МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: Захист вебзастосунків від DDoS атак за допомогою хмарних сервісів Azure.

Здобувача вищої освіти другого (магістерського) рівня,
ІІ курсу, групи КМІ-24-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології в економіці»

(підпис) Іскри Дениса Миколайовича
(прізвище, ім'я, по батькові)

Науковий керівник (підпис) Омельчук Антон Анатолійович, канд. техн. наук
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Керівник освітньо-професійної програми (підпис) Омельчук Антон Анатолійович, канд. техн. наук
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту за рішенням кафедри протокол від «02» січня 2026 № 10

Завідувач кафедри (підпис) Філоненко Михайло Миколайович, канд. фіз.-мат. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Ірпінь – 2026

Реєстрація № 31 22.01.2026 _____
(дата) (підпис відповідальної особи)

Результати перевірки до захисту 02.01.2026 _____
(до захисту, на доопрацювання) (дата) (підпис)

Результат захисту 4 (добре) 09.02.2026 _____
(оцінка) (дата) (підпис)

Голова комісії: _____ О.С. Дюбанов
(підпис)

Члени комісії:

_____ А.Ю. Горбовий
(підпис)

_____ М.М. Філоненко
(підпис)

_____ І.Д. Погорєловська
(підпис)

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії,секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст кваліфікаційної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	25		09.02.2026 Дюбанов О.С. Горбовий А.Ю. Філоненко М.М. Погорєловська І.Д. Суховецька Л.П.
2. Дотримання вимог щодо оформлення	від 0 до 10	9		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	42		

Оцінювання кваліфікаційної роботи науковим керівником - 41 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалоюЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
83	B	4	09.02.2026	Дюбанов О.С. Горбовий А.Ю. Філоненко М.М. Погорєловська І.Д. Суховецька Л.П.

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	3 (задовільно)
50-59	E	
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем
Галузь знань 12 «Інформаційні технології»
Спеціальність 122 «Комп'ютерні науки»
Освітня програма «Інформаційні управляючі системи і технології в економіці»

Затверджую
Завідувач кафедри _____ Філоненко М.М.
«11» грудня 2024

Завдання на кваліфікаційну роботу
здобувачу вищої освіти
Іскрі Денису Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Захист вебзастосунків від DDoS-атак за допомогою хмарних сервісів Azure.
Затверджена наказом ректора від «10» грудня 2024 № 1852
2. Строк здачі закінченої роботи «02» січня 2026
3. Мета роботи: Дослідження та розробка ефективних методів захисту вебзастосунків від DDoS-атак з використанням хмарних сервісів Microsoft Azure, а також оцінка їх ефективності в реальних умовах експлуатації.
Об'єкт дослідження: Процеси забезпечення інформаційної безпеки вебзастосунків у хмарному середовищі.
Предмет дослідження: Методи та засоби захисту вебзастосунків від DDoS-атак із використанням сервісів Microsoft Azure.
Орієнтовна база дослідження: Хмарна платформа Microsoft Azure, зокрема сервіси Azure DDoS Protection, Azure Front Door, Azure Application Gateway та тестовий вебзастосунок, розгорнутий у хмарному середовищі.
4. Вихідні дані до роботи : Статистичні дані щодо DDoS-атак; результати експериментального моделювання атак на вебзастосунок; програмні та апаратні засоби хмарної інфраструктури Azure.
5. Перелік графічного матеріалу : Архітектура захисту вебзастосунку з Azure DDoS Protection та Application Gateway, Налаштування Azure DDoS Protection для Application Gateway, Порівняння показників до і після впровадження Azure DDoS Protection, Оцінка запропонованих заходів щодо вдосконалення системи захисту, Ефективність Заходів Захисту.
6. Зміст кваліфікаційної роботи (перелік питань за кожним розділом) *ВСТУП, РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК, РОЗДІЛ 2. ВИКОРИСТАННЯ ХМАРНОГО СЕРВІСУ MICROSOFT AZURE ДЛЯ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК, РОЗДІЛ 3. ТЕСТУВАННЯ, ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ, ПЕРСПЕКТИВИ ПОКРАЩЕННЯ, ВИСНОВКИ, СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ, ДОДАТКИ.*

