ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:
« Система захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection »

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Тамодін Микола
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
Тамодін Микола
(прізвище, ім'я)

Керівник д. т. н., професор, Кожухівський Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Тамодіну Миколі
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
Система захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection
керівник кваліфікаційної роботи Кожухівський Андрій, д. т. н., професор
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
наукова та технічна література, експлуатаційна документація, нормативні;
документи, міжнародні стандарти;
рішення Imperva DDoS Protection.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження класифікацій та загроз ddos-атак.
2. Аналіз методів та засобів захисту конфіденційної інформації на базі Imperva DDoS Protection.
3. Розроблення рекомендацій щодо захисту кінцевих точок організації на базі Imperva DDoS Protection.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми DDoS-атак для сучасної онлайн-інфраструктури.	03.03.2025 р.	Викон.
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	10.03.2025 р.	Викон.
3.	Дослідження принципів роботи платформи Imperva DDoS Protection.	17.03.2025 р.	Викон.
4.	Моделювання впровадження Imperva в умовах типової компанії (DNS, IP, трафік, аналіз).	05.04.2025 р.	Викон.
5.	Оцінка ефективності фільтрації, аналіз аналітики, тестових даних, порівняння з іншими рішеннями.	20.04.2025 р.	Викон.
6.	Оформлення результатів дослідження.	20.05.2025 р.	Викон.
7.	Підготовка доповіді до захисту.	06.06.2025 р.	Викон. D

Здобувач вищої освіти _____ Микола ТАМОДІН
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача **ТАМОДІН Микола**
на тему: « Система захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection »

Актуальність: Забезпечення безпеки корпоративної онлайн-інфраструктури має ключове значення для підтримки стабільної роботи вебресурсів, API, порталів та інших сервісів. DDoS-атаки є одним із найпоширеніших методів порушення доступності систем, що може призвести до втрат даних, фінансових збитків і зниження довіри клієнтів.
Хмарні системи захисту, такі як Imperva DDoS Protection, забезпечують постійний моніторинг трафіку, виявлення та фільтрацію атак у реальному часі.
Тому тема кваліфікаційної роботи є актуальною та своєчасною в умовах зростання обсягу кіберзагроз.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту корпоративної онлайн-інфраструктури від DDoS-атак, а також визначено мету та завдання даного напрямку забезпечення інформаційної безпеки.
2. Досліджено методи та засоби захисту інфраструктури організації на базі хмарного рішення Imperva DDoS Protection.
3. Запропоновано варіант впровадження системи захисту від DDoS-атак на основі Imperva, а також надано рекомендації щодо її налаштування та використання в умовах реального бізнес-середовища.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз організації захисту від DDoS-атак на прикладі реального підприємства або з використанням фактичних даних.
2. Запропонований порядок впровадження системи Imperva DDoS Protection доцільно було б продемонструвати на конкретному кейсі компанії з реальною інфраструктурою.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач **ТАМОДІН Микола** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ТАМОДІН Микола до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: « Система захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection ».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ТАМОДІН Микола*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ТАМОДІН Микола*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ТАМОДІНА Миколи*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій Кожухівський
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ТАМОДІН Микола** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 9 рисунків, 4 таблиці, 27 джерела.

Об'єкт дослідження – корпоративна онлайн-інфраструктура підприємства.

Предмет дослідження – засоби та методи захисту онлайн-ресурсів від DDoS-атак із використанням Imperva DDoS Protection.

Мета роботи – розробити модель впровадження хмарної системи захисту від DDoS-атак із використанням Imperva та надати практичні рекомендації щодо її реалізації у типових умовах підприємства.

Методи дослідження – аналіз сучасних типів DDoS-атак, вивчення спеціалізованої літератури, технічної документації Imperva, аналіз архітектури хмарних рішень, тестування режимів фільтрації, моделювання впровадження системи захисту, оцінка ефективності.

DDoS-атаки залишаються однією з найнебезпечніших кіберзагроз для онлайн-бізнесу, адже призводять до зупинки сервісів, фінансових втрат і репутаційних втрат. У роботі проаналізовано типи DDoS-атак, їхні наслідки та ефективні методи захисту.

Особливу увагу приділено хмарному сервісу Imperva DDoS Protection, який забезпечує фільтрацію трафіку в реальному часі, автоматичне виявлення атак і підтримку захисту IP, DNS та HTTP/HTTPS без змін у інфраструктурі.

На практиці змодельовано впровадження Imperva в умовах типової компанії, реалізовано режими "always-on" і "on-demand", перевірено ефективність захисту. За результатами сформульовано рекомендації щодо застосування Imperva як надійного рішення для протидії DDoS-атакам.

Галузь використання – кібербезпека інформаційних ресурсів організації.

DDoS, IMPERVA, ХМАРНА БЕЗПЕКА, ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, ФІЛЬТРАЦІЯ ТРАФІКУ, АНАЛІТИКА, ЗАХИСТ ВІД АТАК, HTTP FLOOD, SYN FLOOD, DNS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DDoS – Distributed Denial of Service

DoS – Denial of Service

WAF – Web Application Firewall

GRE – Generic Routing Encapsulation

API – Application Programming Interface

CDN – Content Delivery Network

IP – Internet Protocol

DNS – Domain Name System

SIEM – Security Information and Event Management

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

HTTP/HTTPS – HyperText Transfer Protocol / Secure

SYN – Synchronize

ICMP – Internet Control Message Protocol

VPN – Virtual Private Network

SI – Security Infrastructure

ВСТУП

Актуальність дослідження. У сучасному світі більшість компаній працюють онлайн: вони приймають замовлення через сайти, ведуть комунікацію з клієнтами, використовують різні сервіси через Інтернет. Це зручно, швидко і вигідно. Але водночас така відкритість робить бізнес вразливим до кібератак.

Одна з найнебезпечніших загроз — це DDoS-атаки. Їх суть у тому, що зловмисники навмисно перевантажують сайт або інший онлайн-ресурс величезною кількістю запитів, поки він просто не перестає працювати. І тут уже неважливо, наскільки хороший продукт у компанії — якщо клієнт не може зайти на сайт, він просто піде до конкурента.

За останні роки такі атаки стали дуже частими. Вони б’ють не лише по великих корпораціях, а й по малих та середніх підприємствах. У деяких випадках це може бути просто тест перед більшим нападом або спосіб шантажу. Зупинка роботи навіть на годину може коштувати тисячі доларів.

Щоб захищатися, компанії шукають ефективні рішення. Одне з таких — Imperva DDoS Protection. Це хмарна система, яка не потребує складного обладнання на місці, але при цьому надає потужний захист. Вона здатна виявляти та блокувати шкідливий трафік ще до того, як він дійде до серверів компанії. Це рішення вже активно використовують у фінансовому секторі, ритейлі, державних установах та IT-бізнесі. Саме тому дослідження Imperva є не просто актуальним — воно відповідає на реальний запит часу.

Мета роботи: Показати, як можна налаштувати сучасну систему захисту від DDoS-атак на прикладі Imperva DDoS Protection, протестувати її роботу і зробити висновки щодо ефективності такого підходу для захисту онлайн-сервісів компанії.

Об’єкт дослідження: Інтернет-інфраструктура компанії, яка працює в онлайн-режимі, має вебресурси, API або інші сервіси, доступні через мережу, і, відповідно, піддається ризику DDoS-атак.

Предмет дослідження: Методи і засоби захисту онлайн-інфраструктури

компанії від DDoS-атак, зокрема можливості хмарного рішення Imperva DDoS Protection та його практичне застосування.

Завдання:

1. Зрозуміти, що таке DDoS-атаки, як вони працюють і чим небезпечні для бізнесу.
2. Дослідити, як саме побудована система захисту Imperva, які в неї функції та як вона блокує атаки.
3. Розібратися, як інтегрувати таку систему в інфраструктуру реальної компанії.
4. Провести практичне моделювання і перевірити, чи справляється Imperva з типовими сценаріями атак.
5. Сформувати прості та дієві рекомендації для компаній, які хочуть захиститися від подібних загроз.

Методи дослідження: У роботі використовувався огляд технічної документації, аналіз наукових та спеціалізованих джерел, моделювання ситуацій із кібератаками, порівняння різних засобів захисту, а також практичне тестування захисної системи на прикладі умовної IT-інфраструктури

Практичне значення: Ця робота може бути корисною для компаній, які шукають ефективний і доступний спосіб захистити свої онлайн-сервіси. Результати дослідження, а також опис впровадження Imperva, можуть слугувати інструкцією або прикладом для фахівців з IT та кібербезпеки. Головна цінність — у тому, що описаний захист реально працює, і його можна застосовувати у повсякденній діяльності компаній, не витрачаючи зайвих ресурсів на складні рішення.

1 КЛАСИФІКАЦІЯ ТА ЗАГРОЗИ DDOS-АТАК

1.1 Поняття та класифікація DDoS-атак

Атака розподіленого відмовлення в обслуговуванні (DDoS) – це навмисне перевантаження комп'ютерних ресурсів жертви (мережевого обладнання, серверів або додатків) за рахунок одночасного запуску величезного потоку запитів з багатьох джерел. Уявіть собі Інтернет як магістральну трасу: звичайний DoS-атака – це як один «сміттєвий» вантаж, що блокує проїзд, тоді як DDoS – це наче тисяча автомобілів, одночасно в'їжджають і блокують усі смуги (багато ботів зі всього світу різко надсилають трафік до цілі). Важливі моменти у визначенні DDoS:

Розподіленість: джерела атаки – тисячі або мільйони пристроїв (ботнетів), підконтрольних зловмисникам (рисунок 1.1) [1].

Координація: атака часто запускається одночасно з багатьох скомпрометованих комп'ютерів або IoT-пристроїв, роблячи її складнішою для відслідковування.

Обсяг: потужність DDoS-атаки може сягати терабіт/с, що в рази перевищує пропускну спроможність захищуваних систем.

DDoS-атаки класифікують насамперед за трьома основними рівнями моделі OSI:

Об'ємні (Volumetric) атаки: спрямовані на витіснення корисного трафіку за рахунок простої величезної кількості пакетів. Приклад – UDP-флуд (часті запроси UDP-пакетів) або ICMP-флуд (напр., «ping frenzy»). У перекладі можна сказати, що зловмисники влаштовують «цифрове цунамі», збільшуючи трафік до рівня, який не змогли б опрацювати жодні захисні пристрої.

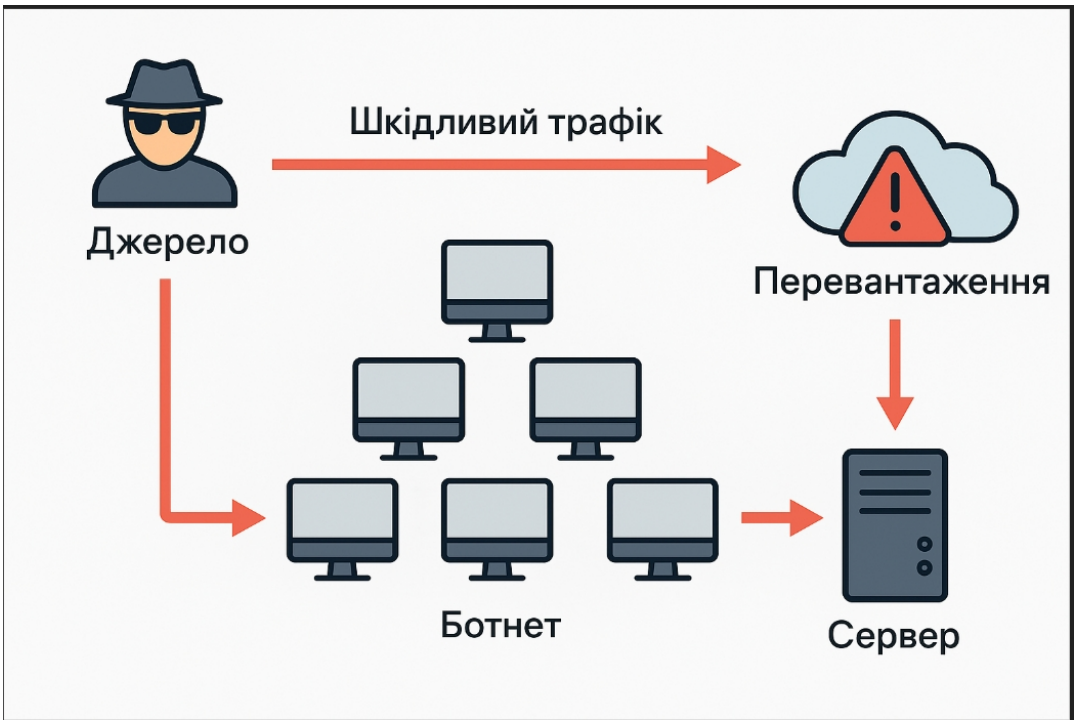

Рис. 1.1 – Схема DDoS-атаки з використанням ботнету [1]

Протокольні атаки**:** націлені на ресурси мережевого стеку (L3/L4). До них належать SYN-flood (занадто багато TCP-запитів на встановлення з'єднань), Smurf/DNS-рефлективні атаки (запити на великі мережеві сервіси, які «відлунюють» трафік назад) та «Slowloris» (медленне відкриття TCP-з'єднань, виснаження ресурсів сервера). Можна сказати, що ці атаки намагаються «забити» критичні вузли комунікацій, як якщо б великі групи людей закривали всі двері та вікна будівлі.

