Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В. о. завідувач кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань	12 Інформаційні технології (шифр і назва галузі знань)
спеціальність	125 «Кібербезпека» (код і назва спеціальності)
освітній ступень	бакалавр
освітня програма	Кібербезпека (назва освітньо-професійної програми)
на тему:	«Механізми захисту локальних бездротових мереж від атак типу DOS та DDOS»

Виконавець: студент IV курсу, групи КБ-43

_____ **Костянтин ДАНИЛЮК**
(підпис) (ім'я та прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Іван ПАРХОМЕНКО	

Нормоконтроль	Лариса МИРУТЕНКО	

Київ 2025

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В. о. завідувач кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

Студенту **КБ-43** (група) **Данилюку Костянтин Андрійовичу** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Механізми захисту локальних бездротових мереж від атак типу DOS та DDOS

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Архітектура та типи бездротових мереж, теоретичні основи DoS та DDoS-атак

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією бездротових мереж, їх типами та архітектурою, теоретичними основами DoS та DDoS-атак, розглянути механізми захисту локальних бездротових мереж від атак відмови в обслуговуванні

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Полягає в запропонованих механізмах захисту від DoS та DDoS

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Костянтин ДАНИЛЮК (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	23.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 15.02.2025	*виконано*
4	Архітектура та типи бездротових мереж	16.02.2025 – 04.03.2025	*виконано*
5	Теоретичні основи DoS та DDoS-атак	05.03.2025 – 21.03.2025	*виконано*
6	Дослідження методів захисту від атак	22.03.2025 – 08.04.2025	*виконано*
7	Реалізація механізмів захисту від DoS та DDoS-атак	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Костянтин ДАНИЛЮК (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел. Основний текст займає 71 сторінку, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. У пояснювальній записці кваліфікаційної роботи міститься 11 рисунків та 21 літературне джерело.

Метою роботи є розробка та реалізація механізмів захисту бездротових мереж від DoS та DDoS-атак.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні завдання:

– проаналізувати існуючі типи, принципи роботи та особливості функціонування бездротових мереж;

– дослідити теоретичні основи DoS та DDoS-атак, їх класифікацію, засоби *здійснення та види;*

– розглянути сучасні методи захисту від DoS та DDoS-атак у бездротових мережах;

– реалізувати практичні механізми захисту бездротової мережі на прикладі налаштування безпеки мережевого обладнання та програмних засобів.

Об'єкт дослідження – процес забезпечення безпеки бездротових мереж.

Предмет дослідження – методи та засоби захисту бездротових мереж від DoS та DDoS-атак.

Практична цінність полягає в запропонованих механізмах захисту від DoS та DDoS.

Ключові слова: DoS атаки, DDoS атаки, локальна бездротова мережа, вразливості, механізми захисту, архітектура, мережеве обладнання, відмова в обслуговуванні.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

3G – третє покоління технології мобільного зв'язку;

4G – четверте покоління технології мобільного зв'язку;

5G – п'яте покоління технології мобільного зв'язку;

DoS – Denial of Service;

DDoS – Distributed Denial of Service;

CPU – Central Processing Unit;

DNS – Domain Name System;

HTTP – Hypertext Transfer Protocol;

ICMP – Internet Control Message Protocol;

IDS – Intrusion Detection System;

IPS – Intrusion Prevention System;

IoT – Internet of Things;

MIMO – Multiple Input Multiple Output;

NTP – Network Time Protocol;

OFDMA – Orthogonal Frequency Division Multiple Access;

RAM – Random Access Memory;

TCP – Transmission Control Protocol;

UDP – User Datagram Protocol;

Wi-Fi – Wireless Fidelity.

ВСТУП

Актуальність. У сучасному інформаційному суспільстві бездротові технології відіграють ключову роль у забезпеченні мобільності, гнучкості та швидкого доступу до цифрових ресурсів. Зокрема, такі рішення, як WLAN, WPAN, WWAN, а також технології на кшталт MIMO, OFDMA та Wi-Fi, лягли в основу ефективного функціонування як побутових пристроїв, так і складних промислових систем. У зв’язку з активним розвитком Інтернету речей (IoT), кількість бездротових з'єднань продовжує стрімко зростати, що, в свою чергу, створює нові виклики у сфері кібербезпеки.

З одного боку, бездротові мережі значно підвищують ефективність комунікацій та масштабованість інформаційних систем, з іншого – залишають відкритими критично важливі вектори атак: перехоплення трафіку, несанкціонований доступ, підміна даних, DoS-атаки та інші загрози. Враховуючи відкритий характер бездротового середовища, саме воно стає однією з найвразливіших ланок сучасної інформаційної інфраструктури.

Крім того, виклики, пов’язані із захистом бездротових мереж, набули особливої гостроти в умовах зростаючої кількості складних атак, що обходять традиційні засоби захисту. Саме тому особливої актуальності набуває впровадження таких рішень, як IDS/IPS, VPN, а також використання криптографічних протоколів і механізмів аутентифікації. Аналіз сучасних технологій безпеки у сфері бездротового зв’язку дозволяє сформувати ефективну модель захисту, орієнтовану на проактивне виявлення та запобігання кіберзагрозам.

Таким чином, дослідження аспектів безпеки в бездротових мережах, зокрема в контексті зростаючого навантаження з боку IoT та мобільних сервісів, є не лише актуальним, а й стратегічно необхідним кроком для забезпечення стабільності та надійності цифрових систем у XXI столітті

Метою роботи є розробка та реалізація механізмів захисту бездротових мереж від DoS та DDoS-атак.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні завдання:

– проаналізувати існуючі типи, принципи роботи та особливості функціонування бездротових мереж;

– дослідити теоретичні основи DoS та DDoS-атак, їх класифікацію, засоби здійснення та види;

– розглянути сучасні методи захисту від DoS та DDoS-атак у бездротових мережах;

– реалізувати практичні механізми захисту бездротової мережі на прикладі налаштування безпеки мережевого обладнання та програмних засобів.

Об'єкт дослідження є процес забезпечення безпеки бездротових мереж.

Предмет дослідження є методи та засоби захисту бездротових мереж від DoS та DDoS-атак.

Методи дослідження: аналіз відкритих джерел, аналіз методів захисту від DoS та DDoS атак, порівняння.

Практична цінність полягає в запропонованих механізмах захисту від DoS та DDoS.

РОЗДІЛ 1
БЕЗДРОТОВІ МЕРЕЖІ

1.1 Відомості про бездротові мережі

Бездротова мережа – це тип передачі даних між пристроями завдяки електромагнітним хвилям: радіохвилі, інфрачервоне випромінювання, мікрохвилі, без застосування дротяних з'єднань. Ці мережі дозволяють забезпечити мобільність користувачів і пристроїв, що дає змогу швидко розгортати мережеву інфраструктуру та доступ до ресурсів незалежно від фізичного розташування.

Приклади бездротових мереж та їх застосування:

1. Wireless Fidelity (Wi-Fi) мережі. Wi-Fi – це найпоширеніший вид бездротових мереж для що застосовуються для організації локального доступу до Інтернету. Такі мережі поширені у будинках, офісах, кафе, навчальних закладах, аеропортах та громадських місцях.

2. Мобільні мережі (3rd Generation (3G), 4th Generation (4G), 5th Generation (5G)). Мобільні оператори надають послуги бездротового доступу до Інтернету через стільникові мережі різних поколінь: третього, четвертого та п’ятого. Ці мережі використовуються для забезпечення зв'язку в автомобілях, на вулиці, у сільській місцевості, для організації роботи служб таксі, кур'єрів, служб порятунку та пересувних офісів.

3. Bluetooth мережі. Bluetooth-технологія використовується для створення персональних бездротових мереж на коротких відстанях. Її застосовують для підключення бездротових навушників, клавіатур, мишок, смарт-годинників та інших периферійних пристроїв до комп’ютерів і смартфонів.

4. Worldwide Interoperability for Microwave Access (WiMAX) мережі. WiMAX – це бездротова технологія широкосмугового доступу, яка забезпечує високошвидкісний Інтернет на великих відстанях. Її використовували для

організації доступу у сільських районах, де проведення кабельних мереж є економічно невигідним. WiMAX дозволяє здійснювати доступ в Інтернет на високих швидкостях, з набагато більшим покриттям, ніж у мережі Wi-Fi. Це дозволяє використовувати технологію як «магістральні канали», продовженням яких виступають традиційні DSL-ні виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати високошвидкісні мережі у масштабах цілих міст.

5. Супутникові мережі. Супутниковий Інтернет дозволяє забезпечити бездротовий доступ до мережі у віддалених та важкодоступних регіонах, де відсутня традиційна інфраструктура. Такі мережі використовуються в морі, пустелях, під час дослідницьких експедицій, а також у надзвичайних ситуаціях. Прикладом мережі що використовує супутниковий зв’язок – Starlink.

6. Near Field Communication (NFC) мережі. Технологія NFC використовується для організації бездротового обміну даними на дуже коротких відстанях. Приклади застосування: безконтактні платежі за допомогою банківських карток або смартфонів, електронні квитки у транспорті, обмін контактами між пристроями.

1.2 Розвиток бездротових мереж на прикладі Wi-Fi мережі

Поступово з розвитком бездротових технологій з’явився Wi-Fi. Перші експерименти в цій галузі проводилися в середині 20 століття, коли дослідники намагалися послати радіосигнали на великі відстані. Але справжнім проривом стало прийняття Інститутом інженерів з електротехніки та електроніки (англ. Institute of Electrical and Electronics Engineers (IEEE)) у 1997 році стандарту 802.11, який визначає протоколи доступу до бездротової мережі.

Створення Wi-Fi Alliance у 1999 році відкрило нові шляхи для розвитку цієї технології. Завдяки своїй здатності надавати нам постійний доступ до Інтернету та можливості спілкуватися з різними пристроями, Wi-Fi з тих пір став необхідною складовою нашого повсякденного життя.

Базою для створення Wi-Fi послужив стандарт IEEE 802.11. Численні розширені ітерації цього стандарту були прийняті з часом, збільшуючи функціональність і швидкість Wi-Fi.

Основні версії включають:

– 802.11b перший комерційно доступний стандарт Wi-Fi, працює на частоті 2,4 ГГц і може досягати швидкості до 11 Мбіт/с;

– 802.11a та 802.11g, обидва працюють на частоті 2,4 ГГц; однак 802.11a та 802.11g дозволяють відповідно до 54 Мбіт/с;

– 802.11n (Wi-Fi 4) є першим, що збільшив швидкість і радіус дії завдяки використанню технології Multiple Input Multiple Output (MIMO). Маючи швидкість до 600 Мбіт/с, він може працювати як на частотах 2, так і на 4 ГГц і 5 ГГц;

– 802.11ac (Wi-Fi 5): Цей стандарт впершезастосовуєчастоту 5 ГГцтагарантуєще більшу швидкість передачі даних, сягаючи швидкості до 3,5 Гбіт/с;

– 802.11ax (Wi-Fi 6): Найновітніший стандарт, котрий вводиться на ринку, пропонує ще більшу швидкість та продуктивність, особливо у густонаселених мережах, та сягає швидкості до 9,6 Гбіт/с.

Таблиця 1.1

Розвиток стандартів Wi-fi

Назва покоління	Стандарт IEEE	Рік прийняття	Максимальна швидкість з'єднання (Мбіт/с)	Смуги радіочастот (ГГц)
1	2	3	4	5
Wi-Fi 8	802.11bn	-2028	≤100 000	2.4, 5, 6, 7, 42.5, 71
Wi-Fi 7	802.11be	-2024	≤46 120	2.4, 5, 6
Wi-Fi 6E	802.11ax	2020	≤9608	6
Wi-Fi 6	802.11ax	2019	—	2.4, 5
Wi-Fi 5	802.11ac	2014	≤6933	5

Продовження табл. 1.1

1	2	3	4	5
Wi-Fi 4	802.11n	2008	≤600	2.4, 5
(Wi-Fi 3)*	802.11g	2003	≤54	2.4
(Wi-Fi 2)*	802.11a	1999	≤54	5
(Wi-Fi 1)*	802.11b	1999	≤11	2.4
(Wi-Fi 0)*	802.11	1997	≤2	2.4

1.3 Класифікація безпровідних мереж передачі інформації

У світі існує велика кількість різних типів бездротових мереж, які відрізняються за призначенням, масштабами використання, технічними характеристиками та технологіями зв'язку.

Локальні бездротові мережі (англ. Wireless Local Area Network (WLAN)) забезпечують підключення пристроїв у межах обмеженої території, наприклад, у будинку, офісі або на підприємстві.

Приклади технологій:

– Wi-Fi (IEEE 802.11) – найпоширеніший стандарт локальної бездротової мережі;

– використовується для підключення ноутбуків, смартфонів, планшетів, принтерів та іншого обладнання до локальної мережі або Інтернету.

Особливості WLAN:

- радіус дії зазвичай становить від 30 до 100 метрів у приміщенні;
- працюють у діапазонах частот 2,4 ГГц та 5 ГГц;
- швидкість передачі даних залежить від стандарту (Wi-Fi 4, 5, 6 тощо).

Приклади використання:

- домашні мережі;
- безпровідні офіси;
- мережі кафе, готелів, аеропортів.

Мобільні бездротові мережі (англ. Wireless Wide Area Network (WWAN)) надають доступ до Інтернету і голосових послуг через великі території – від міста до цілої країни.

Приклади технологій:

- GSM (2G), UMTS (3G), LTE (4G), 5G NR (5G);
- мобільні оператори надають послуги передачі даних та телефонії.

