Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Кувіли Анни Олексіївни

на здобуття ступеня вищої освіти Бакалавра

Система виявлення та захисту від DoS–атак в корпоративних мережах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ. 2101124.21.01.09 ПЗ

Виконала студентка 4 курсу, група КБ–21–1	Підпис, дата	Анна КУВІЛА Ініціали, прізвище
Керівник канд. тех. наук, доцент Науковий ступінь, вчене звання	Підпис, дата	Віра ТІТОВА Ініціали, прізвище
Нормоконтролер старший викладач Науковий ступінь, вчене звання	Підпис, дата	Сергій МОСТОВИЙ Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата Ініціали, прізвище

9 06 2025р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кувіли Анни Олексіївни

1 Тема роботи Система виявлення та захисту від DoS–атак в корпоративних мережах

Керівник роботи к.т.н, доц. кафедри кібербезпеки Віра Юріївна Тітова

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи Створення системи виявлення та захисту від DoS–атак

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Розгляд поняття корпоративної мережі; аналіз існуючих загроз; огляд методів захисту корпоративної мережі; розбір типів DoS–атак та методів їх запобігання; аналіз загроз та їх вирішень за допомогою CORAS моделей; розробка системи виявлення та захисту; тестування розробленої системи

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Модель внутрішніх загроз, модель внутрішніх порушників

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	лютий	
Ознайомлення з предметною областю	лютий	
Дослідження існуючих рішень	березень	
Постановка задачі	березень	
Визначення загальних принципів рішення задачі	березень	
Деталізація принципів рішення задачі	квітень	
Розробка проєктних рішень	квітень	
Апробація проєктних рішень	квітень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	травень	
Захист КР	червень	

Студентка Анна КУВІЛА

Керівник кваліфікаційної роботи Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система виявлення та захисту від DoS–атак в корпоративних мережах».

Авторка роботи: Кувіла Анна Олексіївна.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 63 с., 4 додатки, 9 рис., 40 джерел.

Графічна частина: 3 презентаційних слайдів.

Завданням кваліфікаційної роботи є розробка системи виявлення та захисту від DoS–атак в корпоративній мережі. В роботі проаналізовано існуючі загрози і вразливості, найпоширеніші типи DoS–атак та методи захисту корпоративних мереж. Розроблено моделі загроз для наглядного розбору вразливостей, потенційних загроз та способів їх вирішення. Проведено аналіз існуючих рішень для створення системи виявлення та захисту.

В результаті розроблено систему виявлення та захисту від DoS–атак, яка є незалежною від сторонніх сервісів, гнучкою в налаштуванні. Включає в себе фільтрацію за регіональним походженням, можливість моніторингу та тестування системи в реальному часі. Систему можна вдосконалювати та легко впроваджувати в реальну інфраструктуру.

31.05.2025

ABSTRACT

Theme of the qualification work: «System for detecting and protecting against DoS–attack in the corporate networks.».

Author of the work: Kuvila Anna Oleksiivna.

Supervisor: Titova Vira Yuriivna.

Explanatory note: 63 p., 4 appendices, 9 figures, 40 references.

Graphic part: 3 presentation slides.

The task of the qualification work is to develop a system for detecting and protecting against DoS attacks in the corporate network. The work analyzes existing threats and vulnerabilities, the most common types of DoS attacks and methods of protecting corporate networks. Developed threat models for visual analysis of vulnerabilities, potential threats and ways to solve them. An analysis of existing solutions for creating a detection and protection system was carried out.

As a result, a system for detecting and protecting against DoS attacks has been developed, which is independent of third–party services, flexible in configuration. Includes filtering by regional origin, the ability to monitor and test the system in real time. The system can be improved and easily implemented in real infrastructure.

31.05.2025

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

API – Application Programming Interface

CDN – Content Delivery Network

DDoS – Destributed Denial of Service

DMZ – Demilitarized Zone

DoS – Denial of Service

HTTP – Hypertext Transfer Protocol

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

OSI – Open Systems Interconnection

SQL – Structured Query Language

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

XSS – Cross–Site Scripting

ПЗ – Програмне Забезпечення

ВСТУП

У сучасному цифровому світі, де функціонування бізнесу та суспільства нерозривно пов'язане з інформаційно–комунікаційними технологіями, забезпечення стабільності та доступності мережевих ресурсів набуває критичного значення. Однією з найсерйозніших загроз для цієї доступності є атаки типу «відмова в обслуговуванні» (Denial of Service) та їх розподілений варіант (Distributed Denial of Service). Ці атаки спрямовані на перевантаження цільових систем, мереж або сервісів надмірним обсягом шкідливого трафіку, що призводить до їх уповільнення, нестабільної роботи або повної недоступності для легітимних користувачів. Корпоративні мережі, що підтримують ключові бізнес–процеси, фінансові операції, комунікацію та зберігання конфіденційних даних, є особливо привабливими цілями для таких атак.

Одночасно зі зростанням обсягів, зловмисники вдосконалюють свої методи. Спостерігається зсув у бік більш складних атак, зокрема атак на прикладному рівні, які імітують легітимну поведінку користувачів і складніше виявляються традиційними засобами. Поширюються багатовекторні атаки, що комбінують різні техніки для подолання захисту, та атаки, що одночасно спрямовані на декілька IP–адрес. Важливим фактором є використання штучного інтелекту та машинного навчання зловмисниками для автоматизації розвідки, адаптації атак у реальному часі та обходу захисних механізмів. Зростання кількості пристроїв Інтернету речей (IoT) зі слабким захистом призводить до формування масштабніших та потужніших ботнетів, таких як Mirai, що використовуються для генерації величезних обсягів трафіку.

Сучасна корпоративна мережа є складним середовищем, що включає не лише традиційну локальну інфраструктуру, але й хмарні сервіси (IaaS, PaaS, SaaS), інтерфейси прикладного програмування для інтеграції систем та віддалений доступ через віртуальні приватні мережі. Зловмисники можуть цілеспрямовано атакувати API для порушення критичних бізнес–процесів або

VPN–шлюзи для блокування віддаленого доступу для співробітників. Залежність від хмарних провайдерів також несе ризики, оскільки атаки на інфраструктуру провайдера можуть опосередковано вплинути на корпоративних клієнтів, а неправильні конфігурації хмарних ресурсів створюють додаткові вразливості. Таким чином, традиційні підходи до захисту стають недостатніми, оскільки атаки можуть вплинути на будь–який елемент цієї розподіленої системи.

Спостерігається тенденція до скорочення тривалості багатьох атак але при цьому зростає їхня інтенсивність. Це свідчить про те, що зловмисники можуть використовувати DoS-атаки не лише для тривалого блокування сервісу, але й для швидкого завдання шкоди або як димову завісу для прикриття інших шкідливих дій, таких як проникнення в мережу, крадіжка даних або розгортання програм–вимагачів. Така тактика вимагає від систем захисту надзвичайно швидкої реакції, оскільки ручне втручання адміністраторів часто виявляється занадто повільним.

Існуючі засоби захисту, такі як традиційні міжмережеві екрани та системи виявлення вторгнень, часто виявляються недостатньо ефективними проти сучасних DoS–атак. Мережеві екрани можуть бути перевантажені об'ємними атаками або нездатні розпізнати атаки на прикладному рівні, а сигнатурні IDS безсильні проти нових, невідомих атак. Це зумовлює нагальну потребу в розробці та впровадженні більш досконалих, інтелектуальних та адаптивних систем виявлення та захисту, спеціально розроблених для протидії сучасному спектру загроз у складних умовах корпоративних мереж.

На фоні зростання кількості та складності DoS–атак виникає нагальна потреба у розробці та впровадженні ефективних систем виявлення й захисту, здатних оперативно реагувати на спроби порушення доступності ресурсів. Така система повинна враховувати особливості корпоративної мережі, забезпечувати мінімізацію ризиків та сприяти підтриманню безперервності бізнес–процесів.

Метою даної дипломної роботи є розробка такої системи та оцінка її ефективності.

Для досягнення поставленної мети було поставлено такі задачі:

– аналіз загроз та ризиків, пов’язаних із DoS–атаками на корпоративні мережі, визначення їх впливу на доступність критичних сервісів;

– розробка моделі захисту корпоративної мережі від DoS–атак, з урахуванням специфіки типових загроз, інфраструктури та обмежень організаційного середовища;

– проведення експериментального тестування моделі у симульованому середовищі, здійснення оцінки її ефективності та виявлення потенційних вразливостей для подальшої оптимізації.

1 АНАЛІЗ ОБ’ЄКТУ ЗАХИСТУ

1.1 Загальна характеристика корпоративних мереж

Корпоративна мережа – це інформаційно–комунікаційна інфраструктура, яка об’єднує комп’ютерні пристрої, сервери, програмне забезпечення, бази даних та інші мережеві компоненти в рамках однієї організації. Вона забезпечує обмін даними, зв’язок між співробітниками, спільне використання ресурсів, а також захист інформації.

Основні функції корпоративної мережі:

– обмін даними, спільний доступ до файлів, документів та корпоративних баз даних;

– робота електронної пошти, корпоративних месенджерів, VoIP–телефонії та відеоконференцзв’язку;

– спільне використання ресурсів;

– захист інформації, контроль доступу, запобігання кібератакам, резервне копіювання даних;

– підтримка бізнес–процесів, інтеграція з корпоративними системами, такими як CRM, ERP та інші. [1, 2]

У наш час корпоративні мережі стали критичною інфраструктурою, аналогічною за значенням до енергетичних об'єктів чи транспортних вузлів. Їх стабільна робота безпосередньо впливає на життєздатність бізнесу та економіки в цілому. Однак із зростанням залежності від мережевих ресурсів зростає й загроза DoS–атак, які можуть призвести до серйозних порушень бізнес–процесів та значних фінансових втрат. Особливу загрозу становлять DDoS–атаки, здатні паралізувати роботу будь–якої організації. На сьогодняшній день існує багато сучасних методів захисту корпоративних мереж від DoS–атак.

Кібератаки, зокрема DDoS–атаки, є серйозною загрозою для корпоративних мереж, адже можуть завдати значних фінансових, репутаційних та правових втрат. Простої, спричинені подібними атаками, можуть обійтися підприємствам у мільйони доларів через втрату продажів, виплату штрафів або необхідність

компенсувати збитки клієнтам. При цьому витрати на ліквідацію наслідків кібератак часто значно перевищують витрати на впровадження профілактичних заходів кіберзахисту. [3]

Безпека корпоративного середовища також напряму пов’язана із захистом даних. Компанії оперують великою кількістю конфіденційної інформації, включно з фінансовими звітами, персональними даними клієнтів, співробітників, а також комерційними таємницями. Втрата або витік таких даних також може призвести до серйозних репутаційних збитків, втрати довіри клієнтів і навіть судових процесів. Також важливою є безперервність роботи – атака на банківську систему може зупинити фінансові транзакції, тоді як злам логістичної мережі призведе до зриву постачання товарів і порушення ланцюгів виробництва. Крім того, на організації покладається юридична відповідальність за дотримання регуляторних вимог у сфері кібербезпеки. У багатьох країнах світу, особливо в Європейському Союзі та США, діють суворі стандарти (зокрема, GDPR, NIS2), порушення яких тягне за собою великі штрафи. Для деяких галузей діють додаткові нормативи, як–от PCI DSS для фінансових установ або HIPAA для медичних закладів, які встановлюють ще вищі вимоги до кіберзахисту.

У сучасних умовах кібербезпека корпоративних мереж також є елементом національної безпеки. Великі корпорації в галузях енергетики, фінансів чи телекомунікацій належать до критичної інфраструктури країни, і їх злам або зупинка можуть мати катастрофічні наслідки для економіки. Яскравим прикладом є кібератака на енергосистему України у 2015 році, яка призвела до відключення електропостачання для сотень тисяч людей. Подібні інциденти демонструють, наскільки серйозною загрозою є атаки на цифрову інфраструктуру. Вони можуть становити ризик не лише для економіки, а й для життя та здоров’я громадян – наприклад, у разі зламу інформаційної системи лікарні або втручання в управління транспортом. [4]

Ураховуючи все більшу залежність бізнесу від інформаційних технологій, технологічна стійкість стає ключовим пріоритетом. У сучасному світі більшість

підприємств не можуть функціонувати без цифрової інфраструктури: навіть короткочасний збій у роботі мережі паралізує внутрішні процеси, викликає затримки у виробництві, збої в обслуговуванні клієнтів і загальну втрату ефективності. До того ж, загрози постійно еволюціонують – зловмисники все частіше використовують новітні технології, включно зі штучним інтелектом, для створення складніших атак. Саме тому системи виявлення та захисту від DoS–атак повинні бути не лише сучасними, а й здатними до постійного вдосконалення та адаптації до нових типів загроз.

1.2 Види загроз в корпоративних мережах

Сучасні корпоративні мережі постійно зазнають загроз як із зовнішнього середовища, так і зсередини організації. Розвиток цифрових технологій, збільшення кількості підключених пристроїв та зростання обсягів оброблюваних даних робить такі мережі дедалі вразливішими. З огляду на це, надзвичайно важливо ідентифікувати потенційні загрози, які можуть завдати шкоди як технічній інфраструктурі, так і бізнес–процесам компанії.

Загрози та вразливості в інформаційних системах корпоративних мереж впливають на загальну безпеку бізнесу, збереження даних і стабільність роботи. В умовах цифровізації підприємства дедалі частіше стають об'єктами цілеспрямованих кібератак, що використовують різноманітні методи проникнення, експлуатації вразливостей і виведення систем з ладу.

Загрози можна умовно поділити на внутрішні та зовнішні. Зовнішні загрози – це атаки, ініційовані зловмисниками за межами корпоративної мережі. Найбільш поширеними серед них є DoS–атаки, спрямовані на виведення з ладу вебсайтів чи серверів, фішинг і соціальна інженерія для отримання доступу до облікових записів, експлуатація уразливостей у програмному забезпеченні, атаки типу «zero–day», коли зловмисники використовують ще не виправлені помилки

безпеки, а також розповсюдження шкідливого ПЗ.

Внутрішні загрози, у свою чергу, походять від співробітників або внутрішніх користувачів. Вони можуть бути як навмисними, наприклад витік даних, так і випадковими – через використання слабких або спільних паролів, недотримання політик безпеки, або неправильне налаштування доступів. [5]

Найпоширеніші загрози:

Несанкціонований доступ – отримання доступу до даних без належних повноважень або зловмисне їх використання. Також під цим розуміють ситуації, коли співробітник має обмежений доступ, але навмисно чи випадково його перевищує. Основними причинами є неправильна конфігурація систем захисту, зокрема мережевих екранів і прав доступу, слабкі авторизаційні механізми дозволяють зловмисникам отримувати доступ через викрадені облікові дані або фізичний контакт із незахищеними пристроями. Технічні недоліки в засобах захисту та зловживання службовим становищем також відкривають шлях до конфіденційної інформації. Окрему загрозу становлять атаки через незахищені канали зв'язку та шкідливе програмне забезпечення.

Компанія може зіткнутися з витоком персональних даних співробітників і клієнтів, втратою комерційних таємниць. Кожен такий випадок несе загрозу як репутації організації, так і її фінансовій стабільності.

Шкідливе програмне забезпечення (Malware), включаючи віруси, трояни та програми–шпигуни, може інфікувати корпоративну мережу через фішингові листи, заражені файли або скомпрометовані веб–сайти. Особливо небезпечними є програми–вимагачі, які шифрують дані компанії та вимагають викуп за їх розблокування.

Фішинг та соціальна інженерія ґрунтуються на обмані користувачів із метою отримання доступу до конфіденційної інформації або компрометації облікових записів. Зловмисники маскуються під легітимні сервіси або колег, щоб переконати співробітника розкрити паролі, завантажити шкідливі файли чи здійснити небажані дії. [7]

Атаки на веб–додатки (наприклад, SQL–ін’єкції, XSS) використовують помилки у програмному коді або неправильні налаштування для втручання в роботу онлайн–сервісів компанії. Через ці атаки зловмисник може отримати доступ до баз даних, змінювати або видаляти інформацію, або запускати довільний код на сервері. [8]

Перехоплення даних у мережі (Sniffing) – один із найпростіших методів моніторингу мережевого трафіку. Його суть полягає у перехопленні даних, які передаються через мережу у вигляді пакетів. Можливий у випадках використання незашифрованих протоколів або неправильно налаштованих мережевих пристроїв. Унаслідок цього зловмисник може отримати доступ до переданої інформації – паролів, листування, файлів тощо.

