мережі, підміни маршрутів передачі даних або організації відмови в обслуговуванні. Значну увагу приділено дослідженню атак на відмову в обслуговуванні (Denial of Service) та розподілених атак (Distributed Denial of Service), які належать до найбільш поширених кіберзагроз у сучасних інформаційних системах. Проаналізовано механізми реалізації волюметричних атак, атак транспортного рівня та атак із підсиленням, що використовують уразливості мережевих сервісів для генерації значних обсягів трафіку. Розглянуто роль ботнетів та пристроїв Інтернету речей у формуванні масштабних розподілених атак, здатних суттєво впливати на доступність інформаційних ресурсів. На основі проведеного аналізу обґрунтовано доцільність застосування комплексного підходу до забезпечення безпеки комп'ютерних мереж. Такий підхід передбачає поєднання конфігураційних, криптографічних та організаційних заходів захисту, що реалізуються на різних рівнях мережевої інфраструктури. Показано, що застосування принципу багаторівневого захисту дозволяє підвищити стійкість інформаційних систем до сучасних кіберзагроз, мінімізувати ризики експлуатації вразливостей та забезпечити стабільне функціонування мережевих сервісів. Результати дослідження можуть бути використані під час розроблення політик інформаційної безпеки, проектування захищених корпоративних мереж, проведення аудиту кібербезпеки та навчання фахівців у галузі інформаційних технологій і кіберзахисту.

Ключові слова: комп'ютерні мережі, кібербезпека, мережеві атаки, мережева розвідка, сканування мережі, вразливості мережевих протоколів, DoS-атаки, DDoS-атаки, інформаційна безпека.

Постановка проблеми

Сучасні комп'ютерні мережі є критичною складовою інформаційної інфраструктури державних, промислових та комерційних систем. Водночас зростання складності мережевих архітектур, активне використання хмарних сервісів, Інтернету речей (IoT) та мобільних технологій призводить до підвищення ризику виникнення кіберзагроз. Одними з найбільш критичних є вразливості на канальному та транспортному рівнях, оскільки вони можуть використовуватися як початкові точки проникнення для реалізації складних атак, таких як DoS/DDoS, ARP spoofing, VLAN hopping та інші.

Недостатній контроль доступу, відсутність багатофакторної автентифікації, помилки у конфігурації мережевого обладнання та незашифровані канали передачі даних створюють передумови для витоку інформації, порушення цілісності та доступності ресурсів. В умовах зростання кількості та складності кіберзагроз постає задача систематизації мережевих атак, аналізу методів розвідки та сканування, дослідження архітектурних вразливостей та обґрунтування ефективних механізмів захисту, що включають конфігураційні, криптографічні та організаційні заходи.

Мета та завдання дослідження

Метою дослідження є комплексний аналіз вразливостей комп'ютерних мереж, класифікувати сучасні загрози та атаки, оцінити методи мережевої розвідки та сканування, а також обґрунтувати доцільність застосування багаторівневого підходу до захисту корпоративної мережевої інфраструктури.

Основні завдання дослідження:

1. Проаналізувати сучасний стан проблеми безпеки комп'ютерних мереж.
2. Систематизувати та класифікувати мережеві загрози та атаки за типом, джерелом і рівнем OSI.
3. Дослідити методи мережевої розвідки та сканування, їхню роль у підготовці атак та оцінці захищеності.

4. Проаналізувати механізми DoS/DDoS атак, волюметричних і транспортних атак, а також атак із підсиленням.

5. Обґрунтувати комплексний підхід до захисту мереж, поєднуючи конфігураційні, криптографічні та організаційні заходи.

Аналіз досліджень і публікацій

Проблема захисту комп'ютерних мереж у сучасних умовах розвитку цифрових технологій та зростання частоти кібератак привертає значну увагу наукової спільноти. Аналіз наукових джерел показує, що питання вразливостей мережевої інфраструктури розглядаються як у загальному контексті кібербезпеки, так і в аспекті окремих мережевих протоколів та технологій.

У класичних роботах із мережевих технологій та безпеки, зокрема у працях A. S. Tanenbaum та D. J. Wetherall, розкрито фундаментальні принципи побудови комп'ютерних мереж, що дозволяє зрозуміти природу протокольних механізмів і потенційні зони вразливостей у базових мережевих технологіях [1]. Аналогічно, у виданнях J. F. Kurose і K. W. Ross подано системний опис моделі OSI та стеку TCP/IP, який є основою для подальших досліджень мережевих атак і засобів захисту [2]. Проте такі роботи носять радше освітній характер і не завжди глибоко аналізують специфічні загрози на канальному рівні.

Дослідження W. Stallings спрямовані на прикладні аспекти мережевої безпеки, включаючи криптографічні методи захисту, моделі автентифікації та управління доступом [3]. У цьому контексті підкреслюється важливість криптографії для захисту даних при передачі, однак механізми захисту канального рівня розглядаються побіжно або лише в загальному вигляді.

У дослідженнях R. Anderson висвітлено актуальні концепції безпечної архітектури розподілених систем, у тому числі загрози, що виникають при взаємодії різнорідних мережевих компонентів та сервісів [4]. Він розглядає загальні принципи побудови захищених систем, проте не приділяє достатньої уваги деталям реалізації конкретних атак на канальний рівень.