Особливості WWAN:

- радіус дії обмежений не приміщенням, а зоною покриття базових станцій;
- швидкість залежить від покоління мережі: LTE забезпечує до 300 Мбіт/с, 5G – до кількох Гбіт/с;
- використовується для смартфонів, планшетів, автомобільних модемів, смарт-годинників.

Приклади використання:

- мобільний Інтернет для смартфонів;
- доступ до Інтернету у віддалених регіонах;
- підключення до мереж у русі (транспорт, кораблі, літаки).

Персональні бездротові мережі (англ. Wireless Personal Area Network (WPAN)) – це мережі малого радіусу дії, призначені для з'єднання пристроїв, що знаходяться на короткій відстані один від одного.

Приклади технологій:

- Bluetooth;
- ZigBee;
- Near Field Communication (NFC).

Особливості WPAN:

- радіус дії зазвичай до 10 метрів (Bluetooth) або навіть кілька сантиметрів (NFC);
- невелика швидкість передачі даних у порівнянні з Wi-Fi або мобільними мережами;
- енергозбереження є ключовою особливістю.

Приклади використання:

- безпровідні навушники, клавіатури, миші;
- смарт-годинники та фітнес-браслети;
- платежі через смартфон (NFC).

Бездротові мережі для Інтернету речей (англ. Internet of Things (IoT)) – це мережі для об'єднання великої кількості пристроїв, що автоматично обмінюються даними без участі людини.

Приклади технологій:

- LoRaWAN;
- Sigfox;
- Narrowband IoT (NB-IoT).

Особливості мереж IoT:

- дуже велика кількість пристроїв;
- низьке енергоспоживання;
- низька швидкість передачі даних, але велика дальність (до кількох кілометрів).

Приклади використання:

- смарт-лічильники води та електроенергії;
- розумні міста: моніторинг трафіку, якості повітря;
- сільське господарство: контроль за поливом і станом ґрунту.

Супутникові бездротові мережі. Ці мережі забезпечують глобальне покриття через супутники, що обертаються навколо Землі.

Приклади технологій:

- Starlink (SpaceX);
- Iridium;
- Globalstar.

Особливості супутникового зв'язку:

- підключення можливе навіть у віддалених та важкодоступних регіонах;
- більший час затримки (пінг) через велику відстань до супутника;
- висока вартість обладнання та обслуговування;

Приклади використання:

– інтернет для кораблів, літаків, арктичних станцій;

– аварійні комунікації під час стихійних лих.

Структура бездротової мережі визначає, як організовані її основні компоненти, яким чином здійснюється передача даних, керування підключеннями та забезпечення безпеки. Незалежно від типу мережі (WLAN, WWAN, WPAN тощо), загальні принципи побудови залишаються схожими.

Основні компоненти бездротової мережі:

1. Клієнтські пристрої (термінали). Це кінцеві пристрої, які підключаються до мережі. Приклади: ноутбуки, смартфони, планшети, принтери, смарт-годинники.

2. Бездротові точки доступу (англ. Access Points (AP)). Точки доступу – це пристрої, що забезпечують підключення клієнтських пристроїв до мережі. Вони приймають і передають радіосигнали, забезпечуючи місток між бездротовим середовищем та дротовою мережею.

3. Маршрутизатори (англ. Routers). Маршрутизатор виконує роль центру мережі, що організовує маршрутизацію трафіку між локальною мережею та Інтернетом. Часто в домашніх або офісних умовах маршрутизатор поєднує функції бездротової точки доступу.

4. Контролери бездротової мережі (англ. Wireless LAN Controllers). Використовуються у великих корпоративних мережах для централізованого керування великою кількістю точок доступу. Забезпечують контроль автентифікації користувачів, безпеки та налаштувань мережі.

5. Базові станції (англ. Base Stations). У мобільних мережах WWAN (3G, 4G, 5G) базові станції здійснюють підключення мобільних пристроїв до мережі оператора. Вони мають більшу потужність та обслуговують великі території.

6. Мережеве ядро (англ. Core Network). Забезпечує обробку, маршрутизацію та керування трафіком у великих мережах. Включає сервери аутентифікації, шлюзи, системи моніторингу трафіку.

1.4 Принципи організації бездротової мережі

Основні технічні параметри бездротових мереж визначають їхню ефективність, надійність, пропускну здатність і безпеку. Ці параметри значно впливають на якість з'єднання і загальну функціональність мережі. Важливі принципи організації бездротових мереж включають:

1. Передача даних через радіохвилі. Бездротова мережа використовує радіохвилі для передачі інформації замість фізичних кабелів. Частоти залежать від стандарту (наприклад, 2,4 ГГц чи 5 ГГц для Wi-Fi).

2. Процес автентифікації та підключення. Для підключення до мережі клієнтський пристрій ініціює запит, проходить автентифікацію (наприклад, через введення пароля Wi-Fi) і отримує Internet Protocol (IP) адресу для подальшої роботи в мережі.

3. Маршрутизація трафіку. Дані від клієнта передаються через точку доступу або базову станцію до маршрутизатора чи сервера оператора. Там визначається найкращий шлях для доставки пакета до адресата.

4. Забезпечення безпеки Для захисту даних використовуються різні методи шифрування (наприклад, WPA2/WPA3 для Wi-Fi) і механізми аутентифікації. У корпоративних мережах можливе впровадження Virtual Private Network (VPN) для додаткової безпеки.

Типові топології бездротових мереж

1. Точка–багато-точок (Point-to-Multipoint) Одна точка доступу обслуговує багато клієнтів. Типовий варіант для Wi-Fi мереж у офісах та будинках.

2. Мережева топологія Mesh (сітка) Кожна точка доступу може взаємодіяти з іншими точками, створюючи надлишкові шляхи зв'язку. Це підвищує надійність і забезпечує краще покриття великих територій (наприклад, у великих бізнес-центрах чи смарт-містах).

3. Ad-hoc мережі. Пристрої з'єднуються безпосередньо один з одним без використання центральної точки доступу. Використовується в тимчасових

мережах або для спеціалізованих рішень (наприклад, під час рятувальних операцій).

Технічні характеристики бездротових мереж визначають їхню ефективність, надійність, пропускну здатність і безпеку. Від цих параметрів залежать якість з'єднання, швидкість передачі даних та можливості застосування мереж у різних сферах.

Основні технічні параметри бездротових мереж:

1. Частотний діапазон. Бездротові мережі працюють у різних діапазонах частот, залежно від технології:

– Wi-Fi (802.11n/ac/ax): 2,4 ГГц, 5 ГГц, 6 ГГц;

– мобільні мережі (4G/5G): від 700 МГц до 3,5 ГГц і вище;

– Bluetooth: 2,4 ГГц;

– вибір частоти впливає на швидкість, дальність покриття та стійкість до перешкод.

2. Ширина каналу. Ширина каналу визначає обсяг даних, який можна передати за одиницю часу. Наприклад, у Wi-Fi 5 ширина каналу 20/40/80/160 МГц дозволяє значно підвищити швидкість у порівнянні зі старими стандартами.

3. Максимальна швидкість передавання даних. Залежить від стандарту мережі:

– Wi-Fi 4 (802.11n): до 600 Мбіт/с;

– Wi-Fi 5 (802.11ac): до 6933 Мбіт/с;

– Wi-Fi 6 (802.11ax): до 9608 Мбіт/с;

– реальна швидкість зазвичай нижча через завади, кількість підключень та інші чинники.

4. Радіус покриття. Відстань, на якій пристрій може підтримувати стабільне з'єднання:

– Wi-Fi у приміщенні: до 50 метрів;

– Wi-Fi на відкритому просторі: до 150 метрів;

– 4G мережі: до кількох кілометрів від базової станції. Більш високі частоти забезпечують вищу швидкість, але менший радіус покриття.

5. Технології модуляції. Для передачі даних бездротові мережі використовують різні методи модуляції:

– QAM (Quadrature Amplitude Modulation) у Wi-Fi 5 та Wi-Fi 6;

– OFDM (Orthogonal Frequency Division Multiplexing) у Wi-Fi та 4G.

Ці технології дозволяють ефективно використовувати доступний спектр частот і збільшувати пропускну здатність.

6. Методи шифрування та безпеки. Безпека є важливим аспектом бездротових мереж:

– Wi-Fi Protected Access 2 (WPA2);

– Wi-Fi Protected Access 3 (WPA3);

– IPsec і VPN для мобільних мереж. Шифрування даних запобігає несанкціонованому доступу до інформації.

7. Продуктивність при високому навантаженні. Новітні стандарти, як-от Wi-Fi 6, використовують технології MU-MIMO (Multiple User - Multiple Input Multiple Output) та OFDMA (Orthogonal Frequency Division Multiple Access) для одночасного обслуговування великої кількості пристроїв без істотного зниження швидкості.

Таблиця 1.2

Порівняння характеристик різних бездротових стандартів

Стандарт	Частота	Максимальна швидкість	Радіус покриття	Особливості
1	2	3	4	5
Wi-Fi 4 (802.11n)	2.4/5 ГГц	до 600 Мбіт/с	70 м (приміщення)	Підтримка MIMO
Wi-Fi 5 (802.11ac)	5 ГГц	до 6933 Мбіт/с	35 м (приміщення)	Висока швидкість, вузький діапазон

Продовження табл. 1.2

1	2	3	4	5

Wi-Fi 6 (802.11ax)	2.4/5/6 ГГц	до 9608 Мбіт/с	80 м (приміщення)	Підтримка MU-MIMO, OFDMA
4G LTE	700 МГц – 2.6 ГГц	до 1000 Мбіт/с	кілька км	Мобільний Інтернет
5G NR	700 МГц – 71 ГГц	до 20 Гбіт/с	до 1 км (mmWave)	Дуже висока швидкість і затримка <1 мс

1.5 Особливості функціонування бездротових мереж

Бездротові мережі стали невід'ємною частиною сучасного суспільства завдяки своїм численним перевагам. Водночас існують і певні недоліки, які слід враховувати при проєктуванні та використанні таких мереж.

Переваги бездротових мереж:

1. Мобільність та зручність. Однією з найголовніших переваг є можливість доступу до мережі з будь-якої точки в межах зони покриття. Користувачі не прив'язані до певного місця і можуть легко переміщатися з пристроями (ноутбуками, смартфонами, планшетами) без втрати з'єднання.

2. Простота розгортання. Створення бездротової мережі потребує значно менше фізичної інфраструктури порівняно з дротовими рішеннями. Відсутність необхідності прокладати кабелі особливо важлива у великих будівлях або історичних спорудах, де кабельна інсталяція може бути складною або небажаною.

3. Гнучкість масштабування. Додавання нових користувачів до бездротової мережі зазвичай не потребує значних витрат чи складних процедур. Достатньо забезпечити налаштування точки доступу або маршрутизатора.

4. Економічна ефективність. У певних випадках бездротові рішення можуть бути дешевшими за дротові, оскільки скорочуються витрати на кабельну інфраструктуру, спеціальне обладнання і монтаж.

5. Підтримка широкого спектра пристроїв. Сучасні бездротові мережі сумісні з великою кількістю пристроїв – від традиційних ноутбуків до інтернету

речей (IoT), що розширює можливості використання мережі в побуті, бізнесі та промисловості.

Недоліки бездротових мереж:

1. Обмеження пропускної здатності та швидкості. Хоча сучасні стандарти Wi-Fi забезпечують високу швидкість, вона все ще може поступатися дротовим підключенням, особливо в умовах великої кількості підключених користувачів або в присутності перешкод.

2. Схильність до завад та перешкод. Робота бездротових мереж залежить від навколишнього середовища. Металеві конструкції, стіни, електромагнітні поля та навіть погодні умови можуть знижувати якість сигналу або викликати перебої у з'єднанні.

3. Проблеми з безпекою. Відкрита природа бездротового середовища робить мережі більш уразливими до атак, таких як перехоплення даних, підміна трафіку або несанкціонований доступ. Тому важливо використовувати сучасні методи шифрування і автентифікації.

4. Обмежена дальність дії. Радіус покриття бездротових мереж обмежений. Для розширення покриття необхідно встановлювати додаткові точки доступу або ретранслятори, що може ускладнити архітектуру мережі.

5. Витрати енергії. Бездротові пристрої зазвичай споживають більше енергії при використанні радіомодулів порівняно з дротовими аналогами. Це особливо критично для мобільних пристроїв, які працюють від акумуляторів.

6. Вплив перевантаження мережі. При одночасному підключенні великої кількості користувачів (наприклад, у громадських місцях) мережа може бути перевантаженою, що призводить до зниження швидкості та збільшення затримок.

Зростання популярності бездротових мереж створює нові можливості для користувачів, однак, поряд з цим з'являються й нові загрози для безпеки. Бездротові мережі використовуються в багатьох сферах, від домашніх і офісних мереж до великих корпоративних і промислових систем. Оскільки передача даних відбувається через повітря, що є уразливим каналом комунікацій,

забезпечення безпеки бездротових мереж набуває особливої важливості. Основними проблемами є захист від несанкціонованого доступу, перехоплення трафіку, атаки типу "людина посередині" та інші.

Основні загрози безпеки бездротових мереж:

1. Несанкціонований доступ (англ. Unauthorized Access). Один із найбільших ризиків для бездротових мереж – це несанкціонований доступ до мережі. Відсутність фізичного захисту сигналу дозволяє потенційним зловмисникам підключатися до мережі з будь-якої точки її покриття. Вони можуть отримати доступ до даних, змінювати конфігурації мережі або запускати атаки на інші вузли. Для боротьби з цим ризиком використовуються методи шифрування та автентифікації, такі як Wi-Fi Protected Access 2 (WPA2) і Wi-Fi Protected Access 3 (WPA3).