Прикладні (Application-Layer) атаки (L7): імітують законні запити до конкретних сервісів (наприклад, веб-серверів або баз даних), але у величезній кількості. Наприклад, HTTP-флуд (швидке надсилання запитів на веб-сторінки з реальними заголовками) або атаки на певні функції API. Це схоже на те, як ніби тисяча користувачів дружно заходять на сторінку оплати сайту і постійно оновлюють її, хоча покупців насправді дуже мало.

Крім наведеної класифікації, з'явилися нові форми DDoS: наприклад, запит-вимагачі (RDoS), коли атакуючі вимагають викуп за зупинку атаки, і persisted DDoS (тривалі атаки, що можуть тривати тижнями, із постійною зміною тактики). Загалом, мотиви DDoS-атак дуже різноманітні: від ідеологічних (хактивісти,

політичні мотиви) та конкурентної боротьби – до прямого шантажу і банального «кіберзалякування». Наприклад, під час війни в Україні зловмисники використовували DDoS як одну з форм цифрового тиску.

1.2 Основні види і приклади DDoS-атак

Розглянемо детальніше найтиповіші атаки та їх особливості:

UDP/ICMP-флуд (об’ємні атаки). Маса беззмістовних UDP- чи ICMP-пакетів «накриває» мережеві канали жертви. Приклад – класична UDP-флуд-атака до порту 80 або DNS. Уявіть, що до магазину постійно під’їжджають безліч автівок з людей без покупок: вони забивають паркування і не дають заїхати реальним клієнтам. Захист: мережеві фаєрволи можуть відразу відкидати очевидно неправомірні протокольні запити, але при екстремальних об’ємах «стискач» місця для легітимних даних швидко заповнюється.

Reflected/amplification-атаки (рефлективні). Зловмисник надсилає скеровані запити (з підробленою IP-адресою жертви) на відкриті UDP-сервіси (DNS, NTP тощо), які генерують великі відповіді. Жертва отримує послідовний «відгук» на свій «запит», хоча насправді ніякого запиту не надсилала. Це дозволяє помножити трафік за рахунок малих вхідних потоків. Наприклад, атака Memcached у лютому 2018 на GitHub досягла понад 1,3 Тбіт/с – зловмисники лише відправляли невеликі запити до багаторазово відкритих memcached-серверів, що «пролунали» гігантськими відповідями. У результаті практично увесь канал жертви завантажував «відлуннями» чужого трафіку [2].

DNS Flood (NXDOMAIN-атака). Надзвичайно активні запити до DNS-серверів із некоректними доменами (NXDOMAIN) завантажують процесори DNS, оскільки ці сервери намагаються надати відповідь (що завжди негативна). Це «пригальмовує» будь-які інші операції в DNS-інфраструктурі жертви.

SYN-flood (протокольна атака). Атака на TCP: зловмисник масово надсилає SYN-запити на сервер, але не завершує «рукостискання» (TCP handshake). Сервер

витрачає ресурси на очікування відповіді, поки його таблиці з'єднань переповнюються, і згодом перестає обробляти легітимні підключення. По суті, він «застрягає у переддвер'ї».

Slowloris (повільний DoS). Націлений на веб-сервер: зловмисник відкриває багато HTTP-з'єднань і надсилає заголовки дуже повільно (щоб вони ніколи не закінчувалися). Сервер тримає зв'язок відкритим, витрачаючи пам'ять на відкриті сесії, і швидко досягає граничної кількості обслуговуваних користувачів.

HTTP(S)-флуд (прикладні атаки). Симулюються реальні користувацькі запити (GET/POST) до веб-додатків у дуже великій кількості. Наприклад, атака на сторінки входу або пошук може виглядати як масове натискання кнопки «оновити» користувачами-ботами. Такі атаки особливо підступні тим, що вони виглядають як «законна» активність: браузерні запити, реальні сесії.

Заходи зловмисників: ботнет може складатися з комп'ютерів або «розумних» побутових приладів (IoT). Саме атака на провайдера Dyn (жовтень 2016) і стала відомою через те, що ботнет Mirai використовував тисячі «розумних» пристроїв (камери, ТВ) для перевантаження DNS-сервісу [2]. У підсумку падали Netflix, Amazon, Twitter та багато інших сайтів, оскільки клієнти Dyn не могли вирішити доменні імена.

Таким чином, DDoS-атаки бувають різних видів – від «грубих» об'ємних затоплень до витончених бот-атак на рівні додатків. Усі вони по-своєму ускладнюють роботу сервісів.

Рис. 1.2. Розподіл DDoS-атак у 4-му кварталі 2024 року: 49% були мережевими (L3/4), 51% – HTTP-атаками (L7).[2]

1.3 Вплив DDoS-атак на бізнес-процеси

Наслідки DDoS-атаки для компанії набагато гірші, ніж просте збільшення мережевого трафіку. Це може бути справжньою «цифровою катастрофою» з фінансовими, технічними та іміджевими втратами. Основні ризики для бізнесу:

Фінансові втрати: простої систем призводять до прямих збитків. Згідно з дослідженням Radware, кожна хвилина простою через застосункову DDoS-атаку обходиться організації в середньому приблизно в $6,130. Навіть кілька годин непрацюючого сервісу можуть коштувати сотні тисяч доларів.

Втрата продуктивності: атаковані сервіси (наприклад, онлайн-магазини, платіжні системи, корпоративні портали) відключаються або сповільнюються. Критичні бізнес-функції – обробка замовлень, оплати, комунікації – просто зупиняються. Це може призвести до зриву контрактних зобов’язань і штрафів.

Додаткові витрати на реагування: щоб відновитися, необхідні термінові інвестиції у додаткові ресурси. Компанії змушені орендувати або купувати нове обладнання, залучати експертів з кібербезпеки, оплачувати послуги CDN чи

хмарних сервісів.

Репутаційні ризики: інформація про DDoS-атаку швидко розходиться медіа і соціальними мережами. Клієнти бачать, що сервіс не працює,починаютьсумніватисяунадійностіпровайдера. Втрата довіри може виявитися довготривалою: за статистикою, після серйозних збоїв 30–40% користувачів віддають перевагу конкурентам. Особливо під ударом – банки, e-commerce та сервіси з персональними даними. Збої під час масових розпродажів чи підключення нових послуг можуть сприйматися як «провал» і стати новиною.

Супутні інциденти: атака може слугувати прикриттям для інших атак (APT), розповсюдження шкідливого ПЗ чи викрадення даних. Наприклад, поки IT-відділ усуває наслідки DDoS, зловмисники можуть паралельно використовувати цей час для кібершпигунства або заглибленого проникнення.

Ці наслідки створюють величезний тиск на бізнес. З одного боку, треба забезпечувати безперебійну роботу (SLA 99,9% та вище), з іншого – готовитися до непередбачених катастроф. Не дивно, що дедалі більше організацій вважають захист від DDoS пріоритетом: 31% [3] компаній у світі зазнають DDoS-атак щотижня, а сукупні збитки по підприємствах зростають з кожним роком. У сучасних реаліях навіть хвилинна відсутність сервісу може поставити під сумнів всю бізнес-модель.

Як видно з рисунка 1.3, у 2023 році більшість DDoS-атак були спрямовані на розвинуті регіони — зокрема, регіон EMEA (Європа, Близький Схід і Африка) зазнав близько 57% атак, тоді як Північна Америка — близько 38% [3]. Такий розподіл підтверджує високий ризик для інфраструктури компаній, що працюють у цих регіонах.

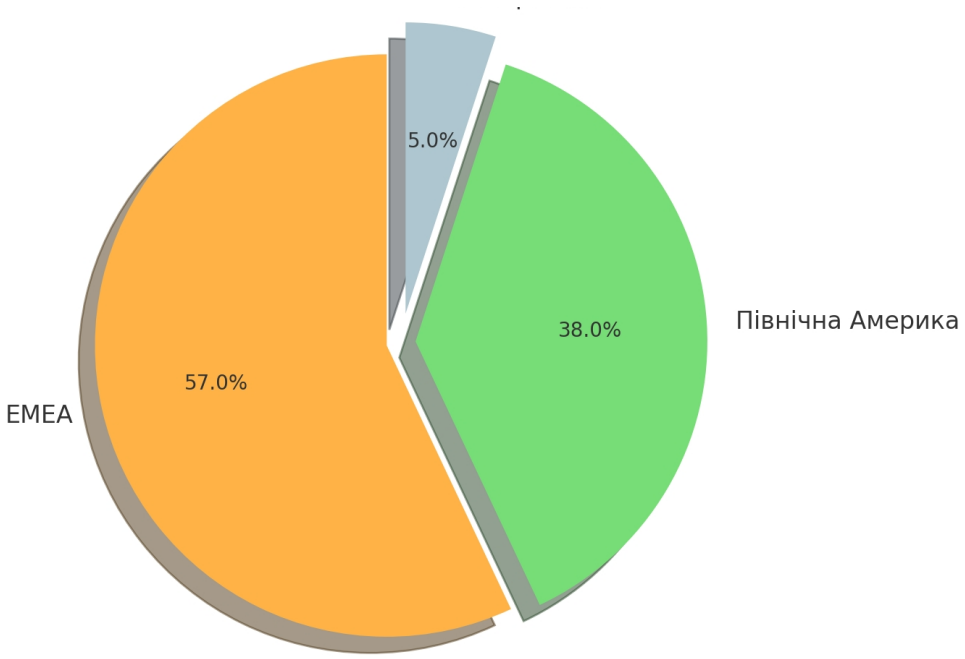

Рис. 1.3. Географічний розподіл зафіксованих DDoS-атак (2023): близько 57% атак націлені на EMEA-регіон і ~38% – на Північну Америку [3].

1.4 Методи захисту від DDoS-атак

Таблиця 1.1.

Порівняльна таблиця методів захисту від DDoS-атак

Метод захисту	Переваги	Недоліки
Фаєрвол	Проста фільтрація портів і IP	Не витримує потужних DDoS
IDS/IPS	Глибокий аналіз, сигнатури	Потребує ресурсів, можна обійти
WAF	Захист HTTP-рівня, правила	Вразливий до об'ємних атак
Rate limiting	Простота, швидке налаштування	Не працює проти ботнетів
Imperva (хмара)	Масштабність, ML, глобальна мережа	Залежність від провайдера, оплата

Щоб протидіяти DDoS, застосовують багато рівнів захисту: від традиційних мережевих фільтрів до хмарних «очисних центрів». Розглянемо ключові підходи:

Локальні мережеві фаєрволи (Firewall): «перший рубіж» оборони. Фаєрволи відсіюють трафік за IP-адресами, портами, протоколами. Наприклад, можна одразу блокувати весь трафік із відомих зловмисних адрес чи фільтрувати нестандартні порти. Однак при масштабній DDoS-атакі сам фаєрвол може не витримати навантаження і обвалитися: якщо через пристрій надходить потокове цунамі, воно перевищує його пропускну здатність. Фаєрвол покликаний ловити відомі атаки на початковому етапі, але сам по собі він рідко справляється з надпотужним об'ємним трафіком.

IDS/IPS (системи виявлення і запобігання вторгненням): аналізують мережевий трафік у режимі реального часу, шукаючи сигнатури відомих атак чи аномальну поведінку. Вони додають глибший рівень розбору пакетів, можуть зупиняти зафіксовані патерни DDoS. Проте IDS/IPS часто витрачають багато обчислювальної потужності: при масових атаках уся черга трафіку йде на аналіз, що може спричинити затримки (таблиця 1.1). Тому IDS/IPS добре доповнюють захист (наприклад, на рівні проміжних шлюзів), але зазвичай не розраховані на терабітні швидкості.

Лімітування частоти запитів (Rate Limiting): на рівні серверів або API визначають, скільки запитів у секунду може надійти від одного джерела чи на певний ресурс. Наприклад, вебсервер може відсікати понад 100 запитів з одного IP на хвилину. Це захищає від ботів, що намагаються «гризти» сайт багаторазовими однаковими запитами. Однак такий механізм не справляється з атаками з великої кількості IP – ботнету. І взагалі, занадто жорсткий ліміт може заважати реальним користувачам (наприклад, коли багато людей користуються одним проксі чи національною IP-маскою). Налаштування лімітів потребує балансу між безпекою та юзер- досвідом.

Веб-фаєрвол (WAF): програмний фільтр на рівні HTTP/HTTPS. WAF аналізує вміст веб-запитів, захищаючи від атак типу SQL-ін'єкцій, XSS та схожих. В

контексті DDoS WAF може виявляти незвичні шаблони запитів (наприклад, дуже часті повторення одного URL з однаковими параметрами) і блокувати підозрілих клієнтів. Проте WAF розраховано на деталізоване розбір поведінки і зазвичай не обробляє величезних обсягів. Якщо сервер отримує сотні тисяч HTTP-запитів на секунду, WAF-система може не встигати їх аналізувати. Тому його частіше використовують в поєднанні з масштабованим фільтром.