Публікації, присвячені безпосередньо мережевим атакам і механізмам їх реалізації, включають роботи, що аналізують технології сканування мереж, відмови в обслуговуванні та посилені атаки, зокрема J. M. Stewart та співавтори в CISSP Official Study Guide [5], а також у контексті класифікації DDoS-загроз [6]. Дані праці детально описують тактики та техніки атак, але переважно охоплюють загальні класи загроз без поглибленого розгляду протоколів канального рівня.

Проблематика забезпечення кібербезпеки комп'ютерних мереж є науковим напрямком досліджень також і українських науковців [7–10]. У роботах значна увага приділяється дослідженню архітектурних особливостей комп'ютерних мереж та механізмів їх захисту. У роботах В. Бурячка, Г.Гулака та В. Толубка [11], розглядаються основні принципи забезпечення інформаційної безпеки в комп'ютерних системах, а також класифікація загроз і методів протидії мережевим атакам. Дослідження М. Корченка [12] присвячені аналізу сучасних кіберзагроз, методам виявлення атак та побудові систем захисту інформаційних ресурсів.

У науковій літературі також широко висвітлюються питання мережевої розвідки та сканування. Дослідники відзначають, що етап збору інформації є важливою складовою більшості кібернападів, оскільки дозволяє зловмисникам отримати відомості про структуру мережі, відкриті порти та використовуване програмне забезпечення. Аналіз відповідних методів дозволяє підвищити ефективність систем виявлення вторгнень та аудиту інформаційної безпеки.

Аналіз наукових публікацій свідчить, що ефективне забезпечення кібербезпеки комп'ютерних мереж потребує комплексного підходу, який поєднує технічні, криптографічні та організаційні засоби захисту. Проте подальших досліджень потребують питання вдосконалення методів виявлення атак, аналізу вразливостей мережевих протоколів та підвищення стійкості інформаційних систем до сучасних кіберзагроз.

Виклад основного матеріалу

1. У сучасних умовах стрімкого розвитку інформаційних технологій комп'ютерні мережі стали невід'ємною складовою функціонування державних, промислових і комерційних інформаційних систем. Активне впровадження хмарних сервісів, мобільних технологій, систем Інтернету речей (IoT) та розподілених обчислювальних платформ сприяє підвищенню ефективності обробки та передачі даних, однак водночас призводить до значного зростання кількості кіберзагроз і ускладнення процесу забезпечення інформаційної безпеки.

Однією з ключових проблем сучасної кібербезпеки є збільшення кількості та різноманітності мережевих атак. Дослідження показують, що комп'ютерні мережі можуть зазнавати впливу різних типів загроз, серед яких найбільш поширеними є атаки відмови в обслуговуванні (DoS/DDoS), перехоплення мережевого трафіку, підміна мережевих адрес, несанкціонований доступ до ресурсів та експлуатація вразливостей програмного забезпечення. Суттєвою тенденцією розвитку кіберзагроз є поява гібридних та багаторівневих атак, які поєднують різні методи впливу на інформаційні системи. Сучасні дослідження демонструють, що для виявлення складних мережевих атак дедалі ширше застосовуються технології машинного навчання та штучного інтелекту, які дозволяють аналізувати великі обсяги мережевого трафіку та виявляти аномалії у поведінці систем. Ще однією важливою проблемою є зростання масштабів кіберзагроз для критичної інформаційної інфраструктури. Зокрема, у сучасному кіберпросторі спостерігається тенденція до використання кібератак як інструменту інформаційного та політичного впливу. Отже, аналіз сучасного стану проблеми безпеки комп'ютерних мереж свідчить про постійне зростання складності кіберзагроз і необхідність застосування комплексних мето-

дів їх протидії. Подальші дослідження у цій сфері мають бути спрямовані на вдосконалення методів виявлення мережевих атак, використання технологій штучного інтелекту для аналізу кіберзагроз та підвищення стійкості інформаційних систем до сучасних кібератак.

2. Класифікація загроз та атак на мережеву інфраструктуру. Мережева атака розглядається як сукупність навмисних дій, спрямованих на експлуатацію вразливостей апаратного або програмного забезпечення з метою порушення конфіденційності, цілісності чи доступності інформації. Для побудови ефективної моделі захисту необхідною є систематизація існуючих типів атак.

За характером впливу атаки поділяються на пасивні та активні. Пасивні атаки не передбачають безпосереднього втручання в роботу системи та спрямовані на перехоплення або аналіз трафіку. Основною небезпекою цього класу загроз є їх прихований характер, оскільки вони не порушують цілісність даних і практично не фіксуються стандартними засобами моніторингу. Єдиним ефективним методом протидії є превентивне шифрування каналів зв'язку.

Активні атаки передбачають безпосередню модифікацію інформаційних потоків або порушення роботи сервісів. До них належать маскарад, модифікація повідомлень, повторна передача перехоплених даних та атаки відмови в обслуговуванні. Реалізація таких атак потребує глибокого розуміння принципів функціонування мережевих протоколів та механізмів маршрутизації.