Атаки типу «людина посередині» (Man–in–the–Middle) дозволяють зловмиснику перехопити й змінити дані між двома сторонами без їх відома. Такі атаки часто здійснюються в публічних або слабо захищених мережах і можуть призвести до викрадення облікових даних або підміни інформації. [9]

Особливої уваги заслуговують атаки типу відмови в обслуговуванні (Denial of Service), які становлять одну з найсерйозніших загроз для доступності інформаційних ресурсів. Основна мета таких атак полягає у створенні надмірного навантаження на цільову систему або мережу з метою порушення її нормального функціонування. У випадку розподіленої атаки (Distributed Denial of Service) зловмисники використовують велику кількість заражених пристроїв для генерації трафіку, що значно ускладнює виявлення джерел атаки та її нейтралізацію.

Існує кілька основних підходів до реалізації DoS–атак. Частина з них орієнтована на перевантаження каналів зв’язку, створюючи великі обсяги штучного трафіку, що унеможливлює обробку легітимних запитів. Інші експлуатують вразливості у протоколах або програмному забезпеченні серверів, викликаючи зависання, перезавантаження або збої в роботі. Ще один різновид DoS–атак зосереджується на рівні прикладних сервісів, таких як веб–сайти або

API, де відправлення великої кількості нібито коректних, але ресурсомістких запитів здатне суттєво уповільнити або повністю заблокувати їхню роботу.

Популярність DoS–атак серед зловмисників пояснюється низкою факторів. По–перше, реалізація таких атак не потребує глибоких технічних знань – існує безліч готових інструментів, доступних у відкритому доступі. По–друге, результат таких атак часто миттєвий, навіть короткотривале порушення доступності сервісу може призвести до фінансових збитків або втрати довіри з боку клієнтів. По–третє, зловмисники можуть використовувати DoS–атаки як засіб шантажу або для відволікання уваги від складніших цільових атак.

Корпоративні мережі найбільш уразливі до DoS–атак, однією з головних уразливостей є недостатня пропускна здатність каналів зв'язку. Якщо інтернет–канал компанії перевантажується навіть при незначному зростанні трафіку, зловмиснику досить здійснити атаку малої інтенсивності для повного блокування доступу до зовнішніх сервісів. Це особливо актуально для філіалів та регіональних офісів з обмеженими мережевими ресурсами. [10]

Ще однією поширеною проблемою є відсутність або слабкість механізмів раннього виявлення аномалій у трафіку. Багато корпоративних мереж не використовують сучасні засоби аналізу поведінки трафіку або обмежуються базовими правилами фільтрації, що не дозволяє вчасно розпізнати атаку, яка імітує легітимну активність.

Невірно налаштовані мережеві пристрої (маршрутизатори, комутатори, міжмережеві екрани) також можуть створювати вразливості. Наприклад, відкриті порти, відсутність обмежень на ICMP–запити, чи неправильно сконфігуровані правила трансляції мережевих адрес можуть бути використані для здійснення DoS–атаки або сприяти її ефективності.

Недосконала архітектура корпоративної мережі, зокрема централізований підхід до розміщення сервісів у межах одного дата–центру без належного резервування каналів зв'язку та механізмів розподілу навантаження, значно підвищує її вразливість. У разі потужної атаки така структура може призвести до

повного припинення роботи критичних сервісів через відсутність кластеризації або системи балансування трафіку.

Використання застарілого програмного забезпечення створює серйозні ризики для безпеки корпоративної мережі, оскільки нерідко містить невиправлені вразливості. Такі недоліки можуть бути використані зловмисниками для здійснення прикладних DoS–атак, зокрема, через перевантаження веб–серверів обробкою великої кількості HTTP–запитів, маніпулювання сесіями користувачів або ініціацію ресурсомістких процесів, що виснажують обчислювальні ресурси системи.

Використання хмарних сервісів без належного контролю доступу та налаштувань також створює додаткові вектори атаки. Погано захищені API, відкриті облікові записи або слабка аутентифікація в хмарному середовищі можуть використовуватись для здійснення або посилення DoS–атак. [11]

Окремо варто згадати відсутність централізованого моніторингу та логування подій, що ускладнює не тільки виявлення атаки, а й подальший аналіз інциденту. Якщо компанія не веде повноцінний облік подій безпеки, то і реагування на інциденти відбувається із затримкою, або взагалі не ініціюється.

1.3 Методи захисту корпоративних мереж від загроз

Ефективний захист корпоративної мережі ґрунтується на глибокому розумінні потенційних загроз, уразливостей та відповідних їм механізмів протидії. Корпоративні мережі щоденно стикаються з низкою викликів, серед яких особливу небезпеку становлять внутрішні порушення, конфігураційні помилки, використання застарілого програмного забезпечення, недосконаліть архітектури, відсутність систем моніторингу та політик безпеки. У цьому підрозділі розглядаються основні підходи до нейтралізації цих загроз.

Недосконаліть архітектури корпоративної мережі – основна причина уразливості інформаційної структури до різних типів атак, включаючи як зовнішні, так і внутрішні загрози. Найпоширенішими прикладами є централізація ресурсів, відсутність засобів масштабування та балансування навантаження.

Централізоване розміщення критичних сервісів наприклад, поштових серверів, CRM–систем, файлових сховищ в одному дата центрі без належного резервування та географічного дублювання значно підвищує ризик порушення доступності. У випадку аварії обладнання, кібератаки або відмови провайдера, втрачається доступ до всіх ключових функцій мережі. Централізована інфраструктура, в якій відсутні механізми розподілу навантаження, географічного резервування та кластеризації. Така структура створює єдину точку відмови. Якщо зловмисник або технічний збій виводить з ладу головний сервер або маршрутизатор, це призводить до повної зупинки сервісів.

Для усунення цієї проблеми доцільно реалізовувати принципи побудови відмовостійких архітектур. Щоб запобігти можливих проблем через надмірну централізацію, потрібно розміщувати критично важливі сервіси на декількох фізичних чи віртуальних платформах, наприклад у хмарних сервісах чи географічно розподілених дата центрах, створення резервних каналів зв'язку, а також сегментацію мережі, яка дозволяє ізолювати окремі служби у випадку загрози. Це дозволить досягти відмовостійкості, зменшення часу простою та можливості балансування навантаження між вузлами.

Також проблематично, якщо всі вузли орпоративної мережі перебувають у єдиному широкому сегменті, атака на один із хостів (через заражений пристрій чи вразливу службу) може швидко поширитися на інші елементи мережі. Сегментування за допомогою VLAN, DMZ або технологій мікросегментації дозволяє локалізувати інциденти, зменшити ризик їх розповсюдження та мінімізувати збитки. Наприклад бази даних, веб–сервери та клієнтські пристрої мають бути в різних сегментах. Сегментація обмежує доступ користувачів лише до тих ресурсів, які їм необхідні та які можуть бути доступними для них.

У разі зростання навантаження на сервіси, тобто під час пікового використання або під час атаки, система може не впоратись з обробкою запитів, тому низький рівень масштабованості також становить загрозу. Відсутність балансувальників навантаження, кластерів або контейнеризованих сервісів унеможливлює ефективне масштабування системи в режимі реального часу. Збільшення ресурсів одного вузла та додавання нових, балансування навантаження між серверами, сервісами та каналами зв'язку забезпечить безперервність обслуговування. Також часто зустрічається ситуація, коли канали зв'язку не мають резервування, а використання одного провайдера робить організацію залежною від його надійності. У разі відмови лінії або маршрутизатора весь доступ до зовнішніх сервісів та інтернету може бути втрачено. Тому корисним буде впровадження систем резервування обладнання та каналів, тобто подвійні маршрутизатори, джерела живлення та провайдери.

Програмне забезпечення, яке тривалий час не оновлювалось, має вразливості, що активно експлуатуються кіберзлочинцями. Це можуть бути помилки в веб–серверах, модулях аутентифікації, поштових службах, або скриптах, які запускають ресурсомісткі операції. Для того, щоб уникнути загроз потрібно регулярно оновлювати операційні системи та використовувані програми. Також варто впровадити централізовану систему управління оновленнями (WSUS або Ansible) та застосовувати засоби контролю вразливостей (Nessus, OpenVAS), які автоматично сканують мережу на наявність відомих експлойтів.

Неправильні налаштування мережевих пристроїв і систем доступу, такі як фаєрволи, відкриті порти, зайві служби, а також некоректні дозволи доступу до файлів, можуть створювати потенційні можливості для зловмисників. Часто це стається через поспішні зміни в налаштуваннях без належного контролю безпеки. Для зменшення ризиків необхідно застосовувати стандартизовані підходи до налаштування, централізоване управління доступом, а також забезпечити регулярний моніторинг і перевірку відповідності конфігурацій політикам безпеки.

Дії співробітників, навіть ненавмисні, можуть призводити до порушення роботи мережі. Наприклад, передача облікових даних, встановлення несанкціонованого програмного забезпечення чи використання особистих пристроїв у корпоративній мережі підвищують ймовірність загроз. Щоб мінімізувати ці ризики, важливо впровадити ефективні політики управління доступом, обмеження прав користувачів, моніторинг дій співробітників і регулярні навчання з питань інформаційної безпеки.

Відсутність систем моніторингу та аналізу подій може призвести до того, що зловмисна активність залишатиметься непоміченою тривалий час. Впровадження систем моніторингу та аналізу логів, а також централізованих рішень для збору та кореляції подій, дозволяє оперативно виявляти аномалії. Важливо також мати чіткі регламенти реагування на інциденти, щоб забезпечити швидке та ефективне реагування на загрози. [12]

Наявність лише технологічних засобів безпеки не гарантує повного захисту, якщо компанія не має чітко визначених процедур для реагування на кіберінциденти, управління доступом до критичних систем і резервного копіювання. Тому важливо розробити політики безпеки, плани відновлення після інцидентів та процедури, що регулюють дії у разі виникнення загроз. Регулярне проведення аудитів та навчань з тестування на проникнення дозволить виявити слабкі місця і підвищити рівень захисту організації.

Загалом, недосконаліть архітектури створює численні вектори атак, ускладнює реагування на інциденти та знижує стійкість до збоїв. Для мінімізації цих ризиків необхідно проєктувати інфраструктуру відповідно до принципів надійності, резервування, відмовостійкості та масштабованості, враховуючи поточні та майбутні потреби підприємства.

Методи захисту від DoS–атак можна розділити на дві групи: це методи, що передують початку атаки та спрямовані на запобігання самій атаці, та методи, які застосовуються вже після початку атаки – активна протидія та пом’якшення наслідків атаки.

До методів запобігання атаці можна віднести організаційно–правові заходи. Наприклад, уникнення конфліктних ситуацій або заходи, спрямовані на ліквідацію результатів, яких прагне досягти зловмисник, наприклад, розмежування та маскування критично важливих ресурсів.

На цьому етапі також здіснюється усунення вразливостей та підтримка апаратно–програмного комплексу в актуальному стані. Деякі види мережевих атак спрямовані саме на використання різних вразливостей. Це можуть бути вразливості в програмному забезпеченні сервера слабкі місця у використанні неоптимізованих програмних скриптів, які можуть надмірно витрачати ресурси сервера. У цьому випадку для досягнення бажаного ефекту зловмиснику знадобиться організувати менш потужну атаку.

Після початку атаки використовуються активні заходи протидії. Основними з цих заходів є нарощування ресурсів та фільтрація трафіку.

Перед нарощуванням ресурсів проводиться детальний аналіз завантаженості сервера та мережевого сегмента, щоб визначити вузькі місця. Наприклад, якщо сервер у нормальному робочому режимі використовує значну частину каналу зв’язку, можна припустити, що у разі атаки зловмисник може повністю заповнити канал шкідливими запитами. У такому випадку доцільно заздалегідь збільшити пропускну здатність каналу зв’язку.

Виділені в результаті аналізу «вузькі місця» забезпечуються додатковими ресурсами. Якщо основним споживачем ресурсів на фізичному сервері є сервер баз даних, можливо, доцільно розмістити його на окремому виділеному сервері або навіть створити розподілений кластер серверів баз даних. Аналогічно можна вчинити і з іншими сервісами.

Якщо розглядати web–сервер як об’єкт атаки, то, окрім баз даних, підвищене навантаження може генерувати сам web–сервер або розміщені на ньому скрипти. У цьому випадку необхідно збільшити ресурси самого сервера: додаткова пам’ять, потужніший процесор, тощо. Або ж за допомогою спеціальних

інструментів виділити веб–сервери в окремий кластер. Наприклад, це можна зробити через використання зв'язки web–серверів Apache і Nginx.

Такий підхід до збільшення ресурсів не є захистом від усіх мережевих атак і має ряд недоліків:

– нарощування ресурсів пов'язане зі зміною апаратного комплексу і не може бути оперативно проведене в момент початку атаки;

– підтримка надмірних ресурсів економічно недоцільна у період очікування атаки.

Для подолання цих недоліків оптимальним є використання хмарних технологій, які дозволяють нарощувати ресурси за потребою. Наприклад, на сьогоднішній день на ринку представлені пропозиції від хостинг–провайдерів щодо надання послуг хмарного хостингу. Внаслідок такої послуги клієнтам надається необхідна кількість ресурсів у конкретний момент. У разі збільшення навантаження, яке може бути викликане як зростанням кількості легітимних користувачів, так і збільшенням шкідливих запитів, відбувається надання додаткових потужностей, що дозволяють обробити кожен запит.

У результаті сервер не виходить з ладу. Єдиним мінусом цього підходу є його економічний аспект, оскільки клієнту хмарного хостингу доведеться оплачувати додаткові потужності, тобто фактично платити за обробку шкідливих запитів.

Інший підхід до збільшення ресурсів дозволяє нарощувати їх у межах мережі доставки контенту (Content Delivery Network). У результаті реалізації цього підходу відбувається кешування вмісту web–сервера та його доставка через розподілену мережу вузлів.

При виборі оптимального маршруту зазвичай враховується географічне розташування клієнта мережі щодо найближчого вузла. У результаті мережевих атак шкідливий трафік розподіляється між різними вузлами мережі та втрачає свою потужність. Також можливий варіант, коли шкідливий трафік просто не потрапить на вузол, який здебільшого використовується легітимними

користувачами. Наприклад, у разі ботнет–атаки, з розташованої за кордоном мережі, шкідливі запити будуть концентруватися на найближчому до них вузлі CDN–мережі.

У будь–якому випадку використання цих підходів напряму не є доцільним, оскільки передбачає обробку всіх запитів без винятку, включно зі зловмисними.

Тому наступною групою методів, спрямованих на запобігання атаці, є методи, пов’язані з фільтрацією трафіку. Блокування завідомо шкідливих запитів та обробка надійних і підозрілих дозволяють суттєво заощадити кошти, які виділяються на збільшення ресурсів.

Для фільтрації шкідливого трафіку застосовуються різні програмні та апаратні засоби, що базуються на кількісному і якісному аналізі трафіку. В основі методів аналізу лежать методи кластерного аналізу, математичної статистики, теорії ймовірності, поведінкові методи, тощо.

Для ефективних заходів протидії та фільтрації трафіку необхідно вирішити дві тісно пов’язані задачі. Перша – виявлення факту початку атаки, друга – визначення джерела атаки, тобто джерела шкідливого трафіку. Чим точніше будуть вирішені ці питання, тим ефективнішими будуть заходи протидії.

На сьогоднішній день існує два підходи до визначення початку атаки. Перший ґрунтується на аналізі зловживань, другий – на аналізі аномалій. У першому підході виявлення атаки здійснюється шляхом порівняння даних, що характеризують поточний стан системи, з даними, характерними для типових атак. Другий підхід оцінює поточний стан системи щодо її нормального стану.

Обидва підходи мають свої недоліки. Наприклад, перший може бути неефективним для виявлення принципово нових типів атак, що особливо актуально у контексті DoS–атак, оскільки зловмисники прагнуть імітувати дії реальних користувачів. Для успішного застосування другого підходу необхідно накопичувати статистичні дані про нормальне функціонування системи.

Таким чином, для побудови ефективної системи виявлення доцільно використовувати обидва підходи. У результаті роботи такої системи відбувається

постійний збір даних про стан системи, їх обробка та аналіз на предмет відмінностей від нормальних даних. У разі початку атаки активуються механізми виявлення джерела трафіку. [13]

Отже, для ефективного захисту від DoS–атак необхідно використовувати комплексний підхід. Це включає превентивні заходи, такі як усунення вразливостей, маскування критично важливих ресурсів та підтримку актуального стану системи.

Після початку атаки критично важливо оперативно застосувати механізми нарощування ресурсів – хмарні технології, чи розподілені серверні кластери, щоб зменшити вплив атаки. Використання CDN також може сприяти розподілу навантаження, проте не виключає обробку шкідливого трафіку.