Хмарні сервіси захисту (Cloud Scrubbing): один із найефективніших підходів сьогодні. Припустимо, компанія під'єднується до глобальної мережі захисту (сервісів типу Imperva, Cloudflare, Akamai, AWS Shield тощо). У разі підозри на атаку весь трафік перенаправляється до хмарної інфраструктури провайдера (через BGP анонси, DNS-заміну, GRE/VPN тунелі). Там стоять спеціалізовані «скраббери» – гігантські розподілені дата-центри з великими запасами пропускної здатності. Наприклад, мережа Imperva наразі вміщує більше 10 Тбіт/с потужності та обробляє до 65 млрд пакетів/с. У хмарі трафік «очищається» за допомогою різних алгоритмів: від простих чорних списків IP і сигнатур до машинного навчання, що вчиться виявляти аномальні патерни. Після очищення до сервера компанії доходить лише «чистий» легітимний трафік.

Додаткові прийоми: є й інші способи зменшити вплив DDoS. CDN (Content Delivery Network) зазвичай кешує статичні ресурси (зображення, сторінки) в багатьох локаціях, що автоматично розвантажує основний сервер – при атаці завантаження переходить до CDN. Проте у надпотужній DDoS навіть CDH може вичерпати свої ресурси (відомий випадок атаки на Dyn у 2016, коли були перевантажені сервіси DNS). Чорнолісування (Blackholing): за цією методикою весь трафік на певну IP-адресу просто вказується в «чорну діру» — тобто по суті зникає в Інтернеті. Зловмисницький трафік вимикається цілком, але разом з ним і сервіс стає недоступним для всіх. Тому таке рішення – крайній захід, коли іншого виходу нема.

Ідеальний захист – це комплексний підхід. Мережеві фаєрволи і IDS/IPS аналізують та фільтрують більшість простих атак на кроці відразу. WAF відсікає

складні “запитні” загрози на рівні застосунків. А при дуже великому напливі трафіку маршрутизатори мають можливість перенаправити підозрілий трафік у хмарний скраббінг центр (наприклад, Imperva). Таким чином кожен рівень захисту «підстраховує» інші – локальні засоби зберігають ресурс для нормальних користувачів, а хмара поглинає екстремальні атаки. Приклад використання: якщо раптово на сайт приходить потужний сплеск, система може автоматично замінити основну IP-адресу на захищену адресну в мережі Imperva, направляючи весь трафік через скраббери; після закінчення загрози – повернути первісну адресу. Це забезпечує баланс між продуктивністю і безпекою.

1.5 Переваги комплексного захисту

В сучасних умовах одиничні рішення не гарантують безпеки. Ефективна оборона від DDoS вимагає шарування та поєднання методів. Класична стратегія виглядає так:

Always-on (перший рівень): завжди активовані базові фільтри на рівні мережі (L3/L4) [1]. Вони автоматично відсіюють очевидні загрози та плямові потоки трафіку (за чорними/білими списками IP, порогами запитів тощо). Таким чином «захоплюються» перші і найпростішої атаки.

On-demand / second level (другий рівень): у разі підозрілих аномалій активується детальна перевірка на рівні застосунків (L7). Використовуються WAF-інструменти та поведінкова аналітика – наприклад, при збільшенні інтенсивності запитів система починає викликати для клієнтів CAPTCHA чи JavaScript-челендж. Реальні люди проходять ці перевірки, отримуючи «квиток» (cookie) для подальшого трафіку, а боти – відсікаються. Одночасно застосовуються алгоритми ML, що навчилися відокремлювати легітимні патерни від бот-атак.

Хмарне блокування (третій рівень): якщо «перше інфільтрування» не справляється (наприклад, трафік перевищує налаштовані пороги), підозрілий потік динамічно перенаправляється до хмарної мережі Imperva. Там він проходить «глибоке скраббування»: аналізується послідовність запитів, відключаються

ботнети, застосовуються додаткові тести. У хмарі використовується великий обсяг обчислень і пропускної спроможності (сотні Гбіт/с) – що гарантує, що «шторм» не дійде до локальних серверів.

Цей багаторівневий підхід дозволяє налаштувати оборону під будь-яку інфраструктуру. З одного боку, постійний моніторинг забезпечує превентивний захист, з іншого – наявність on-demand режиму дозволяє не витрачати ресурси даремно, включаючи потужні фільтри лише при реальній небезпеці. Наприклад, можна налаштувати так: за умов нормальної роботи трафік обробляється на всіх рівнях усередині мережі компанії, а при підвищенні ризику – комутація на захищений канал із Imperva. Після стабілізації трафіку – повернення на початкову схему. Таким чином, об’єднання місцевих і глобальних фільтрів створює «сітку безпеки», де кожен шар підтримує інший.

1.6 Висновки до розділу

Отже, теоретична база показує: DDoS-атака – це багатогранна кіберзагроза, яка здатна миттєво «паралізувати» будь-який бізнес. За статистикою, майже третина компаній щотижня стикається з такими атаками, а вартість простою обчислюється тисячами доларів за хвилину. Ключові висновки:

Миттєве збільшення ризиків: DDoS легко виводить із ладу критичні сервіси, адже в атаці можуть брати участь сотні тисяч пристроїв. Наслідки відчуваються одразу – від фізичного перевантаження мережі до збоїв у бізнес-процесах.

Різноманіття тактик: аналіз основних типів атак підтверджує їхню різноманітність. Об’ємні атаки, складні протокольні комбінації та витончені прикладні флуди можуть йти одночасно, маскуючись під звичайний трафік. Саме тому важливо розуміти кожен рівень DDoS-атаки і бути готовим оборонятися «на всіх фронтах».

Необхідність багатошарового захисту: поодинокі рішення (лише фаєрвол або тільки WAF) часто не справляються. Для стійкості потрібно комбінувати локальні

фільтри з хмарними сервісами очищення. Класична схема полягає у поєднанні: мережеві фільтри та локальні WAF відсікають базові атаки, а масштабний аномальний трафік спрямовується через глобальну мережу захисту. Такий комплексний підхід дозволяє залишати основні сервіси доступними, навіть коли на них здійснюється потужна атака.

Таким чином, ефективний захист бізнесу вимагає поєднання різних засобів кібербезпеки. Наступні розділи детальніше розглянуть конкретну систему Imperva DDoS Protection та практичне її застосування в корпоративній мережі.

2 СИСТЕМА ЗАХИСТУ ВІД DDOS IMPERVA: АРХІТЕКТУРА ТА МОЖЛИВОСТІ

2.1 Архітектура та компоненти Imperva DDoS Protection

Існує низка платформ, які надають послуги захисту від DDoS-атак, серед яких найбільш поширеними є Imperva, Cloudflare, Radware та Arbor Networks. У таблиці 2.2. наведено порівняння основних характеристик цих систем.

Imperva DDoS Protection – це хмарно-апаратний сервіс, призначений для цілодобового захисту веб-ресурсів, мережевих інфраструктур і DNS. Його архітектура (дивитись рис. 2.1) [4] спирається на глобальну мережу дата-центрів (Points of Presence, PoP), розміщених у різних частинах світу. Коли клієнт активує захист, увесь його трафік або окремі IP-адреси спрямовуються в один із PoP Imperva, де виконується фільтрація та очищення від атакуючих пакетів, після чого трафік передається далі в мережу клієнта.

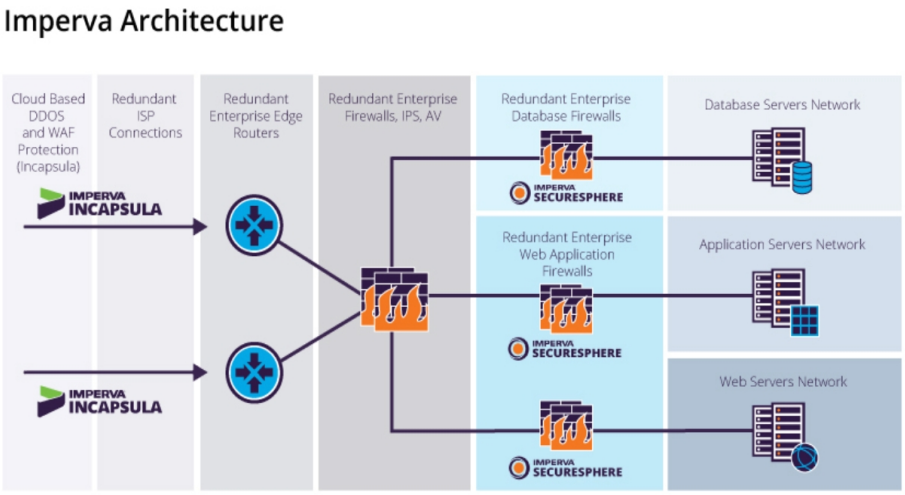

Рис. 2.1. Архітектура захисту від DDoS-атак за допомогою Imperva [4].

Таблиця 2.1.

Основні компоненти Imperva DDoS Protection

Компонент	Призначення
Глобальна мережа PoP	Розподілена мережа дата-центрів Imperva, яка приймає трафік від користувачів з усього світу, фільтрує його та запобігає перевантаженню інфраструктури.
Тунелювання і маршрутизація	GRE-тунелі та BGP-анонси, які дозволяють перенаправляти увесь вхідний трафік через захищену мережу Imperva для фільтрації у режимі «always-on» або «on-demand».
DDoS Rule Engine	Інтелектуальна система виявлення загроз. Аналізує трафік у реальному часі за шаблонами атак і нетиповою поведінкою, виявляючи потенційно шкідливі дії.
Веб-фаєрвол (WAF)	Захищає вебдодатки від типових загроз (SQL-ін’єкції, XSS, бот-атаки). Аналізує запити та блокує небезпечні дії до того, як вони досягнуть серверу.
Панель управління і аналітика	Центральна консоль для адміністрування, налаштувань безпеки, перегляду логів, графіків трафіку й отримання звітів про атаки в режимі реального часу.

Усі компоненти тісно взаємодіють між собою. Наприклад, при активації Always-On-сервісу DNS клієнта вказує на адреси Imperva, і весь трафік спочатку йде в мережу PoP. У випадку On-Demand під час атаки компанія відправляє BGP-

анонс в Imperva, після чого весь трафік перенаправляється для очищення. Imperva підтримує необмежені об’єми трафіку – до ~9 Тбіт/с і 65 млн пакетів/сек. У кожному PoP виконується повний стек захисту (фільтрація DDoS, WAF, захист API і антибот-рішення).

2.2 Принципи фільтрації трафіку в Imperva

Imperva застосовує багаторівневу стратегію. Основні кроки фільтрації такі:

Маршрутизація трафіку. Весь вхідний трафік перенаправляється у мережу Imperva (через DNS-перенаправлення або тунелі).

Фільтрація мережевих атак (L3/L4). На мережевому рівні Imperva відсіює підозрілі пакети (надлишкова кількість SYN, фрагментовані пакети, відображені запити). IP, що перевищують встановлені ліміти, заносяться в чорні списки.

Захист прикладного рівня (L7). WAF перевіряє структуру HTTP/HTTPS-запитів. Якщо запит виглядає як типовий бот (наприклад, занадто багато запитів на одну сторінку) або містить шкідливі характеристики, він блокується.

Адаптивні правила. Imperva використовує алгоритми машинного навчання. Наприклад, Adaptive Threshold автоматично порівнює поточний трафік із історичними моделями і підлаштовує ліміти. Також імплементовано систему тестів (напр., CAPTCHA) для підозрілих користувачів.

Моніторинг та логування. Усі дії фіксуються: система генерує логи атак, статистику по IP, геолокації та патернах трафіку. Адміністратор бачить панель з графіками та таблицями в реальному часі.

Такий підхід забезпечує мінімальний вплив на легітимних користувачів і максимальну ефективність протидії атакам. Imperva надає гарантію митигування протягом 3 секунд – тобто після початку атаки захист включається майже миттєво і відновлює нормальну роботу, практично не порушуючи сервісу.

2.3 Переваги Imperva над традиційними рішеннями

На відміну від локальних фаєрволів і апаратних засобів захисту, Imperva пропонує глобальну, масштабовану архітектуру з потужними ресурсами. Головні переваги Imperva:

Максимальна пропускна здатність. Мережа Imperva обробляє атаки до ~9 Тбіт/с (таблиця 2.2), тобто блокує навіть найпотужніші DDoS. Жодне локальне обладнання не витримає таких обсягів.

Глобальне покриття. Imperva має розподілені дата-центри по всьому світу, кожен з яких оснащений повним стеком фільтрації. Запуск Always-On означає, що будь-який користувач підключається до найближчого PoP, а всі атаки розподіляються і локалізуються.

Інтеграція з веб-захистом. Крім чистого DDoS-фільтра, Imperva включає захист веб-додатків (WAF), захист API та антибот-функції. Всі ці сервіси об’єднані в єдине рішення, що полегшує управління безпекою.

Швидке розгортання і зручність. Підключення Imperva не вимагає закупівлі нового обладнання – зазвичай досить змінити налаштування DNS чи маршрутизації. Наприклад, клієнти відзначають: розгортання Imperva «легко налаштувати, воно зайняло лише тиждень». Система «transparent» – відвідувачі сайту майже не бачать перевірок чи додаткових затримок.

Розширена аналітика (Attack Analytics). Imperva забезпечує глибоке логування та кореляцію подій. Адміністратор отримує детальну інформацію про джерела атак і їхні характеристики, що скорочує час розслідування інцидентів.