За джерелом загрози атаки поділяються на зовнішні та внутрішні. Внутрішні загрози є особливо небезпечними, оскільки внутрішній трафік часто підлягає менш жорсткому контролю. Саме це зумовлює необхідність сегментації мережі та впровадження механізмів контролю доступу на канальному рівні.

3. Технічний аналіз методів мережевої розвідки та сканування. Етап збору інформації є обов'язковою складовою більшості цілеспрямованих мережевих атак. На цьому етапі зловмисник визначає активні вузли, відкриті порти та версії сервісів, що дозволяє сформувати карту мережі та підготувати подальшу експлуатацію.

У сучасних умовах цифровізації важливого значення набуває дослідження методів мережевої розвідки та сканування. Дані методи застосовуються як у діяльності фахівців із кібербезпеки для оцінювання захищеності інформаційних систем, так і потенційними зловмисниками з метою виявлення вразливостей мережевої інфраструктури. Мережева розвідка є початковим етапом аналізу комп'ютерної мережі, що передує більш складним формам кібернападів або, навпаки, використовується для проведення аудиту безпеки.

У науковій та практичній літературі виділяють два основних типи мережевої розвідки: *пасивну* та *активну*.

Пасивна мережева розвідка передбачає збір інформації без прямої взаємодії з цільовою системою. У межах такого підходу використовуються відкриті джерела інформації, аналіз доменних записів, публічних мережевих сервісів, метаданих та інші методи OSINT (Open Source Intelligence). Основною перевагою цього методу є низька ймовірність виявлення, оскільки безпосередній контакт із досліджуваною системою відсутній.

Активна мережева розвідка, навпаки, передбачає безпосередню взаємодію з мережею або її вузлами шляхом надсилання запитів до серверів, сканування портів, перевірки доступності сервісів тощо. Такий підхід дозволяє отримати більш детальну інформацію, однак може бути зафіксований системами виявлення вторгнень або мережевими засобами моніторингу. Мережеве сканування є ключовим інструментом активної розвідки та використовується для виявлення доступних вузлів мережі, відкритих портів, активних сервісів та конфігурації операційних систем. Основною метою сканування є визначення потенційних точок доступу до мережевої інфраструктури. Серед найбільш поширених методів мережевого сканування виділяють такі.

– Сканування портів (Port Scanning). Цей метод спрямований на визначення відкритих, закритих або фільтрованих портів у мережевих вузлах. Відкриті порти можуть свідчити про наявність активних мережевих сервісів, таких як вебсервери, поштові служби або віддалений доступ. Аналіз відкритих портів дозволяє ідентифікувати потенційні точки проникнення до системи.

– Сканування хостів (Host Discovery). Даний метод використовується для визначення активних пристроїв у мережі. Найчастіше він реалізується за допомогою ICMP-запитів, ARP-сканування або TCP-запитів. Результатом такого аналізу є формування переліку доступних мережевих вузлів.

– Сканування сервісів (Service Scanning). Після виявлення відкритих портів здійснюється аналіз запущених на них сервісів. Це дозволяє визначити тип програмного забезпечення, його версію та конфігурацію. Отримана інформація є важливою для подальшого аналізу потенційних вразливостей.

– Визначення операційної системи (OS Fingerprinting). Метод передбачає аналіз особливостей мережевих відповідей системи з метою встановлення типу операційної системи та її версії. Визначення операційної системи дозволяє звузити коло можливих експлойтів або вразливостей.

– Сканування вразливостей (Vulnerability Scanning). Цей метод полягає у порівнянні отриманої інформації про систему з відомими базами вразливостей. На основі такого аналізу формується перелік потенційних загроз безпеці мережі.

Для реалізації описаних методів використовуються спеціалізовані програмні інструменти, які автоматизують процес аналізу мережевої інфраструктури. Такі системи дозволяють здійснювати комплексне дослідження мережі, включаючи виявлення вузлів, аналіз портів, ідентифікацію сервісів та оцінювання рівня безпеки.

Сучасні інструменти мережевої розвідки забезпечують високу швидкість сканування, підтримку різних протоколів та можливість інтеграції з системами управління інформаційною безпекою (рис. 1).

Їх використання є важливим елементом процесу тестування на проникнення (penetration testing) та аудиту інформаційної безпеки.

Розуміння механізмів мережевого сканування є критично важливим для коректного налаштування систем виявлення вторгнень і фільтрації трафіку.