Найефективнішою стратегією залишається фільтрація трафіку, яка базується на аналізі даних та виявленні аномальної активності. Поєднання методів аналізу зловживань та аномалій дозволяє своєчасно виявляти загрози та їх джерела, що підвищує ефективність заходів протидії.

Комбінація всіх цих методів дозволяє значно зменшити ризик успішної DoS–атаки та забезпечити стабільну роботу системи.

1.4 Постановка задачі

Метою даної дипломної роботи є розробка системи захисту корпоративної мережі від DoS–атак та оцінка її ефективності.

Для досягнення цієї мети необхідно провести аналіз загроз та ризиків, дослідити характер DoS–атак, їх механізмів, поширених методів реалізації та впливу на доступність корпоративних сервісів.

Розробка моделі захисту, створення ефективної архітектури безпеки, що враховує особливості корпоративної інфраструктури, типові загрози та обмеження організаційного середовища. Провести експериментальне тестування

моделі, тобто перевірку працездатності запропонованої моделі у симульованому середовищі, аналіз її ефективності та виявлення потенційних вразливостей для подальшої оптимізації.

Результатом роботи має стати система, здатна ефективно протидіяти DoS–атакам, забезпечувати стабільність корпоративної мережі та мінімізувати ризики порушення роботи критичних сервісів.

2 АНАЛІЗ ЗАГРОЗ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Об'єкт захисту

Корпоративна мережа – це мережа, головним призначенням якої є підтримка роботи якогось підприємства, що володіє даною мережею. Тільки співробітники підприємства можуть бути користувачами мережі.

Сучасна корпоративна мережа є багаторівневою інформаційною системою, що забезпечує функціонування бізнес–процесів, збереження, обробку та передавання даних. Структура об’єкта захисту охоплює кілька логічних і фізичних рівнів, кожен з яких може бути вразливим до DoS–атак.

Корпоративна мережа складається з кількох взаємопов’язаних рівнів. На фізичному рівні інфраструктура включає серверне обладнання, маршрутизатори, комутатори, точки доступу, пристрої зберігання даних, а також системи електроживлення та резервного копіювання. Всі ці елементи забезпечують базову комунікацію між пристроями, а також доступ до мережевих сервісів. Вони об’єднані через внутрішню локальну мережу, що може бути структурованою у вигляді ієрархічної або сегментованої топології.

На рівні програмного забезпечення функціонують операційні системи серверів та користувацьких пристроїв, прикладні служби, віртуалізаційні середовища, системи резервного копіювання та моніторингу. Серверна частина забезпечує роботу внутрішніх сервісів, таких як файловий доступ, електронна пошта, веб–додатки, бази даних, а також системи управління обліковими записами та політиками безпеки. У хмарних або гібридних архітектурах часто використовується віддалена інфраструктура, що додає новий рівень складності та потенційної вразливості.

Клієнтський рівень інфраструктури включає робочі станції співробітників, мобільні пристрої з корпоративним доступом, а також периферійне обладнання та пристрої Інтернету речей (IoT). Ці елементи взаємодіють із внутрішніми та зовнішніми сервісами, отримуючи та передаючи дані, що робить їх потенційними точками проникнення для атак, зокрема і у формі DoS.

На рівні мережевих сервісів функціонують веб–сервери, проксі–сервери, VPN–шлюзи, засоби контролю трафіку, системи автентифікації, інструменти логування та аналітики. Вони забезпечують як базову функціональність, так і засоби для виявлення вторгнень, обмеження доступу та підтримку політик безпеки. Особливу увагу слід приділяти зовнішнім каналам зв'язку, які забезпечують взаємодію з Інтернетом, хмарними сервісами, а також віддаленим доступом співробітників. Відкритість таких каналів зумовлює їхню вразливість до зовнішніх атак, включно з масованими DoS–атаками, які можуть спричинити повне перевантаження каналів зв'язку, виведення з ладу веб–ресурсів або внутрішніх серверів.

Усі перелічені рівні взаємодіють між собою за допомогою інформаційних потоків, серед яких внутрішній міжсервісний обмін, обробка запитів клієнтів, віддалене адміністрування, обмін файлами, та інші механізми. Порушення будь–якого з цих процесів може призвести до зупинки бізнес–функцій.

Вразливості в корпоративній мережі можуть бути як технічними наприклад, відсутність обмежень на кількість одночасних з'єднань, відкрите програмне забезпечення без належного контролю, так і організаційними – відсутність політик реагування на атаки, неналаштовані механізми моніторингу. Уразливі також користувацькі пристрої, що під'єднуються до корпоративної мережі через VPN або бездротові канали. Наявність цих вразливостей робить інфраструктуру потенційно відкритою для реалізації DoS–атак ззовні або зсередини. [14]

2.2 Класифікація DoS–атак

У першому розділі було розглянуто безліч видів загроз, які можуть виникнути в корпоративній мережі. Так як завданням дипломної роботи є створення системи захисту від DoS–атак, далі буде розглядатись лише цей тип атак. [15]

DoS–атаки класифікуюсь за:

1. За рівнем OSI–моделі

OSI представляють собою «забивання» каналу. Прикладом може бути CMP–флуд–атака, яка використовує ICMP–повідомлення, що знижують пропускну здатність атакованої мережі та перевантажують фаєрвол. Хост постійно «пінгується» зловмисниками, змушуючи його відповідати на ping–запити. Коли їх надходить значна кількість, мережа не здатна обробити весь трафік, і відповіді на запити надходять із суттєвими затримками. [16]

Атаки за рівнем OSI–моделі також поділяються на:

– атаки на транспортному рівні;

– на сеансовому рівні;

– високорівневі атаки на прикладному рівні.

Атаки на транспортному рівні виглядають як порушення функціонування та перехоплення трафіку. Наприклад, SYN–флуд або атака ICMP–запитами зі зміненими адресами. Наслідками такої DoS–атаки є перевищення кількості доступних з'єднань та перебої в роботі мережевого обладнання.

Атакам на сеансовому рівні піддається мережеве обладнання. Використовуючи вразливості програмного забезпечення Telnet–сервера на комутаторі, зловмисники можуть заблокувати можливість управління комутатором для адміністратора. [17]

Атаки на прикладному рівні спрямовані на знищення пам’яті або даних з диска, крадіжку ресурсів сервера, вилучення та використання інформації з баз даних. Це може призвести до критичної нестачі ресурсів для виконання найпростіших операцій на пристроях.

2. DoS–атаки а способом виконання

Об’ємні атаки спрямовані на перевантаження пропускної здатності мережі. Найпоширенішим прикладом є UDP flood, коли зловмисники масово надсилають UDP–пакети на випадкові порти цільового сервера. Це змушує сервер обробляти кожен запит та надсилати відповідь про недоступність, що поступово виснажує

ресурси та забиває канал зв’язку. Такі атаки складні для виявлення, оскільки можуть виглядати як легітимний трафік.

Атаки на ресурси спрямовані на виснаження обчислювальних потужностей цільової системи. Наприклад, SYN flood експлуатує механізм встановлення TCP–з’єднання, надсилаючи велику кількість запитів без завершення тристороннього рукостискання. Як наслідок, сервер резервує пам’ять для кожного запиту, поки не досягне ліміту, що призводить до неможливості обробки нових підключень. Вразливість таких атак особливо критична для веб–серверів з обмеженими ресурсами.

Атаки на рівні використовують логіку роботи веб–серверів та інших онлайн–сервісів. Одним із прикладів є атака Slow HTTP Post, коли зловмисник надсилає HTTP–запити з дуже малими обсягами даних, але з повільною передачею. Це змушує сервер підтримувати відкриті з’єднання, витрачаючи ресурси без реальної користі. Іншим подібним методом є атака Slowloris, що утримує велику кількість неповних HTTP–запитів, не дозволяючи серверу обслуговувати нових клієнтів.

3. За джерелом атаки (одноточкові та розподілені).

Одноточкові – походять з одного джерела, тобто зловмисник використовує одну IP–адресу для ініціації великої кількості шкідливих запитів. Це робить атаку більш передбачуваною, а отже легше виявляється та блокується через налаштування фаєрволу або обмеження швидкості запитів.

Розподілені значно складніші для протидії, оскільки вони здійснюються з множинних джерел, які можуть бути об’єднані у ботнети мережі заражених пристроїв, керованих зловмисниками. Ці пристрої можуть знаходитися в різних географічних регіонах, що ускладнює їхнє блокування. Одним із варіантів подібних атак є використання серверів–підсилювачів, таких як DNS або NTP, коли атакуючі надсилають невеликі запити, що генерують масивні відповіді, перенаправлені на цільову систему. Це створює значне навантаження, яке швидко перевантажує сервер або канал зв’язку. [18]

У таблиці 2.1 відображено класифікацію DoS–атак за рівнем OSI–моделі, способом виконання та джерелом атаки. Для кожного типу вказано складність виявлення та протидії.

Таблиця 2.1 – порівняння DoS–атак за складністю виявлення та усунення

Класифікація	Тип атаки	Складність виявлення та протидії
1	2	3
За рівнем OSI–моделі	На транспортному рівні	Можна виявити через аналіз трафіку, протидія вимагає налаштування фаєрволу та фільтрів
	На сеансовому рівні	Потребує моніторингу активності обладнання, можливе блокування через обмеження доступу
	На прикладному рівні	Важко відрізнити від легітимної активності, потребує аналізу поведінки
За способом виконання	Атаки на ресурси	Атаки складно ідентифікувати без глибокого аналізу, можна протидіяти через обмеження з’єднань
	Атаки на рівні додатків	Атаки складно ідентифікувати без глибокого аналізу, протидія через обмеження з’єднань
	Об’ємні атаки	Легко виявляються за обсягом трафіку, усунення блокуванням джерел та фільтрація трафіку
За джерелом атаки	Одноточкові	Легко відслідковуються за IP–адресою, ефективна протидія через фаєрволи

Кінець таблиці 2.1

1	2	3
	Розподілені	Атаки з різних джерел, потребують складної фільтрації

Найбільш простими виявились об’ємні та одноточкові атаки, які можна блокувати базовими мережевими засобами. Водночас, атаки на прикладному рівні, на рівні додатків і розподілені атаки вважаються найскладнішими для виявлення та нейтралізації, оскільки маскуються під звичайний трафік і потребують спеціалізованих засобів захисту.

Особливістю DoS–атак є те, що вони не обов’язково спрямовані на проникнення в систему, як це буває при крадіжці даних або викраденні облікових записів. Їх основна мета порушити стабільну роботу цільової системи, вивести її з ладу, призупинити обслуговування клієнтів, спричинити фінансові та репутаційні втрати.

При цьому DoS–атаки є дешевими у реалізації для зловмисника, але потенційно дуже дорогими для жертви. За даними галузевих звітів, навіть короткочасне припинення обслуговування клієнтів може обійтися підприємству в тисячі або мільйони гривень через втрату прибутку, клієнтів, штрафи за невиконання контрактів.

2.3 Модель загроз та порушників

Загрози можуть бути зовнішніми та внутрішніми, а також походити від людей або інших факторів наприклад, природні явища, чи фізичні або технічні інциденти.

Для побудови моделей загроз використовувалась програма CORAS. Метод CORAS був розроблений для задоволення потреби в системному підході до

аналізу ризиків у сфері інформаційної безпеки, що поєднує точні кількісні оцінки з наочною та доступною візуалізацією, зрозумілою як для технічних фахівців, так і для керівників. Основу CORAS становить побудова сценаріїв загроз, які описують послідовність подій і причинно–наслідкові зв'язки між компонентами системи. Цей підхід дозволяє формалізувати ключові поняття, зокрема «актив», «загроза», «вразливість», «наслідки» та «контрзаходи», та подати їх у вигляді діаграм, що забезпечують чітке трактування кожного елемента та його взаємозв'язків.

Початковий етап аналізу ризиків CORAS передбачає чітке визначення активів, що підлягають захисту. Методологія CORAS була розроблена для забезпечення системного та структурованого підходу до аналізу ризиків інформаційної безпеки, що особливо актуально в умовах зростаючої загрози DoS–атак у корпоративних мережах. Вона поєднує формальні кількісні оцінки ризиків із зручним візуальним представленням, яке дозволяє ефективно аналізувати результати як технічним фахівцям, так і менеджменту. Основна ідея CORAS полягає у створенні сценаріїв атак, що відображають не лише послідовність дій, але й причинно–наслідкові зв'язки між різними компонентами мережевої інфраструктури.

Застосування CORAS у контексті DoS–атак починається з чіткого визначення активів, які потребують захисту. У корпоративному середовищі такими активами можуть бути сервери додатків, канали зв'язку, інфраструктура обробки запитів клієнтів або інші критичні компоненти мережі. Наступним кроком є ідентифікація загроз, зокрема сценаріїв DoS–атак, які можуть включати спроби перевантаження серверів, зловживання протоколами або експлуатацію вразливих точок доступу. CORAS дозволяє змоделювати ці сценарії у вигляді діаграм, де кожна загроза представлена як послідовність умов і дій, що призводять до відмови в обслуговуванні. При цьому враховуються як технічні аспекти наприклад, наявність вразливих портів або слабкість в алгоритмах обробки запитів, так і організаційні чи людські фактори – недостатній контроль

доступу до мережевого обладнання. Модель також включає вразливості, які дозволяють зловмиснику реалізувати атаку наприклад, недостатня пропускна здатність, неправильно налаштовані брандмауери або відсутність системи виявлення аномалій.

Також важливою частиною в моделюванні задопомогою CORAS є оцінювання ймовірності реалізації кожного сценарію та потенційних наслідків. У випадку DoS–атак наслідки можуть включати простої критичних сервісів, втрату доходів, зниження продуктивності або репутаційні збитки. Ймовірність реалізації таких загроз може визначатися на основі статистики подібних інцидентів у галузі або внутрішніх журналів подій компанії.

CORAS забезпечує представлення всієї цієї інформації у візуальній формі: активи, загрози, вразливості та контрзаходи позначаються стандартними символами, а типи зв'язків – стрілками, що відображають логіку атак. Така структура дозволяє не лише наочно ідентифікувати найбільш критичні точки ризику, але й швидко вносити зміни у модель відповідно до розвитку інфраструктури або появи нових типів DoS–атак.

Завершальним етапом застосування CORAS є валідація моделі за участю всіх зацікавлених сторін: системних адміністраторів, спеціалістів з кібербезпеки, керівників IT–підрозділів. Після узгодження проводиться коригування оцінок і, за необхідності, впровадження додаткових контрзаходів. У контексті DoS–захисту до таких заходів можуть належати впровадження механізмів фільтрації трафіку, балансування навантаження, обмеження швидкості запитів, використання хмарних сервісів із захистом від DDoS, а також розробка політик реагування на інциденти.

Метод CORAS демонструє високу ефективність на різних етапах функціонування інформаційної системи, зокрема корпоративної мережі. На стадії проектування вона дає змогу врахувати потенційні ризики DoS–атак уже на рівні архітектури, закладаючи відповідні механізми захисту. Під час впровадження CORAS допомагає виявити уразливості в налаштуваннях, конфігураціях або

організаційних процесах, які можуть бути використані зловмисниками. У процесі подальшої експлуатації методологія забезпечує супровід та актуалізацію моделі ризиків, що дозволяє враховувати нові загрози та зміни в інфраструктурі. [19]

Завдяки гнучкому підходу та стандартизованій візуальній нотації CORAS легко поєднується з іншими методами управління ризиками та інтегрується з відповідним програмним забезпеченням. Це сприяє формуванню єдиного джерела знань про загрози, вразливості та контрзаходи, що підвищує ефективність прийняття рішень у сфері кіберзахисту. Загалом CORAS є потужним інструментом для комплексного аналізу ризиків, який допомагає розробляти й реалізовувати стратегії захисту корпоративних мереж від DoS–атак та забезпечувати їхню надійність в умовах зростаючої кібернебезпеки.

З огляду на зростаючу кількість кібератак, особливо розподілених атак типу відмови в обслуговуванні, захист корпоративних мереж є дуже важливим. Ці мережі оперують значними обсягами цінних даних, що робить їх привабливою мішенню для зловмисників, які прагнуть порушити роботу важливих сервісів і заблокувати доступ до інформації. Для ефективної протидії таким загрозам необхідно використовувати системний підхід, який охоплює виявлення слабких місць, аналіз потенційних небезпек та розробку дієвих заходів захисту. Методологія CORAS є цінним інструментом у цьому контексті. Вона допомагає чітко визначити всі ключові елементи моделі ризиків, такі як цінне майно компанії, джерела загроз, існуючі вразливості та можливі наслідки атак, і наочно представити їх у вигляді графічних схем. Такий підхід дає змогу моделювати типові сценарії DDoS–атак, враховуючи всі взаємозв'язки між причинами та наслідками, що значно покращує планування та впровадження ефективних заходів безпеки в корпоративному середовищі.