Підтримка 24/7. Imperva надає підтримку у цілодобовому режимі. Якщо атака вражає критичні системи, команда сервісу оперативно працює над її нейтралізацією (аналогово центру реагування Radware ERT).

Таким чином, Imperva радше пропонує стратегію «захисту на периметрі + у хмарі», натомість традиційні системи (локальні фаєрволи/IDS/IPS) виконують роль першого сигналу. Великі компанії з критичними онлайн-сервісами (банківська справа, e-commerce, держструктури) віддають перевагу Imperva саме через ці його

переваги.

Нижче наведено порівняльну таблицю Imperva DDoS Protection з іншими популярними рішеннями (Cloudflare, Radware)

Таблиця 2.2.

Порівняння Imperva з іншими платформами захисту

Платформа	Модель розгортання	Основні можливості / переваги
Imperva DDoS Protection	Хмарно-апаратний сервіс (глобальна мережа PoP). Працює у режимі *always-on* або *on-demand* (GRE/BGP).	Захист від атак рівнів L3–L7 (мережа, веб, DNS, IP). Пропускна здатність до 9 Тбіт/с і 65 млн пакетів/сек. Інтегрований WAF, захист API, антибот-фільтрація. SLA — 3 секунди. Детальна аналітика атак (Attack Analytics).
Cloudflare	Хмарне рішення на основі Anycast CDN. Доступні як безкоштовний, так і платні тарифи.	Дуже широка мережа (>100 Тбіт/с). Постійний захист HTTP/HTTPS, вбудований WAF і система захисту від ботів. Безкоштовний рівень підходить для базового захисту. Підтримка нестандартних сервісів через Cloudflare Spectrum.
Radware	Гібридна модель: апаратні пристрої клієнта + хмарні сервіси. Підтримує режими *always-on*, *on-demand*, керований захист.	Захищає L3–L7, включаючи SSL-атаки (є можливість SSL-вивантаження). Фокус на виявлення атак нульового дня, є команда швидкого реагування 24/7. Рішення для великих підприємств і телеком-операторів.

		Єдина консоль для керування.

2.4 Приклади використання Imperva DDoS Protection

Imperva застосовується в різних галузях для захисту бізнес-критичних сервісів. Декілька яскравих прикладів:

E-commerce: 13 листопада 2023 року Imperva зафіксувала та нейтралізувала рекордну DDoS-атаку на індонезійський онлайн-маркетплейс, яка досягла піку в 2,3 млн HTTP-запитів на секунду. Ця атака була класичного прикладного типу і мала змусити сайт працювати повільно чи впасти. Проте фільтрація Imperva (глобально розподіленою мережею та WAF) дозволила бізнесу залишатися доступним у піковий момент, що зберегло прибутки та довіру клієнтів.

Банківська сфера: фінансові установи є привабливою ціллю для зловмисників, адже відмова у доступі до онлайн-банкінгу може спричинити великі збитки. Наприклад, у період ескалації конфлікту 2023 року 54% атак Imperva фіксувала на державний та фінансовий сектор. Найбільша з них вдарила по ізраїльському урядовому порталу – пік зловмисного трафіку склав понад 1 млн RPS. Всі ці атаки були успішно погашені Imperva, і сервіси залишались функціональними. Аналогічні заходи захисту застосовують банки, щоб захиститися від періодичних хвиль DDoS на їхні сайти.

Державні установи: веб-портали уряду та громадських служб містять багато відкритої інформації й часто стають цілями «кібервійськових» операцій. Imperva захищає державні ресурси (портали інформації, електронні сервіси) від DDoS-атак, що можуть бути частиною інформаційних воєн. Наприклад, у війнах XXI століття спостерігалося застосування DDoS проти урядових сайтів, але завдяки Imperva такі атаки не призводили до тривалого простою.

Інші галузі: Imperva DDoS Protection також впроваджується в енергетиці, охороні здоров’я, ритейлі, телекомі та інших секторах, де критичні сервіси не повинні припиняти роботу. Наприклад, великі e-commerce компанії, SaaS-

провайдери та дата-центри використовують Imperva для захисту своїх API і сайтів від пікових навантажень.

Отже, Imperva DDoS Protection доводить свою універсальність: рішення адаптується під потреби e-commerce, фінансових установ, держорганів та інших підприємств, забезпечуючи багаторівневий захист.

2.5 Висновки до розділу

Завдяки поєднанню глобальної інфраструктури і розумної фільтрації, Imperva DDoS Protection демонструє високу ефективність. Її можливості дозволяють успішно протистояти як традиційним флуд-атакам, так і складним мультивекторним загрозам. Порівняння з іншими платформами показує, що Imperva забезпечує дуже швидке реагування (SLA 3 секунди) і комплексну безпеку на всіх рівнях (L3–L7). Аналіз практичних кейсів підтверджує, що в екстремальних умовах (наприклад, 2,3 млн запитів/с у роздрібній торгівлі) Imperva справляється з навантаженням, зберігаючи доступність послуг. Таким чином, рішення Imperva повністю відповідає сучасним вимогам бізнесу до безперервності сервісів та швидкості захисту від новітніх DDoS-атак

3 ВПРОВАДЖЕННЯ IMPERVA DDOS PROTECTION НА ПРИКЛАДІ УМОВНОЇ КОМПАНІЇ

3.1 Структура умовної компанії та її потреби

Розглянемо уявну середню IT-компанію, щоб ілюструвати проєкт з DDoS-захисту. Компанія має два основні майданчики – ДЦ1 (основний дата-центр) та ДЦ2 (резервний). У ДЦ1 розгорнуті бізнес-критичні сервіси: публічний веб-сайт фірми, клієнтський портал, внутрішні ERP/CRM, API для мобільних додатків. ДЦ2 слугує для копіювання даних та аварійного відновлення: там дублюються бази даних і є резервна копія веб-сервера. Окрім того, компанія має віддалений офіс, співробітники якого підключаються через захищені VPN-канали. Мережа побудована за принципом гібриду: низка потужних серверів і віртуальних машин (VMware-кластери), балансувальники навантаження на веб-шари, кластер баз даних.

Ключові цінності бізнесу: доступність сервісів та безперервність роботи. Компанія обслуговує критичних клієнтів, тому в SLA позначено ≥99,9% uptime. Окрім цього, бізнес має витримувати очікувані пікові навантаження – наприклад, під час презентації нового продукту або масового розсилання новин. Також компанія обробляє конфіденційні дані, тож їй потрібно відповідати стандартам безпеки (наприклад, ISO 27001). Найважливіше: клієнтам критично, щоб сервіси були завжди під рукою. Будь-який тривалий збій негайно позначиться на грошах та репутації.

Поточні загрози: раніше періоди високої активності викликані в основному легітимними причинами (сезонні коливання, рекламні акції). Але з часом з’являються й реальні кібератаки. Перші спроби DDoS змусили директорів задуматися: «А що, якщо завтра замість звичайного трафіку прийде шторм?». І дійсно, кількість DDoS-атак у регіоні росте (багато конкурентів скаржаться на атаки). Бачачи це, IT-служба сформулювала вимоги до захисту:

У рамках моделювання також було враховано ситуацію з потенційною DDoS-атакою на бізнес-критичні сервіси. На рисунку 3.1 [5] представлено типовий стан мережі в момент атаки без активного захисту. Видно, що весь вхідний трафік, включаючи шкідливий, проходить без обробки, що створює надмірне навантаження на веб-сервери компанії.

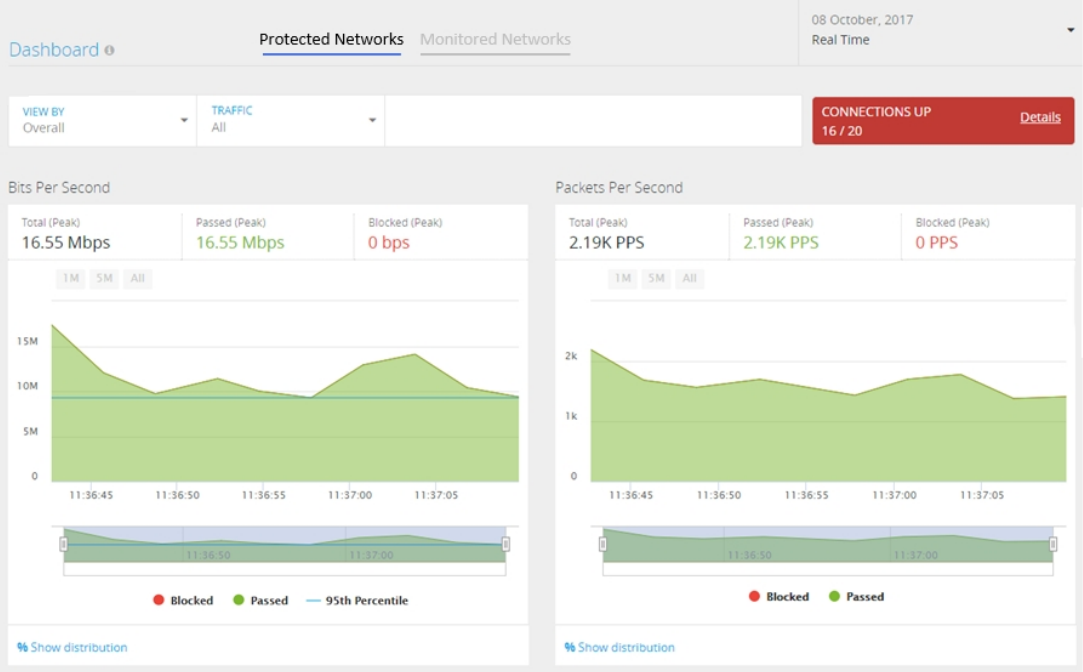

Рис. 3.1. – Панель моніторингу Imperva: стан мережі під час атаки (трафік проходить без блокувань)[5].

Після активації захисту Imperva система почала автоматично фільтрувати шкідливий трафік. На рисунку 3.2 [6] показано стан мережі після нейтралізації атаки: видно стабілізацію трафіку, значну кількість заблокованих пакетів та нормальну пропускну здатність для легітимних запитів.

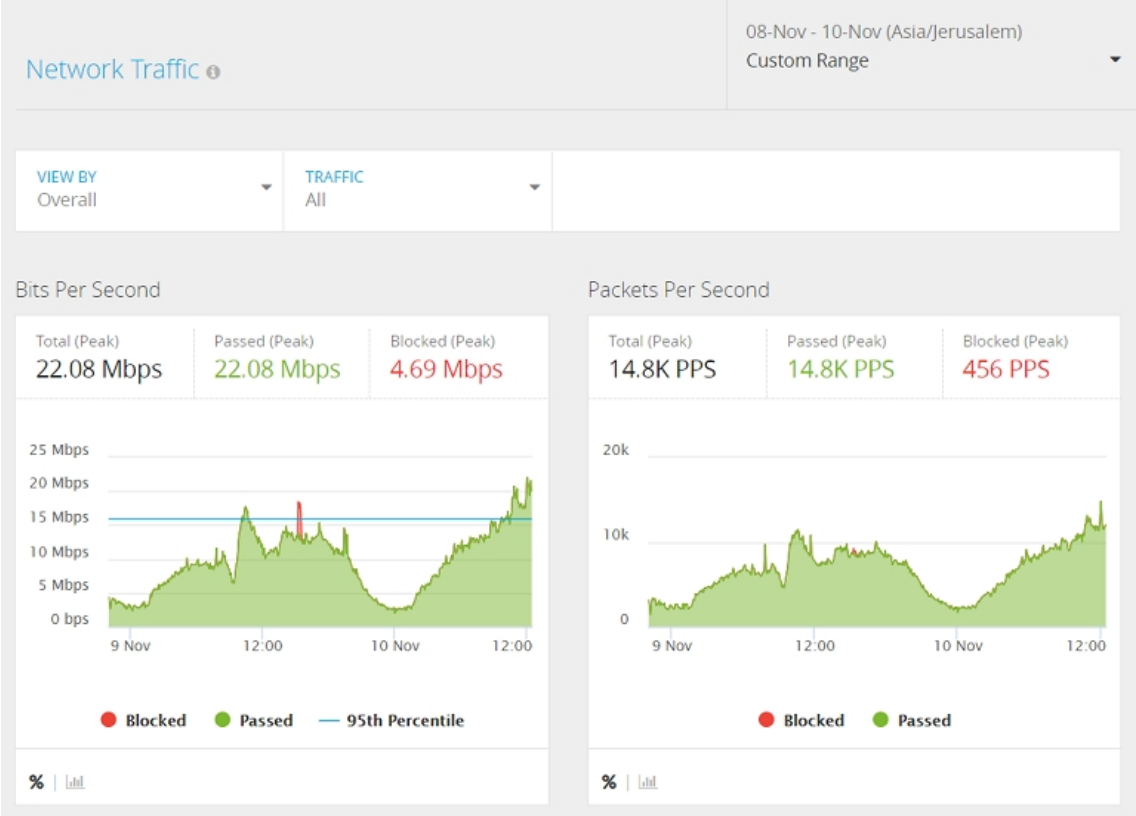

Рис. 3.2. – Стан мережі після нейтралізації DDoS-атаки системою Imperva [6].

Мінімальні зміни в архітектурі: бажано, щоб новий захист «вписався» у існуючу мережу без глобальних реконфігурацій.