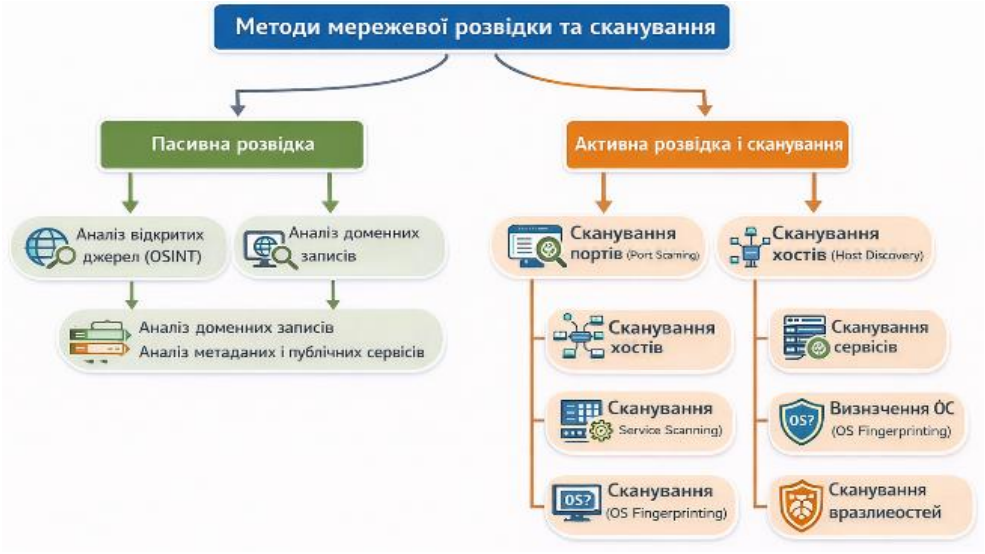

Рис. 1. Методи мережевої розвідки та сканування

4. Атаки на відмову в обслуговуванні (Denial of Service, DoS) та розподілені атаки відмови в обслуговуванні (Distributed Denial of Service, DDoS) належать до найбільш поширених і небезпечних типів кіберзагроз у сучасному інформаційному середовищі. Їх основною метою є порушення доступності інформаційних ресурсів, мережевих сервісів або обчислювальних систем шляхом навмисного перевантаження інфраструктури великою кількістю запитів чи мережевого трафіку. У результаті таких дій легітимні користувачі не можуть отримати доступ до вебсайтів, серверів, мережевих сервісів або інших інформаційних ресурсів, що призводить до фінансових втрат, зниження довіри до організації та порушення безперервності бізнес-процесів.

Атака типу DoS зазвичай здійснюється з одного джерела або з обмеженої кількості пристроїв, що генерують значний обсяг запитів до цільової системи. У свою чергу, атаки типу DDoS реалізуються за допомогою великої кількості скомпрометованих пристроїв, об'єднаних у так звані ботнети. До складу таких мереж можуть входити тисячі або навіть мільйони заражених комп'ютерів, серверів або пристроїв Інтернету речей (IoT), які координовано надсилають запити до цільового ресурсу. Використання розподіленої інфраструктури значно ускладнює виявлення джерела атаки та підвищує її ефективність. З технічної точки зору атаки на відмову в обслуговуванні можуть реалізовуватися на різних рівнях моделі взаємодії відкритих систем (OSI). Найбільш поширеними є атаки мережевого, транспортного та прикладного рівнів. Кожен із цих типів має свої особливості та механізми впливу на інформаційні системи.

Однією з найбільш поширених категорій є *волюметричні атаки* (volumetric attacks), які спрямовані на перевантаження пропускної здатності мережевого каналу цільової системи. У межах таких атак генерується значний обсяг мережевого трафіку, який перевищує можливості обробки або передачі даних сервером чи мережевим обладнанням. У результаті мережеві канали стають перевантаженими, що призводить до різкого зниження швидкості доступу або повної недоступності сервісу. До цієї категорії належать, зокрема, UDP-флуд атаки, ICMP-флуд та інші види масованого надсилання пакетів.

Іншою важливою категорією є атаки *транспортного рівня*, які спрямовані на виснаження ресурсів серверів або мережевого обладнання шляхом експлуатації механізмів встановлення мережевих з'єднань. Одним із найбільш відомих прикладів є SYN-flood атака, яка використовує особливості встановлення TCP-з'єднання. У процесі такої атаки сервер отримує велику кількість запитів на встановлення з'єднання, але завершення процедури рукостискання (TCP three-way handshake) не відбувається. У результаті сервер змушений утримувати велику кількість напіввідкритих з'єднань, що поступово призводить до вичерпання його обчислювальних ресурсів та неможливості обслуговувати легітимні запити. Окрему категорію становлять *атаки з підсиленням* (*amplification attacks*), які базуються на використанні мережевих сервісів, здатних генерувати відповіді значно більшого обсягу, ніж початковий запит. У такому випадку атакуючий надсилає невеликі запити до відкритих серверів із підробленою IP-адресою жертви. Сервери, у свою чергу, надсилають відповіді значно більшого розміру на адресу цільової системи, що призводить до різкого збільшення обсягу трафіку. Прикладами таких атак є DNS amplification, NTP amplification та інші варіанти використання відкритих мережевих служб для підсилення атаки. Крім зазначених типів, значного поширення набули *атаки прикладного рівня*, спрямовані на перевантаження конкретних вебсервісів або прикладних програм. У межах таких атак генеруються численні запити до вебсторінок, API або баз даних, що призводить до перевантаження серверних проце-

сів. Особливість цього типу атак полягає в тому, що вони часто імітують легітимну поведінку користувачів, що значно ускладнює їхнє виявлення традиційними мережевими засобами захисту.