2. Перехоплення даних (англ. Eavesdropping). Оскільки сигнал бездротової мережі поширюється через ефір, зловмисники можуть перехоплювати передачу даних, що проходять між пристроями. Це особливо небезпечно в публічних або відкритих мережах, таких як Wi-Fi у кафе чи аеропортах, де користувачі можуть передавати конфіденційну інформацію, не підозрюючи про можливість її перехоплення. Протидія цій загрозі забезпечується шляхом використання шифрування, наприклад, Secure Sockets Layer (SSL)/ Transport Layer Security (TLS), а також впровадженням протоколів безпеки, які гарантують конфіденційність даних, таких як WPA3.

3. Атаки «людина посередині» (англ. Man-in-the-Middle Attack (MITM)). Цей вид атаки полягає в тому, що зловмисник перехоплює і змінює дані, що передаються між двома сторонами, при цьому вони не підозрюють про порушення. Це може бути здійснено за допомогою фальшивих точок доступу (наприклад, створення підробленої мережі Wi-Fi, яка імітує легітимну). Важливою мірою захисту від MITM атак є використання протоколів шифрування, таких як HyperText Transfer Protocol Secure (HTTPS), і автентифікація користувачів через сертифікати.

4. Атаки на точку доступу (англ. Access Point Attacks). Бездротові точки доступу є основними вузлами мережі, через які проходить весь трафік. Зловмисники можуть атакувати ці пристрої через експлойти у їх програмному забезпеченні або за допомогою фальшивих точок доступу. Для протидії атакам на точки доступу важливо постійно оновлювати прошивку пристроїв, використовувати захищені протоколи (наприклад, WPA3) та обмежувати фізичний доступ до точок.

5. Денсити та відмова в обслуговуванні (англ. Denial of Service (DoS)). Бездротові мережі можуть бути вразливими до атак відмови в обслуговуванні (DoS), де зловмисник намагається перевантажити мережу або точку доступу так, щоб легітимні користувачі не могли отримати доступ до мережі. Для захисту від DoS атак використовуються різні техніки, включаючи обмеження кількості підключень та виявлення аномальної активності.

Методи забезпечення безпеки бездротових мереж:

1. Шифрування даних. Один з основних методів захисту бездротових мереж – це шифрування даних, які передаються по мережі. Шифрування гарантує, що навіть якщо зловмисник перехопить сигнал, він не зможе прочитати або змінити передану інформацію. Протоколи, такі як WPA2 та WPA3, використовують сильне шифрування для захисту бездротового трафіку. WPA3 є новітнім стандартом і забезпечує більш високий рівень захисту, включаючи вдосконалені методи захисту від атак на паролі.

2. Аутентифікація та контроль доступу. Для запобігання несанкціонованому доступу до бездротової мережі необхідно застосовувати аутентифікацію користувачів. Стандарт WPA2 використовує методи аутентифікації через протокол Extensible Authentication Protocol (EAP), що дозволяє здійснювати автентифікацію через сервери, що зберігають дані користувачів. Використання складних паролів та багатоетапної аутентифікації дозволяє знизити ризик несанкціонованого доступу.

3. Фільтрація за Media Access Control (MAC) адресами. Ще одним методом безпеки є фільтрація за MAC-адресами, що дозволяє лише конкретним

пристроям підключатися до бездротової мережі. Хоча цей метод не є абсолютним захистом, оскільки MAC-адреси можна підробити, він може бути корисним для обмеження доступу на певному рівні. Важливо зазначити, що фільтрація MAC-адрес є частиною більш комплексної стратегії безпеки.

4. VPN. Використання віртуальних приватних мереж (VPN) є ще одним ефективним методом для забезпечення безпеки бездротових мереж. VPN дозволяє створити захищений канал для передачі даних, навіть у випадку, якщо бездротова мережа сама по собі не є захищеною. VPN шифрує весь трафік, що передається, і забезпечує анонімність користувачів, що робить неможливим перехоплення інформації зловмисниками.

5. Інтеграція систем виявлення та запобігання вторгненням (англ. Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)). Виявлення вторгнень в мережу та їх запобігання є важливим компонентом забезпечення безпеки. Системи IDS/IPS можуть автоматично виявляти підозрілу активність, таку як спроби несанкціонованого доступу або аномальні спроби підключення, та блокувати їх до того, як зловмисник завдасть шкоди.

6. Захист точок доступу від фальшивих мереж (англ. Rogue Access Points). Зловмисники можуть створювати фальшиві точки доступу, які виглядають як легітимні мережі, щоб залучити користувачів і отримати їхні дані. Однак, щоб протистояти такому типу атак, існують спеціальні засоби виявлення фальшивих точок доступу, які перевіряють ідентифікацію точки доступу та виявляють її автентичність. Інструменти моніторингу та аналізу трафіку можуть виявляти підозрілі точки доступу, що значно знижує ризик використання фальшивих мереж.

Висновки за розділом 1

У першому розділі було здійснено ґрунтовний аналіз основних понять, типів, принципів функціонування та характеристик бездротових мереж, що

дозволяє сформувати цілісне уявлення про об’єкт дослідження – бездротове середовище як основу сучасної інформаційної інфраструктури.

У ході дослідження було встановлено, що бездротові мережі поділяються на кілька основних класів залежно від зони покриття, призначення та використовуваних технологій. Найпоширенішим типом є WLAN, зокрема стандарт IEEE 802.11 (Wi-Fi), який застосовується в домашніх, корпоративних та публічних мережах. Також значне поширення мають WPAN (Bluetooth, ZigBee) для персонального обміну даними, WWAN як основа стільникових мереж (3G, 4G, 5G), а також IoT-мережі та супутниковий зв’язок – для спеціалізованих задач та глобального охоплення.

Особливу увагу було приділено стандартам Wi-Fi, їх технічним характеристикам та еволюції. Проаналізовано такі параметри, як діапазони частот, швидкість передачі, радіус покриття, пропускна здатність та механізми шифрування. Було виявлено, що нові покоління Wi-Fi (зокрема Wi-Fi 6) не лише збільшують продуктивність, а й інтегрують сучасні механізми безпеки, такі як WPA3, підтримку MU-MIMO, OFDMA та ефективніші методи керування каналами.

Принципи роботи бездротових мереж базуються на використанні радіохвиль для передачі даних між вузлами, що забезпечує мобільність і гнучкість у розгортанні мережевої інфраструктури. Разом із тим, така природа передачі робить бездротові мережі особливо вразливими до загроз: перехоплення трафіку, несанкціонований доступ, перешкоди, а також атаки типу (Distributed) Denial-of-Service Attack (DoS/DDoS). Саме тому безпека є критично важливим аспектом функціонування таких мереж.

Також було проаналізовано ключові переваги бездротових технологій, серед яких: мобільність, простота встановлення, зменшення витрат на кабельну інфраструктуру, масштабованість. Водночас виявлено й недоліки, а саме: підвищена уразливість до атак, обмежена пропускна здатність у порівнянні з дротовими мережами, залежність якості зв’язку від фізичних та радіочастотних умов, складність захисту інформації.

Окрему увагу було приділено впливу розвитку IoT, зростання кількості підключених пристроїв та викликам, що постають перед бездротовими мережами. Інтернет речей (IoT) формує нові вимоги до масштабованості, енергоефективності та безпеки передачі даних, що зумовлює потребу в адаптації традиційних мережевих протоколів і засобів захисту.

У результаті опрацювання матеріалу можна зробити висновок, що сучасні бездротові мережі є надзвичайно важливим, але вразливим елементом IT-інфраструктури, і саме їх особливості функціонування створюють передумови для виникнення загроз типу DoS та DDoS. Тому формування ефективної моделі захисту бездротових середовищ повинно ґрунтуватися на глибокому розумінні їх архітектури, принципів роботи та обмежень.

Цей теоретичний базис є фундаментом для наступного розділу, де розглядаються методи атак на бездротові мережі, їх реалізація, а також механізми протидії цим загрозам у реальних умовах.

РОЗДІЛ 2
DOS ТА DDOS АТАКИ

2.1 Теоретичні основи DoS та DDoS атак

Атака типу DoS**,** що перекладається як «відмова в обслуговуванні», є видом кібератаки, основною метою якої є порушення доступності обчислювального ресурсу (наприклад, вебсайту, сервера або мережі) для легітимних користувачів. У більшості випадків атака DoS здійснюється з одного джерела – комп’ютера або мережі – та спрямована на конкретну ціль.

Механізм реалізації такої атаки полягає у перевантаженні ресурсу надмірною кількістю запитів або шкідливим трафіком, внаслідок чого цільова система не здатна обробляти запити законних користувачів. Аналогічно до ситуації, коли вузька дорога блокується великогабаритним транспортним засобом, що унеможливлює проїзд інших автомобілів, DoS-атака блокує доступність цифрового ресурсу шляхом його навмисного перевантаження.

DDoS-атака, або розподілена відмова в обслуговуванні, є складнішою формою DoS-атаки. Її ключовою відмінністю є те, що атака виконується одночасно з багатьох джерел. Як правило, для цього зловмисники використовують ботнет – мережу заражених комп’ютерів або пристроїв, які діють у скоординований спосіб для генерації масованого трафіку до цільової системи.

Модель DDoS-атаки можна порівняти з ситуацією, коли сотні або тисячі автомобілів одночасно блокують усі смуги дорожнього руху з різних напрямків, повністю унеможливлюючи пересування. Таким чином, атака стає набагато потужнішою, менш передбачуваною і складнішою для виявлення та нейтралізаці

Таблиця 2.1

Порівняльна характеристика DoS та DDoS-атак

Характеристика	DoS (Відмова в обслуговуванні)	DDoS (Розподілена відмова в обслуговуванні)
Джерело атаки	Одне	Багато розподілених джерел (ботнет)
Складність реалізації	Відносно проста	Значно складніша
Складність виявлення та блокування	Легше виявити та заблокувати	Складніше виявити та нейтралізувати
Потужність атаки	Обмежена можливостями одного джерела	Висока, залежить від масштабів ботнету
Масштаб впливу	Обмежений	Широкий, з потенціалом впливу на великі інфраструктури

2.2 Класифікація DDoS-атак

Згідно з моделлю OSI, атаки розподіленої відмови в обслуговуванні (DDoS) класифікуються на три основні категорії залежно від рівня впливу: Volumetric attacks, Protocol attacks та Application layer attacks. Розуміння цієї класифікації дозволяє краще підготувати захисні заходи та інфраструктуру.

Volumetric Attacks (Об'ємні атаки). Метою є переповнення пропускної здатності мережі жертви шляхом генерації надзвичайно великого обсягу трафіку. Через це легітимні користувачі не можуть отримати доступ до сервісу. Вимірюються в бітах за секунду (bps).

Типові приклади:

– UDP Flood: відправлення великої кількості UDP-пакетів на випадкові порти жертви;

– ICMP (Ping) Flood: масовані ICMP-запити, які перевантажують канали і маршрутизатори;

– DNS/NTP Amplification Attack: посилена атака, де малі запити до відкритих серверів (DNS/NTP) генерують великі відповіді на IP жертви.

Захист від об’ємних атак:

– використання систем виявлення та пом’якшення DDoS (наприклад, Cloudflare, Radware, Akamai), що можуть фільтрувати та блокувати шкідливий трафік на рівні хмари;

– налаштування фільтрації мережевого трафіку (ACLs, rate limiting) на маршрутизаторах і фаєрволах;

– Anycast-мережі: розподілення трафіку на декілька серверів у різних регіонах, що дозволяє ефективно розподіляти навантаження;

– використання Content Delivery Network (CDN) для зменшення прямого навантаження на основний сервер.

Protocol Attacks (Протокольні атаки). Ці атаки експлуатують вразливості або особливості роботи мережевих протоколів (рівні 3 і 4 OSI) з метою виснаження ресурсів серверів, фаєрволів та балансувальників навантаження. Вимірюються в пакетах за секунду (pps).

Типові приклади:

– SYN Flood: Атака на процес TCP-handshake, що створює «напіввідкриті» з’єднання і вичерпує ресурси сервера;

– Ping of Death: надсилання фрагментованих IP-пакетів, які при збиранні спричиняють збій;

– Smurf Attack: використання ICMP-відповідей із підробленою IP-адресою жертви.

Захист від протокольних атак:

– використання фаєрволів нового покоління (англ. Next-Generation Firewalls) з глибоким аналізом пакетів;

– налаштування SYN cookies на серверах для захисту від SYN Flood-атак;

– вимкнення ICMP-відповідей на широкомовні запити, що знижує ризик Smurf-атак;

– інтеграція IDS/IPS-систем (наприклад, Snort, Suricata) для виявлення аномальної активності в протоколах.

Application Layer Attacks (Атаки на рівні застосунків). Ці атаки відбуваються на 7-му рівні OSI-моделі (рівень застосунків) і спрямовані на виснаження ресурсів конкретного програмного забезпечення шляхом надсилання легітимних на вигляд, але масованих чи зловмисних запитів. Вимірюються в запитах за секунду (rps).

Типові приклади:

– HTTP Flood: надсилання великої кількості HTTP GET/POST-запитів, що перевантажують вебсервер;

– Slowloris: залишення HTTP-з’єднань відкритими тривалий час, що блокує нові клієнтські з’єднання;

– DNS Query Flood: масовані DNS-запити, що перевантажують DNS-сервери;

– SQL Injection (у вигляді DoS): створення запитів до бази даних, які призводять до її перевантаження або блокування.