Масштабованість: рішення має автоматично підтримувати обробку будь-яких ударів трафіку (від регулярних до рекордних).

Непомітність для користувача: сервіс не має «гальмувати» під час атаки. У ідеалі користувачі не повинні відчувати втручання захисту (жодних додаткових CAPTCHA чи довгих очікувань).

Моніторинг і управління: потрібна зручна консоль для налаштувань, щоби розробники могли оперативно коригувати фільтри відповідно до потреб бізнесу.

Гібридність: компанія хотіла, щоби частина захисту була в «хмарі», а частина – локально (без великих витрат на нове обладнання).

Виходячи з цього, було ухвалене рішення впровадити Imperva DDoS Protection. Вона повністю відповідала вимогам: прихована від користувача («прозора»), гнучко масштабується завдяки глобальній хмарі, і просто інтегрується з існуючими мережевими протоколами.

3.2 Процес впровадження Imperva в компанії

Впровадження Imperva відбулося у кілька етапів, які забезпечили плавний перехід:

*Аналіз та проєктування***.** На початку команда IT спільно з консультантами Imperva провела аудит інфраструктури: визначили, які сервіси виходять у мережу, які IP-адреси використовує компанія, і які мають бути «захищені». Було прийняте рішення підключити Imperva у режимі *Always-On* для найважливіших сервісів – це означало, що весь вхідний трафік на ці сервіси постійно проходитиме через хмару Imperva. Для кожної такої служби призначили «захищену» публічну IP-адресу Imperva. Паралельно обговорили режими резервування трафіку: вирішили використовувати BGP анонс резервних мережевих маршрутів у разі пік-атаки, а також реалізувати до ДЦ GRE-тунель як резервну опцію.

Налаштування мережевої маршрутизації. Щоб перенаправляти трафік, в системі DNS компанії оновили записи: замінили оригінальні A-записи публічних сервісів на IP-адреси Imperva (з дуже малим TTL, щоби зміни швидко розійшлися). Також налаштували BGP-анонс: у разі атаки система передавала інформацію провайдерам, що весь трафік до даного блоку адрес має йти через мережу Imperva. Додатково встановили GRE-тунель між мережевим обладнанням у основному дата-центрі та Imperva. Цей тунель був запасним каналом: у разі критичного навантаження трафік міг «падати» на нього автоматично.

Конфігурація політик захисту. Інженери підготували детальні профілі трафіку компанії: встановили базові пороги навантаження, що вважати нормальним. Потім створили списки «білих» IP (довірені партнери, корпоративні мережі) та «чорних» (відомі зловмисники за попередніми інцидентами). Далі вказали, які дії виконувати при сплесках: наприклад, при різкому зростанні HTTP-запитів понад певного ліміту включати JavaScript-аналіз і CAPTCHA для нових сесій. Було протестовано різні схеми: коли система бачить перевищення порогу, вона миттєво розпочинає глибоку фільтрацію. Також активували моніторинг на

нетипові порти і сканування.

Для забезпечення ефективного захисту в різних сценаріях атаки в Imperva використовуються налаштовані політики безпеки. До них входять обмеження за частотою запитів, активація CAPTCHA для підозрілих ботів, географічне блокування та специфічні WAF-правила для типових векторів атак. На рисунку 3.3 [7] наведено приклад активних політик безпеки в інтерфейсі Imperva.

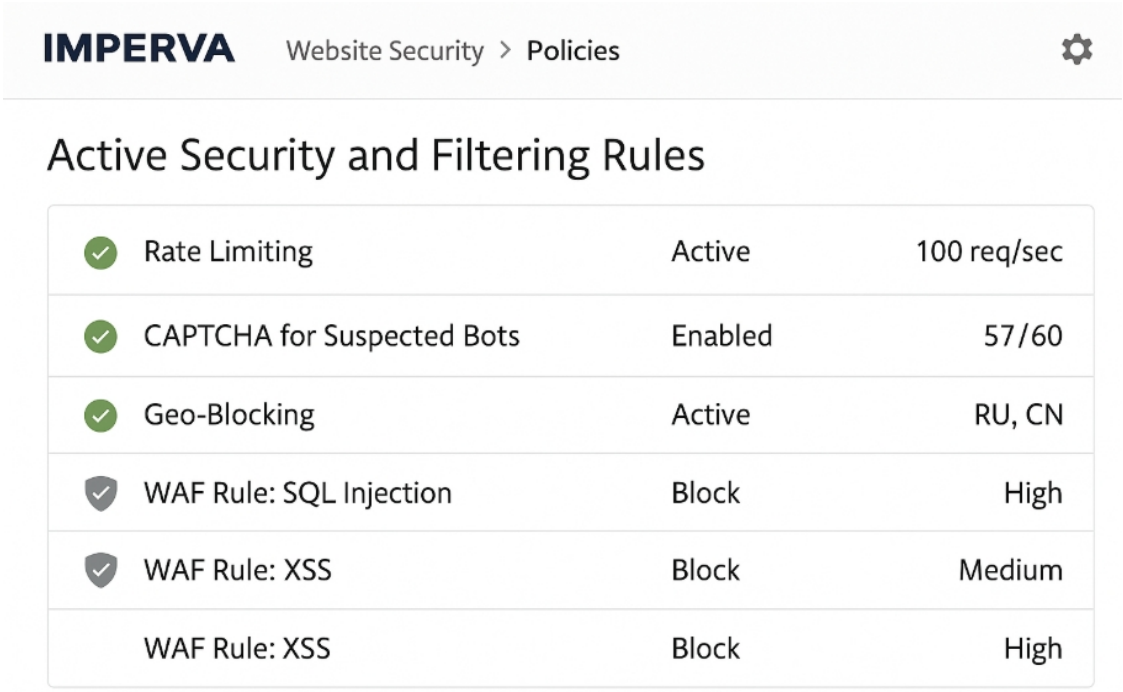

Рис. 3.3. – Активні правила фільтрації та захисту від DDoS в системі Imperva [7].

Тестування: перед запуском в бойовому режимі провели симуляцію DDoS-атак. За допомогою інструментів генерували «штормові» потоки UDP, TCP і HTTP. Наприклад, імітували UDP-флуд із масштабом до 5–6 Гбіт/с: система Imperva показала себе добре – майже весь цей трафік спрямувався у «скраббери», а на локальну мережу дійшло лише кілька сотень Мбіт/с реальних запитів. У відповідь скрапбер автоматично збільшував ресурси хмари і безшумно підчищав шкідливі пакети. Потім перевірили «тихі» атаки (Slowloris): WAF виявив багато частих TCP-запитів без повної завершальності й швидко заблокував їх. На основі цих тестів

оптимально відпрацювали порогові значення та поведінкові правила.

Введення в експлуатацію: на фінальному етапі почали пускати захист «у живий режим». Спочатку включили Imperva поступово – щоб уникнути стрибків обриву трафіку. Протягом перших хвилин фільтрація активувалась плавно, перевіряючи стабільність. Паралельно провели навчання IT-персоналу: показали, як користуватися Imperva-консоллю, читати логи та виконувати процедури реагування. Оновили внутрішню документацію: прописали план дій при підозрі на DDoS, додали контактні канали з підтримкою Imperva. Після декількох днів моніторингу, коли очевидних проблем не виникло, перевели захист у повністю «включений» стан. Тепер весь вхідний трафік компанії проходить через Imperva – відтепер сервіс завжди під захистом, навіть якщо зловмисники спробують атаку.

Загалом, весь процес – від початкового аналізу до активної експлуатації – тривав декілька тижнів. Важливо, що не виникло жодних критичних проблем. Використовуючи стандартні протоколи (BGP, DNS, VPN), інженери швидко інтегрували рішення, і гнучкі налаштування дозволили врахувати індивідуальні особливості компанії. Водночас захист виявився абсолютно прозорим для клієнтів: для них сайт продовжував працювати так само, як і раніше. Цей досвід показав: навіть суттєве дообладнання мережі новими компонентами може пройти плавно, не порушуючи бізнес-процеси.

3.3 Аналітика та моніторинг після впровадження

Після запуску системи важливо було налагодити постійний моніторинг і аналітику. Панель керування Imperva (доступна через браузер) надає широкий спектр інформації в реальному часі.

Моніторинг трафіку в реальному часі: на головному дашборді відображаються графіки загального об’єму вхідного трафіку, а також окремо обсяг легітимного і заблокованого (малий та виділений ділянками графіка). Кількість запитів і швидкість їх обробки видно щохвилини. Наприклад, якщо ввечері трафік

зростає в 3 рази (через онлайн-продажі), адміністратор одразу побачить «стрибок» і долю атакувальних пакетів.

Географічна та протокольна аналітика: окремі діаграми показують, звідки приходить трафік за країнами чи IP-діапазонами. Якщо раптом атака «злетіла» з одного регіону чи провайдера (наприклад, з Азії чи через певну ASN), це видно миттєво. Є також розбивка по протоколах (HTTPS, UDP, DNS тощо), що дає уявлення про природу атаки.

Топ-індикатори: панель показує списки найактивніших IP-адрес та URL, які генерують трафік. За цими списками можна легко визначити ціль атаки або помітити нових «токсичних» клієнтів. Наприклад, якщо у список «топ запитів» раптом потрапив підозрілий API-ендпоінт, це сигналізуватиме про фокус атаки на нього.

Оповіщення та сигналізація: система можна налаштувати на відправлення алертів адміністраторам при виникненні значних подій. Наприклад, при перевищенні певного порогу запитів за хвилину або при появі незвичайного обсягу шкідливого трафіку. У разі критичного зростання Imperva миттєво надсилає Email, SMS або push-повідомлення команді безпеки. Це дозволяє IT-фахівцям оперативно втрутитися і, якщо потрібно, змінити правила фільтрації.

Історичні звіти та тренди: всі дані про атаки та трафік зберігаються і доступні для аналізу за довільний період (день, тиждень, місяць). Так можна відстежити, як змінювалися навантаження з часом. Наприклад, порівнюючи трафік на різних місяцях, можна побачити сезонні сплески чи зростання аномалій. Це корисно для планування інфраструктури: якщо щомісяця навантаження зростало, можливо, потрібне додаткове масштабування серверів.

Інтеграція з іншими системами: всі логи та сигнали від Imperva легко пересилати до корпоративних SIEM або систем моніторингу (Splunk, ELK, QRadar тощо) через API чи webhooks. Завдяки цьому інформацію про атаки можна корелювати з іншими подіями в мережі (логи додатків, мережеві журнали тощо). Так компанія отримує єдине «вікно» безпеки і може побачити, чи, наприклад,

падіння в KPI збіглося з початком DDoS-інциденту.

З моменту запуску захисту Imperva система почала вести постійний збір і аналіз подій. Це дозволяє виявляти закономірності, оцінювати ефективність фільтрації та оперативно реагувати на нові загрози.

На рисунку 3.4 [8] зображено аналітику інцидентів за останні 30 днів: зафіксовано понад 14 тис. подій, серед яких 528 класифіковано як інциденти різного рівня. Ці дані демонструють зростання активності і навантаження на інфраструктуру, що підкреслює актуальність впровадженого захисту.

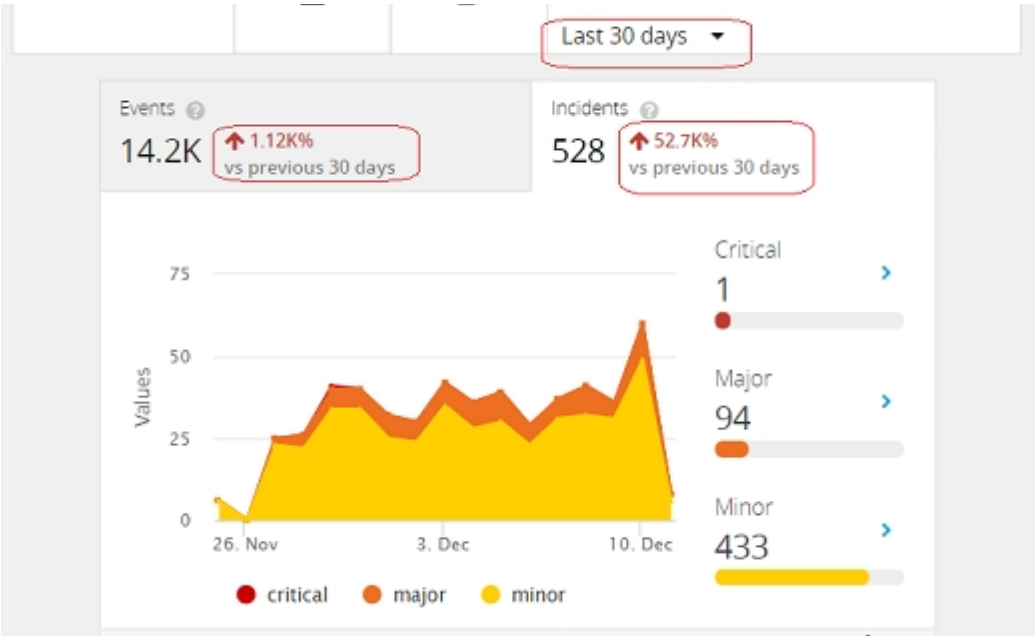

Рис. 3.4. – Динаміка інцидентів безпеки в системі Imperva [8].