Важливою тенденцією останніх років є використання *розподілених мереж заражених пристроїв (ботнетів)* для проведення масштабних DDoS-атак (рис. 2).

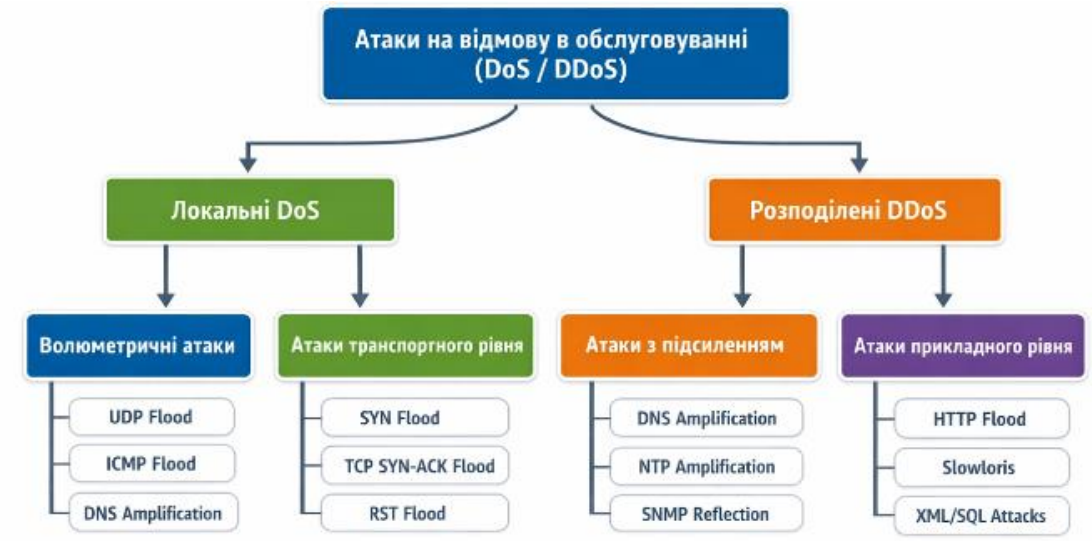

Рис 2. Класифікації DoS/DDoS атак

Значну частину таких мереж становлять пристрої Інтернету речей, зокрема маршрутизатори, відеокамери спостереження, мережеві накопичувачі та інші пристрої з недостатнім рівнем захисту. Уразливості програмного забезпечення або використання стандартних облікових даних дозволяють зловмисникам отримувати контроль над великою кількістю пристроїв та використовувати їх для генерації шкідливого трафіку.

Зростання масштабів і складності DDoS-атак зумовлює необхідність впровадження комплексних механізмів захисту інформаційних систем. До таких механізмів належать системи виявлення та запобігання вторгненням, фільтрація трафіку на рівні мережевого обладнання, використання балансування навантаження, застосування технологій розподіленої доставки контенту (CDN) та спеціалізованих сервісів захисту від DDoS-атак. Крім того, важливу роль відіграє моніторинг мережевої активності та аналіз аномалій у трафіку, що дозволяє своєчасно виявляти підозрілу активність і запобігати порушенню доступності інформаційних ресурсів.

Отже, атаки на відмову в обслуговуванні та розподілені мережеві атаки становлять серйозну загрозу для сучасних інформаційних систем і мережевої інфраструктури. Їхня ефективність зумовлена можливістю використання великої кількості розподілених джерел трафіку, механізмів підсилення та вразливостей мережевих протоколів. У зв’язку з цим дослідження механізмів реалізації таких атак і розроблення ефективних методів протидії є важливим завданням сучасної кібербезпеки та одним із ключових напрямів забезпечення стабільності функціонування інформаційних систем.

5. Зростання кількості кіберзагроз, ускладнення мережевих архітектур, а також активне використання хмарних сервісів, мобільних технологій і розподілених інформаційних систем зумовлюють необхідність впровадження ефективних механізмів захисту інформаційних ресурсів. У цьому контексті дедалі більшого значення набуває застосування *комплексного підходу до забезпечення безпеки комп’ютерних мереж*, що передбачає поєднання конфігураційних, криптографічних та організаційних заходів захисту.

Доцільність використання комплексного підходу зумовлена тим, що сучасні кіберзагрози характеризуються багаторівневим і багатоетапним характером. Зловмисники використовують комбінацію технічних, програмних і соціальних методів впливу на інформаційні системи, що дозволяє їм обходити окремі механізми захисту. У зв’язку з цим використання лише одного типу засобів безпеки не забезпечує достатнього рівня захищеності мережевої інфраструктури. Ефективна система інформаційної безпеки повинна базуватися на принципі багаторівневого або «глибокого» захисту (defense in depth), коли різні механізми безпеки доповнюють один одного та створюють комплексну систему протидії кіберзагрозам.

Важливим компонентом такого підходу є *конфігураційні заходи безпеки*, які передбачають правильне налаштування мережевого обладнання, серверів, операційних систем та програмного забезпечення. Належна конфігурація мережевих пристроїв дозволяє обмежити несанкціонований доступ до інформаційних ресурсів, контролювати мережевий трафік та запобігати використанню відомих вразливостей. До конфігураційних заходів належать налаштування міжмережевих екранів, сегментація мережі, використання систем виявлення та запобігання вторгненням, контроль доступу до мережевих сервісів, а також регулярне оновлення програмного забезпечення. Правильна конфігурація інфраструктури дозволяє зменшити площу потенційної атаки та мінімізувати ризики експлуатації технічних уразливостей.