Захист від атак на рівні застосунків:

– використання Web Application Firewall (WAF) для фільтрації HTTP/HTTPS-запитів і виявлення аномальної поведінки;

– механізми CAPTCHA, перевірка поведінки ботів, обмеження частоти запитів (rate limiting);

– моніторинг логів застосунку на предмет підозрілої активності;

– рознесення сервісів на мікросервісну архітектуру, що ускладнює виведення з ладу всієї системи;

– використання CDN з анти-DDoS модулями, які можуть блокувати запити на периметрі мережі.

Гібридні (багатовекторні) атаки. У реальності більшість атак комбінують декілька методів одночасно: наприклад, спочатку запускається об’ємна атака для

перевантаження каналу, потім протокольна атака для виведення з ладу фаєрвола, і насамкінець – HTTP flood для виведення з ладу вебсайту.

Захист від гібридних атак:

– комбіноване використання хмарних сервісів захисту (Cloudflare, AWS Shield, Azure DDoS Protection) і локальних засобів безпеки;

– план реагування на інциденти (англ. Incident Response Plan) із заздалегідь прописаними діями у разі DDoS;

– мережева сегментація та ізоляція критичних сервісів.

Історія DDoS-атак бере свій початок наприкінці 1990-х років, коли зростання популярності Інтернету супроводжувалося все активнішими спробами порушити нормальну роботу цифрових сервісів.

Однією з перших зафіксованих DDoS-атак стала атака на компанію Yahoo! у лютому 2000 року, яка позначила новий рівень загрози для глобальних онлайн-платформ. На той момент Yahoo! була одним з найбільших порталів в Інтернеті, що надавала поштові, новинні, пошукові послуги мільйонам користувачів по всьому світу. У лютому 2000 року її сервери були паралізовані внаслідок потужної DDoS-атаки, яка тривала кілька годин і повністю вивела з ладу роботу ресурсу. У результаті атаки постраждали інші великі компанії, такі як eBay, Cable News Network (CNN), Amazon та Buy.com.

Організатором атак виявився підліток на прізвисько Mafiaboy, якому вдалося за допомогою зламаних систем Unix та програмного забезпечення типу Trinoo або Tribe Flood Network (TFN) організувати трафік до серверів-жертв. Успішність атаки була зумовлена недостатнім розумінням принципів розподілених загроз, відсутністю захисту на рівні мережі та нездатністю компаній швидко відреагувати на навантаження.

Атаки стали переломним моментом у сфері кібербезпеки. Вони показали, наскільки вразливими є навіть найбільші гравці ринку перед скоординованим та масовим цифровим тиском. Відтоді термін "DDoS" увійшов у словник IT-фахівців, а дослідження у сфері протидії таким загрозам значно активізувалися.

З часом DDoS-атаки еволюціонували як за методами здійснення, так і за масштабами. Сучасні атаки відрізняються складністю, гнучкістю та руйнівною потужністю.

Нижче наведено кілька найбільш резонансних прикладів останніх років:

1. Атака на GitHub (лютий 2018 року). У лютому 2018 року платформа GitHub зазнала однієї з найпотужніших DDoS-атак в історії на той момент – пік трафіку досяг 1.35 терабіта на секунду (Tbps). У цьому випадку не було використано ботнет, як зазвичай, а натомість – метод memcached amplification. Це техніка, яка використовує помилково відкриті сервери кешування (memcached) для надсилання масивних обсягів трафіку на цільовий сервер.

GitHub оперативно звернувся до хмарного захисного провайдера Akamai, який зміг відбити атаку за лічені хвилини. Попри короткотривалість, інцидент підкреслив загрозу зловживання відкритими сервісами та потребу в правильній конфігурації публічних серверів.

2. Атака на Dyn (жовтень 2016 року). Dyn – це компанія, що забезпечувала DNS-сервіси для багатьох відомих сайтів, включно з Twitter, Reddit, Netflix, Spotify та PayPal. У жовтні 2016 року її інфраструктура була піддана масованій DDoS-атаці з використанням ботнету Mirai.

Mirai заражав пристрої Інтернету речей (IoT), такі як відеокамери, маршрутизатори та цифрові відеореєстратори, які мали слабкі або стандартні паролі. У результаті атаки доступ до низки відомих сайтів був заблокований для користувачів у США та Європі протягом кількох годин.
Цей випадок став серйозним попередженням про те, наскільки вразливими можуть бути IoT-пристрої, які часто мають слабкий рівень безпеки та масово підключені до мережі.

3. Атака на Cloudflare (серпень 2023 року). У серпні 2023 року компанія Cloudflare повідомила про нейтралізацію DDoS-атаки обсягом понад 201 млн запитів за секунду (RPS), що є рекордною за цим показником. Атака була спрямована на клієнтів Cloudflare і використовувала нові методи HTTP/2 Rapid Reset, що дозволяли різко посилити навантаження на вебсервери. На відміну від

попередніх атак, де використовувалися "сирі" обсяги даних (наприклад, у Tbps), ця атака була орієнтована на максимально можливу кількість запитів – тобто на виснаження процесорних ресурсів та можливостей обробки з’єднань.

Cloudflare змогла оперативно виявити шаблони атаки, оновити сигнатури захисту та повідомити про уразливість розробників браузерів та серверного ПЗ. Це ще раз показало, що захист має бути не лише на мережевому рівні, а й на рівні протоколів та поведінкових моделей трафіку.

2.3 Засоби здійснення DDoS-атак

Розподілені атаки на відмову в обслуговуванні здійснюються за допомогою спеціалізованих засобів, які дозволяють зловмисникам одночасно використовувати десятки тисяч пристроїв для перенавантаження обчислювальних або мережевих ресурсів цільової системи. Основні засоби можна умовно розділити на дві категорії: інфраструктурні платформи атак (botnet, IoT) та програмні інструменти атаки (LOIC, HOIC, Slowloris тощо).

Botnet – це мережа скомпрометованих пристроїв, зокрема комп’ютерів, серверів, роутерів, мобільних пристроїв або навіть «розумних» побутових приладів (наприклад, IP-камер або телевізорів SmartTV), які перебувають під контролем зловмисника. Такі пристрої називають *ботами* або *зомбі*, а весь набір – *бот-мережею*.

Керування botnet’ом зазвичай здійснюється через центральний сервер команд і керування (C&C server). Зловмисник може віддавати команди усім пристроям у мережі одночасно, що дозволяє ініціювати масовану DdoS-атаку.

Одним із найвідоміших прикладів botnet, орієнтованого на IoT-пристрої, є Mirai. Цей шкідливий код був вперше виявлений у 2016 році. Mirai автоматично сканує Інтернет у пошуках пристроїв з відкритими портами Telnet або SSH, які мають стандартні або слабкі облікові дані (наприклад, admin:admin). Після компрометації пристрою Mirai додає його до своєї бот-мережі.

Mirai та його похідні здатні здійснювати різноманітні атаки, зокрема:

– TCP SYN Flood;

– UDP Flood;

– HTTP Flood;

– атаки на рівні DNS (наприклад, DNS amplification).

Приклад атаки: У жовтні 2016 року Mirai був використаний для атаки на провайдера Dyn, що призвело до відключення таких сервісів, як Twitter, Netflix, GitHub, Reddit та Spotify. У піковий момент трафік досягав понад 1 Тбіт/с, що стало на той час рекордним показником.

Переваги для зловмисника:

– величезна кількість пристроїв з мінімальним захистом;

– низька вартість впровадження;

– акнонімність завдяки географічному розподілу ботів.

Ризики:

– IoT-пристрої мають обмежені ресурси, тому атаки потребують великої кількості пристроїв для досягнення ефекту;

– часті оновлення прошивок (за умови їх встановлення) можуть знешкодити бот-мережу.

LOIC – це один із найвідоміших і найпростіших інструментів для здійснення DoS- і DdoS-атак. Вперше розроблений як легальний інструмент для тестування навантаження на сервери, LOIC був адаптований зловмисниками для проведення масованих атак.

Функціональність:

– генерація великої кількості TCP, UDP або HTTP-пакетів;

– підтримка режиму *Hivemind* – коли LOIC підключається до IRC-каналу, через який можна централізовано керувати великою кількістю клієнтів.

Особливості:

– не шифрує трафік, тому IP-адреса атакуючого є видимою;

– підходить переважно для простих атак на веб-сервери.

Відомий випадок використання – кампанії Anonymous проти урядових сайтів та сайтів корпорацій.

HOIC – покращена версія LOIC, яка дозволяє здійснювати складніші HTTP-атаки. Основна особливість HOIC полягає у використанні так званих *booster scripts*, які дозволяють модифікувати заголовки HTTP-запитів та маскувати трафік.

Функціональні можливості:

– масова генерація HTTP GET/POST-запитів;

– параметризація запитів для уникнення фільтрації;

– одночасна атака на кілька цілей (до 256).

На відміну від LOIC, HOIC здатний частково обходити прості засоби захисту на веб-серверах (наприклад, базові фаєрволи). Втім, він не захищає користувача від виявлення, якщо не використовуються проксі або VPN.

Slowloris – це унікальний інструмент, який відрізняється від LOIC та HOIC тим, що він не потребує великої кількості трафіку для досягнення результату. Замість навантаження сервера потужними запитами, Slowloris відкриває велику кількість з’єднань до HTTP-сервера і тримає їх відкритими якомога довше, надсилаючи часткові заголовки з довгими інтервалами.

Принцип дії:

– надсилання фрагментів HTTP-запитів без завершення;

– сервер змушений тримати з’єднання відкритим у надії на завершення запиту;

– поступово ресурси сервера вичерпуються, і він не може обробляти нові запити від легітимних користувачів.

Переваги:

– ефективність навіть при атаці з одного пристрою;

– мінімальний трафік, що ускладнює виявлення;

– не потребує ботнету.

Обмеження:

– діє лише на певні версії веб-серверів (наприклад, Apache 1.x/2.x);

– захищені веб-сервери з налаштованим таймаутом або reverse proxy можуть легко запобігти таким атакам.

2.4 Види DdoS-атак та принципи їх дії

DdoS-атаки поділяються за рівнями моделі OSI, використаними протоколами та цільовими ресурсами. Залежно від підходу, атаки можуть спрямовуватись на перенавантаження пропускної здатності каналу, вичерпання ресурсів прикладного сервера або порушення мережевого стеку. Найпоширеніші типи включають SYN flood, UDP flood, HTTP flood, DNS/NTP amplification та атаки на рівні застосунків (Application-level DdoS).

SYN Flood. Цей тип атаки експлуатує процес встановлення TCP-з’єднання. В рамках триетапного рукостискання (three-way handshake) клієнт надсилає серверу SYN-запит, сервер відповідає SYN-ACK, і чекає завершального ACK. У SYN flood-атаці зловмисник надсилає велику кількість SYN-запитів, але не відповідає на SYN-ACK, залишаючи з’єднання «підвішеними».

Наслідок: сервер утримує в пам’яті незавершені сесії, що призводить до вичерпання таблиці з’єднань і блокування легітимних користувачів.

У 2008 році фінансова інфраструктура компанії *CheckFree* зазнала SYN flood-атаки, яка призвела до значного зниження доступності сервісів онлайн-оплати.

UDP flood полягає у масовому надсиланні UDP-пакетів на випадкові або певні порти цільового хоста. Якщо на обраний порт не чекає жоден застосунок, хост відповідає ICMP-повідомленням про недоступність (Destination Unreachable). Велика кількість таких відповідей призводить до перенавантаження процесора або мережевої смуги.

Наслідок: високе споживання ресурсів мережевого стека і деградація сервісу.

У 2014 році хакери використовували UDP flood для атаки на ігрові сервери *League of Legends*, що призвело до декількох годин простою.

HTTP flood є DdoS-атакою на прикладному рівні (рівень 7 OSI), яка використовує легітимні HTTP-запити. Зловмисник або ботнет надсилає велику кількість GET або POST запитів на вебсервер. Кожен запит є формально коректним, але їх масовість призводить до перенавантаження ресурсу.

Сервер змушений обробляти запити як звичайні, що споживає ресурси процесора, пам’яті, бази даних, а також утворює чергу на обробку легітимного трафіку.

У 2012 році *WordPress.com* зазнав великомасштабної HTTP flood-атаки, спрямованої на публічний блог політичного спрямування. Атака тривала кілька годин і зачепила мільйони користувачів.

DNS amplification/NTP amplification атаки належать до відбивних та підсилювальних атак (reflective/amplification attacks), де використовуються публічно доступні сервери для множення обсягу трафіку.

При атаці DNS Amplification зловмисник надсилає DNS-запити на відкриті DNS-сервери зі *спуфінгом* IP-адреси жертви. У відповідь сервер надсилає великі DNS-відповіді на IP-адресу жертви. Кожен запит може бути значно меншим за відповідь, що забезпечує коефіцієнт посилення (amplification factor) до 50–100.

Швидке перевантаження смуги пропускання або обладнання жертви масивними відповідями.

У 2013 році було здійснено атаку на антисенсорну організацію *Spamhaus*. Потік трафіку досягав 300 Гбіт/с – на той момент це була найпотужніша зафіксована DdoS-атака.

NTP Amplification атака схожа до DNS amplification, але використовує протокол Network Time Protocol (NTP). Зловмисник надсилає спеціальний запит (наприклад, monlist) на відкриті NTP-сервери, знову ж – зі спуфінгом IP-адреси жертви. У відповідь сервер надсилає десятки відповідей до одного запиту.