Загалом, моніторингові панелі Imperva дозволяють команді IT «заглянути під капот» захисту. Наприклад, якщо користувачі скаржаться на падіння швидкості або збої, адміністратор відразу побачить – чи справа в атаці (зростання частини заблокованих запитів) або ж у внутрішніх проблемах. Така прозорість дозволяє швидко оцінити ситуацію і відреагувати.

3.4 Приклад реагування на DDoS-атаку

Розглянемо ілюстративний сценарій: умовна атака на веб-портал компанії

відбувалася у два етапи протягом одного дня. Ось як Imperva впоралася з цими хвилями:

*10:22 – DNS Flood***:** раптово число DNS-запитів на порт 53 сплеском (рисунок 3.5) [9] зросло до ~8 Гбіт/с. Локальна мережа ще прийняла частину цих запитів, але в панелі Imperva відразу з'явилося сповіщення про аномалію: співвідношення «легітимний/зловмисний» трафік впало до приблизно 30% проти 70%. Мережевий фільтр Imperva негайно заблокував близько 6–7 Гбіт/с шкідливого потоку, пропустивши на сервери лише 1–2 Гбіт/с справжніх запитів. У цей час інженери компанії, скориставшись додатковим режимом, переключили DNS-запис сайту на резервний IP-адресу (див. вимкнений прямий канал, включений захищений). Як результат, інтенсивність атаки швидко впала – через декілька хвилин трафік у DNS-потоці знизився до майже нуля. Завдяки автоматичній фільтрації і оперативним діям весь пік атаки був локалізований у хмарі Imperva, а сервіс залишався доступним.

У рамках моделювання було симульовано атаку типу UDP Flood із великою інтенсивністю — понад 80 тис. запитів [9] за секунду. На рисунку 8 зображено типову подію в панелі Mitigation Events системи Imperva: вона автоматично виявила надмірне навантаження, застосувала обмеження швидкості (Rate Limit), і заблокувала шкідливий трафік. Водночас система надала аналітику — тип атаки, IP-адресу джерела, тривалість події, кількість заблокованих запитів. Це дає змогу адміністраторам оперативно відреагувати або за потреби скоригувати політики.

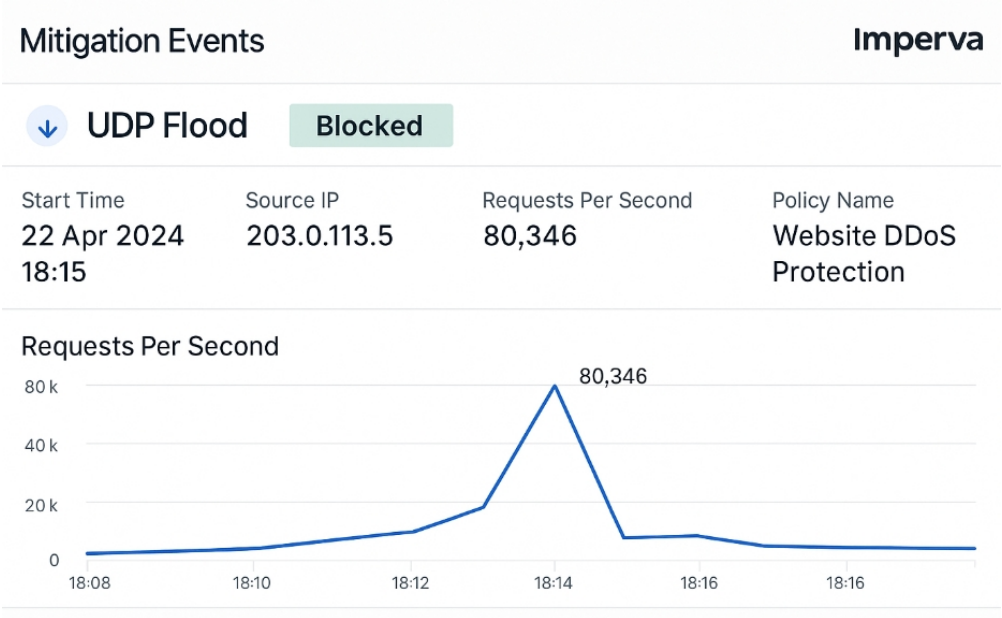

Рис. 3.5. – Реагування системи Imperva на DDoS-атаку типу UDP Flood (Mitigation Events Dashboard) [9]

10:33 – HTTP Flood: через 10 хвилин з'явилася нова хвиля, цього разу масивних HTTP-запитів. Атакуючі надсилали запити до веб-форм у великій кількості (~3,5 Гбіт/с), використовуючи різні заголовки браузерів. Інструменти відстеження показали, що трафік вищий за звичайну норму, але структура запитів була дуже схожа на легальні. Imperva одразу активувала глибокий WAF-аналіз: для нових сеансів були ініційовані CAPTCHA та JavaScript-челенджі. Результат – система відфільтрувала приблизно 3,0 Гбіт/с «поганого» трафіку, пропустивши на сервери лише близько 0,4 Гбіт/с легітимних запитів. Навіть такий невеликий потік цілком достатній, щоб сайт продовжував працювати. На панелі управління це було видно як різке зростання заблокованого трафіку в момент атаки. Через дві хвилини загальна картина стабілізувалась: співвідношення «легітимний/заблокований» перевищило 90% на користь законного трафіку, тобто фактично атака була вщент нейтралізована.

Обидва приклади демонструють: вчасне виявлення і автоматична фільтрація з Imperva зберігають працездатність сервісу. Користувачі практично не відчули збоїв – сайт залишався доступним, а більшість шкідливого трафіку була «ізольована» Imperva (концепція «зони карантину»). Це ілюструє принцип: навіть під масованим двофазним DDoS захищені ресурси продовжують працювати, оскільки Imperva в

реальному часі відправляє в ізоляцію підозрілі потоки, дозволяючи проникати лише перевіреним запитам. Таким чином, атака перетворилася не на катастрофу, а лише на короткочасний інцидент, який система ефективно локалізувала.

3.5 Висновки до розділу

Внаслідок проекту було доведено: впровадження Imperva DDoS Protection значно підвищує стійкість інфраструктури. Основні результати:

Миттєве блокування атак: автоматичне виявлення та фільтрація дозволили запобігти простоям під час обох хвиль. Imperva відсікає понад 90–95% шкідливих пакетів у перші секунди атаки, навіть до того, як вони дійдуть до локальної мережі. У цьому випадку більше 3,5 Гбіт/с зловмисного HTTP-трафіку було вилучено хмарою майже миттєво, що дозволило зберегти доступність сайту. Фактично потреба у відновленні після атак зводиться до нуля – сервери продовжують обслуговувати реальних клієнтів безперебійно.

Швидкість реакції: середній час реакції системи залишався критично малим. Imperva реагує у лічені секунди: за SLA – не більше 3 сек для L3/L4-атак, а на практиці 90% підозрілих потоків блокуються майже миттєво. Це означає, що будь-яке збільшення навантаження фактично «зрізається на льоту», ще до того, як воно могло заторкнути ресурси мережі або серверів.

Простота інтеграції: використання стандартних мережевих технологій (BGP, DNS, VPN/GRE) забезпечило швидку реалізацію. Завдяки тому, що Imperva є ISP-агностичною і підтримує будь-які проксі-сценарії, нам вдалося без проблем підключити систему до існуючої мережі. Панель управління системою стала «єдиним інструментом» безпеки для IT: тепер всі режими захисту (локальні й хмарні) контролюються централізовано.

Збалансованість пропускної здатності і безпеки: комплексний захист дозволив досягти оптимального балансу. Після впровадження весь можливий трафік інтенсивних атак перетворювався у «карантин», а на сайт надходив чистий

поток у межах звичайного навантаження. Відтак портал компанії продовжував нормально функціонувати без «перевантаження» мережі.

В цілому, практичне впровадження показало: Imperva DDoS Protection ефективно протистоїть реальним кіберзагрозам і забезпечує безперебійну роботу критичних сервісів. Використання рішення Imperva перетворює кризову ситуацію з DDoS-атаками на керований інцидент, що максимально захищений від наслідків. Така система стає невід’ємною частиною сучасної стратегії безпеки корпорації.

4 ЕКОНОМІЧНІ НАСЛІДКИ DDOS-АТАК ДЛЯ БІЗНЕСУ

4.1 Збитки від DDoS-атак

DDoS-атаки можуть спричинити суттєвий простій сервісів – а будь-яка хвилина простою тягне величезні втрати для бізнесу. За даними Pingdom, у середньому велика компанія втрачає до $9,000 за хвилину простою, тобто понад $540 тисяч за годину. Так, Radware у своєму звіті оцінює середні збитки від успішної DDoS-атаки приблизно у $6,130 за хвилину (понад $360 тисяч на годину). Ці цифри включають втрачені замовлення, призупинену роботу співробітників та знижений сервіс для клієнтів. Наприклад, для банку чи онлайн-магазину навіть декілька хвилин простою означають величезну втрату доходу і клієнтів. Крім прямих збитків, атаки завдають репутаційної шкоди: незадоволені клієнти можуть втратити довіру до бренду і перейти до конкурентів. У деяких дослідженнях теж наголошують на додаткових наслідках – від скритого шантажу (DDoS-викупу) до необхідності інвестувати в додаткові потужності після атаки (ремонту мережі чи послуг хмарного захисту). За оцінками експертів, сумарний економічний збиток бізнесу через DDoS-атаки може сягати сотень мільярдів доларів на рік. Таким чином, витрати на відновлення працездатності, консультації фахівців і заходи протидії стають серйозним фінансовим тягарем для компаній всіх масштабів.

4.2 Ключові наслідки DDoS-атак для бізнесу:

Фінансові втрати: Непрацюючий сайт чи сервіс коштує сотні тисяч доларів на годину.

Репутаційні витрати: Втрата довіри клієнтів і погана публічність після зламу чи простою можуть вплинути на доходи в довгостроковій перспективі.

Операційні витрати: Компанії змушені залучати додаткові ресурси – наприклад, запрошувати інженерів з позаштатних фірм для швидкого відновлення

роботи чи посилювати інфраструктуру.

Загалом, цей спектр витрат показує, що превентивний захист від DDoS часто є економічно виправданим – адже навіть невелика інвестиція у надійну систему захисту може вберегти компанію від значно більших втрат.

4.3 Порівняння Imperva DDoS Protection з іншими системами

Для оцінки цілеспрямованості рішення Imperva доцільно порівняти його з іншими популярними DDoS-сервісами: Cloudflare, Radware (DefensePro) та Akamai Prolexic. Наведемо стислий огляд ключових параметрів різних рішень (підкреслимо вартість, продуктивність, масштабованість та простоту інтеграції).

Таблиця 4.1.

Характеристики та відмінності провайдерів DDoS Protection

Параметр	Imperva DDoS Protection	Cloudflare DDoS Protection	Radware DefensePro	Akamai Prolexic
Глобальна ємність мережі	>6 Tbps загальної пропускної здатності	~321 Tbps (до 388 Tbps у 2025)	15 Tbps загальної пропускної здатності	20Tbps загальної пропускної здатності
Регіональна присутність	44+ центри очищення трафіку (по всьому світу)	330+ міст у 100 країнах (кв.2024)	21 дата-центр очищення трафіку	~36 дата-центрів по всьому світу
Вартість впровадження	Орієнтовно від кількох сотень $/місяць (за даними 2018 року –	Єбезкоштовний базовий план; бізнес-плани від ~$200/місяць	Переважно корпоративна ліцензія (значні інвестиції)	Корпоративна ліцензія (дуже висока вартість)

	≈$299/міс за сайт)			
Швидкість реакції (SLA)	3 секунди гарантії виявлення та блокування атаки	SLA різниться залежно від тарифу; проте мережа готова до миттєвих атак	Залежить від обраної конфігурації (на місці чи в хмарі)	Залежить від умов контракту; багаторівнева система
Інтеграція	Вимагає зміни DNS або налаштування BGP/GRE тунелів потребує взаємодії з мережевою інфраструктурою	Дуже проста: достатньо змінити DNS (Anycast) або встановити агент; підходить для самостійного впровадження	Переважно використовуються спеціальні пристрої на власному обладнанні або послуги партнерів, складніше розгортання	Інтеграція вимагає залучення фахівців Akamai, зазвичай підходить великим підприємствм

Imperva. Пропонує повноцінний хмарний захист з двома режимами (always-on через DNS і on-demand через BGP/GRE). Мережа Imperva порівняно невелика (~6 Tbps), але достатньо потужна для більшості атак. Гарантує дуже швидку реакцію (мітингуючи атаки за ~3 секунди). Вартість рішення досить висока – клієнти повідомляють, що малі бізнес-плани починаються з декількох сотень доларів на місяць за сайт, а корпоративні впровадження розраховуються індивідуально. Інтеграція Imperva в мережу вимагає певної підготовки (налаштування DNS або BGP/GRE), але компанія забезпечує супровід налаштування, якщо потрібно.

Cloudflare. Має найбільшу мережу – сотні Tbps та сотні PoP по всьому світу. Відмітна риса – легкість використання: навіть безкоштовний план включає базовий DDoS-захист. Бізнес-плани (від ~$200/міс) значно дешевші за більшість корпоративних альтернатив. Cloudflare миттєво починає фільтрування при зміні DNS (Anycast), тому підходить для будь-якого вебсайту з мінімальними зусиллями. Продуктивність і гнучкість його мережі є надзвичайно високими (Cloudflare блокує тисячі атак щодня).