Не менш важливим елементом системи захисту є криптографічні механізми, які забезпечують конфіденційність, цілісність і автентичність інформації, що передається мережею. Використання сучасних криптографічних алгоритмів і протоколів дозволяє захистити дані від перехоплення, модифікації або підміни під час передачі між мережевими вузлами. До таких механізмів належать шифрування мережевого трафіку, застосування протоколів захищеного з'єднання, використання цифрових сертифікатів, електронного підпису та інфраструктури відкритих ключів. Криптографічні засоби є особливо важливими в умовах використання відкритих мереж зв'язку, де існує підвищений ризик перехоплення інформації.

Разом із технічними засобами захисту важливу роль відіграють організаційні заходи безпеки, які спрямовані на регулювання процесів використання інформаційних систем і формування культури кібербезпеки в організації. До таких заходів належать розроблення політик інформаційної безпеки, регламентів доступу до інформаційних ресурсів, проведення навчання персоналу, аудит безпеки та контроль дотримання встановлених правил. Значна частина кіберінцидентів пов'язана саме з людським фактором, зокрема використанням слабких паролів, необережним поводженням із конфіденційною інформацією або недостатньою обізнаністю користувачів щодо сучасних кіберзагроз. У зв'язку з цим організаційні заходи є необхідним доповненням до технічних засобів захисту.

Поєднання конфігураційних, криптографічних і організаційних механізмів дозволяє сформувати багаторівневу систему захисту, яка забезпечує протидію різним типам кіберзагроз. У межах такого підходу кожен рівень безпеки виконує власну функцію: конфігураційні механізми обмежують доступ до мережевої інфраструктури, криптографічні засоби захищають інформаційні потоки, а організаційні заходи регулюють діяльність користувачів і забезпечують дотримання політик безпеки. Взаємодія цих елементів створює цілісну систему, здатну ефективно протидіяти як технічним, так і соціальним методам кібератак.

Отже, застосування комплексного підходу до захисту комп'ютерних мереж є обґрунтованим та необхідним у сучасних умовах розвитку інформаційних технологій (рис. 3).

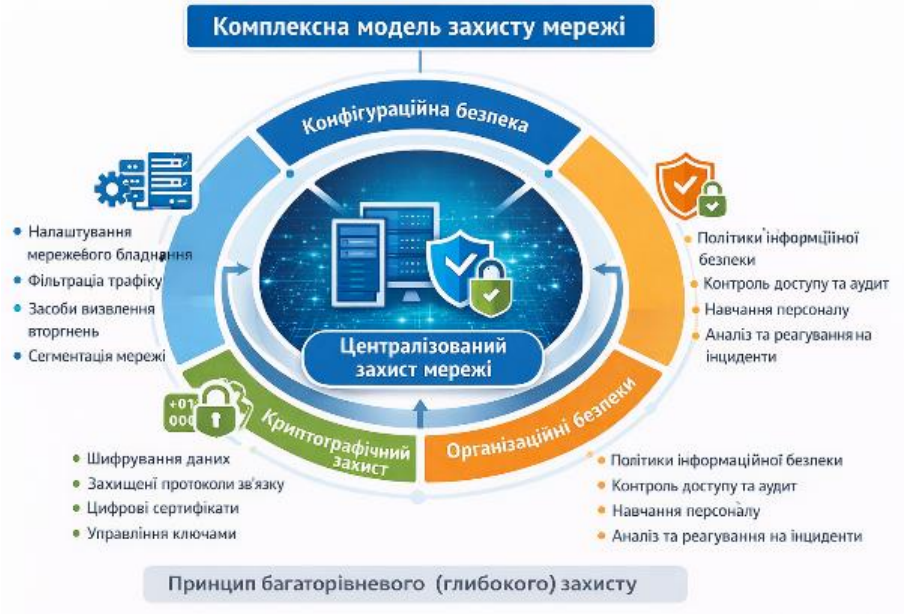

Рис 3. Модель комплексного захисту мережі

Поєднання конфігураційних, криптографічних і організаційних заходів дозволяє підвищити рівень захищеності мережевої інфраструктури, забезпечити надійний захист інформаційних ресурсів та мінімізувати ризики реалізації кіберзагроз. Такий підхід сприяє створенню стійкої системи інформаційної безпеки, здатної ефективно функціонувати в умовах постійної еволюції кіберзагроз та зростання складності сучасних інформаційних систем.

Висновки

У результаті проведеного дослідження було здійснено комплексний аналіз сучасних загроз безпеці комп'ютерних мереж, а також розглянуто основні механізми реалізації мережевих атак та підходи до побудови ефективних систем захисту інформаційної інфраструктури. Отримані результати дозволяють сформулювати низку узагальнених висновків.