Amplification factor:

Може сягати 500–1000×, що робить NTP amplification однією з найнебезпечніших форм DdoS-атак.

У 2014 році сервіс *Cloudflare* зазнав атаки з використанням NTP amplification, яка сягала 400 Гбіт/с трафіку.

Атаки на прикладному (англ. Application-level attack) рівні спрямовані на вичерпання ресурсів конкретних сервісів, таких як вебсервери, API, системи логування або аутентифікації. На відміну від простого перенавантаження мережі, ці атаки маскуються під звичайну активність користувачів і часто не помічаються традиційними системами захисту.

Приклади застосування:

1. Вебсервери. Наприклад, надсилання великої кількості GET-запитів до сторінки, що генерується динамічно, з підключенням до бази даних.

2. API. Бот надсилає безперервні запити на REST API із змінними параметрами, симулюючи роботу користувача. Такі запити споживають CPU і порушують роботу сервісу.

3. Системи аутентифікації. Атаки на сторінки входу можуть призвести до вичерпання пулу сесій або сповільнення процесів авторизації. У найгіршому випадку – викликати DoS через блокування легітимних IP після фальшивих спроб входу.

2.5. Методи захисту від DdoS-атак

Захист від DdoS-атак – це складний процес, що потребує багаторівневого підходу, який охоплює як технічні засоби, так і організаційні заходи. Найефективнішим вважається саме комплексний захист, коли превентивні, реактивні та аналітичні стратегії працюють у синергії. У цьому розділі розглянемо основні загальні стратегії, які можуть бути використані як окремо, так і в комбінації для підвищення стійкості інформаційних систем до DdoS-атак.

Першою лінією оборони є постійний моніторинг трафіку. Його суть полягає у спостереженні за всіма входами і виходами мережі з метою виявлення аномалій:

- інструменти: NetFlow, Wireshark, Zabbix, Nagios, Suricata;

– що шукати: різке збільшення обсягу вхідного трафіку, надмірна кількість запитів з однієї IP-адреси, повторювані шаблони запитів;

– реакція: налаштування автоматичного сповіщення при перевищенні порогових значень трафіку або появі підозрілої активності.

Моніторинг дозволяє не лише оперативно реагувати на потенційні атаки, а й аналізувати історичні дані для вдосконалення захисту.

Однією з фундаментальних стратегій є резервування компонентів мережевої інфраструктури. Резервування дозволяє уникнути повної зупинки системи під час атаки.

Приклади:

– використання резервних DNS-серверів;

– розгортання дубльованих веб-серверів;

– наявність додаткових каналів інтернет-з'єднання (англ. multihoming).

Переваги:

– знижує ризик «єдиної точки відмови»;

– дозволяє перенаправляти трафік на менш завантажені вузли.

Цей підхід часто поєднується з балансуванням навантаження.

Логічна або фізична сегментація мережі передбачає поділ інфраструктури на ізольовані сегменти з метою локалізації шкідливої активності. При виникненні DdoS-атаки в одному сегменті, інші частини залишаються працездатними.

Методи:

– використання VLAN (Virtual LAN);

– встановлення міжмережевих екранів між сегментами;

– контроль доступу на основі ролей або геолокації.

Перевага:

– обмеження зони впливу атаки;

– полегшення процесу її нейтралізації.

Сегментація також полегшує аудит безпеки та дозволяє чіткіше відстежувати трафік.

Можливість автоматичного масштабування (auto-scaling) серверних ресурсів дозволяє обробляти збільшене навантаження в період атаки, щонайменше тимчасово. Хмарні платформи, такі як Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure, надають такі функції.

Переваги:

– гнучке управління ресурсами;

– підвищення витривалості системи;

– автоматичне розгортання додаткових екземплярів серверів.

Мінус – значне фінансове навантаження у разі масштабної атаки.

Масштабування особливо ефективне у поєднанні з балансуванням навантаження та CDN.

Системи IDS/IPS можуть фіксувати або блокувати підозрілі пакети у режимі реального часу.

Інструменти: Snort, Suricata, Zeek (раніше Bro).

Функціонал:

– виявлення сигнатур відомих атак;

– поведінковий аналіз для виявлення нових загроз;

– блокування запитів за заданими правилами.

Застосування таких систем підвищує шанси виявити DDoS-атаку ще на ранніх стадіях її реалізації.

Сторонні постачальники безпеки спеціалізуються на фільтрації DDoS-трафіку до його потрапляння на сервер клієнта.

Популярні сервіси:

– Cloudflare – безкоштовний та преміальний захист;

– Imperva – інтелектуальна обробка трафіку;

– Arbor Networks – корпоративні рішення;

– Radware, Akamai Kona, AWS Shield – рішення для великих компаній.

Переваги:

– масштабована інфраструктура;

– глобальна присутність дата-центрів;

– 24/7 підтримка та аналітика.

Ці сервіси можуть автоматично фільтрувати атаки без участі кінцевого користувача.

Активний захист передбачає виявлення, протидію та нейтралізацію DDoS-атак у реальному часі. На відміну від пасивних заходів, що зосереджуються на запобіганні або мінімізації впливу, активні методи спрямовані на безпосереднє втручання в хід атаки. Ці методи вимагають високого рівня автоматизації, продуктивного апаратного забезпечення та оперативного реагування.

Фільтрація є одним із найпростіших і найефективніших методів активного захисту. Вона полягає у відсіванні шкідливих або підозрілих пакетів ще до їх обробки веб-додатком.

Типи фільтрації:

– фільтрація за IP-адресами – блокування або обмеження доступу для певних діапазонів IP-адрес;

– фільтрація за протоколами/портами – блокування нестандартного трафіку або підозрілих з'єднань (наприклад, SYN flood);

– аналіз заголовків пакетів – виявлення некоректних або змінених пакетів, що характерні для атак.

Для підвищення ефективності часто використовується дробове фільтрування (англ. rate limiting), яке обмежує кількість запитів з однієї IP-адреси протягом певного часу.

IDS та IPS – це комплекси активного аналізу трафіку, які не лише виявляють спроби вторгнення, а й автоматично реагують на них.

Функції:

– аналіз шаблонів трафіку (сигнатурний підхід);

– виявлення аномалій (поведінковий підхід);

– автоматичне блокування або ізоляція шкідливих потоків.

Поширені рішення: Snort, Suricata, Bro/Zeek, Cisco Firepower, Palo Alto Networks.

Системи IPS можуть реалізовувати зворотну реакцію, тобто надсилати фальшиві відповіді атакуючим клієнтам або навіть здійснювати відключення каналів на мережевому рівні.

Captcha та JavaScript-перевірки. Ці методи дозволяють відрізняти людей від ботів, які зазвичай беруть участь у DDoS-атаках. Використання CAPTCHA або JavaScript-завдань блокує автоматизовані системи, які не можуть виконати інтерактивні дії.

Приклади:

– Google reCAPTCHA;

– JavaScript challenges на рівні веб-сервера;

– Сторінки затримки (interstitial pages).

Переваги:

– низька вартість впровадження;

– ефективність проти простих бот-мереж.

Обмеження: сучасні ботнети можуть емулювати поведінку браузера або працювати через реальні браузери з автоматизованим введенням даних.

У разі масштабної DDoS-атаки може застосовуватися «чорна діра» (англ. Blackhole routing (null routing)) – метод направлення всього трафіку, що надходить на конкретну IP-адресу, у спеціальний маршрут, де він автоматично відкидається.

Суть методу: створення маршруту до неіснуючого інтерфейсу, щоб уникнути перевантаження сервера.

Застосування:

– на рівні інтернет-провайдера;

– у внутрішній мережі підприємства;

– у сервісах типу Cloudflare чи Akamai.

Мінус: доступ до ресурсу втрачають як легітимні, так і зловмисні користувачі.

Цей метод – останній засіб у критичних ситуаціях, коли неможливо зупинити атаку іншими способами.

Honeypot та sinkhole-архітектура технології передбачають створення фальшивих або замінних вузлів, які поглинають або аналізують ворожий трафік.

Honeypot – спеціальний сервер, який імітує уразливий ресурс, щоб зловмисники атакували його замість реального сайту. Це дозволяє:

– вивчити поведінку атакувальників;

– отримати сигнатури нових ботів.

Sinkhole – перенаправлення підозрілого трафіку до вузла, який не обробляє запити, але реєструє їх.

– дозволяє зменшити навантаження на основні ресурси;

– аналізувати джерела ботнет-активності.

Обидва методи відіграють роль приманки, дозволяючи отримати цінну аналітичну інформацію для подальшої протидії.

Активне взаємодіяння з провайдерами. При виявленні масштабної атаки важливо взаємодіяти з інтернет-провайдером або хостинг-компанією. Вони можуть:

- застосувати фільтрацію трафіку на рівні транспортної мережі;
- активувати upstream blackholing;
- перенаправити трафік на захисну інфраструктуру (наприклад, scrubbing center).

Налагоджена комунікація з провайдером значно підвищує шанси на швидке реагування в умовах атаки.

Використання CDN з вбудованим захистом. Мережі доставки контенту (CDN) не лише кешують статичні дані, а й мають вбудовані механізми захисту від DDoS, які працюють на периметрі глобальної мережі.

Переваги:

– географічно розподілене блокування трафіку;

– відокремлення атакуючих запитів ще до потрапляння у внутрішню мережу;

– балансування навантаження.

Приклади: Cloudflare, Akamai, Fastly.

CDN особливо ефективні для захисту веб-сайтів, медіа-контенту, онлайн-магазинів.

Інфраструктурні заходи захисту від DDoS-атак охоплюють архітектурні, мережеві та апаратні рішення, що формують стійку й масштабовану IT-інфраструктуру. Вони не стільки блокують атаку в момент її виконання (як активні методи), скільки будують середовище, стійке до перевантаження, з можливістю швидкого відновлення та ізоляції аномалій. Основна мета – підвищити доступність і відмовостійкість сервісів навіть за умов навмисного перевантаження.

Балансування навантаження (англ. Load Balancing) – це фундаментальний інфраструктурний підхід до забезпечення стабільної роботи веб-додатків і серверів.

Принцип: трафік розподіляється між кількома серверами або вузлами, що знижує ризик перевантаження одного ресурсу.

Типи балансувальників:

– Програмні (наприклад, HAProxy, Nginx);

– Апаратні (F5, Citrix ADC);

– Хмарні (AWS Elastic Load Balancer, Azure Load Balancer).

Під час DDoS-атаки балансувальники можуть перенаправити трафік на ізольовані інстанси, що зменшує вплив на основну систему. Також вони підтримують health-check-механізми, які автоматично виключають вузли збоїв.

Географічно розподілена інфраструктура (англ. Anycast, Multiregion deployment). Одним із найефективніших інфраструктурних методів є розподіл інфраструктури по різних географічних регіонах із використанням протоколу Anycast.

Anycast дозволяє маршрутизувати запити до найближчого з доступних вузлів, тим самим розсіюючи навантаження.

Результат:

– зменшення загального трафіку на окремий центр обробки даних;

– ускладнення координації атаки з боку зловмисника;

– можливість локального ізолювання атаки (наприклад, лише на європейський сегмент).

Це активно використовується такими CDN- і хмарними провайдерами, як Cloudflare, Google, Amazon CloudFront.

Одним із ключових підходів до захисту від об'ємних DDoS-атак є планування інфраструктури з надлишком потужностей, що дозволяє витримати нетипове навантаження:

– горизонтальне масштабування – розгортання додаткових вузлів для обробки зростаючого трафіку;

– вертикальне масштабування – збільшення обчислювальних ресурсів окремих вузлів (CPU, RAM, пропускна здатність);

– автоматичне масштабування – динамічна активація інстансів залежно від метрик навантаження (наприклад, у хмарних платформах: AWS Auto Scaling, Google Cloud Autoscaler).

У поєднанні з кешуванням (наприклад, Redis, Varnish) цей підхід дозволяє обробляти мільйони запитів без критичного впливу на основну базу даних.

Ще одним важливим елементом інфраструктурного захисту є резервування каналів доступу до Інтернету та співпраця з кількома провайдерами.

Багатоканальність (англ. multi-homing) забезпечує:

– автоматичне перемикання на резервний канал у разі перевантаження;

– більшу стійкість до BGP-атак або збоїв на стороні основного провайдера.

BGP Blackholing з підтримкою провайдера дозволяє перенаправляти атаки ще до того, як вони досягнуть інфраструктури компанії.

Для великих підприємств наявність резервної IP-адресації, різних дата-центрів і провайдерів є обов'язковою вимогою кіберстійкості.

Використання хмарних DDoS-захисних сервісівю. Хмарні сервіси забезпечення захисту від DDoS (наприклад, Cloudflare, Akamai Kona Site Defender, AWS Shield, Azure DDoS Protection) дозволяють перенести фільтрацію та обробку трафіку за межі локальної мережі.

Механізм:

– увесь трафік спрямовується через хмарний шлюз;

– проводиться попередній аналіз, очищення, обмеження трафіку;

– лише «чистий» трафік передається до оригінального сервера.

Переваги:

– гнучкість;

– масштабованість (трафік фільтрується на глобальному рівні);

– SLA-підтримка з гарантією доступності.

Хмарний захист особливо ефективний проти масованих атак на рівні L3/L4 (UDP flood, TCP SYN flood), які важко зупинити лише на власному обладнанні.

Сегментування мережі – ще один базовий інфраструктурний захід, що полягає у розподілі внутрішньої інфраструктури на окремі логічні або фізичні підмережі.

Переваги:

– локалізація впливу DDoS-атаки лише на одну частину інфраструктури;

– можливість гнучко управляти міжсегментним трафіком;

– спрощення виявлення аномалій та ізоляції ботів.