Модель на рисунку 2.1 ілюструє загрози, пов’язані з несанкціонованим доступом до даних у корпоративній мережі, що можуть бути як результатом зовнішніх атак, так і внутрішніх порушень безпеки з боку працівників.

Найголовнішою загрозою є зловмисники, які проводять атаки, метою яких є вивід з ладу всієї мережі та викрадення даних.

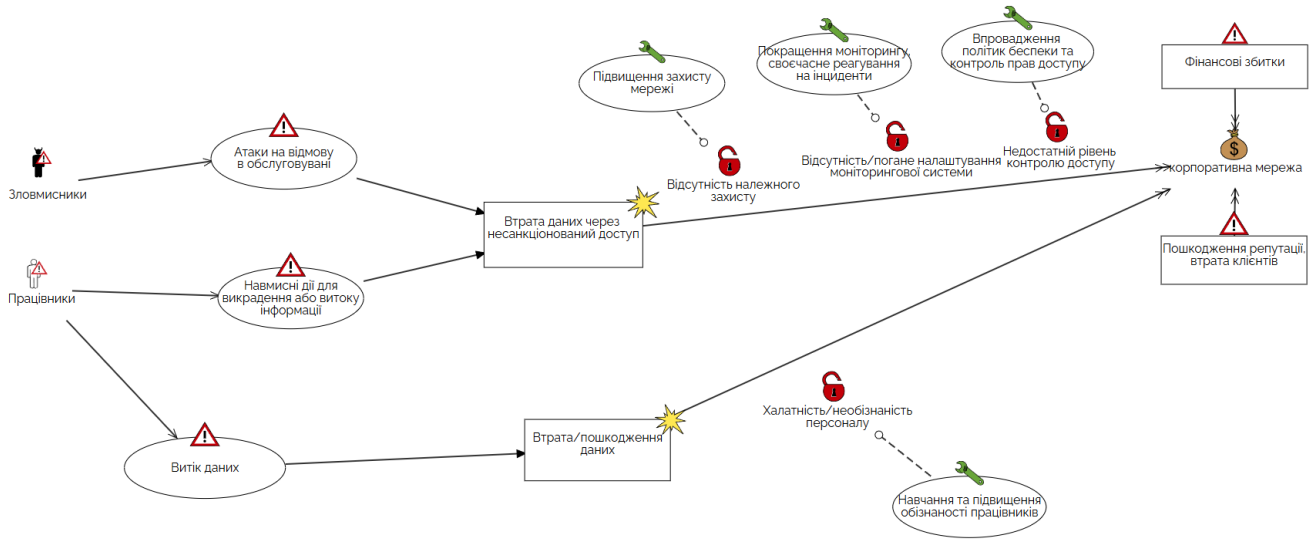


Рисунок 2.1 – Модель порушників

Дії працівників також можуть загрожувати безпеці мережі. Хтось є необізнаним або не приділяє значної уваги тому, що робить, через що трапляється витік даних, а хтось може мати погані наміри. Такі дії приводять до втрати конфіденційної інформації, що у подальшому може бути використана для компрометації компанії чи її клієнтів. Недостатня обізнаність працівників підвищує ймовірність того, що вони випадково або навмисно порушать політику безпеки підприємства. Саме тому навчання персоналу і підвищення рівня їхньої обізнаності є критично важливим елементом захисту даних.

Крім того, одною з причин подібних інцидентів є відсутність або недостатній рівень захисту мережі через відсутність належного контролю доступу, неефективне налаштування моніторингових систем, розповсюджені паролі або загальні облікові записи, які легко зламати. У деяких випадках це може негативно вплинути на стабільність функціонування корпоративної мережі та всієї організації в цілому.

На рисунку 2.2 зображена модель внутрішніх загроз. Основними причинами збою в корпоративній мережі зазвичай виступають технічні збої, помилки в конфігурації або неправильні налаштування мережі чи обладнання.

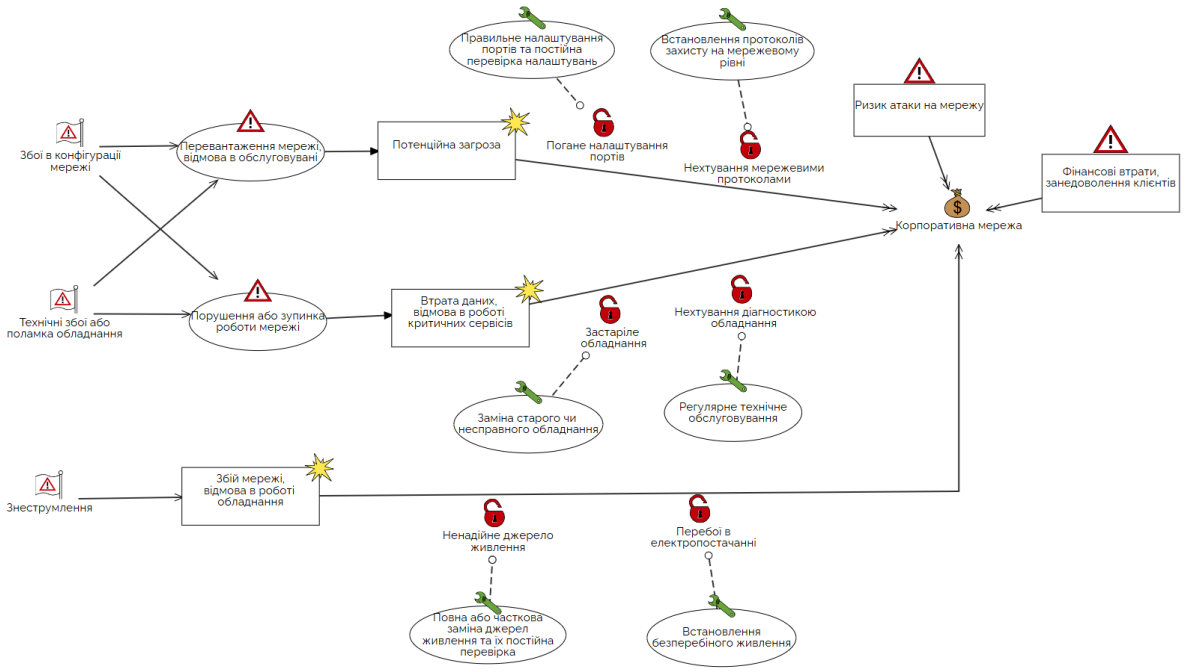


Рисунок 2.2 – Модель внутрішніх загроз

Усі зображенні вразливості можуть викликати перевантаження та зупинку роботи мережі, а також несправність або поламку технічного обладнання, що приводить до пошкодження або втрати даних, відмову в обслуговувані веб–сервісів та, найголовніше, до потенційного ризику виникнення атаки на мережу. Злочинці можуть скористатись тим, що мережа ослаблена та провести DoS–атаку, яка ще більше доб'є її. Наслідку компанія, в якій знаходиться мережа, може потерпіти фінансові збитки – клієнти будуть відмовлятись від послуг, а репутація погіршуватись. Щоб запобігти цим загрозам, необхідно впроваджувати профілактичні заходи: своєчасну заміну обладнання, налаштування захисту на мережевому рівні, забезпечення безперебійного живлення та безпосередньо регулярну перевірку та тестування роботи.

Порушники поділяються на внутрішніх та зовнішніх, на рисунку 2.3 зображено модель внутрішніх порушників.

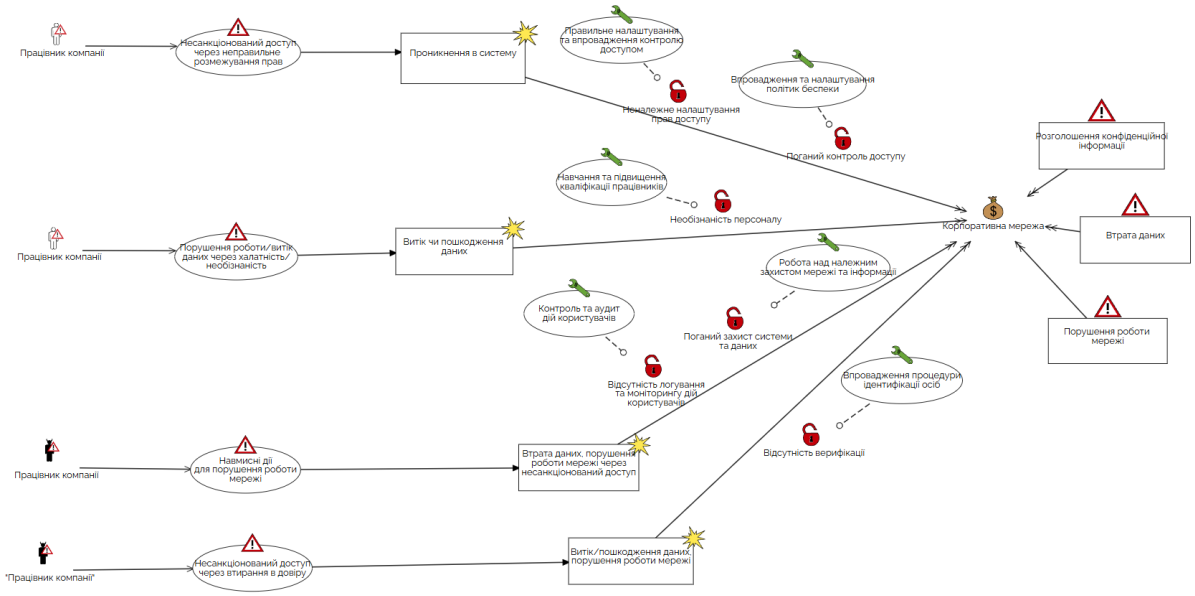


Рисунок 2.3 – Модель внутрішніх порушників

Схема, що наведена вище, ілюструє структуру внутрішніх загроз в інформаційній системі, зосереджуючи увагу на діях співробітників організації, які можуть нести загрозу інформаційним ресурсам. Сюди входять як ненавмисні, так і свідомі дії, які порушують принципи конфіденційності, цілісності та доступності інформації.

На схемі виділено кілька шляхів порушення безпеки. Перший із них стосується несанкціонованого доступу, пов’язаного з неконтрольованим делегуванням повноважень через неналежну конфігурацію прав доступу і політик безпеки. Це може дозволити зловмиснику отримати доступ до конфіденційної інформації, змінити або знищити критичні дані, а також вивести з ладу мережеву інфраструктуру. Для того щоб уникнути подібних інцидентів, слід формувати і контролювати політики безпеки всіх ступенів, уживати заходів контролю користувача до всіх дій на системі.

Інший ризик виникає через недбалість або недостатню обізнаність персоналу, що може призвести до втрати або пошкодження інформації.

Неналежне поводження з даними в офісному середовищі також здатне спричинити перебої в роботі системи або навіть відмову в обслуговуванні. Ефективним засобом зниження цього ризику є регулярне навчання співробітників, яке дозволяє підвищити рівень їхньої обізнаності щодо захисту інформації та контролю дій у системі.

У моделі також розглядаються навмисні дії співробітників, які мають на меті порушення функціонування мережі. Зокрема, загроза полягає у свідомому нанесенні шкоди інфраструктурі компанії. Додаткову небезпеку становлять зловмисники, які втерлися в довіру до компанії, скористалися відсутністю верифікації або належної ідентифікації осіб і отримали несанкціонований доступ до критичних систем. Такі дії можуть спричинити масштабні наслідки – втрату даних, витік інформації або зупинку роботи мережі.

Загалом, модель демонструє, що внутрішні загрози можуть мати різну природу – як технічну, так і соціальну. Їх ефективне виявлення та запобігання вимагає комплексного підходу, що включає технічні заходи, політики безпеки, контроль дій користувачів і розвиток культури інформаційної безпеки в організації.

До зовнішніх загроз відносяться усі загрози, що виникають за межами корпоративної мережі. До них відносяться дії сторонніх осіб та зовнішні фактори. Зображена на рисунку 2.4 модель, детально ілюструє ризики для інформаційної безпеки корпоративної мережі, що виникають внаслідок несанкціонованого доступу. Зловмисники часто намагаються отримати несанкціонований доступ до мережі через людський фактор. Є багато випадків, коли люди переходили по небезпечним фішинговим посиланням, чи навіть добровільно давали конфіденційну інформацію шахраям, які психологічно впливали на них через переписку, компроментуючи свою безпеку чи безпеку мережі. В результаті люди ставали жертвами так званої соціальної інженерії або фішингу й мали серйозні проблеми. Тому, проблема несанкціонованого доступу до корпоративної мрежі, є одною з ключових вразливостей в організаціях.

На діаграмі чітко простежуються джерела, що можуть призвести до цього несанкціонованого проникнення в мережу. Серед них також виділяються спроби зловмисників шляхом сканування мережі виявити наявні вразливості, що можуть стати точкою входу для подальших атак. Сканування мережі – це процес активного дослідження мережевої інфраструктури організації з метою виявлення відкритих портів, запущених сервісів, версій програмного забезпечення та інших потенційних вразливостей. Зловмисники використовують спеціалізовані інструменти та техніки для надсилання запитів до різних мережевих адрес та портів, аналізуючи отримані відповіді для складання "карти" мережі та ідентифікації слабких місць, які можна використати для подальших атак.

Наслідки несанкціонованого доступу можуть бути різноманітними та мати серйозний вплив на функціонування корпоративної мережі. Одним з таких наслідків як раз є реалізація DoS–атак, спрямованих на перевантаження мережевих ресурсів і виведення їх з ладу. Недостатня обізнаність працівників, неналежне налаштування мережевих портів або відкриті невикористані порти можуть сприяти успішному проведенню таких атак. Також результатом є витік даних, який може статися через слабкий контроль доступу або неправильне розмежування прав доступу між різними категоріями користувачів. Крім того, люба спроба отримати незаконний доступ до мережі може призвести до безпосереднього порушення її роботи, викликаючи нестабільність або повну зупинку в роботі.

У нижній частині діаграми розглядається ще одне джерело загроз – природні явища. Стихійні лиха можуть завдати фізичної шкоди обладнанню, що призведе до втрати його працездатності та, відповідно, до порушення роботи корпоративної мережі. Для мінімізації потенційних негативних наслідків, особливо у випадку пошкодження обладнання та втрати його функціональності, модель відображає ряд контрзаходів. Серед них – розміщення критично важливого обладнання в спеціальних зонах обслуговування та безпечних приміщеннях для забезпечення його фізичного захисту. Важливим аспектом є

наявність аварійного живлення, такого як генератори або безперебійні джерела живлення, для забезпечення безперервної роботи у випадку відключення основного електропостачання. Регулярне резервне копіювання даних дозволяє відновити важливу інформацію у разі її втрати. Наявність актуальних резервних копій даних дуже допомагає при відновленні після таких інцидентів.

Кінцевим об'єктом впливу всіх розглянутих загроз та наслідків є сама корпоративна мережа. Успішна реалізація загроз може призвести до значних фінансових втрат, завдати шкоди репутації компанії, порушити важливі бізнес–процеси та призвести до інших негативних наслідків.

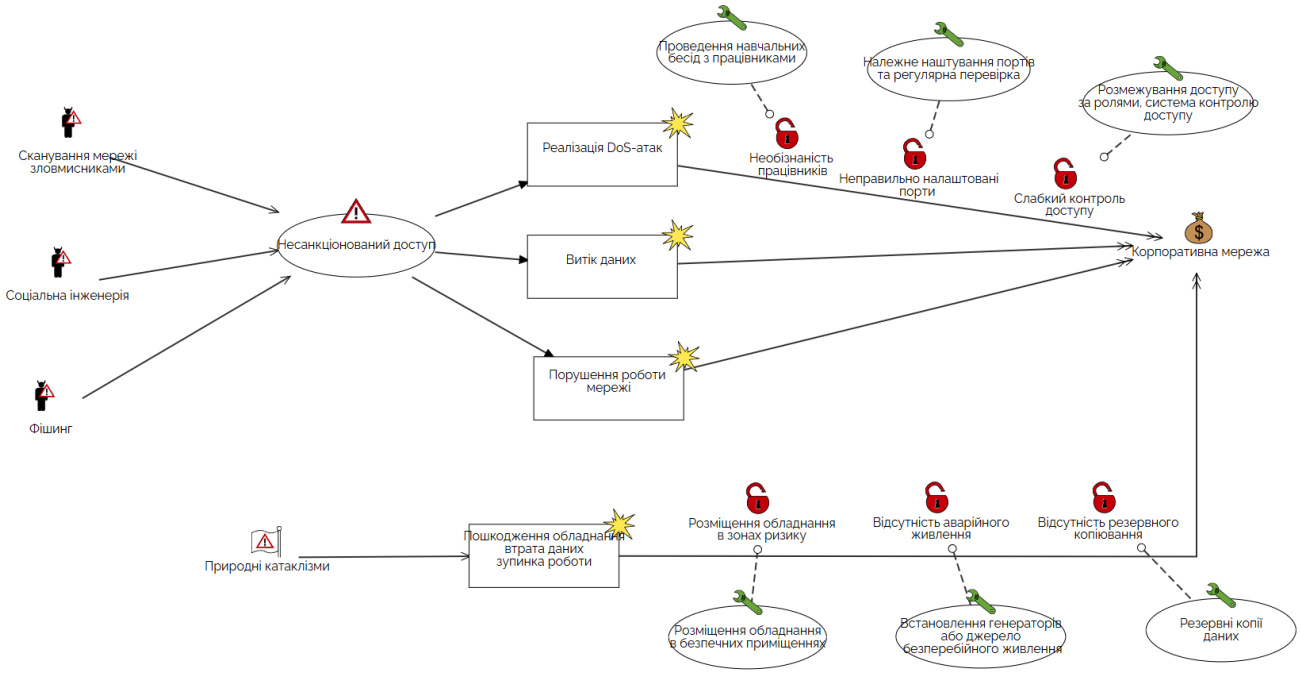


Рисунок 2.4 – Модель зовнішніх загроз

Зовнішніми порушниками можуть бути люди, які раніше працювали в компанії та мають намір за щость помститись, хакери та конкуренти з інших організацій. В усіх одна мета – отримати несанкціонований доступ до мережі. Навіть незначні вразливості в системі являються потенційними способами втручання в мережу.