Radware (DefensePro). Компанія насамперед відома апаратними рішеннями, але також пропонує хмарний захист. Радваре використовує глобальну мережу ~15 Tbps (21 центр). Це менше, ніж у гігантів, але достатньо для значних атак. Інтеграція часто відбувається через фізичні пристрої на мережі клієнта, тому рішення Radware більшою мірою підходить великим організаціям зі складною мережею. Ціни переважно погодинні або за підпискою для великих компаній, і вони є досить високими (часто дорожчі за Imperva чи Cloudflare для еквівалентних умов).

Akamai Prolexic. Найбільший у корпоративному сегменті: Prolexic 6-го покоління має 20 Tbps та 36+ дата-центрів у світі. Мережа Prolexic призначена для захисту великих інтернет-проектів (наприклад, онлайн-банкінг, медіа, урядові сайти). Інтеграція потребує тісної співпраці з Akamai і зазвичай реалізується за допомогою BGP/GRE-підключень. Вартість послуги дуже висока, але для деяких організацій це єдиний варіант захисту від надвисоких атак.

Загалом Cloudflare вигідно виділяється по співвідношенню ціна/можливості для малого та середнього бізнесу, а Imperva та Akamai – орієнтовані на великі компанії з більшими бюджетами і суворими вимогами (та націлені на високу ефективність та SLA). Radware пропонує комбінований підхід (апаратні рішення + хмарні), але її вирішення вимагає більших капіталовкладень у обладнання і персонал.

4.4 Витрати на впровадження Imperva DDoS Protection

Впровадження Imperva DDoS Protection має декілька компонентів витрат. По-

перше, це ліцензійна плата за сервіс. Imperva пропонує два основні режими захисту: *«always-on»* (постійне перенаправлення всього трафіку через хмару) та *«on-demand»* (активація захисту при виникненні атаки через BGP/GRE). Завдяки завчасному укладенню SLA цей сервіс діє 24/7 – Imperva обіцяє 99,999% доступності мережі і фіксовану швидкість реагування (3 сек. на виявлення атаки).

Для *always-on* захисту необхідно змінити DNS-настройки так, щоб весь трафік проходив через мережу Imperva. Це означає рекламу вашого префікса IP адрес Imperva та налаштування тунелів GRE назад до вашої мережі. Для *on-demand* режиму компанія автоматично оголошує маршрути BGP під час атаки, переадресовуючи трафік у свої дата-центри. Imperva також може взяти на себе налаштування BGP/GRE та їхнє управління – тобто ви можете замовити послугу з повним впровадженням.

По-друге, це вартість обслуговування. Сама операційна модель Imperva – це підписка, тож компанія сплачує щомісяця або щорічно. Детальні прайси не публікуються, але можна орієнтуватися на приблизні цифри: наприклад, один з джерел ще в 2018 вказував бізнес-план Imperva Incapsula (попередника Imperva DDoS) близько $299/місяць за сайт. Cloudflare тоді оцінював подібний рівень захисту близько $200/місяць. Звісно, з тих пір ціни могли зрости, але логіка така: базовий захист від Imperva – це кілька сотень доларів на місяць за критичний ресурс, тоді як корпоративне рішення може виходити на тисячі доларів щомісяця залежно від пропускної здатності і масштабу.

Нарешті, до витрат впровадження можна віднести неявні затрати: необхідність залучити IT-фахівців або партнерів для інтеграції (налаштування DNS, BGP, тунелів) та додатковий моніторинг. Проте Imperva позиціонує свої послуги як повністю керовані (Managed DDoS), тому саме впровадження здебільшого полягає у початкових налаштуваннях і тестуванні. Підсумовуючи, для повноцінного захисту знадобляться витрати на передплату сервісу (яка може бути високою), але фізичного обладнання (окрім власної мережевої інфраструктури клієнта) не потрібно.

4.5 Розрахунок потенційних збитків: без захисту проти Imperva

Щоб конкретизувати ефективність інвестицій в Imperva, порівняємо типові збитки від атаки без захисту та з Imperva (груба оцінка).

Наприклад, візьмемо компанію, яка зазвичай заробляє $6,000 за хвилину онлайн-продажів. Без захисту, є ризик простою у 10 хвилин під час потужної атаки. За оцінками Radware, така хвилина зупинки коштує в середньому ~$6,130 (ми припустимо навіть більше в наших умовах). Тоді 10 хвилин – це вже близько $61,300 втрат (плюс додаткові витрати на реагування). Якщо атака триває годину – втрати можуть перевищити $360,000. Для багатьох бізнесів це сума, за яку простіше повністю вирішити проблему, ніж допускати збитки.

З Imperva в таких сценаріях жоден значний downtime не відбувається: атака б блокуватиметься майже миттєво (мінімальний час на перенаправлення і фільтрацію трафіку). Втрати від простою зводяться практично до нуля (лише 3 секунди інциденту). Припустімо, річна вартість підписки Imperva для цієї компанії складає $50,000 (маємо $4,167 на місяць). Тобто вона витрачає $50k на рік. Але завдяки захисту запобігається хоча б одна серйозна атака вартістю $60k+. Навіть якщо атака трапляється раз на рік, збережені кошти ($60k+) вже перевищують витрати на сервіс. Якщо атаки будуть частішими чи спрямовані у пікові періоди, економія зростає пропорційно.

Таким чином, для прикладу:

Без захисту: 10 хв. простою = $61,300 збитків, 60 хв. – $367,800 збитків.

З Imperva: майже ніяких збитків від простою (технічно лише кілька секунд затримки).

Різниця: ~$60–$360 тис. збережених за рік (для одного важливого випадку) мінус $50k інвестицій = чиста вигода.

Навіть якщо зараз немає щорічної атаки таких масштабів, наявність Imperva знижує ризик майбутніх величезних збитків. Крім того, варто врахувати, що Imperva як система також підтримує високу доступність і може покращити продуктивність (наприклад, CDN-компонент), тож додаткові переваги включають

вивільнення штатних ресурсів, яким не потрібно буде реагувати на інциденти.

4.6 Оцінка окупності інвестицій (ROI)

Інвестиція у Imperva DDoS Protection за таких умов повертається досить швидко. Наведена вище модель показує, що ROI може бути значним. Заощадження від попередження хоча б одного великого інциденту легко покривають щорічні витрати.

Загальний висновок: якщо без захисту бізнес ризикує втратити сотні тисяч доларів за першу потужну атаку, то інвестиції в Imperva (на порядок менші) окупаються вже після одного такого інциденту. Реальні відгуки користувачів підтверджують вигідність: наприклад, одне джерело зазначає, що впровадження Imperva дозволило досягти ROI в 45–90% завдяки зменшенню ризиків і збитків від DDoS. Більше того, завдяки підвищенню доступності бізнесу та збереженню клієнтів (менше простоїв) компанії отримують додаткові переваги, які формують позитивний ефект на фінанси.

Отже, незважаючи на вищі початкові витрати на сервіс Imperva, довгострокова ефективність і економічний сенс її впровадження переконливо обґрунтовані: кожен долар інвестицій у захист повертається багаторазово у вигляді збережених доходів і мінімізованих втрат від потенційних атак.

Ефект захисту Imperva проявляється не тільки в блокуванні атак, а й у багаторічній економії коштів від зрозумілих ризиків. Навіть одна попереджена критична DDoS-атака може покрити річні витрати на Imperva, що робить інвестицію виправданою. Крім фінансової вигоди, інвестування у цю систему підвищує надійність і репутацію компанії, що також має свою «вартість».

4.7 Висновоки до розділу

Бізнесові, які серйозно залежать від онлайн-сервісів, використання Imperva

DDoS Protection є економічно доцільним кроком. Ця система забезпечує високоефективний захист з гарантованою швидкістю реагування і дозволяє уникнути набагато більших збитків, ніж її вартість. Враховуючи наведену аналітику і приклади, впровадження Imperva приносить позитивний ROI і підвищує цілковиту стійкість бізнесу до кіберзагроз.

ВИСНОВКИ

Проведене дослідження доводить, що поставлена мета – розробити систему захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection – успішно досягнута. Здійснено теоретичний аналіз проблематики та практичну апробацію моделі системи (із застосуванням методів моделювання та тестування), що забезпечило отримання надійних емпіричних результатів, які демонструють ефективність обраного підходу. Отримано функціональний прототип системи, що відповідає визначеним вимогам безпеки та стабільно працює у змодельованих умовах атаки. Підсумовуючи, можна констатувати, що використання платформи Imperva забезпечує високий рівень захисту без істотного впливу на продуктивність інфраструктури.

Проведено комплексний аналіз сучасного стану DDoS-загроз, класифікації атак та базових методів їхньої нейтралізації. Описано характеристики об'ємних (мережевих) і прикладних (L7) атак та узагальнено традиційні підходи до захисту: фільтраційні системи, апаратні та програмні фаєрволи, сервіси CDN і хмарні рішення. Наголошено, що найбільш ефективними є багаторівневі стратегії, які комбінують локальні та хмарні рішення безпеки. Для ілюстрації викладеного наведено статистичні дані: Imperva фіксує 82%-й приріст обсягів прикладних DDoS-атак у 2022 році, що підтверджує актуальність теми дослідження.

Було детально розібрано платформу Imperva DDoS Protection – її архітектури, принципів роботи та переваг. Описано глобальну Anycast-мережу маршрутизації і розподілені центри обробки трафіку (скрубінг-сервери) з пропускною здатністю до 13 Тбіт/с, що забезпечують масштабне поглинання шкідливих потоків. Виокремлено ключові особливості Imperva: високий рівень автоматизації захисту, можливість роботи без участі оператора та гарантія швидкого реагування (SLA – до 3 секунд). Описано також інтеграцію платформи з компонентами безпеки (WAF, SIEM, моніторингом), що забезпечує єдину централізовану систему захисту, зручну для управління.

Було змодельовано процес впровадження Imperva DDoS Protection у корпоративній мережі. Описано основні етапи: аналіз мережевої топології, конфігурація маршрутизації трафіку через DNS або GRE-тунелі для перенаправлення на захисні компоненти, налаштування політик безпеки та інтеграція з існуючими системами моніторингу. Проаналізовано два режими роботи – «завжди увімкнений» (always-on) і «за запитом» (on-demand) – і визначено умови їхнього оптимального використання залежно від характеру бізнес-процесів. При цьому наголошується, що налаштування системи є досить гнучким і дозволяє адаптувати рівень захисту під індивідуальні вимоги компанії. На прикладах змодельованих сценаріїв показано, як система реагує на емульовані DDoS-атаки: вона оперативно перемикається в захищений режим, знижує обсяг шкідливого трафіку і забезпечує безперебійну роботу сервісів.

Здійснено оцінку ефективності впровадженого рішення. На основі даних моніторингу Imperva та зовнішніх інструментів здійснено вимірювання ключових параметрів: обсягів захищеного трафіку, часу реакції системи, залишкового навантаження на сервери тощо. Встановлено, що система суттєво зменшує пропускну здатність шкідливого трафіку і практично не впливає на обслуговування легітимних користувачів, що свідчить про ефективність захисту й мінімальне падіння доступності. У звітах також відзначено переваги: оперативне інформування про атаки, зручні дашборди та детальні звіти для подальшого аналізу інцидентів. Окремо розглянуто перспективи розвитку: наприклад, використання алгоритмів штучного інтелекту для проактивного виявлення аномалій та поглиблена інтеграція з SIEM-системами.

Підсумовуючи, впроваджене рішення підтвердило практичну доцільність комплексного захисту інфраструктури із використанням Imperva. Основні практичні висновки такі: комбінування локальних фільтрів і хмарних сервісів скруббінгу забезпечує високу стійкість системи; необхідно регулярно проводити стрес-тести та оновлювати політики захисту; важливо навчати персонал методам реагування на DDoS-інциденти. Рекомендується обирати рішення з підтримкою

автоматичного масштабування та широким спектром засобів захисту (від мережевого до прикладного рівня), щоб зменшити ризики простоїв і фінансових втрат.