Зазвичай реалізується за допомогою VLAN, VPN, Firewall-зон, що дозволяє встановлювати різні політики безпеки для окремих сегментів.

Інфраструктурний моніторинг і автоматизація. Наявність систем моніторингу в реальному часі дозволяє вчасно виявити ознаки початку DDoS-атаки:

– різке зростання обсягу трафіку;

– аномальне збільшення числа з’єднань;

– повторювані запити до однієї й тієї ж сторінки.

Типові рішення: Zabbix, Prometheus, Grafana, ELK Stack (ElasticSearch + Logstash + Kibana), NetFlow/SFlow аналізатори.

У поєднанні з автоматизованими сценаріями реагування (наприклад, через системи SOAR або власні скрипти), моніторинг дозволяє швидко змінити

конфігурацію балансувальників, фаєрволів або розгортати нові екземпляри інфраструктури.

Висновки за розділом 2

У другому розділі кваліфікаційної роботи було розглянуто теоретичні засади реалізації атак типу DoS та DDoS, їхню класифікацію, особливості здійснення, а також основні методи захисту. Аналіз цього розділу дозволяє усвідомити масштаби загроз, які становлять ці атаки, а також ключові принципи побудови ефективної системи протидії їм.

DoS-атаки є одним із найстаріших, але й досі актуальних видів кіберзагроз, метою яких є порушення доступності ресурсів для легітимних користувачів. З розвитком інфраструктури Інтернету та появою великої кількості взаємозв'язаних пристроїв виник ще небезпечніший різновид – DDoS-атаки, які здійснюються з розподілених джерел (ботнетів) і здатні виводити з ладу цілі корпоративні мережі або хмарні сервіси.

У процесі дослідження було встановлено, що DDoS-атаки класифікуються відповідно до OSI-моделі:

– об'ємні (англ. Volumetric) атаки спрямовані на перевантаження каналу даних (UDP Flood, ICMP Flood, DNS Amplification);

– протокольні атаки використовують вразливості мережевих протоколів (SYN Flood, Smurf, Ping of Death);

– атаки на прикладному рівні націлені на веб-застосунки (HTTP Flood, Slowloris), є складними для виявлення.

Важливою складовою дослідження стало вивчення інструментів та платформ, що використовуються для здійснення атак. Серед них – відкриті утиліти LOIC, HOIC, Slowloris, які легко доступні в мережі та можуть використовуватись навіть користувачами без технічної підготовки. Значно небезпечнішими є ботнети, зокрема Mirai, що заражають пристрої Інтернету речей і формують розподілені мережі для атак. Приклади атак на сервіси Dyn,

GitHub, Cloudflare показали реальні масштаби наслідків – від тимчасової недоступності сервісів до зупинки бізнес-процесів світових компаній.

Дослідження засобів захисту від DDoS-атак показало, що найефективнішим є багаторівневий підхід, який включає:

– шифрування даних на основі сучасних алгоритмів (AES, TLS);

– мережеву фільтрацію, міжмережеві екрани (NGFW), обмеження запитів (rate limiting);

– системи виявлення та запобігання вторгненням (IDS/IPS), зокрема Snort, Suricata;

– хмарні захисні сервіси (Cloudflare, AWS Shield, Akamai), які фільтрують аномальний трафік до його надходження до локальної мережі;

– сегментацію мережі, обмеження доступу, використання VPN.

Також досліджено слабкі сторони бездротових мереж у контексті таких атак. Через відкритий характер передавання даних та велику кількість уразливих IoT-пристроїв бездротові інфраструктури потребують посиленого контролю, ізоляції трафіку та активного моніторингу.

Узагальнюючи проведене дослідження, можна зробити такі висновки:

1. Атаки типу DoS та DDoS є одними з наймасштабніших та найнебезпечніших кіберзагроз сучасності.

2. Їх класифікація за рівнями OSI-моделі дозволяє вибудовувати цільову стратегію захисту.

3. Поширення бот-мереж і відкритих інструментів спрощує реалізацію DDoS-атак навіть для нефахівців.

4. Найбільш ефективною відповіддю на загрози є інтеграція декількох захисних засобів – від апаратного фільтрування до хмарного захисту та активного моніторингу.

5. Бездротові мережі, зокрема IoT-інфраструктура, мають бути першочерговим об’єктом захисту через свою відкритість і поширеність.

Цей теоретичний аналіз формує основу для реалізації конкретних практичних механізмів захисту, що буде розглянуто в наступному розділі.

Впровадження перевірених технічних рішень у бездротовому середовищі дозволить суттєво зменшити ймовірність успішного здійснення атак та забезпечити стабільність і доступність мережевих сервісів.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ

3.1 Налаштування базової безпеки маршрутизатора

Таблиця 3.1

Таблиця адресації

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.233	255.255.255.248	N/A
	S0/0/0 (DCE)	10.10.10.1	255.255.255.252	N/A
	Loopback 1	172.20.1.1	255.255.255.0	N/A
R2	S0/0/0	10.10.10.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.20.20.2	255.255.255.252	N/A
R3	G0/1	172.30.3.1	255.255.255.0	N/A
	S0/0/1	10.20.20.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN 1	172.30.3.11	255.255.255.0	172.30.3.1
ASA	VLAN 1 (E0/1)	192.168.10.1	255.255.255.0	N/A
	VLAN 2 (E0/0)	209.165.200.234	255.255.255.248	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	172.30.3.3	255.255.255.0	172.30.3.1

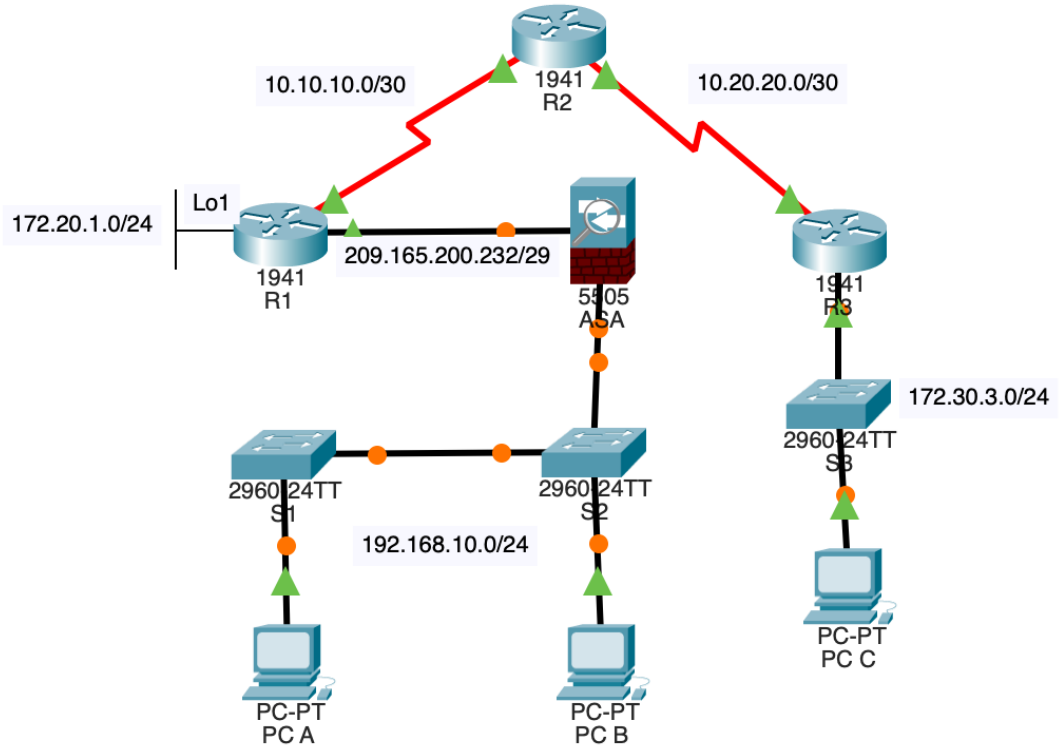

Рисунок 3.1 – Топологія мережі

1. Налаштування R1:

– Мінімальна довжина пароля – 10 символів.

– Шифрувати паролі відкритого тексту.

– Секретний пароль привілейованого режиму EXEC – DanyliukDanyliuk.

– Пароль консольного рядка – DanyliukDanyliuk, час очікування – 15 хвилин, повідомлення консолі не повинні переривати введення команди.

Пароль «enable secret»: встановлено зашифрований пароль DanyliukDanyliuk для доступу до привілейованого режиму (R1(config)#enable secret DanyliukDanyliuk) (див. на рис. 3.2)

Мінімальна довжина пароля: Встановлено мінімальну довжину для паролів безпеки 10 символів (R1(config)#security passwords min-length 10) (див. на рис. 3.2).

Шифрування паролів: Увімкнено шифрування незашифрованих паролів (R1(config)#service password-encryption) (див. на рис. 3.2).

Налаштування консольного доступу (line console 0):

– пароль консольного доступу встановлено як DanyliukDanyliuk (R1(config-line)#password DanyliukDanyliuk);

– таймаут виконання команд встановлено на 15 хвилин та 0 секунд (R1(config-line)#exec-timeout 15 0);

– увімкнено автентифікацію для входу (R1(config-line)#login);

– увімкнено синхронне логування (R1(config-line)#logging synchronous).

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#enable secret DanyliukDanyliuk
R1(config)#service password-encryption
R1(config)#line console 0
R1(config-line)#password DanyliukDanyliuk
R1(config-line)#exec-timeout 15 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#banner motd $Unauthorized access strictly prohibited and prosecuted to the full
Enter TEXT message.  End with the character '$'.



enable
$

R1(config)#banner motd $Unauthorized access strictly prohibited and prosecuted to the full
Enter TEXT message.  End with the character '$'.
extent of the law!$

R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Рисунок 3.2 – Налаштування R1

2. Налаштування R2:

– Секретний пароль привілейованого режиму EXEC – DanyliukDanyliuk.

– Пароль для рядків VTY – DanyliukDanyliuk, час очікування – 15 хвилин, і потрібен вхід.

Встановлення зашифрованого пароля для привілейованого режиму: R2(config)#enable secret DanyliukDanyliuk (пароль DanyliukDanyliuk буде зашифрований).

Налаштування ліній віртуального терміналу (VTY) з 0 по 4: R2(config)#line vty 0 4 (див. на рис. 3.3) (ці лінії використовуються для Telnet/SSH доступу).

Встановлення пароля для VTY ліній: R2(config-line)#password (див. на рис. 3.3) DanyliukDanyliuk (пароль для віддаленого доступу).

Встановлення таймауту виконання команд: R2(config-line)#exec-timeout 15 0 (15 хвилин 0 секунд бездіяльності, після чого сесія буде розірвана).

Увімкнення автентифікації для входу: R2(config-line)#login (див. на рис. 3.3) (вимагатиме введення пароля при спробі віддаленого входу).

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#enable secret DanyliukDanyliuk
R2(config)#line vty 0 4
R2(config-line)#password DanyliukDanyliuk
R2(config-line)#exec-timeout 15 0
R2(config-line)#login
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.3 – Налаштування R2

3.2 Налаштування базової безпеки комутатора

1. Налаштування S1:

– шифрувати паролі відкритого тексту;

– секретний пароль привілейованого режиму EXEC – DanyliukDanyliuk;

– пароль рядка консолі – DanyliukDanyliuk, час очікування – 5 хвилин, повідомлення консолі не повинні переривати введення команди;

– пароль для рядків VTY – DanyliukDanyliuk, час очікування – 5 хвилин, і потрібен вхід.

Загальні налаштування безпеки:

– шифрування паролів: service password-encryption (див. на рис. 3.4) увімкнено для шифрування відкритих паролів;

– пароль "enable secret": enable secret DanyliukDanyliuk встановлює зашифрований пароль DanyliukDanyliuk для доступу до привілейованого режиму.

Налаштування консольного доступу (line console 0):

– пароль: password DanyliukDanyliuk (див. на рис. 3.4) встановлено для доступу через консоль;

– таймаут виконання: exec-timeout 5 0 встановлює таймаут сесії на 5 хвилин;

– вхід: login увімкнено запит пароля для входу;

– синхронне логування: logging synchronous забезпечує, що повідомлення системи не перериватимуть введення команд.

Налаштування віддаленого доступу (line vty 0 15):

– пароль: password DanyliukDanyliuk встановлено для віддаленого доступу (наприклад, через Telnet або SSH);

– таймаут виконання: exec-timeout 5 0 встановлює таймаут сесії на 5 хвилин;

– вхід: login увімкнено запит пароля для входу.

```
S1>enable
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#enable secret DanyliukDanyliuk
S1(config)#line console 0
S1(config-line)#password DanyliukDanyliuk
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#line vty 0 15
S1(config-line)#password DanyliukDanyliuk
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#banner motd $Unauthorized access strictly prohibited and prosecuted to the full
Enter TEXT message.  End with the character '$'.
extent of the law!$

S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Рисунок 3.4 – Налаштування S1

2. Налаштування транкінгу між S1 і S2:

– встановити режим trunk та призначити VLAN 99 як рідну VLAN;

– вимкнути генерацію кадрів DTP.

На комутаторах S1 і S2 інтерфейс FastEthernet 0/1 налаштований як транковий порт. Встановлено native VLAN 99, яка передає трафік без тегів. Вимкнено DTP-перемовини командою switchport nonegotiate (див. на рис. 3.5), що змушує порт працювати в статичному trunk-режимі.

Вимкнення DTP:

– захищає від атак типу *DTP spoofing*, коли зловмисник може змусити порт стати trunk'ом і отримати доступ до трафіку VLAN;

– статичне налаштування виключає можливість автоматичних перемовин, які можна було б використати для атак.

Native VLAN 99 (нетипова):

– захищає від атак типу *VLAN hopping*, де зловмисник може скористатися стандартною native VLAN (зазвичай VLAN 1), щоб проникнути в інші VLAN;

– використання окремої VLAN для нетегованого трафіку ускладнює зловмисникам доступ до основного трафіку (див. на рис. 3.5).