Як вище вже згадувалось, найпоширенішими вразливостями є неправильно налаштовані політики безпеки та порти, погане розмежування прав доступу, відсутність моніторингу та логування дій користувачів. Модель зовнішніх порушників зображена на рисунку 2.5.

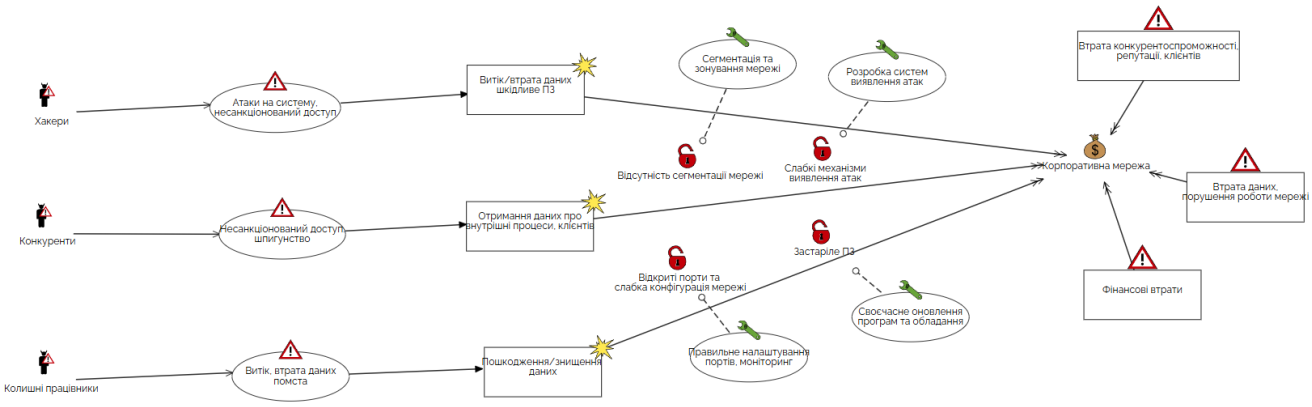


Рисунок 2.5 – Модель зовнішніх порушників

Конкуренти можуть отримати доступ до корпоративної мережі або через використання вразливостей, або шляхом залучення працівників до витоку інформації. Колишні працівники становлять ризик, якщо їхні облікові дані не були своєчасно деактивовані. У результаті можливий витік даних або навмисне пошкодження, фінансові втрати, витік важливих комерційних даних та порушення репутації компанії.

2.4 Способи захисту мережі

Першим важливим напрямом захисту є архітектурні рішення. Недосконала архітектура, зокрема централізована інфраструктура без механізмів кластеризації, географічного резервування та балансування навантаження, часто призводить до повної зупинки роботи сервісів або технічного збою у разі атаки. Щоб уникнути цього, необхідно будувати відмовостійку архітектуру.

Щоб зміцнити ресурси проти DDoS–атак, важливо зробити архітектуру максимально стійкою. Удосконалення мережевої архітектури є важливим кроком не лише для захисту мережі від DDoS, але й для забезпечення безперервності роботи та захисту від будь–яких збоїв або аварійних ситуацій. [20]

Наступні кроки допоможуть розпорошити активи організації, щоб уникнути представлення зловмиснику єдиної багатоцільової цілі:

– розташування серверів в різних центрах обробки даних;

– розташування центрів обробки даних в різних мережах;

– центри обробки даних повинні мати різні шляхи підключення до мережі;

– центри обробки даних або мережі, до яких вони підключені, не мають помітних вузьких місць або окремих точок відмови.

Для організації, яка залежить від серверів і присутності в Інтернеті, важливо переконатися, що ресурси географічно розподілені, а не розташовані в одному центрі обробки даних.

Якщо ресурси вже географічно розподілені, важливо розглядати кожен дата–центр як такий, що має більше одного каналу до Інтернету, і переконатися, що не всі дата–центри підключені до одного Інтернет–провайдера.

Існує також гібридна хмарно–локальна архітектура захисту. Така модель дає змогу гнучко реагувати на різні типи атак і адаптувати ресурси відповідно до навантаження. Об’ємні атаки, що спрямовані на перевантаження мережевих каналів наприклад, UDP flood або amplification–атаки, фільтруються на рівні хмарних центрів очищення трафіку. Хмарні платформи забезпечують велику пропускну здатність та можуть зупинити значний обсяг шкідливого трафіку ще до того, як він досягне внутрішньої інфраструктури організації. Їх використання зменшує ризик перенавантаження зовнішніх каналів зв’язку.

Більш складні атаки на рівні додатків, обробляються на локальному рівні всередені мережі. У цій частині архітектури використовуються засоби WAF та IDS, які аналізують поведінку запитів, ідентифікують підозрілу активність та блокують атаки, що маскуються під легітимний трафік.

Найбільшою перевагою гібридної архітектури є масштабованість. В моменти зростання навантаження, хмари можуть надавати додаткові ресурси, забезпечуючи обробку великої кількості трафіку, тоді як локальні системи виконують поглиблену перевірку запитів, орієнтуючись на встановлені політики безпеки, сигнатури загроз та поведінковий аналіз.

Хмарна частина системи, як правило, виконує роль фільтраційного центру, який приймає весь вхідний трафік, аналізує його, видаляє шкідливі дані та передає лише легітимні запити у внутрішню мережу.

Для ефективної взаємодії між хмарними й локальними компонентами використовуються захищені канали зв'язку або API, які дозволяють обмінюватися інформацією про загрози, фіксувати аномальну активність та ініціювати автоматизовану відповідь на інциденти.

Для підвищення стійкості до DoS–атак також рекомендується впровадження сегментації мережі та використання зон демілітаризованої зони (DMZ), [34, 35] що дозволяє ізолювати критичні ресурси та обмежити доступ до них, зменшуючи ризик поширення атак у мережі. Наприклад, використаня фаєрволу back to back забезпечує додатковий захист, розподіляючи внутрішню та зовнішню мережі.

Іншим способом захисту є використання програмно–апаратних комплексів. Використання фаєрволів також відноситься до цього методу захисту. Вони контролюють вхідний та вихідний трафік на основі встановлених правил безпеки. Однак їх ефективність обмежена в питанні розрізнення легітимного та шкідливого трафіку під час маштабних атак.

Системи виявлення та запобігання вторгненням моніторять мережевий трафік для виявлення підозрілої активності. Системи виявлення (IDS) виявляє потенційні загрози та повідомляє систему, але нічого не робить для того, щоб запобігти їм, в той час як система запобігання (IPS) блокує шкідливий трафік. Ці дві системи можна об'єднати в одну, яка має назву система виявлення та запобігання вторгнень (IDPS). [36]

Важливим методом захисту проти несанкціонованого доступу є використання VPN–шлюзів з багатофакторною автентифікацією. VPN–шлюзи забезпечують захищений доступ до внутрішніх ресурсів мережі, а впровадження багатофакторної автентифікації на цих шлюзах значно знижує ризик несанкціонованого доступу, навіть якщо облікові дані користувача були скомпрометовані.

Частіше всього для атак зловмисники використовують вразливості в операційних системах, веб–серверах, програмах та базах даних.

Використання застарілого програмного забезпечення значно підвищує ризик атаки. Тому потрібно регулярно його оновлювати. Але у великих системах, де використовується багато різних приладів, це буває дуже важко робити. Для таких випадків існують програми для системного адміністрування та керування великою кількістю машин. Наприклад Windows Server Update Services, який дозволяє централізовано керувати оновленнями операційної системи Windows у корпоративних мережах, або Ansible – інструмент, що надає засоби для управління конфігурацією, встановлення застосунків та оновлень, налаштувань великої кількості серверів. [37]

Крім того, важливо проводити сканування вразливостей для того, щоб виявити нові вразливості та запобігти їх використанню зловмисниками. Nessus та Nikto добре справляються з цією задачою, а також є безкоштовними в користуванні.

Дії компанії також дуже значні. Вони охоплюють створення правил захисту даних, стратегії обробки порушень безпеки, резервних планів та постійного спостереження за діяльністю користувачів. Найважливішою частиною є покращення обізнаності персоналу. Відсутність знань серед персоналу може призвести до порушення даних або випадкової активації згубних програм, що сприяє виконанню DOS–атак.

2.5 Висновок

У розділі було приділено увагу основним видам DoS–атак в корпоративних мережах – рівнями OSI–моделі, способом виконання та джерелом атаки. Проведено аналіз складності їх виявлення та усунення, що дозволило краще зрозуміти рівень ризику кожного типу загроз.

Опираючись на це, було побудовано моделі потенційних загроз та порушників інформаційної безпеки корпоративної мережі. Внутрішні загрози, що походять від працівників компанії, зокрема ненавмисні дії через халатність або необізнаність, а також цілеспрямовані порушення з боку зловмисників, які мають доступ до ресурсів компанії. Внутрішні загрози, які не походять від людей, зокрема знеструмлення чи вихід з ладу обладнання. Також проаналізовано зовнішні загрози, пов’язані з діями хакерів, конкурентів та колишніх працівників.

Побудовані схеми загроз та порушників демонструють, як саме ці суб’єкти можуть завдати шкоди корпоративній мережі через несанкціонований доступ, витік даних або порушення цілісності системи, шляхи виникнення інцидентів, ключові вразливості, способи їх вирішення та можливі наслідки для системи. Виявлені основні вразливості, такі як відсутність сегментації мережі, слабкий контроль доступу та недостатній моніторинг дій користувачів.

Також були розглянуті способи захисту мережі, такі як покращення архітектури мережі, сканування вразливостей, впровадження системи моніторингу та багаторівневої автентифікації. Жоден із компонентів не може забезпечити повноцінний захист окремо – лише їх поєднання та узгоджена взаємодія створюють умови для стійкої та адаптивної безпеки мережі.

Результати аналізу вказують на необхідність створення системи захисту від DoS–атак, з урахуванням як зовнішніх, так і внутрішніх факторів. Розуміння природи порушників і моделювання типових сценаріїв атак є ключем до побудови ефективної архітектури інформаційної безпеки.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ ВІД DOS–АТАК

3.1 Інструментарій системи виявлення та захисту від DoS–атак в корпоративній мережі

В рамках дипломної роботи необхідно було реалізувати систему виявлення та захисту від DoS–атак в корпоратвній мережі. Проаналізувавши види атак, їх складність та частоту, було обрано розробити програму для захисту від атак типу HTTP–flood.

HTTP–flood – атаки на прикладному рівні, при яких генерується велика кількість HTTP–запитів, які замасковані під легітимний трафік. Такі атаки не потребують передачі великого об’єму даних, але значно навантажує сервер за рахунок великої кількості запитів. [38–39]

Першочерговою задачою був вибір мови програмування. Для розробки поставленної задачі найкраще підходять мови C# та Python, але Python має низку суттєвих переваг, через що вибір пав саме на неї. Однією з головних переваг Python є наявність широкого спектру зручних бібліотек, в яких реалізується безліч алгоритмів, що значно спрощують розробку, бо не потрібно створювати їх з початку. Більше того, бібліотеки супроводжуються зрозумілою документацією, що дозволяє налаштовувати алгоритми відповідно до потреб розробника. Саме тому систему було розроблено на мові Python з мінімальною кількістю сторонніх залежностей, виключаючи необхідність використання зовнішніх сервісів та баз даних.

Середовищем розробки було обрано Visual Studio Code. VS Code – зручне сучасне середовище розробки, яке активно використовується розробниками для програмування різними мовами, зокрема Python. Перевагою є швидкодія, гнучкість, функціональність та можливість комфортно працювати на слабких комп’ютерах. Має інтуїтивно зрозумілий інтерфейс, який можна налаштовувати під індивідуальні потреби. Також Vs Code підтримує велику кількість розширень, серед яких є інструменти для роботи з мовою Python. Наприклад Pylint, Python

Extension, Jupyter. Усі ці розширення спрощують роботу з кодом на Python. Я обрала розширення Python Extension – воно підсвічує синтаксис, має автодоповнення, інструменти для налагодження коду та підтримку віртуальних середовищ.

Система захищає від атак вказаного типу, виявляючи та блокуючи зловмисників на основі кількості та частоти запитів. Крім того, враховуючи ситуацію на сьогодняшній день, було введено можливість фільтрації запитів по регіону та блокування доступу по IP–адресі. Система повинна легко інтегруватись в існуючі веб–системи, не залежати від конкретного фреймворку та працювати як пов'язуюча ланка між веб–сервером та основною програмою. Таке рішення зумовлено тим, що більшість сучасних веб–додатків, особливо невеликі проекти, не використовують платні сервіси для захисту, залишаючись вразливими до атак типу HTTP–flood. Цей факт підтверджують недавні події, пов'язані з проведенням DDoS–атак навіть на великі компанії. Наприклад в березні 2025 року було проведену маштабну DDoS–атаку на соціальну мережу X, що спричинило значні перебої в роботі сервісу. [40] Хоча компанія велика й відома, деякі сервери не мали належного захисту, що посприяло зловмисникам.

Для гнучкого налаштування, повної автономії та повного контролю над роботою, було прийнято рішення не використовувати сторонні інструменти для захисту, в користь розробки своєї системи захисту. Також, враховуючи те, що значна кількість користувачів використовує не лише операційну систему Windows, а й Linux – система є кросплатформною.

На початковому етапі розробки системи було проаналізовано існуючі підходи до обмеження та фільтрації вхідного трафіку. Найбільш поширені – вбудовані засоби веб–серверів, використання спеціальних сервісів та реалізація власного способу на рівні застосунку.

Вбудовані засоби використовують загальні функції веб–сервера, як наприклад модуль limit_req в nginx. Такі інструменти дозволяють обмежувати кількість запитів з однієї IP–адреси за певний проміжок часу. Метод відзначається

високою продуктивністю та ефективністю проти простих атак. Тим не менш, має недолік в необхідності ретельного налаштування конфігурації, що вимагає глибокого розуміння внутрішньої логіки сервера. А ще подібні засоби зазвичай не забезпечують достатньої гнучкості для реалізації складнішої фільтрації.

До зовнішніх сервісів захисту відносяться раніше згадувані хмарні платформи, програмні забезпечення та комплексні системи. Ці інструменти надають розширені можливості для зниження навантаження при атаках, блокування IP–адрес, фільтрування трафіку та багаторівневого захисту. Попри всю потужність, цей спосіб вимагає переадресації трафіку через сторонні сервіси, що є абсолютно неприйнятним при вимогах до конфіденційності. Також варто враховувати залежність від компаній, які надають такі послуги – якщо виникне якась непередбачувана ситуація і сервіси перестануть працювати, то це приведе до проблем. Необхідність додаткових фінансових витрат в деяких випадках також може стати приводом для того, щоб не користуватись даними послугами.

Не зважаючи на потребу самостійної реалізації та тестування, для розробки системи захисту більш доцільний третій спосіб – розробка власного механізму, що обробляє всі вхідні HTTP–запити до їх передачі в основний застосунок. Повна незалежність дозволила налаштувати усе так, як того вимагало завдання. До того ж, самостійна реалізація гарантує максимальну конфіденційність та повний контроль над даними.