По-перше, встановлено, що вразливості комп'ютерних мереж мають системний характер і можуть виникати на різних рівнях мережевої архітектури. Особливо вразливим є канальний рівень моделі OSI, який історично розроблявся для роботи в межах довіреного середовища та не передбачає вбудованих механізмів автентифікації мережевих кадрів. Це створює передумови для реалізації атак, спрямованих на перехоплення трафіку, порушення сегментації мережі та несанкціонований доступ до інформаційних ресурсів.

По-друге, у роботі систематизовано основні типи мережевих загроз та атак на мережеву інфраструктуру. Встановлено, що за характером впливу

вони можуть бути пасивними або активними, а за джерелом походження — внутрішніми та зовнішніми. Пасивні атаки спрямовані переважно на перехоплення та аналіз мережевого трафіку, тоді як активні передбачають модифікацію інформаційних потоків або порушення функціонування сервісів. Така класифікація дозволяє більш системно підходити до розроблення механізмів захисту та формування політик інформаційної безпеки.

По-третє, проаналізовано методи мережевої розвідки та сканування, які є важливим етапом підготовки більшості кібернападів. Встановлено, що процес збору інформації про мережеву інфраструктуру може здійснюватися як пасивними, так і активними методами. Пасивна розвідка базується на використанні відкритих джерел інформації та аналізі доступних мережевих даних, тоді як активна розвідка передбачає безпосередню взаємодію з мережевими вузлами через сканування портів, визначення операційних систем, ідентифікацію сервісів та аналіз потенційних вразливостей. Отримані результати підтверджують, що розуміння механізмів мережевого сканування є важливим для належного налаштування систем моніторингу та виявлення вторгнень.

По-четверте, у дослідженні розглянуто механізми реалізації атак на відмову в обслуговуванні (DoS) та розподілених атак відмови в обслуговуванні (DDoS), які належать до найбільш поширених загроз для сучасних інформаційних систем. Показано, що ефективність таких атак обумовлена можливістю використання розподілених ботнет-мереж, механізмів підсилення трафіку та вразливостей мережевих протоколів. Особливу небезпеку становлять волюметричні атаки, атаки транспортного рівня та атаки прикладного рівня, які можуть призводити до перевантаження мережевих каналів, серверних ресурсів та прикладних сервісів.

По-п’яте, обґрунтовано доцільність застосування комплексного підходу до захисту комп’ютерних мереж, що поєднує конфігураційні, криптографічні та організаційні заходи безпеки. Доведено, що сучасні кіберзагрози мають багаторівневий характер, тому ефективний захист інформаційних систем можливий лише за умови реалізації принципу багаторівневої оборони (defense in depth). Конфігураційні заходи дозволяють мінімізувати технічні вразливості мережевої інфраструктури, криптографічні механізми забезпечують конфіденційність і цілісність інформації під час її передавання, а організаційні заходи сприяють формуванню належної культури інформаційної безпеки та підвищенню рівня підготовки персоналу.

Таким чином, результати дослідження підтверджують, що забезпечення безпеки комп’ютерних мереж потребує системного підходу, який враховує як технічні особливості мережевих протоколів, так і організаційні аспекти управління інформаційною безпекою. Практичне значення отриманих результатів полягає у можливості їх використання під час проєктування та модернізації корпоративних мережевих інфраструктур, а також у процесі розроблення політик кібербезпеки.

Перспективи подальших досліджень полягають у розробленні методів автоматизованого виявлення мережевих атак на основі аналізу мережевого трафіку, використанні технологій машинного навчання для прогнозування кіберзагроз, а також удосконаленні механізмів захисту мережевої інфраструктури в умовах розвитку хмарних обчислень, Інтернету речей та розподілених інформаційних систем.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Список літератури

1. Tanenbaum A. S., Wetherall D. J. *Computer Networks*. 5th ed. Upper Saddle River: Pearson, 2011. 960 p. URL: https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188
2. Kurose J. F., Ross K. W. *Computer Networking: A Top-Down Approach*. 9th ed. New York: Pearson, 2025. 864 p. URL: https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000013385
3. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Boston: Pearson, 2017. 464 p. URL: https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials/P200000003180
4. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken: Wiley, 2020. 1248 p. – URL: https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787
5. Stewart, J. M., Chapple, M., Gibson, D. *ISC2 CISSP Certified Inf. Systems Security Prof. Official Study Guide*. Hoboken: Wiley, 2024. 1248 p. URL:https://www.wiley.com/en-us/ISC2+CISSP+Certified+Information+Systems+Security+Professional+Official+Study+Guide%2C+10th+Edition-p-9781394254705?utm_source=copilot.com
6. IEEE Computer Society. *IEEE Standard for Virtual Bridged Local Area Networks (IEEE 802.1Q)*. New York: IEEE, 2018. URL: https://standards.ieee.org/standard/802_1Q-2018.html
7. Деркач Т. М., Лавренко М. Кіберпростір: аналіз загроз та методи захисту. *Innovative Education: Problems and Prospects of Scientific Research*: матеріали L Міжнар. наук.-практ. конф. (4–6 грудня 2024 р.). Stuttgart, 2024. С. 112–115. URL: https://reposit.nupp.edu.ua/handle/PoltNTU/18104
8. Лахно В. та ін. Модель захисту локальної мережі навчального закладу. *Кібербезпека: освіта, наука, техніка*. 2022. № 18. С. 6–23. DOI: https://doi.org/10.28925/2663-4023.2022.18.62
9. Сидоренко В., Максимець А. Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. *Кібербезпека: освіта, наука, техніка*. 2025. № 27. С. 560–571. DOI: https://doi.org/10.28925/2663-4023.2025.27.779