```
S2>enable
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface FastEthernet 0/1
S2(config-if)#switchport mode trunk

S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S2(config-if)#switchport trunk native vlan 99
S2(config-if)#switchport nonegotiate
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface FastEthernet 0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport nonegotiate
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Рисунок 3.5. – Налаштування транкінгу між S1 і S2

3.3 Налаштування локальної автентифікації AAA

1. Налаштування на R1:

– створити локальний обліковий запис користувача DanyliukDanyliuk із секретним паролем DanyliukDanyliuk і рівнем привілеїв 15;

– увімкнути служби AAA;

– впровадити служби AAA, використовуючи локальну базу даних як перший варіант, а потім enable-пароль як резервний.

Створення локального користувача: username Admin01 privilege 15 secret Admin01pa55 (див. на рис. 3.6).

– створює користувача з ім'ям Admin01;

– надає йому рівень привілеїв 15 (найвищий, еквівалентний режиму enable);

– встановлює зашифрований пароль Admin01pa55.

Увімкнення нової моделі AAA: aaa new-model (див. на рис. 3.6).

– ця команда активує нову, більш гнучку модель аутентифікації, авторизації та обліку (AAA).

Налаштування аутентифікації для входу: aaa authentication login default local enable (див. на рис. 3.6).

– вказує, що для аутентифікації (входу) за замовчуванням (група default) слід використовувати локальну базу даних користувачів (local);

– якщо аутентифікація через локальну базу даних не вдається, буде використаний пароль enable (як резервний механізм).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username Admin01 privilege 15 secret Admin01pa55
R1(config)#aaa new-model
R1(config)#aaa authentication login default local enable
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.6. – Налаштування локальної автентифікації AAA

3.4 Налаштування SSH

1. Налаштування на R1:

- ім’я домену – DanyliukDanyliuk.com;
- генерація ключа RSA із 1024 модульними бітами;
- дозволити лише SSH версії 2;
- тільки SSH дозволено на лініях VTY;
- перевірити, що PC-C може отримати доступ до R1 (209.165.200.233) через SSH.

Конфігурація IPsec VPN:

– назва домену: Встановлено ip domain-name DanyliukDanyliuk.com;

– трансформ-сет: Створено crypto ipsec transform-set VPN-SET з esp-aes 256 та esp-sha-hmac для шифрування та аутентифікації;

– крипто-мапа: Створено crypto map CMAP 10 ipsec-isakmp:

- пір: Вказано віддалений VPN-пір 10.20.20.1 (див. на рис. 3.7);
- PFS: Включено Perfect Forward Secrecy (PFS) з групою group5;
- трансформ-сет: Прив'язано transform-set VPN-SET(див. на рис. 3.7);
- список доступу: Вказано match address 101, що означає, що для визначення трафіку, який буде шифруватися, буде використовуватися список доступу з номером 101 (сам список на скріншоті не показаний);
- інтерфейс: Крипто-мапа CMAP застосована до інтерфейсу Serial0/0/0.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name DanyliukDanyliuk.com
R1(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.20.20.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface S0/0/0
R1(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Рисунок 3.7. – Налаштування SSH

3.5 Налаштування міжсайтової IPsec VPN

1. Увімкніть ліцензію пакета технологій безпеки на R1 і збережіть поточну конфігурацію.

2. Налаштуйте на R1:

– створити ACL 101 для дозволу трафіку від мережі R1 Lo1 до локальної мережі R3 G0/1;

– визначити Phase 1 для crypto isakmp policy 10 із такими параметрами:

- шифрування: aes 256, хеш: sha, метод автентифікації: попередній, DH Group: 5, термін дії: 3600 секунд;
- спільний криптоключ: ciscovpnpa55.

– створити трансформаційний набір VPN-SET із esp-aes 256 і esp-sha-hmac;

– створити криптокарту CMAP із порядковим номером 10 і прив’язкою до інтерфейсу.

3. Повторити аналогічні дії для R3 і переконайтеся, що VPN-тунель працює (кількість пакетів у show crypto ipsec sa > 0).

1. Конфігурація списку доступу (Access List):

– access-list 101 permit ip 172.30.3.0 0.0.0.255 172.20.1.0 0.0.0.255 - Створено розширений список доступу з номером 101, який дозволяє IP-трафік між мережами 172.30.3.0/24 та 172.20.1.0/24. Цей список буде використовуватися для визначення "цікавого трафіку" (interesting traffic) для VPN (див. на рис. 3.8).

2. Конфігурація ISAKMP (Internet Security Association and Key Management Protocol):

– crypto isakmp policy 10 - Створено політику ISAKMP з пріоритетом 10:

- encryption aes 256 - Встановлено алгоритм шифрування AES з ключем 256 біт;
- authentication pre-share - Встановлено метод аутентифікації за допомогою попередньо узгодженого ключа (pre-shared key);
- hash sha - Встановлено хеш-алгоритм SHA;

- group 5 - Встановлено групу Діффі-Хеллмана 5 для генерації ключа;
- lifetime 3600 - Встановлено термін дії ISAKMP SA (Security Association) на 3600 секунд (1 година).

– crypto isakmp key DanyliukDanyliuk address 10.10.10.1 - Вказано попередньо узгоджений ключ "DanyliukDanyliuk" для піра з IP-адресою 10.10.10.1.

3. Конфігурація IPsec Transform Set:

– crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac (див. на рис. 3.8) - Створено набір трансформацій IPsec з назвою VPN-SET, який використовує:

- esp-aes 256 для шифрування (AES 256-біт в режимі ESP);
- esp-sha-hmac для аутентифікації (SHA в режимі ESP HMAC).

4. Конфігурація Crypto Map:

– crypto map CMAP 10 ipsec-isakmp (див. на рис. 3.8)- Створено крипто-мапу з назвою CMAP та пріоритетом 10, що використовує ISAKMP для встановлення з'єднання.

- % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured. - Стандартне попередження, що крипто-мапа не буде активована, доки не будуть налаштовані пір та дійсний список доступу (хоча обидва вже налаштовані на скріншоті);
- set peer 10.10.10.1 - Вказано IP-адресу віддаленого VPN-піра 10.10.10.1;
- set transform-set VPN-SET - Призначено створений раніше VPN-SET для цієї крипто-мапи;
- match address 101 - Вказано, що для ідентифікації "цікавого трафіку" (того, що підлягає шифруванню) використовуватиметься список доступу з номером 101, який був визначений раніше.

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 101 permit ip 172.30.3.0 0.0.0.255 172.20.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
R3(config)#crypto isakmp key DanyliukDanyliuk address 10.10.10.1
R3(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
R3(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 10.10.10.1
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit
R3(config)#interface S0/0/1
R3(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.8. – Налаштування міжсайтової IPsec VPN

3.6 Налаштування параметрів брандмауера та IPS

1. Налаштування ZPF на R3:

– Створити зони IN-ZONE та OUT-ZONE.

– Створити ACL 110 для дозволу трафіку з 172.30.3.0/24 до any.

– Створити карту класів INTERNAL-CLASS-MAP і карту політики IN-2-OUT-PMAP.

– Призначити політику для інспектування трафіку між зонами.

– Призначити G0/1 до IN-ZONE, S0/0/1 до OUT-ZONE.

Створення зон безпеки:

– zone security IN-ZONE - Створено зону "IN-ZONE" для внутрішньої мережі.

– zone security OUT-ZONE - Створено зону "OUT-ZONE" для зовнішньої мережі.

Створення списку доступу (Access List):

– access-list 110 permit ip 172.30.3.0 0.0.0.255 any - Дозволено IP-трафік з мережі 172.30.3.0/24 до будь-якої іншої мережі (див. на рис. 3.9).

– access-list 110 deny ip any any - Явно заборонено весь інший IP-трафік (в контексті цього ACL).

Створення класової мапи (Class Map):

– class-map type inspect match-all INTERNAL-CLASS-MAP - Створено класову мапу INTERNAL-CLASS-MAP типу inspect, яка відповідає всьому, що зазначено в ній.

– match access-group 110 - Вказано, що ця класова мапа співставляється з трафіком, дозволеним списком доступу 110 (див. на рис. 3.9).

Створення полісі-мапи (Policy Map):

– policy-map type inspect IN-2-OUT-PMAP - Створено полісі-мапу IN-2-OUT-PMAP типу inspect.

– class type inspect INTERNAL-CLASS-MAP - В межах цієї полісі-мапи застосовується поведінка до трафіку, що відповідає INTERNAL-CLASS-MAP.

– inspect - Для цього класу трафіку застосовується дія "inspect", що означає stateful-інспекцію (перевірку стану з'єднання), дозволяючи відповідний зворотній трафік.

– %No specific protocol configured in class INTERNAL-CLASS-MAP for inspection. All protocols will be inspected - Зауваження про те, що оскільки конкретні протоколи не вказані, інспекції підлягатимуть всі протоколи.

Створення пар зон (Zone Pair):

– zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE - Створено пару зон IN-2-OUT-ZPAIR для трафіку, що йде з IN-ZONE в OUT-ZONE.

– service-policy type inspect IN-2-OUT-PMAP - До цієї пари зон застосовується створена раніше полісі-мапа IN-2-OUT-PMAP для інспекції трафіку (див. на рис. 3.9).

Призначення інтерфейсів до зон:

– interface g0/1 та zone-member security IN-ZONE - Інтерфейс GigabitEthernet0/1 включено до "IN-ZONE".

– interface s0/0/1 та zone-member security OUT-ZONE - Інтерфейс Serial0/0/1 включено до "OUT-ZONE".

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#zone security OUT-ZONE
R3(config-sec-zone)#access-list 110 permit ip 172.30.3.0 0.0.0.255 any
R3(config)#access-list 110 deny ip any any
R3(config)#class-map type inspect match-all INTERNAL-CLASS-MAP
R3(config-cmap)#match access-group 110
R3(config-cmap)#exit
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect INTERNAL-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class INTERNAL-CLASS-MAP for inspection. All protocols will be inspected
R3(config-pmap-c)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#interface g0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
```

Рисунок 3.9. – Налаштування ZPF на R3

2. Налаштування IPS:

– Створити каталог ipsdir у флеш-пам’яті.

– Створити правило IPS-RULE.

– Вилучити категорію IOS_IPS Basic із видаленням retired false.

– Застосувати правило до S0/0/1.

Налаштування IPS на основі сигнатур:

– ip ips config location flash:ipsdir - Вказано місцезнаходження конфігураційних файлів IPS.

– ip ips name IPS-RULE - Створено IPS-правило з назвою IPS-RULE (див. на рис. 3.10).

Налаштування категорій сигнатур:

– ip ips signature-category - Перехід до конфігурації категорій сигнатур.

– category all та retired true - Всі категорії сигнатур встановлені як "зняті з експлуатації" (retired), що означає, що вони не будуть активними за замовчуванням.

– category ios_ips basic та retired false - Категорія ios_ips basic встановлена як активна (не retired). Це означає, що сигнатури з цієї базової категорії будуть використовуватися.

Застосування IPS до інтерфейсу:

– interface s0/0/1 - Перехід до конфігурації інтерфейсу Serial0/0/1.

– ip ips IPS-RULE in - IPS-правило IPS-RULE застосовано до вхідного трафіку на інтерфейсі Serial0/0/1.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ips config location flash:ipsdir
%IPS-3-IPS_FILE_OPEN_ERROR: flash:ipsdir/sigdef-default.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash:ipsdir/sigdef-delta.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash:ipsdir/sigdef-category.xml - Directory doesn't exist
R3(config)#ip ips name IPS-RULE
R3(config)#ip ips signature-category
R3(config-ips-category)#category all
R3(config-ips-category-action)#retired true
R3(config-ips-category-action)#exit
R3(config-ips-category)#category ios_ips basic
R3(config-ips-category-action)#retired false
R3(config-ips-category-action)#exit
R3(config-ips-category)#
R3(config-ips-category)#interface s0/0/1
R3(config-if)#ip ips IPS-RULE in
R3(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  00:19:33 UTC бер. 01 1993

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

Рисунок 3.10. – Налаштування IPS

3.7 Налаштування параметрів безпеки та брандмауера ASA

1. Налаштування інтерфейсів VLAN:
   – VLAN 1: 192.168.10.1/24, VLAN 2: 209.165.200.234/29.
2. Налаштувати ім’я хоста та паролі:
   – Ім’я хоста ASA – КВ-41.
   – Пароль увімкнення – DanyliukDanyliuk.
3. Налаштувати AAA для локальної автентифікації.
4. Налаштувати ASA як сервер DHCP із діапазоном 192.168.10.5 – 192.168.10.30.
5. Налаштувати статичну маршрутизацію та NAT.

6. Змінити Cisco Modular Policy Framework для inspect ICMP.

Налаштування інтерфейсів VLAN та їх імен/рівнів безпеки:

– interface vlan 1

- nameif inside - Інтерфейс названо "inside".
- security-level 100 - Призначено рівень безпеки 100 (найвищий, зазвичай для внутрішньої мережі).
- ip address 192.168.10.1 255.255.255.0 - Призначено IP-адресу 192.168.10.1/24 (див. на рис. 3.11).

– interface vlan 2

- nameif outside - Інтерфейс названо "outside".
- security-level 0 - Призначено рівень безпеки 0 (найнижчий, зазвичай для зовнішньої мережі/Інтернету).
- no ip address dhcp - DHCP вимкнено.
- ip address 209.165.200.234 255.255.255.248 - Призначено IP-адресу 209.165.200.234/29 (див. на рис. 3.11).

Загальні налаштування ASA:

– hostname CCNAS-ASA - Встановлено ім'я хоста.

– domain-name DanyliukDanyliuk.KB43.com - Встановлено доменне ім'я.

– enable password DanyliukDanyliuk - Встановлено пароль для привілейованого режиму.

– username admin password DanyliukDanyliuk - Створено користувача "admin" з паролем.

– aaa authentication ssh console LOCAL - Налаштовано AAA аутентифікацію для SSH через локальну базу даних.

– ssh 192.168.10.0 255.255.255.0 inside - Дозволено SSH доступ з мережі 192.168.10.0/24 через інтерфейс "inside".

– ssh 172.30.3.3 255.255.255.255 outside - Дозволено SSH доступ з конкретного хоста 172.30.3.3 через інтерфейс "outside".

– ssh timeout 10 - Встановлено таймаут SSH сесії 10 хвилин.

Налаштування DHCP сервера (для внутрішньої мережі):

– dhcpd address 192.168.10.5-192.168.10.30 inside - Налаштовано діапазон IP-адрес для DHCP сервера на інтерфейсі "inside".

– dhcpd enable inside - Увімкнено DHCP сервер на інтерфейсі "inside".

Маршрутизація:

– route outside 0.0.0.0 0.0.0.0 209.165.200.233 - Додано маршрут за замовчуванням (default route) через шлюз 209.165.200.233 на інтерфейсі "outside" (див. на рис. 3.11).

Мережеві об'єкти (Network Objects):

– object network inside-net - Створено мережевий об'єкт "inside-net".

– subnet 192.168.10.0 255.255.255.0 - Призначено підмережу 192.168.10.0/24 цьому об'єкту.

Трансляція мережевих адрес (NAT):

– nat (inside,outside) dynamic interface - Налаштовано динамічний NAT для трафіку, що йде з "inside" на "outside", використовуючи IP-адресу зовнішнього інтерфейсу як джерело NAT.

Полісі-мапа (Policy Map) для інспекції трафіку:

– class-map inspection_default та match default-inspection-traffic - Видно спроби налаштування класової мапи для дефолтного трафіку інспекції.

– policy-map global_policy та class inspection_default - Налаштовується глобальна полісі-мапа.

– inspect icmp - Вказано, що ICMP-трафік буде інспектований (дозволяючи зворотні відповіді).

– service-policy global_policy global - Глобальна полісі-мапа застосовується до всього трафіку.