Таким чином, порівнюючи усі способи, вибір пав на самостійну розробку механізму, який реалізує захист на рівні застосунку.

3.2 Структура системи виявлення та захисту від DoS–атак в корпоративній мережі

Розробка системи відбувалась поетапно, із поступовим нарощуванням функціональності та постійним тестуванням на кожному етапі. Реалізована у

якості модульного Python–додатку, архітектура якого побудована з чітким розділенням логіки за функціональними зонами. Така будова допомагає легко модифікувати окремі компоненти, масштабувати систему та підключати нові функціонали без суттєвого втручання в весь інший код, що спрощує як підтримку проекту, так і його подальше доопрацювання. Структуру системи можна побачити на рисунку 3.1.

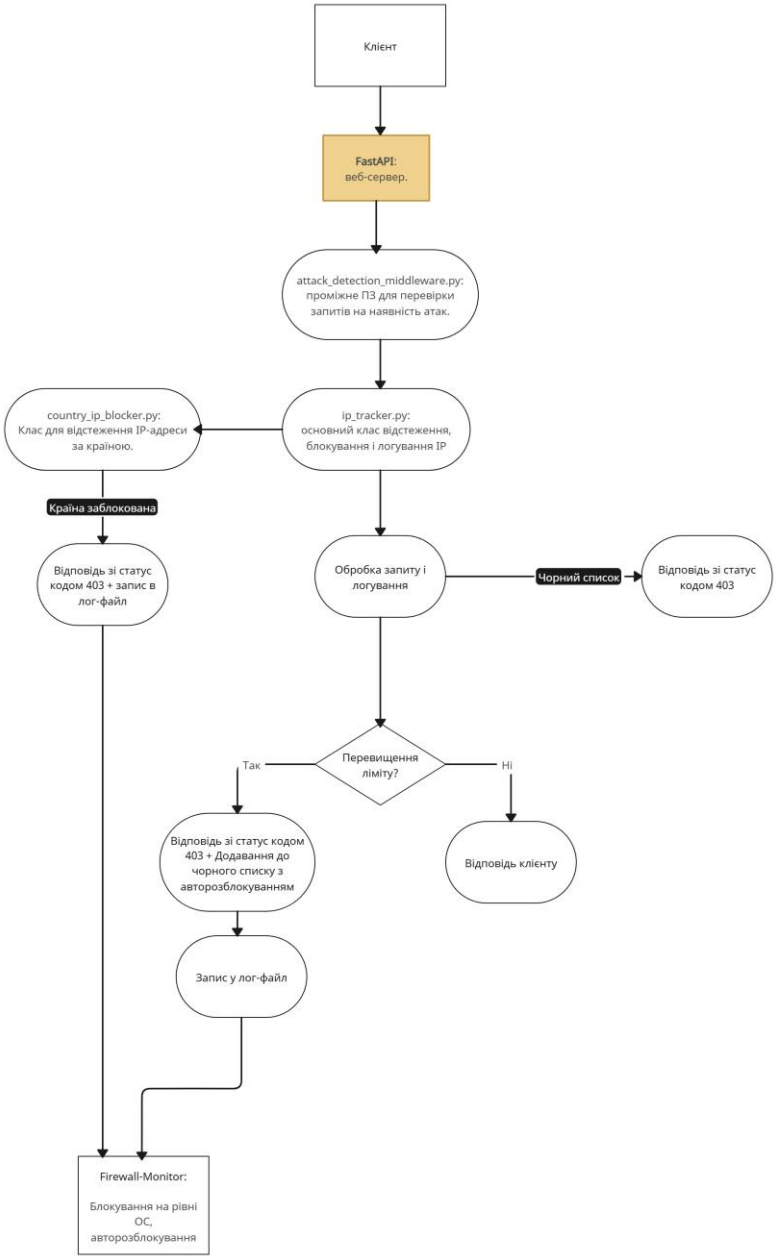


Рисунок 3.1 – Структурна схема програми

Спершу були визначені критерії виявлення атаки. Як основний механізм захисту було обрано обмеження частоти запитів: якщо кількість запитів від однієї IP–адреси перевищує встановлений поріг у заданий проміжок часу, цей IP блокується. Центральна логіка проекту зосереджена в проміжному обробнику, який інтегрується між веб–сервером та основним застосунком. Цей компонент перехоплює всі вхідні запити ще до того, як вони дійдуть до мережі і виконує перевірку частоти звернень, а також походження IP–адреси, виконуючи фільтрацію трафіку за географічною приналежністю. Така організація дозволяє відсіювати потенційно небезпечні запити.

```python
from fastapi import Request, Response
from fastapi.responses import JSONResponse
from utils.ip_tracker import tracker


async def attack_detection_middleware(request: Request, call_next):
    ip = request.client.host

    if tracker.is_whitelisted(ip):
        return await call_next(request)

    if tracker.is_banned(ip):
        return Response("Forbidden", status_code=403)

    if tracker.is_blocked(ip):
        return JSONResponse(status_code=403, content={"detail": "IP blocked by country"})
    response = await call_next(request)

    tracker.track_request(ip, status_code=response.status_code)

    if tracker.too_many_requests(ip):
        tracker.ban_ip(ip)
        return JSONResponse(status_code=403, content={"detail": "IP auto-banned"})

    return response
```

Рисунок 3.2 – Механізм проміжної обробки запитів

Додатково, в архітектуру інтегровані модулі з утилітами, які виконують допоміжні завдання, зокрема роботу з IP–адресами, визначення регіональної приналежності, блокування за IP–адресою, ведення лічильників тощо. Їхнє виділення в окремі логічні блоки забезпечує чистоту та повторне використання коду.

```python
import ipaddress

class CountryIPBlocker:
    def __init__(self):
        self.blocked_networks = []

    def load_russian_ips(self):
        ip_ranges = [
            "5.136.0.0/13",
            "95.24.0.0/13",
            "176.208.0.0/13",
            "178.64.0.0/13",
            "2.60.0.0/14",
        ]

        for cidr in ip_ranges:
            try:
                network = ipaddress.ip_network(cidr)
                self.blocked_networks.append(network)
            except ValueError:
                continue

    def is_blocked(self, ip: str) -> bool:
        ip_obj = ipaddress.ip_address(ip)
        return any(ip_obj in net for net in self.blocked_networks)
blocker = CountryIPBlocker()
blocker.load_russian_ips()

test_ips = ["5.136.0.1", "8.8.8.8", "95.24.0.1"]
for ip in test_ips:
    print(f"{ip} bocked: {blocker.is_blocked(ip)}")
```

Рисунок 3.3 – Модуль блокування IP–адрес за регіоном

Окремим блоком виділена підсистема моніторингу, яка відповідає за збір даних про активність захисту. Вона може інформувати про спроби атак, фіксувати заблоковані IP–адреси та допомагає в оцінці ефективності застосованих правил. Для модуля моніторингу також було створено допоміжний IP–трекер, який відстежує активність IP–адрес і зберігає дана про частоту звернень. Завдяки цьому користувач отримує уявлення про поточний стан системи в реальному часі.

```python
import platform
import subprocess

_banned = set()

def ban_ip(ip: str):
    if ip in _banned:
        return
    _banned.add(ip)

    if platform.system() == "Linux":
        subprocess.run(["iptables", "-A", "INPUT", "-s", ip, "-j", "DROP"], check=False)
    elif platform.system() == "Windows":
        subprocess.run(["netsh", "advfirewall", "firewall", "add", "rule",
                        "name=BlockIP", f"dir=in", f"action=block", f"remoteip={ip}"], check=False)

def unban_ip(ip: str):
    if ip not in _banned:
        return
    _banned.remove(ip)

    if platform.system() == "Linux":
        subprocess.run(["iptables", "-D", "INPUT", "-s", ip, "-j", "DROP"], check=False)
    elif platform.system() == "Windows":
        subprocess.run(["netsh", "advfirewall", "firewall", "delete", "rule",
                        "name=BlockIP", f"remoteip={ip}"], check=False)
```

Рисунок 3.4 – Модуль моніторингу

Для того, щоб протестувати та перевірити роботу системи, було розроблено симуляційний інструмент, який імітує типові атаки, надсилаючи велику кількість запитів з однієї або кількох IP–адрес. З його допомогою можна перевіряти стійкість системи до перенавантаження та ефективність механізмів блокування. Також є можливість протестувати безпосередньо саме блокування, чи коректно воно працює.

Конфігураційні параметри задані у файлі config.py, який винесено в корінь проекту. У ньому задаються основні обмеження такі як ліміт запитів, часовий інтервал, список країн для блокування, а також параметри журналювання. Так можна швидко адаптовувати поведінку системи щодо тих чи інших ситуацій без змін вихідного коду.

```python
from pydantic_settings import BaseSettings
from pydantic import Field
from typing import Set
from appdirs import user_log_dir
import os

APP_NAME = "simple-anti-dos"

log_dir = user_log_dir(APP_NAME)
os.makedirs(log_dir, exist_ok=True)

log_file_path = os.path.join(log_dir, "banned_ips.log")

if not os.path.exists(log_file_path):
    with open(log_file_path, "w") as f:
        pass

class Settings(BaseSettings):
    TIME_WINDOW: int = Field(60, description="Window size for rate limit in seconds")
    MAX_REQUESTS: int = Field(100, description="Max requests per IP in time window")
    BAN_DURATION: int = Field(30, description="Ban duration in seconds")
    LOG_FILE_PATH: str = log_file_path
    COUNTRY_REGIONS_TO_BLOCK: Set[str] = Field(default_factory=lambda: {"CN", "RU"})
    class Config:
        env_file = ".env"
        extra = "ignore"

settings = Settings()
```

Рисунок 3.5 – Конфіг

На завершальному етапі були створені допоміжні скрипти для автоматизованого запуску та налаштування. Підтримується багатоплатформність і зручне розгортання, система легко встановлюється, запускається та конфігурується як у середовищах Windows, так і Linux. Це робить її доступною для широкого кола користувачів. Це забезпечило зручність у використанні та полегшило розгортання системи на нових серверах або в середовищах тестування.

Загалом, розробка проходила послідовно: від ідеї та базових механізмів до гнучкої конфігурації, симуляції атак та автоматизації. В результаті вийшла організована загальна структура проекту яка підтримує подальший розвиток – за потреби її можна доповнити веб–інтерфейсом для управління, інтегрувати з існуючими фреймворками або розгорнути в хмарному середовищі.

3.3 Тестування системи виявлення та захисту від DoS–атак в корпоративній мережі

Після завершення основної розробки було проведено комплексне тестування системи з метою перевірки її стійкості до навантажень, коректності блокування запитів та відповідності очікуваним параметрам конфігурації. Тестування охоплювало як модульний рівень, так і інтеграційні сценарії, максимально наближені до реальних умов.

Основна мета полягала у перевірці таких характеристик системи:

- здатність виявляти та блокувати IP–адреси при перевищенні допустимої кількості запитів;
- коректна робота географічної фільтрації;
- правильне зчитування конфігураційних параметрів та їх вплив на поведінку системи;
- стабільність системи при високому навантаженні;
- відсутність помилок при багаторазових запусках та тривалій роботі.

Для тестування було використано розроблений симулятор, в якому мінялась конфігурація в залежності від запитів. Було проведено атаку з однієї IP–адреси; розподілену по часу атаку з декількох IP–адрес; атаки з IP–адрес, які внесені в список заборонених та зсимульовано звичайний трафік з інтервалами між запитами. Результати тестування наведені в таблиці 3.1

Таблиця 3.1 – Результати тестування

Сценарій атаки	Інтенсивність	Очікуванна реакція	Результат
1 IP–адреса	2000 запитів/хв	Блокування IP	Заблоковано
5 IP–адрес	1000 запитів/хв з кожної адреси	Блокування усіх 5 IP–адрес	Заблоковано
IP з забороненого регіону	10 запитів/хв з забороненої адреси	Блокування забороненої адреси	Заблоковано за регіоном
Нормальний трафік	10 запитів/хв	Надання доступу	Запити оброблено

Усі задані сценарії система успішно пройшла, підтвердивши функціональність, стабільність та ефективність у запобіганні типовим DoS–атакам. Завдяки зручності конфігурації та можливості проведення тестування, є придатною до використання як у локальних так і в глобальних мережах.

3.4 Висновок

Був проведений аналіз існуючих методів захисту від DoS–атак, включаючи вбудовані механізми веб–серверів, зовнішні сервіси та рішення, реалізовані на рівні самого застосунку. Враховуючи обмеження кожного з цих підходів, було розроблено власну систему захисту. Основною вимогою було створення гнучкої в налаштуванні та простої у використанні системи, яка легко адаптується до будь–якого Python–застосунку. В результаті виконання завдання було успішно розроблено систему виявлення та захисту від DoS–атак, яка не залежить від сторонніх сервісів та не вимагає складної інтеграції з серверною інфраструктурою.

Система побудована як модульний Python–застосунок із структурованою архітектурою. Вбудовано фільтр по регіональній приналежності а також IP–трекер. Її можна налаштовувати так, як заманеться користувачу. Також для перевірки роботи та ефективності розроблено модуль для тестування системи та безпосередньо проведено саме тестування. Результати виявились успішними – система оперативно реагує виявляє та блокує запити, що перевищують задані ліміти, успішно фільтрує адреси за регіонами та демонструє стабільність під час високих навантажень. Згідно з тестами на продуктивність, рішення здатне реагувати на атаки менш ніж за секунду.

У майбутньому систему можна розширити, додавши підтримку розподіленого зберігання інформації про блокування, наприклад через Redis, що дозволить синхронізувати дані між кількома вузлами. Також можливе

інтегрування аналітичних модулів та застосування машинного навчання для адаптивного виявлення атак. А для зручного адміністрування та моніторингу системи можна розробити веб–інтерфейс.

ВИСНОВКИ

В рамках виконання дипломної роботи, було проведено комплексне дослідження методів виявлення та захисту від DoS–атак, що мають велике значення для нормального функціонування інформаційної інфраструктури. Зважаючи на критичну важливість безперервного функціонування сервісів у корпоративному середовищі, питання своєчасного виявлення аномальної активності, пов'язаної з DoS–атаками, є надзвичайно актуальним. Метою даного дослідження було створення ефективного та гнучкого інструменту для протидії таким атакам, орієнтованого на використання у реальних умовах.

На першому етапі роботи було здійснено глибокий аналіз архітектури об'єкта захисту, його функціональних компонентів, взаємозв'язків між вузлами, а також характеристик трафіку, притаманних типовим користувачам. Детально розглянуто можливі вектори атак, включаючи як зовнішні загрози з боку шкідливих ботнетів і мережевих сканерів, так і внутрішні ризики, що виникають унаслідок неправильної конфігурації, недбалості користувачів або зловмисних дій усередині системи. Особливу увагу було приділено аналізу типових вразливостей, які можуть бути використані для ініціації DoS–атак, а також їхньому впливу на функціональність і доступність сервісів.

У рамках побудови інформаційної моделі захисту було здійснено класифікацію типових загроз і потенційних порушників. Для візуалізації моделей загроз застосовано метод CORAS, що дозволило змоделювати можливі сценарії атак, визначити критичні активи, оцінити ризики та виявити найбільш уразливі точки у структурі інформаційної системи. Такий підхід допоміг глибше зрозуміти характер загроз і сформувати вимоги до архітектури захисної системи.

У практичній частині дипломної роботи було спроєктовано та реалізовано систему виявлення та захисту від DoS–атаки. Система розроблена на мові програмування Python із повним урахуванням вимог автономності, мінімальної залежності від сторонніх сервісів та гнучкої конфігурацій. Система розроблялась

без використання сторонніх сервісів, тому є незалежною, з можливістю гнучкого налаштування без втручання в основний код. Було реалізовано модульну архітектуру, що дозволяє легко оновлювати окремі компоненти, додавати нові правила фільтрації трафіку, налаштовувати критерії виявлення аномалій, а також адаптувати систему до різних умов експлуатації. Зокрема, у систему інтегровано фільтрацію трафіку за географічним походженням IP–адрес, механізми виявлення надмірної кількості запитів, журналювання подій та сповіщення адміністратора про можливу атаку.

Окремо було приділено увагу практичному тестуванню системи. У рамках тестування було реалізовано чотири різних сценарії: нормальний користувацький трафік, симуляція атаки HTTP–flood шляхом надсилання великої кількості запитів, запити з IP–адрес, які належать до заборонених країн, а також змішані атаки, що імітують поведінку внутрішніх і зовнішніх порушників. Результати тестування підтвердили працездатність та ефективність системи, вона коректно виявляє аномальну активність, блокує потенційно небезпечні з’єднання та не порушує обробку легітимного трафіку. Затримка обробки запитів залишалась у межах прийнятних значень, що свідчить про придатність розробленого рішення для використання в реальному середовищі.