10. Хомчак М. Оцінка ризиків кібербезпеки для вибору хмарного провайдера. *Кібербезпека: освіта, наука, техніка*. 2025. № 27. С. 549–559. DOI: https://doi.org/10.28925/2663-4023.2025.27.773
11. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Львів «Магнолія-2006», 2024. 448 с. URL:https://magnolia.lviv.ua/wp-content/uploads/2024/04/INF-TA-KIBERPROSTORY-pidruchnyk_zmist.pdf
12. Корченко О. Г., Іванченко Є. В., Бакалінський О. В. та ін. Метод оцінювання рівня підвищення кібербезпеки об'єктів критичної інфраструктури держави. *Наукоємні технології*. 2024. № 61(1). С. 3-20. DOI: https://doi.org/10.18372/2310-5461.61.18509

Received (Надійшла) 22.01.2026
Accepted for publication (Прийнята до друку) 15.04.2026
Publication date (Дата публікації) 22.05.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Деркач Тетяна Миколаївна – доктор філософії, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна
Tetyana Derkach – PhD, Associate Professor, Associate Professor of the Department of Computer and Information Technologies and Systems, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine
e-mail: tanider@ukr.net ORCID Author ID: https://orcid.org/0000-0001-8062-9105
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57204846765

Головко Геннадій Вячеславович – кандиат технічних наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Gennadii Golovko – Candidate of Technical Sciences (PhD in Engineering), Associate Professor, Associate Professor of the Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine.;
e-mail: GenVGolovko@ukr.net , Контактний тел.: 096-57-40-227, ORCID: http://orcid.org/0000-0002-1745-1321

Дмитренко Андрій Олександрович – доктор філософії, доцент, доцент кафедри будівельних конструкцій, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Andrii Dmytrenko – PhD, Associate Professor, Associate Professor of Department of building structures, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: andmyt@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-8715-7646;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57217604473.

Клочко Ліна Андріївна – доктор філософії, інженер-геотехнік, геологічне бюро BEG SA, Швейцарія
Lina Klochko – Ph.D., Geological Bureau BEG SA, Switzerland
e-mail: lina.dmitrenko@gmail.com; ORCID Author ID: http://orcid.org/ 0000-0002-6064-2887;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57217278708.

Threat and vulnerability analysis of computer networks and a comprehensive approach to cybersecurity

Tetyana Derkach, Gennadii Golovko, Andrii Dmytrenko, Lina Klochko

Abstract. The article presents a comprehensive analysis of modern threats and vulnerabilities affecting computer networks in the context of the rapid development of digital technologies and the growing number of cyber threats targeting information infrastructures. Particular attention is paid to the study of architectural and protocol vulnerabilities in computer networks, especially at the data link and transport layers of the Open Systems Interconnection (OSI) model, which are often exploited as initial entry points for sophisticated cyberattacks. The study provides a systematic classification of network threats and attacks according to their nature, origin, and the layer of the network architecture in which they occur. Passive and active attacks, as well as internal and external threats, are analyzed in terms of their impact on the confidentiality, integrity, and availability of information resources. Special emphasis is placed on the analysis of modern network reconnaissance and scanning techniques, which are widely used both by cybersecurity professionals for security auditing and penetration testing and by malicious actors to identify vulnerabilities in network infrastructures. A separate section of the article focuses on the analysis of architectural vulnerabilities at the data link layer caused by the lack of authentication mechanisms in fundamental protocols of the IEEE 802 family. The study describes several common attack techniques based on manipulation of Ethernet frames, including MAC table flooding, Address Resolution Protocol (ARP) spoofing, VLAN hopping, as well as attacks targeting Dynamic Host Configuration Protocol (DHCP) infrastructure and the Spanning Tree Protocol (STP). Considerable attention is also devoted to the analysis of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which remain among the most widespread and dangerous cyber threats affecting modern information systems. The study also highlights the role of botnets and compromised Internet of Things (IoT) devices in the execution of large-scale distributed attacks. The increasing number of poorly secured IoT devices significantly expands the attack surface and enables cybercriminals to generate extremely high traffic volumes capable of disrupting the availability of critical information resources. Based on the conducted analysis, the article substantiates the necessity of implementing a comprehensive approach to computer network security. Such an approach integrates configuration-based, cryptographic, and organizational security measures implemented at different layers of the network infrastructure. The results of the study may be applied in the development of information security policies, the design of secure corporate network infrastructures, cybersecurity auditing, and the training of specialists in the fields of information technology and cybersecurity.

Keywords: computer networks, cybersecurity, network attacks, network reconnaissance, network scanning, protocol vulnerabilities, DoS attacks, DDoS attacks, information security.