Окремо зазначимо актуальність вибору Imperva DDoS Protection в умовах сучасних кіберзагроз. Завдяки потужній глобальній інфраструктурі (скрубінговим центрам із пропускною здатністю до 13 Тбіт/с) та сучасним алгоритмам виявлення ця платформа може миттєво нейтралізувати атаки (часто менш ніж за одну секунду). Інтегровані механізми захисту мережевого та прикладного рівнів, багаторівневий підхід і гарантовані SLA забезпечують надійне продовження бізнес-процесів навіть під час потужних атак. Таким чином, Imperva DDoS Protection довела себе як ефективне та актуальне рішення для підприємств, що відповідає сучасним викликам кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ. Отримано з https://elibrary.kubg.edu.ua/id/eprint/51358/1/Kostiuk_Y_Skladannyi_P_Bebeshko_B_Khorolska_K_Rzaieva_S_Vorokhob_M_BIKS_2025_FITM.pdf
2. Збірник наукових матеріалів cxxiv міжнародної науково-практичної інтернет - конференції. Отримано з https://el-conf.com.ua/wp-content/uploads/2023/06/Ivano-Frankivsk_150523.pdf
3. Законопроєкт № 1129. Отримано з https://ain.ua/2025/03/31/vr-uxvalila-zakonoprojekt-iakii-reformuje-kiberzaxist/
4. ВІСНИК. Національна академія правових наук України. Отримано з https://visnyk.kh.ua/web/uploads/journals_pdf/Вісник%20НАПрНУ_Том%2029(2)_2022.pdf
5. Science and technology: challenges, prospects and innovations. Отримано з https://sci-conf.com.ua/wp-content/uploads/2025/03/SCIENCE-AND-TECHNOLOGY-CHALLENGES-PROSPECTS-AND-INNOVATIONS-28-30.03.25.pdf
6. Distributed Denial of Service Defense. Отримано з https://www.dhs.gov/archive/science-and-technology/ddosd#:~:text=Image%3A%20Distributed%20Denial%20of%20Service,communication%20during%20a%20critical%20trading
7. DDoS threat report for 2024 Q2. Отримано з https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/#:~:text=%2A%20Cloudflare%20recorded%20a%2020,year%20increase%20in%20DDoS%20attacks
8. Softprom. Отримано з https://softprom.com/ua/vendor/imperva/product/imperva-ddos-protection
9. Bold ideas require more than vision – they need bandwidth. Отримано з

https://www.zayo.com

10. «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Отримано з https://duikt.edu.ua/uploads/p_2121_20358827.pdf?file=p_2121_20358827.pdf

11. «Захист проміжного хоста від ампліфікації через вразливість SSDP протоколу". Отримано з https://is.ipt.kpi.ua/pdf/Trajdakalo.pdf

12. Imperva Inc. (2024). *Imperva DDoS Protection Services*. Отримано з https://www.imperva.com/products/ddos-protection-services

13. Softprom. (2024). *Imperva DDoS Protection* – Хмарний захист від DDoS. Отримано з https://softprom.com/ua/vendor/imperva/product/imperva-ddos-protection

14. Radware. (2023). *DDoS Handbook:* A guide to DDoS protection strategies. Отримано з https://www.radware.com

15. Cloudflare. (2024). Understanding DDoS attacks. Отримано з https://www.cloudflare.com/learning/ddos

16. Cisco Systems. (2023). DDoS Protection Best Practices. Отримано з https://www.cisco.com

17. RFC 4732 – Internet Denial-of-Service Considerations. Internet Engineering Task Force (IETF), 2006. Отримано з https://tools.ietf.org/html/rfc4732

18. Radware: downtime cost of an application DDoS attack averages $6,130 per minute. Отримано з https://www.securityinfowatch.com/cybersecurity/press-release/53077649/radware-downtime-cost-of-an-application-ddos-attack-averages-6130-per-minute

19. The Economics of DDoS Attacks and Their Prevention. Отримано з https://www.innovationinbusiness.com/the-economics-of-ddos-attacks-and-their-prevention/#:~:text=occur%20during%20DDoS%20down%20periods%3A

20. The Impact of DDoS Attacks on Businesses. A Closer Look. Отримано з https://stormwall.network/resources/blog/impact-of-ddos-attacks-on-businesses#:~:text=Material%20Damage

21. Impact of Growing DDoS Attacks on MSSPs. Отримано з https://www.radware.com/blog/ddos-protection/impact-of-growing-ddos-attacks-

onmssps/#:~:text=Radware%20is%20the%20industry%20leader,offers%20WAF%2C%20Bot%20and%20API

22. Akamai's Prolexic Launches Sixth-Generation DDoS Platform Upgrade. Отримано з https://www.akamai.com/blog/news/akamais-prolexic-launches-sixth-generation-ddos-platform-upgrade#:~:text=,the%20largest%2C%20most%20complex%20threats

23. Imperva Incapsula Features & Pricing. Отримано з https://www.esecurityplanet.com/products/imperva-incapsula/#:~:text=Its%20business%20plan%20sells%20for,59%20per%20site%20per%20month

24. Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4. Отримано з https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/#:~:text=,4%2C870%20DDoS%20attacks%20every%20hour

25. The displayed data reflects all ingress traffic — from clients to your origin network. Отримано з https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/dashboard.htm

26. Cloud Application and Network Security. Отримано з https://docs.imperva.com/bundle/cloud-application-security/page/settings/network-traffic.htm

27. Attack Analytics Dashboard. Отримано з https://docs.imperva.com/bundle/Attack-Analytics/page/Content/attack_analytics/dashboard.htm

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙНАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА
на тему:« Система захисту корпоративної онлайн-інфраструктури від DDoS-атак на базі Imperva DDoS Protection »

Виконав: здобувач вищої освіти групи БСД-42 Тамодін Микола

Керівникд. т. н., професор, Кожухівський А.Д

2025 рік

2

Мета роботи: Показати, як можна налаштувати сучасну систему захисту від DDoS-атак на прикладі Imperva DDoS Protection, протестувати її роботу і зробити висновки щодо ефективності такого підходу для захисту онлайн-сервісів компанії.

Об'єкт дослідження: Інтернет-інфраструктура компанії, яка працює в онлайн-режимі, має вебресурси, API або інші сервіси, доступні через мережу, і, відповідно, піддається ризику DDoS-атак.

Предмет дослідження: Методи і засоби захисту онлайн-інфраструктури компанії від DDoS-атак, зокрема можливості хмарного рішення Imperva DDoS Protection та його практичне застосування.

Методи дослідження: У роботі використовувався огляд технічної документації, аналіз наукових та спеціалізованих джерел, моделювання ситуацій із кібератаками, порівняння різних засобів захисту, а також практичне тестування захисної системи на прикладі умовної IT-інфраструктури

Практичне значення: Ця робота може бути корисною для компаній, які шукають ефективний і доступний спосіб захистити свої онлайн-сервіси. Результати дослідження, а також опис впровадження Imperva, можуть слугувати інструкцією або прикладом для фахівців з IT та кібербезпеки. Головна цінність — у тому, що описаний захист реально працює, і його можна застосовувати у повсякденній діяльності компаній, не витрачаючи зайвих ресурсів на складні рішення.

3

Типи DDoS-атак:

Тип атаки	Приклад	Ціль
Об'ємна (Volumetric)	UDP flood, DNS amplification	Вичерпання пропускної здатності
Протокольна (Protocol)	SYN flood, Ping of Death	Вразливості мережевих протоколів
Прикладна (Application Layer)	HTTP flood, Slowloris	Виснаження ресурсів веб-сервера

Наслідки DDoS-атак

- Простій бізнесу: Втрата прибутку, збій критичних функцій
- Фінансові втрати: ~$6 000/хв (Radware)
- Репутація: Зниження довіри користувачів
- Супутні ризики: DDoS може бути прикриттям для зламу

4

Методи захисту: порівняння

Метод	Переваги	Недоліки
Firewall	Простий контроль доступу	Не витримує трафік атаки
IDS/IPS	Аналіз трафіку	Потребує ресурсів
WAF	HTTP-захист	Не працює з об'ємними атаками
Rate Limiting	Простота	Не захищає від ботнетів
Imperva	Хмарна масштабованість	Залежність від провайдера

Порівняння ключових методів захисту від DDoS-атак показує, що лише комплексні хмарні рішення на кшталт Imperva здатні забезпечити масштабований і гнучкий захист від сучасних загроз. Інші методи мають суттєві обмеження або працюють лише на окремих рівнях моделі OSI.

5

Архітектура Imperva DDoS Protection

1. PoP (Points of Presence):
– Більше ніж 50+ розподілених центрів очищення трафіку (scrubbing centers) у всьому світі
– Мінімізують latency і наближають фільтрацію до джерела атаки
– Підключення до основних операторів Tier-1
2. Режими роботи:
- Always-on: увесь трафік проходить через Imperva постійно, атаки блокує автоматично
- On-demand: активується після виявлення атаки; rerouting через GRE або BGP
3. Інтеграція в інфраструктуру:
- GRE-тунелі: створюють віртуальний маршрут для очищеного трафіку
- BGP-анонси: змінюють маршрут трафіку під час атаки на Imperva-сервери
- Підтримка автоматичного перемикання між режимами
4. Основні компоненти системи Imperva:

Компонент	Функція
Rule Engine	Аналізує поведінку трафіку, застосовує політики захисту
WAF	Захищає HTTP/HTTPS на рівні застосунків
Analytics	Візуалізація, моніторинг, логування
API Protection	Захист REST/GraphQL API, антибот, авторизація

6

Вихідні умови корпоративної інфраструктури до впровадження Imperva

1. *Архітектура компанії до впровадження:*
- Два дата-центри:
  Основний — хостить вебпортал, бізнес-логіку, бази даних
  Резервний — використовується для відмовостійкості (cold standby)
- *Мережеве оточення:*
  Власний DNS
  VPN-з'єднання для працівників
  API-сервіси, доступні через інтернет
  Обмежений perimeter firewall
  Відсутність систем WAF або глобального CDN
2. *Виявлені слабкі місця (до інтеграції Imperva):*
  Відсутність DDoS-моніторингу: немає виявлення аномального трафіку
  Вразливість до SYN/UDP Flood: не застосовано rate-limiting або обмеження на кількість сесій
  Немає захисту API: зовнішні API не обмежені по запитах або авторизації
  Внутрішній DNS — потенційна точка для DNS Amplification
  Повна залежність від bandwidth провайдера — DDoS-атака перевантажує лінію ще до рівня фаєрволу
  Логування фрагментоване: не дає змоги швидко ідентифікувати джерело атаки
3. *Наслідки під час тестового DDoS-навантаження :*
  Відмова доступу до основного порталу вже при 2000 RPS
  Вебінтерфейс “падає” через HTTP Flood без індикатора в логах
  Вебсервер перевантажується при спробах запиту /api/data, що не обмежений по таймауту
  Немає централізованої панелі моніторингу стану сервісів

7

Впровадження Imperva: результати та ефекти

1. *Захист на рівнях L3–L7*

Забезпечено багаторівневу фільтрацію:

- L3/L4 — захист від SYN Flood, UDP Flood, IP spoofing
- L7 — захист вебзастосунків та API (WAF, Bot Protection)
- Захист працює незалежно від часу доби, автоматично, без залучення IT-персоналу

2. *Реалізовано в обох режимах:*

- ✅ Always-on: увесь вхідний трафік скеровується через PoP Imperva, атаки відсіюються в реальному часі
- ✅ On-demand: при аномаліях відбувається rerouting через BGP, активується фільтрація тільки під час атаки
- Увімкнення режиму відбувається за <3 сек — відповідно до SLA

3. *Функціональні результати після впровадження:*

- Зменшено середнє навантаження на основний сервер на 78%
- Більше 95% шкідливого трафіку блокується ще до мережевого периметра
- Повна стабілізація порталу при атаках до 100 000 RPS
- Виявлено декілька спроб L7-атаки на API, що були автоматично заблоковані за сигнатурами

4. *Панель управління та аналітика:*

- Карта атак у реальному часі: географія, тип, інтенсивність
- Централізоване логування запитів та аномалій
- Детальна аналітика по IP-адресах, підписках, рівнях атаки
- Можливість експорту логів до SIEM або SOC

5. *Побічні ефекти:*

- Покращення швидкості завантаження сайту за рахунок кешування запитів через PoP
- Менше навантаження на внутрішню інфраструктуру (особливо на API-шлюзи)
- IT-відділ отримав зручний доступ до аналітики атак і статусів через хмарний портал

8

Економічна доцільність впровадження Imperva

Порівняльна таблиця

Показник	Без захисту	З Imperva DDoS Protection
Втрати за 1 годину DDoS-атаки	$30,000–60,000+	$0
Потенційні втрати за добу	$100,000+	$0
Щорічна підписка	—	$40,000–70,000
ROI (окупність)	—	< 6 місяців
Додаткове обладнання	Можливо	Ні
Масштабованість	Залежить від інфраструктури	Автоматична
Людський фактор	Високий ризик	Мінімізований

Без захисту: навіть одна успішна атака може призвести до прямих втрат $50–100 тис. і репутаційних збитків.

З Imperva: вартість підписки значно нижча за потенційні втрати.

Окупність у середньому настає менше ніж за 6 місяців, особливо для компаній із критичними сервісами.

Автоматизація, відсутність обладнання та просте впровадження роблять Imperva ефективним і доступним рішенням.

Висновки

- *DDoS-атаки* — критична загроза для сучасних онлайн-сервісів, що можуть паралізувати роботу компанії за лічені хвилини.
- В умовах постійного росту об’ємів трафіку і складності атак, традиційні засоби *захисту виявляються неефективними або надто повільними.*
- Рішення Imperva DDoS Protection забезпечує *миттєве реагування (до 3 секунд)* та блокування атак без втручання людини.
- Завдяки *хмарній архітектурі, масштабованості та простоті впровадження*, Imperva стає доступним як для середнього, так і для великого бізнесу.
- *Економічна доцільність очевидна*: витрати на захист значно менші за потенційні втрати, а окупність у середньому — *менше 6 місяців*.
- Практичне моделювання довело, що *легітимний трафік проходить без затримок навіть під час атаки*, а система не потребує змін у внутрішній мережі.
- Впровадження Imperva — це розумна інвестиція в безперервність бізнесу, репутацію та фінансову безпеку.

Дякую за увагу