Підсумовуючи проведену роботу, можна стверджувати, що поставлена мета досягнута в повному обсязі. У дипломній роботі було обґрунтовано актуальність проблеми, здійснено глибокий аналіз об'єкта захисту, розроблено архітектуру системи виявлення DoS-атак, реалізовано її та підтверджено ефективність рішення експериментальним шляхом.

Розроблену систему можна вдосконалювати, налаштувати для використання зовнішніх сервісів та легко адаптувати для використання в реальній корпоративній мережі.

ПЕРЕЛІК ДЖЕРЕЛ

1. Загальне поняття корпоративної мережі. Структура корпоративної мережі. Scribd. URL: https://scribd.com/presentation/606901011/20–корпоративні–мережі (дата звернення 25.02.2025)

2. Об'єкти критичної інфраструктури України: все, що варто знати. KyivPost. URL: https://www.kyivpost.com/uk/post/28283 (дата звернення: 26.02.2025).

3. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1882–20#Text (дата звернення: 26.02.2025).

4. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/rada/show/v0023519–21#Text (дата звернення: 26.02.2025).

5. Фішинг та інші техніки соціальної інженерії. Освітній проект «На Урок» для вчителів. URL: https://naurok.com.ua/post/fishing–ta–inshi–tehniki–socialno–inzheneri (дата звернення: 26.02.2025).

6. Державна служба спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs/sho–take–ddos–ataka (дата звернення: 26.02.2025).

7. Атака на ланцюг постачання – втручання в кібербезпеку ланцюга постачання. ESET Cybersecurity Enterprise, Business and Home Solutions URL: https://www.eset.com/ua/about/newsroom/blog/business–security/kolichestvo–atak–na–tsep–postavok–rastet–kto–pod–pritselom–i–kak–protivostoyat/?srsltid=AfmBOoq8RP (дата звернення: 27.02.2025).

8. Securing web applications against XSS and SQLi attacks using a novel deep learning approach. Scientific reports. URL: https://www.nature.com/articles/s41598–023–48845–4#:~:text=SQLi%20attacks%20exploit%20database%20security,redirecting%20users%20to%20malicious%20websites. (дата звернення: 27.02.2025)

9. Man–in–the–Middle Attack: Types And Examples. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/man–in–the–middle–attack (дата звернення 28.02.2025)

10. Що таке Зловмисне програмне забезпечення – Терміни та визначення кібербезпеки.
URL: https://www.vpnunlimited.com/ua/help/cybersecurity/malware?srsltid=AfmBOorzo9_35EkF7vu95j4mt8971pH5oVnPpgwAL6E3I0YEk8U_MGi1 (дата звернення: 26.02.2025).

11. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Освітній проект «На Урок». URL: https://naurok.com.ua/test/problemi–zabezpechennya–bezpeki–v–komp–yuternih–sistemah–i–merezhah–2493352.html (дата звернення: 02.03.2025).

12. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Освітній проект «На Урок». URL: https://naurok.com.ua/test/problemi–zabezpechennya–bezpeki–v–komp–yuternih–sistemah–i–merezhah–2493352.html (дата звернення: 02.03.2025).

13. Аутентифікація і авторизація: що це і в чому відмінність. QualityAssuranceGroup. URL: https://qagroup.com.ua/publications/autentyfikatciia–i–avtoryzatciia/ (дата звернення: 02.03.2025).

14. Захист корпоративних мереж від загроз: засоби та методи. Netwave. URL: https://netwave.ua/blog/zahist–korporativnih–merezh–vid–zagroz–zasobi–ta–metodi/ (дата звернення: 03.03.2025)

15. Небезпека особистих пристроїв в корпоративних мережах – як зменшити ризики. UnianUA. URL: https://www.unian.ua/techno/nebezpeka–osobistih–pristrojiv–v–korporativnih–merezhah–yak–zmenshiti–riziki–12542439.html (дата звернення: 05.03.2025)

16. Five Reasons Why Network Security Training Should Be Your Next Move. Cisco Blogs. URL: https://blogs.cisco.com/learning/five–reasons–why–network–security–training–should–be–your–next–move (дата звернення 05.03.2025)

17. Dos Attack vs Ddos Attack. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/dos–vs–ddos (дата звернення 10.03.2025)

18. Threat Modeling. OWASP. URL: https://owasp.org/www–community/Threat_Modeling (дата звернення 12.03.2025)

19. Mirkovic J. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms / J. Mirkovic, P. Reiher // ACM SIGCOMM Computer Communications Review – Los Angeles, 2004. – V. 34 – P. 39–52.

20. Побудова та адміністрування корпоративної мережі підприємства. VTime Group. URL: https://v–time.com.ua/it–posluhy/pobudova–ta–administruvannya–korporatyvnoyi–merezhi/ (дата звернення: 21.03.2025)

21. Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response. SEI Blog. URL: https://insights.sei.cmu.edu/blog/distributed–denial–of–service–attacks–four–best–practices–for–prevention–and–response/ (дата звернення 21.03.2025)

22. DDoS Architecture Diagrams and White Paper. Nginx. URL: https://www.nginx–cn.net/resources/white–papers/ddos–architecture–diagrams–and–white–paper (дата звернення: 21.03.2025)

23. Що таке DdoS–атака? FoxmindEd. URL: https://foxminded.ua/ddos–ataka/ (дата звернення: 30.03.2025)

24. HTTP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/http–flood–ddos–attack/ (дата звернення 02.04.2025)

25. Снігур В. А. Захист інформації в комп'ютерних системах і мережах: навч. посібник. / В. А. Снігур – Київ: Видавництво «Слово», 2020. – 272 с.

26. Behal, S. Trends in validation of DDoS research / S. Behal, K. Kumar, M. Sachdeva, G. Singh // Procedia Computer Science, 2017. – V. 85 – P. 7–15.

27. The CORAS Method. CORAS Sourceforge. URL: https://coras.sourceforge.net/ (дата звернення: 19.04.2025).

28. Галузі критичної інфраструктури України. YC Market Blog. URL: https://blog.youcontrol.market/galuzi–kritichnoyi–infrastrukturi–ukrayini/ (дата звернення: 20.04.2025)

29. Що таке IPS/IDS і де застосовується – Блог – HostZealot. HostZealot. URL: https://www.hostzealot.com.ua/blog/about–solutions/shho–take–ipsids–i–de–zastosovujetsya (дата звернення: 20.04.2025).

30. Деякі питання об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1109–2020–п#Text (дата звернення: 25.04.2025).

31. Типи DoS–атак за моделлю OSI. HyperHost. URL: https://hyperhost.ua/info/uk/tipi–ddos–atak–za–modellyu–osi (дата звернення: 27.04.2025)

32. Типи DDoS–атак та способи захисту від них. HostZealot. URL: https://www.hostzealot.com.ua/blog/about–web–hosting/tipi–ddos–atak–ta–sposobi–zahistu–vid–nih (дата звернення: 27.04.2025)

33. Defending against distributed denial of service (DDoS) attacks. Government of Canada URL: https://www.cyber.gc.ca/en/guidance/defending–against–distributed–denial–service–ddos–attacks–itsm80110 (дата звернення: 30.04.2025)

34. Microsoft denial–of–service defense strategy. Microsoft. URL: https://learn.microsoft.com/en–us/compliance/assurance/assurance–microsoft–dos–defense–strategy (дата звернення: 02.05.2025)

35. Components of DdoS Defense System. ResearchGate. URL: https://www.researchgate.net/figure/Components–of–DDoS–Defense–System_fig10_357687712 (дата звернення: 05.05.2025)

36. Li Y., Li D. Research based on OSI model. / Y. Li, D. Li, W. Cui, R. Zhang // IEEE 3rd International Conference on Communication Software and Networks, 2011 – P. 554–557.

37. Що таке IPS/IDS і де застосовується – Блог – HostZealot. HostZealot. URL: https://www.hostzealot.com.ua/blog/about–solutions/shho–take–ipsids–i–de–

zastosovujetsya (дата звернення: 01.03.2025).

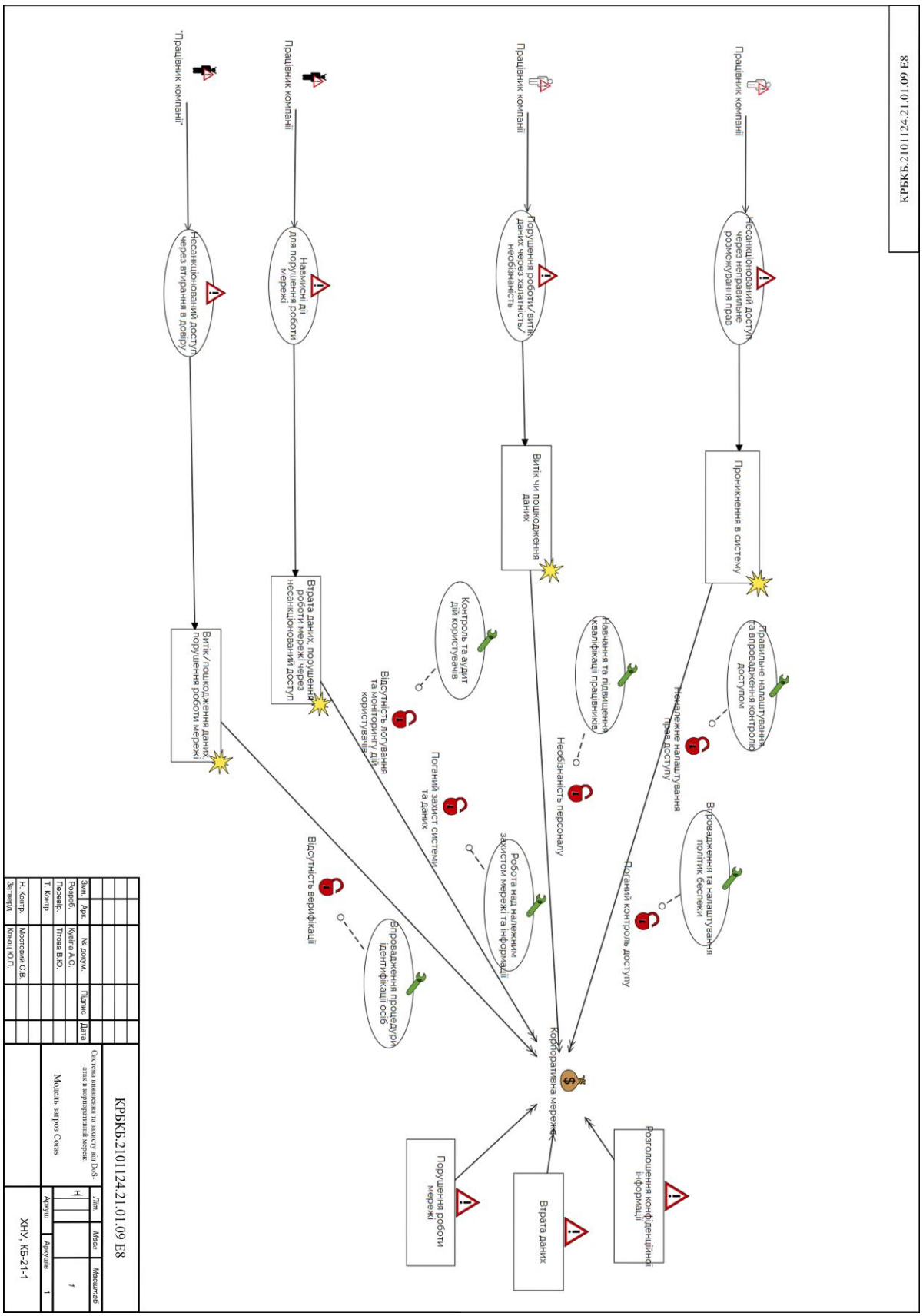
38. HTTP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/http–flood–ddos–attack/ (дата звернення 02.04.2025)

39. Prasad K. M. (2017). BIFAD: Bioinspired anomaly based HTTP–flood attack detection. / K. M. Prasad, A. R. M. Reddy, K. V. Rao // Wireless Personal Communications, 2017. V. 1 – P. 281–308.

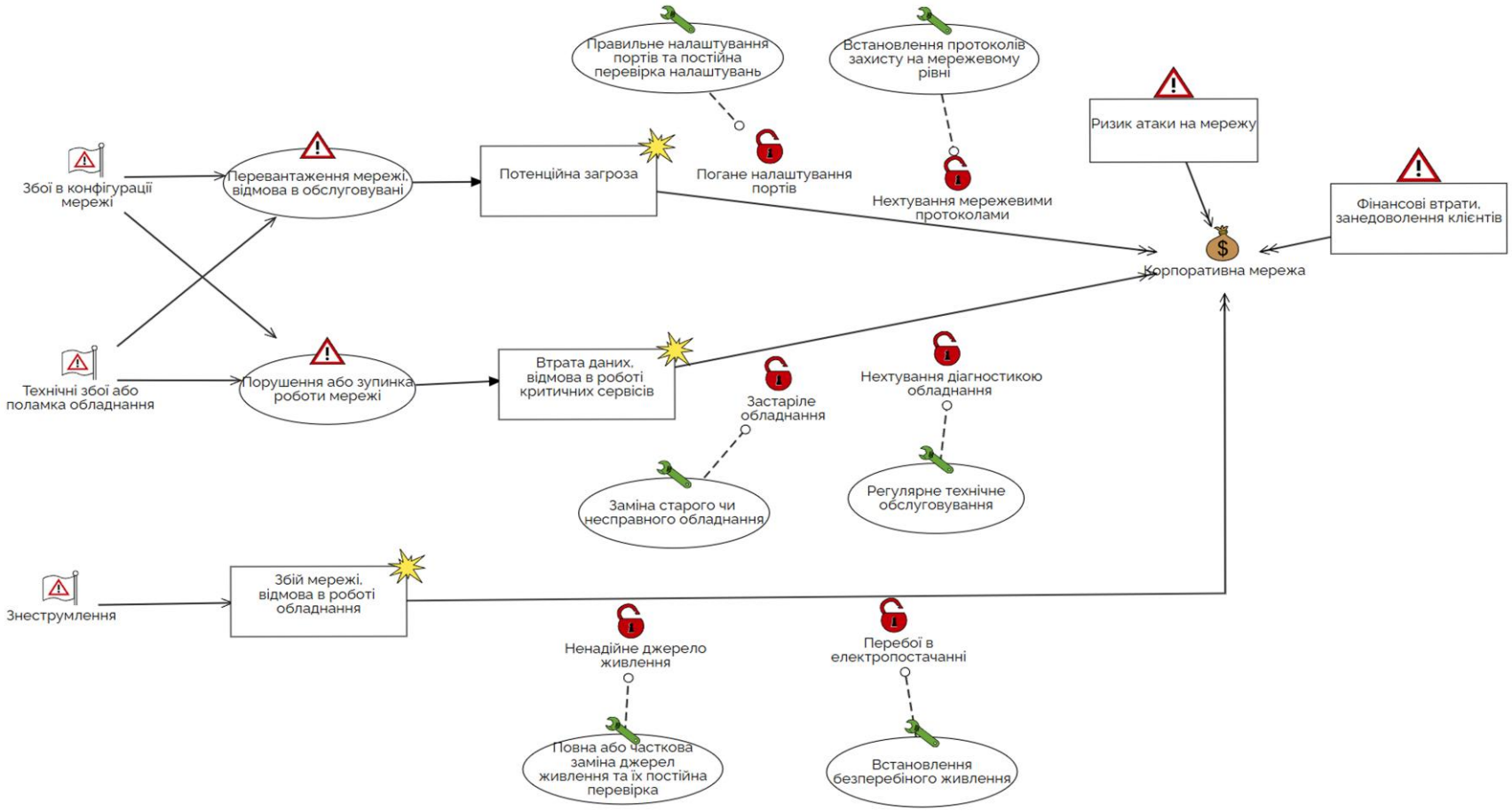
40. What Really Happened With the DdoS Attack That Took Down X. Wired. URL: https://www.wired.com/story/x–ddos–attack–march–2025/ (дата звернення 03.04.2025)