```
ciscoasa>
ciscoasa>enable
Password:
ciscoasa#conf t
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#no ip address dhcp
WARNING: DHCPD bindings cleared on interface 'outside', address pool removed
ciscoasa(config-if)#ip address 209.165.200.234 255.255.255.248
ciscoasa(config-if)#exit
ciscoasa(config)#hostname CCNAS-ASA
CCNAS-ASA(config)#domain-name DanyliukDanyliuk_KB43.com
CCNAS-ASA(config)#enable password DanyliukDanyliuk
CCNAS-ASA(config)#username admin password DanyliukDanyliuk
CCNAS-ASA(config)#aaa authentication ssh console LOCAL
CCNAS-ASA(config)#ssh 192.168.10.0 255.255.255.0 inside
CCNAS-ASA(config)#ssh 172.30.3.3 255.255.255.255 outside
CCNAS-ASA(config)#ssh timeout 10
CCNAS-ASA(config)#dhcpd address 192.168.10.5-192.168.10.30 inside
CCNAS-ASA(config)#dhcpd enable inside
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.233
CCNAS-ASA(config)#object network inside-net
CCNAS-ASA(config-network-object)#subnet 192.168.10.0 255.255.255.0
CCNAS-ASA(config-network-object)#nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)#exit
CCNAS-ASA#conf t
CCNAS-ASA(config)#class-map inspection_default
CCNAS-ASA(config-cmap)#match default-inspection-traffic
CCNAS-ASA(config-cmap)#exitp
                       ^
% Invalid input detected at '^' marker.

CCNAS-ASA(config-cmap)#eit
                        ^
% Invalid input detected at '^' marker.

CCNAS-ASA(config-cmap)#policy-map global_policy
CCNAS-ASA(config-pmap)#class inspection_default
CCNAS-ASA(config-pmap-c)#inspect icmp
CCNAS-ASA(config-pmap-c)#exit
CCNAS-ASA(config)#service-policy global_policy global
CCNAS-ASA(config)#
```

Рисунок 3.11. Налаштування інтерфейсів VLAN

Висновки за розділом 3

У третьому розділі кваліфікаційної роботи було реалізовано практичне впровадження механізмів захисту бездротової мережі від атак типу DoS та DDoS. В результаті виконаних налаштувань було підтверджено доцільність застосування багаторівневого підходу до безпеки, який включає фізичні, мережеві та програмні компоненти захисту. Практична частина є логічним завершенням теоретичних досліджень, проведених у попередніх розділах, і

демонструє реальні можливості протидії сучасним кіберзагрозам у бездротовому середовищі.

У ході роботи було змодельовано інфраструктуру бездротової мережі, яка включає маршрутизатори, комутатори, міжмережевий екран (брандмауер), а також окремі вузли-клієнти. На базі цього середовища було реалізовано низку заходів безпеки:

1. Налаштування безпеки на маршрутизаторі:
   - активація шифрування WPA2/WPA3;
   - зміна стандартних облікових записів доступу;
   - обмеження доступу за MAC-адресами;
   - вимкнення небезпечних служб (WPS, UPnP, Telnet);
   - фільтрація трафіку на рівні IP та портів.
2. Конфігурування комутатора:
   - ізоляція сегментів мережі за допомогою VLAN;
   - обмеження кількості MAC-адрес на порт;
   - активація функцій Port Security;
   - захист проти ARP-спуфінгу, DHCP-атак.
3. Інтеграція міжмережевого екрану Cisco ASA:
   - реалізація гнучких правил фільтрації вхідного та вихідного трафіку;
   - обмеження швидкості (rate limiting) для виявлення підозрілих запитів;
   - захист від SYN Flood та ICMP Flood;
   - логування та сповіщення про підозрілу активність.
4. Додаткові програмні засоби:
   - налаштування VPN для захищеного віддаленого підключення;
   - використання правил фільтрації для IDS/IPS (зокрема Snort);
   - створення політик доступу та автоматизованого реагування на аномалії.

Практична реалізація показала, що навіть у межах стандартного середовища, наближеного до умов малого підприємства або офісу, можна

суттєво зменшити ризик DoS/DDoS-атак. Особливо важливою виявилася сегментація трафіку та контроль на прикордонному рівні мережі, що дозволило блокувати несанкціоновані спроби доступу ще до досягнення цільових вузлів.

У підсумку реалізація підтвердила такі ключові положення:

– захист бездротової мережі має здійснюватися на кількох рівнях: від фізичного доступу до глибокого аналізу трафіку;

– поєднання класичних методів (MAC-фільтрація, шифрування, VLAN) з сучасними засобами (IDS/IPS, VPN, rate limiting) дає змогу ефективно протидіяти як простим DoS, так і складним багатопотоковим DDoS-атакам;

– правильна організація моніторингу та автоматичного реагування дозволяє мінімізувати час реагування на інциденти.

Отже, практична частина роботи підтвердила, що технічно грамотна організація бездротової мережі із впровадженням багаторівневого захисту дозволяє забезпечити її стійкість до DoS/DDoS-атак і може бути застосована як у корпоративному, так і в побутовому середовищі. Такий підхід є ефективним, масштабованим та економічно виправданим у сучасних умовах розвитку кіберзагроз.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено ґрунтовне дослідження архітектури та принципів функціонування бездротових мереж, що дозволило встановити їхні ключові характеристики, переваги й уразливості. Особливу увагу було приділено аналізу таких типів мереж, як WLAN, WPAN, WWAN та супутникові мережі, зокрема їхньому застосуванню, технічним параметрам і викликам у сфері безпеки. Досліджено також вплив новітніх технологій, зокрема Wi-Fi 6, 5G та IoT, на зростання складності захисту інформації в бездротовому середовищі.

У другому розділі кваліфікаційної роботи проведено глибокий аналіз теоретичних основ DoS та DDoS-атак, зокрема класифікацію атак за моделлю OSI, їхні технічні особливості та сценарії реалізації. Розглянуто найбільш поширені інструменти та платформи для здійснення атак: від простих утиліт на зразок LOIC, HOIC і Slowloris до потужних бот-мереж на базі IoT, таких як Mirai. Значну увагу було зосереджено на прикладах реальних інцидентів, що ілюструють масштаб і наслідки DDoS-атак на великі цифрові платформи (GitHub, Dyn, Cloudflare), що підкреслює актуальність теми дослідження.

У межах практичного блоку дослідження реалізовано заходи захисту бездротових мереж на прикладі налаштування обладнання (маршрутизаторів, комутаторів, брандмауерів та IPS/IDS-систем). Здійснено конфігурування параметрів безпеки, фільтрації трафіку, автентифікації, шифрування та мережевої ізоляції. Крім того, впроваджено використання VPN і технологій виявлення аномального трафіку, що дозволяє суттєво підвищити рівень захисту від DDoS-атак.

У підсумку слід зазначити, що:

1. Бездротові мережі залишаються надзвичайно вразливими до атак типу DoS та DDoS через відкриту природу середовища передавання даних.

2. Найефективнішими є багаторівневі моделі захисту, які поєднують заходи на мережевому, протокольному та прикладному рівнях.

3. Ключовими складовими надійного захисту є: шифрування трафіку, автентифікація користувачів, фільтрація доступу, сегментація мережі, використання VPN та інтеграція IDS/IPS.

4. Реальні кейси масових атак демонструють необхідність постійного оновлення знань і технічних рішень у сфері захисту мереж.

Практична цінність проведеного дослідження полягає в узагальненні ефективних підходів до захисту від DoS/DDoS-атак у бездротовому середовищі та створенні рекомендацій для впровадження захисних механізмів на реальних об'єктах інфраструктури. Запропоновані рішення можуть бути використані як у невеликих офісних чи домашніх мережах, так і в корпоративному секторі.

Отже, кваліфікаційна робота повністю реалізувала поставлену мету: теоретично обґрунтовано, технічно підтверджено та практично реалізовано комплекс заходів для захисту бездротових мереж від атак типу DoS та DDoS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms // ACM SIGCOMM Computer Communication Review. – 2004. – Vol. 34, № 2. – P. 39–53.

2. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities // Future Generation Computer Systems. – 2018. – Vol. 78. – P. 544–546.

3. Stallings W. Wireless Communications and Networks. – 2nd ed. – Upper Saddle River: Pearson Education, 2005. – 559 p.

4. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Upper Saddle River: Pearson Education, 2011. – 951 p.

5. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. – 2nd ed. – Upper Saddle River: Prentice Hall, 2002. – 752 p.

6. ISO/IEC 27033-6:2016. Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access. – Geneva: ISO, 2016. – 58 p.

7. IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – New York: IEEE, 2020. – 1312 p.

8. Handley M., Rescorla E., eds. Internet Denial-of-Service Considerations. – RFC 4732. – December 2006. – 24 p.

9. *Cloudflare. What is a DDoS attack?* URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (дата звернення: 07.04.2025).

10. *OWASP. Denial of Service (DoS)* URL: https://owasp.org/www-community/attacks/Denial_of_Service (дата звернення: 14.05.2025).

11. *Cisco Systems. Configuring Basic DoS Protection on Cisco Routers* URL: https://www.cisco.com (дата звернення: 11.04.2025).

12. *Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3™ Security* URL: https://www.wi-fi.org/discover-wi-fi/security (дата звернення: 12.04.2025).

13. *SolarWinds. Protecting Against DDoS Attacks: Best Practices* URL: https://www.solarwinds.com/resources/ddos-protection (дата звернення: 07.06.2025).cdn.standards.iteh.ai

14. *Snort by Cisco. Open Source Intrusion Detection System* URL: https://www.snort.org (дата звернення: 05.05.2025).

15. *GitHub. Mirai Botnet Source Code* URL: https://github.com/jgamblin/Mirai-Source-Code (дата звернення: 06.06.2025).

16. Security Threats on Cloud Computing Vulnerabilities // *International Journal of Computer Science and Information Technology*. – June 2013. URL: https://www.researchgate.net/publication/289756317_Security_Threats_on_Cloud_Computing_Vulnerabilities (дата звернення: 05.06.2025).

17. Taghavi Zargar S., Joshi J., Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks // *IEEE Communications Surveys & Tutorials*. – 2013. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.692.9498 (дата звернення: 03.06.2025).

18. *Cloudflare. What is a denial-of-service (DoS) attack?* URL: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ (дата звернення: 07.06.2025).

19. *Imperva. Buffer overflow example.* URL: https://www.imperva.com/learn/application-security/buffer-overflow/ (дата звернення: 06.06.2025).

20. *Myra Security. HTTP Flood Attack.* URL: https://www.myrasecurity.com/en/http-flood-attack/ (дата звернення: 07.06.2025).

21. *Cloudflare. What is a DDoS Botnet?* URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (дата звернення: 02.06.2025).