ДОДАТОК А

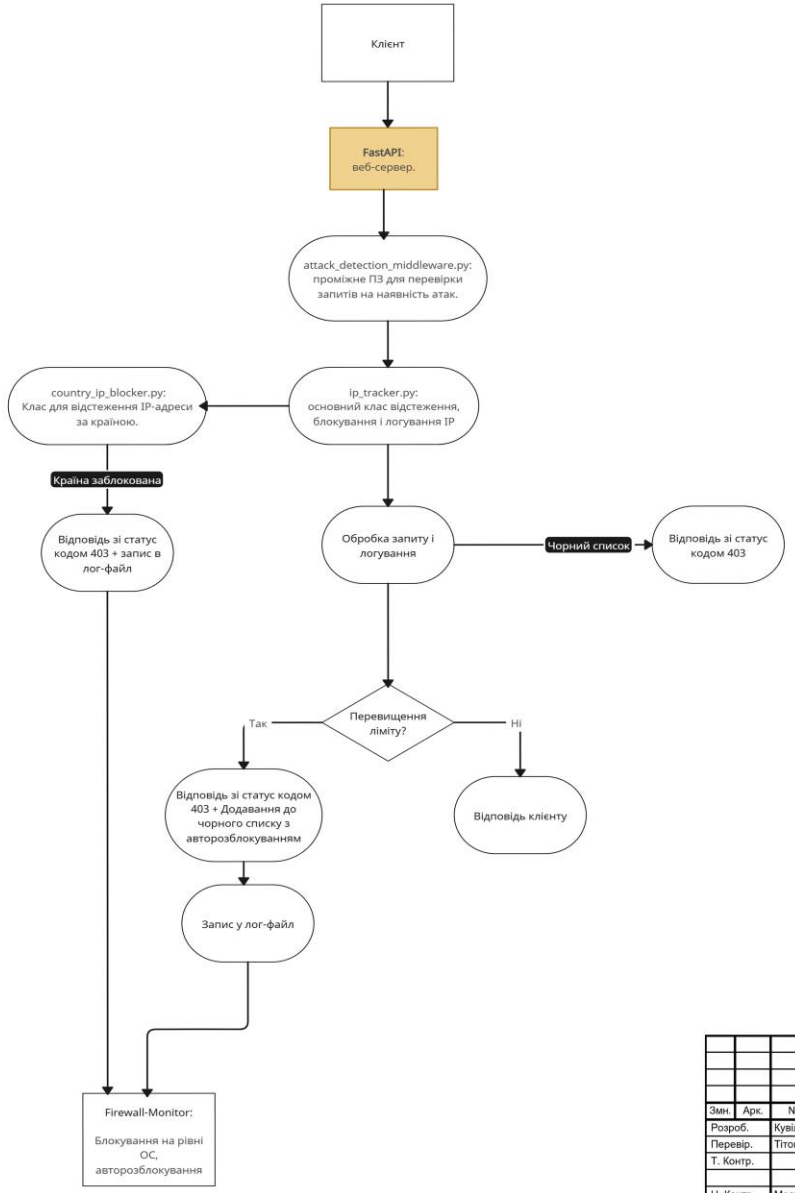
Копії графічної частини



КРБКБ.2101124.21.01.09 Е8



					КРБКБ.2101124.21.01.09 Е8			
Змн.	Арк.	№ докум.	Підпис	Дата	Система виявлення та захисту від DoS-атак в корпоративній мережі	Літ.	Маса	Масштаб
Розроб.		Кувіпа А.О.				Н		1
Перевір.		Тітова В.Ю.			Модель загроз Coras			
Т. Контр.						Аркуш	Аркушів	1
Н. Контр.		Мостовий С.В.				ХНУ, КБ-21-1		
Затверд.		Кльоц Ю.П.						



					КРБКБ.2101124.21.01.09 Е8	
Змн.	Арк.	№ докум.	Підпис	Дата	Система виявлення та захисту від DoS-атак в корпоративній мережі	Літ. / Маси / Масштаб
Розроб.		Кувіла А.О.			Алгоритм роботи	Н / / 1
Перевір.		Тітова В.Ю.				Аркуш / Аркушів 1
Т. Контр.						
Н. Контр.		Мостовий С.В.				ХНУ, КБ-21-1
Затверд.		Кльоц Ю.П.				

ДОДАТОК Б

Програмний код

Main.py

```
from fastapi import FastAPI
from fastapi.responses import JSONResponse
from middlewares.attack_middleware import attack_detection_middleware

app = FastAPI()
app.middleware("http")(attack_detection_middleware)

def factorial(n):
    factorial = n
    while(n > 1):
        factorial = factorial * (n – 1)
        n = n – 1
    return factorial

@app.get("/")
def index():
    return {"msg": "Welcome"}

@app.get("/test")
def test(number: int = 1):
    fact = factorial(number)
    return {"msg": fact}

@app.get("/error")
def error():
```

```
    return {"msg": "This is a fake error"}, 500
```

Simulation.py

```
import asyncio
import sys
import aiohttp
import random
import time

TARGET_URL = "http://127.0.0.1:8000/test"
REQUESTS_PER_CLIENT = 10000
CONCURRENT_CLIENTS = 2
DELAY_BETWEEN_REQUESTS = 0.1
SYM_RU_IP = False
async def flood(ip_id):
    if SYM_RU_IP:
        headers = {
                    "X–Forwarded–For": f"195.208.208.{ip_id}"
        }
    else:
        headers = {
            "X–Forwarded–For": f"192.168.1.{ip_id}"
        }
    async with aiohttp.ClientSession() as session:
        for _ in range(REQUESTS_PER_CLIENT):
            try:
                random_number = random.randint(1, 1000)
                async with session.get(f"{TARGET_URL}?number={random_number}",
headers=headers) as resp:
```

```
                status = resp.status
                print(f"[IP {ip_id}] Status: {status}")
            except Exception as e:
                print(f"[IP {ip_id}] Error: {e}")
            await asyncio.sleep(DELAY_BETWEEN_REQUESTS)

async def main():
    tasks = [flood(ip_id) for ip_id in range(CONCURRENT_CLIENTS)]
    await asyncio.gather(*tasks)

if __name__ == "__main__":
    start = time.time()
    if sys.platform == "win32":
        asyncio.set_event_loop_policy(asyncio.WindowsProactorEventLoopPolicy())
    asyncio.run(main())
    print("Completed in", time.time() – start, "seconds.")
```

Firewall–monitor.py

```
import platform
import subprocess

_banned = set()

def ban_ip(ip: str):
    if ip in _banned:
        return
    _banned.add(ip)

    if platform.system() == "Linux":
```

```
        subprocess.run(["iptables", "–A", "INPUT", "–s", ip, "–j", "DROP"], check=False)
    elif platform.system() == "Windows":
        subprocess.run(["netsh", "advfirewall", "firewall", "add", "rule",
                        "name=BlockIP", f"dir=in", f"action=block", f"remoteip={ip}"],
check=False)

def unban_ip(ip: str):
    if ip not in _banned:
        return
    _banned.remove(ip)

    if platform.system() == "Linux":
        subprocess.run(["iptables", "–D", "INPUT", "–s", ip, "–j", "DROP"], check=False)
    elif platform.system() == "Windows":
        subprocess.run(["netsh", "advfirewall", "firewall", "delete", "rule",
                        "name=BlockIP", f"remoteip={ip}"], check=False)
```

Config.py

```
from pydantic_settings import BaseSettings
from pydantic import Field
from typing import Set
from appdirs import user_log_dir
import os

APP_NAME = "simple–anti–dos"

log_dir = user_log_dir(APP_NAME)
os.makedirs(log_dir, exist_ok=True)
```

```
log_file_path = os.path.join(log_dir, "banned_ips.log")

if not os.path.exists(log_file_path):
    with open(log_file_path, "w") as f:
        pass

class Settings(BaseSettings):
    TIME_WINDOW: int = Field(60, description="Window size for rate limit in seconds")
    MAX_REQUESTS: int = Field(100, description="Max requests per IP in time window")
    BAN_DURATION: int = Field(30, description="Ban duration in seconds")
    LOG_FILE_PATH: str = log_file_path
    COUNTRY_REGIONS_TO_BLOCK: Set[str] = Field(default_factory=lambda: {"CN", "RU"})
    class Config:
        env_file = ".env"
        extra = "ignore"

settings = Settings()
```

Country ip blocker.py

```
import ipaddress
class CountryIPBlocker:
    def __init__(self):
        self.blocked_networks = []

    def load_russian_ips(self):
        ip_ranges = [
```

```
            "5.136.0.0/13",
            "95.24.0.0/13",
            "176.208.0.0/13",
            "178.64.0.0/13",
            "2.60.0.0/14",
            "2.92.0.0/14",
            "5.2.32.0/19",
            "5.3.0.0/16",
            "5.8.0.0/20",
            "5.8.48.0/20",
            "5.8.160.0/20",
            "31.173.64.0/18",
            "37.144.0.0/14",
            "46.8.0.0/15",
            "77.120.0.0/13",
            "91.192.0.0/12"
        ]

        for cidr in ip_ranges:
            try:
                network = ipaddress.ip_network(cidr)
                self.blocked_networks.append(network)
            except ValueError:
                continue

    def is_blocked(self, ip: str) –> bool:
        ip_obj = ipaddress.ip_address(ip)
        return any(ip_obj in net for net in self.blocked_networks)

blocker = CountryIPBlocker()
```

```
blocker.load_russian_ips()

test_ips = ["5.136.0.1", "8.8.8.8", "95.24.0.1"]
for ip in test_ips:
    print(f"{ip} blocked: {blocker.is_blocked(ip)}")
```

IP–tracker.py

```
import heapq
import time
import threading
from collections import defaultdict, deque
from config import settings
from utils.country_ip_blocker import CountryIPBlocker

blocker = CountryIPBlocker()
for country_code in settings.COUNTRY_REGIONS_TO_BLOCK:
    blocker.load_country_ips(country_code.lower())

class IPTracker:
    def __init__(self):
        self.request_logs = defaultdict(deque)
        self.banned_ips = {}
        self.banned_heap = []
        self.whitelisted_ips = set()
        self.time_window = settings.TIME_WINDOW
        self.max_requests = settings.MAX_REQUESTS
        self.ban_duration = settings.BAN_DURATION
        self.log_file_path = settings.LOG_FILE_PATH
        self._lock = threading.Lock()
```

```
    self._stop_event = threading.Event()
    self._start_unban_thread()

def _start_unban_thread(self):
    def cleanup_loop():
        while not self._stop_event.is_set():
            now = time.time()
            with self._lock:
                while self.banned_heap and self.banned_heap[0][0] <= now:
                    expiry, ip = heapq.heappop(self.banned_heap)
                    if ip in self.banned_ips and self.banned_ips[ip] <= now:
                        del self.banned_ips[ip]
                        print(f"[TRACKER] Unbanned IP: {ip}")

            time.sleep(5)

    thread = threading.Thread(target=cleanup_loop, daemon=True)
    thread.start()

def shutdown(self):
    self._stop_event.set()

def is_whitelisted(self, ip: str) –> bool:
    return ip in self.whitelisted_ips

def is_banned(self, ip: str) –> bool:
    return ip in self.banned_ips
def is_blocked(self, ip: str) –> bool:
    blocked = blocker.is_blocked(ip)
    if blocked:
```

```
            self.ban_ip(ip, 3600*24)

        return blocked
    def ban_ip(self, ip: str, duration: int = None):
        if self.is_banned(ip):
            return
        with self._lock:

            if ip in self.request_logs:
                del self.request_logs[ip]
            if duration is None:

                self.banned_ips[ip] = time.time() + self.ban_duration
                heapq.heappush(self.banned_heap, (self.banned_ips[ip], ip))
                with open(self.log_file_path, "a") as f:
                    f.write(f"{ip},{int(self.ban_duration)}\n")
            else:
                self.banned_ips[ip] = time.time() + duration
                heapq.heappush(self.banned_heap, (self.banned_ips[ip], ip))
                with open(self.log_file_path, "a") as f:
                    f.write(f"{ip},{int(duration)}\n")
        print(f"[TRACKER] Banned IP: {ip}")

    def unban_ip(self, ip: str):

        self.banned_ips.pop(ip, None)
        print(f"[TRACKER] Unbanned IP: {ip}")

    def whitelist_ip(self, ip: str):
        self.whitelisted_ips.add(ip)
```

```
        print(f"[TRACKER] Whitelisted IP: {ip}")

    def remove_from_whitelist(self, ip: str):
        self.whitelisted_ips.discard(ip)

    def track_request(self, ip: str, status_code: int):
        now = time.time()
        log = self.request_logs[ip]
        log.append((now, status_code))

        while log and now – log[0][0] > self.time_window:
            log.popleft()

    def too_many_requests(self, ip: str) –> bool:
        return len(self.request_logs[ip]) > self.max_requests

    def clear(self):
        with self._lock:
            self.request_logs.clear()
            self.banned_ips.clear()
        self.whitelisted_ips.clear()

tracker = IPTracker()
```

Test protection.py

```
import pytest
import asyncio
import httpx
from config import settings
from utils.ip_tracker import tracker
```

```
BASE_URL = "http://localhost:8000"

@pytest.fixture(autouse=True)
def clear_tracker_state():
    """Reset IP tracker before each test"""
    tracker.clear()
    yield
    tracker.clear()

@pytest.mark.asyncio
async def test_rate_limiting_triggered():
    ip = "127.0.0.1"
    url = f"{BASE_URL}/test"

    async with httpx.AsyncClient() as client:
        tasks = [client.post(url, headers={"X–Forwarded–For": ip}) for _ in
range(settings.MAX_REQUESTS + 10)]
        responses = await asyncio.gather(*tasks)

    limited = sum(r.status_code == 403 for r in responses)
    assert limited > 0, "Rate limiting did not trigger"

@pytest.mark.asyncio
async def test_error_ban_triggered():
    ip = "127.0.0.1"
    url = f"{BASE_URL}/non–existent"

    async with httpx.AsyncClient() as client:
        for _ in range(settings.MAX_ERRORS + 2):
```

```
            await client.get(url, headers={"X–Forwarded–For": ip})

        response = await client.get(f"{BASE_URL}/", headers={"X–Forwarded–For": ip})
        assert response.status_code == 403 or response.status_code == 429

@pytest.mark.asyncio
async def test_whitelist_bypass():
    ip = "127.0.0.1"
    tracker.whitelist_ip(ip)

    url = f"{BASE_URL}/test"

    async with httpx.AsyncClient() as client:
        tasks = [client.get(url, headers={"X–Forwarded–For": ip}) for _ in
range(settings.MAX_REQUESTS + 50)]
        responses = await asyncio.gather(*tasks)

    assert all(r.status_code != 429 for r in responses), "Whitelisted IP was rate–limited"
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Кувіли Анни Олексіївни
ПІБ здобувача вищої освіти

Студентки ФІТ, 4 курсу, групи КБ-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (StrikePlagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

31.05.2025
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Кувіла Анна Олексіївна

Співавтор:

Назва: Система виявлення та захисту від DOS-атак в корпоративних мережах

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:3.6%

Коефіцієнт подібності 2:0.4%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-01 18:55:00.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

02.06.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 12%**

ID: 242705 Title: Система виявлення та захисту від DOS-атак в корпоративних мережах Added in a DB: 2025-06-01 Authors: Кувіла Анна Олексіївна Heads: Тітова В.Ю. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	74767	1142	1191 (2%)	25 (2%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система виявлення та захисту від DoS–атак в корпоративній мережі

Автор: Кувіла Анна Олексіївна

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою виявлення і запобігання плагіату StrikePlagiarism складає 96,4%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віра ТІТОВА

Гарант ОПП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Кувіла Анна Олексіївна
Тема: «Система виявлення та захисту від DoS–атак в корпоративній мережі»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 63;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи виявлення та захисту від DoS-атак в корпоративній мережі. В роботі проаналізовано існуючі загрози і вразливості, найпоширеніші типи DoS-атак та методи захисту корпоративних мереж. Розроблено моделі загроз для наглядного розбору вразливостей, потенційних загроз та способів їх вирішення. Проведено аналіз існуючих рішень для створення системи виявлення та захисту.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі наведено загальну характеристику корпоративних мереж, проаналізовано загрози даним типам мереж та методи захисту від цих загроз. У другому розділі побудовано моделі загроз та порушників корпоративної мережі, обґрунтовано вибір технологій захисту від них. У третьому розділі наведено реалізацію системи захисту та проведено її тестування.

4. Позитивні сторони кваліфікаційної роботи полягають у аналізі загроз та ризиків, пов'язаних із DoS–атаками на корпоративні мережі, визначення їх впливу на доступність критичних сервісів; розробці моделі захисту корпоративної мережі від DoS–атак, з урахуванням специфіки типових загроз, інфраструктури та обмежень організаційного середовища; проведенні експериментального тестування моделі у симульованому середовищі, здійснення оцінки її ефективності та виявлення потенційних вразливостей для подальшої оптимізації.

5. Негативні сторони кваліфікаційної роботи: у роботі проведено оцінювання акуратності та ефективності розробленої системи, проте не наведено аналогічного порівняльного аналізу по відношенню до вже існуючих аналогів.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) ___ завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 06 » червня 2025. _____ (підпис)