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційноїроботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	До 15.12.2024	До 15.12.2024
2	**І розділ** (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	28.05.2025	28.05.2025
3	**ІІ розділ** (аналіз експериментальної частини про методики досліджень)	08.09.2025	08.09.2025
4	**ІІІ розділ** (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	17.11.2025	17.11.2025
5	**Висновки**	08.12.2025	08.12.2025
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	22.12.2025	22.12.2025
7	Отримання відгуку керівника	20.01.2026	20.01.2026
8	Отримання зовнішньої рецензії	23.01.2026	23.01.2026

8. Дата видачі завдання «11» грудня 2024

9. Керівник кваліфікаційної роботи

(підпис) Омельчук А.А.
(прізвище, ініціали)

10. Керівник освітньо-професійної програми

(підпис) Омельчук А.А.
(прізвище, ініціали)

11. Завдання до виконання отримав здобувач вищої освіти

(підпис) Іскра Д.М,
(прізвище, ініціали)

АНОТАЦІЯ

Захист вебзастосунків від DDoS-атак за допомогою хмарних сервісів Microsoft Azure.

Мета роботи полягає в дослідженні та розробці ефективних методів захисту вебзастосунків від DDoS-атак з використанням хмарних сервісів Microsoft Azure.

Завдання роботи:

- проаналізувати загрози DDoS-атак та сучасні підходи до їх протидії;
- спроєктувати архітектуру захищеного вебзастосунку в хмарному середовищі;

Предметом дослідження є Методи та засоби захисту вебзастосунків від DDoS-атак із використанням сервісів Microsoft Azure.

Об'єктом дослідження є Процеси забезпечення інформаційної безпеки вебзастосунків у хмарному середовищі.

Базою дослідження виступає Хмарна платформа Microsoft Azure, зокрема сервіси Azure DDoS Protection, Azure Front Door, Azure Application Gateway та тестовий вебзастосунок, розгорнутий у хмарному середовищі.

За результатами дослідження сформульовано підхід та етапи впровадження комплексної системи захисту вебзастосунку від DDoS-атак із використанням хмарних сервісів Microsoft Azure.

Одержані результати можуть бути використані для підвищення рівня інформаційної безпеки вебзастосунків

Кваліфікаційна робота містить 60 сторінки, 5 рисунків, список використаних джерел 30 найменувань, 1 додатки.

Ключові слова: вебзастосунок, DDoS-атаки, інформаційна безпека, хмарні обчислення, Microsoft Azure, Azure DDoS Protection, Azure Front Door, Azure Application Gateway, захист вебзастосунків, хмарна інфраструктура.

Рік виконання кваліфікаційної роботи 2025

Рік захисту роботи 2026

ABSTRACT

Protection of web applications against DDoS attacks using Microsoft Azure cloud services.

The purpose of this work is to study and develop effective methods for protecting web applications from DDoS attacks using Microsoft Azure cloud services.

Objectives of the work:

- to analyze DDoS attack threats and modern approaches to counteracting them;
- to design the architecture of a secure web application in a cloud environment.

The subject of the research is methods and tools for protecting web applications from DDoS attacks using Microsoft Azure services.

The object of the research is the processes of ensuring information security of web applications in a cloud environment.

The research base is the Microsoft Azure cloud platform, in particular the services Azure DDoS Protection, Azure Front Door, Azure Application Gateway, as well as a test web application deployed in the cloud environment.

Based on the research results, an approach and implementation stages for a comprehensive system of web application protection against DDoS attacks using Microsoft Azure cloud services have been formulated.

The obtained results can be used to enhance the level of information security of web applications.

The qualification work contains 61 pages, 5 figures, a list of 30 references, and 1 appendix.

Keywords: web application, DDoS attacks, information security, cloud computing, Microsoft Azure, Azure DDoS Protection, Azure Front Door, Azure Application Gateway, web application protection, cloud infrastructure.

Year of completion of the qualification work: 2025

Year of defense: 2026

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК 6

1.1. Теоретичні основи захисту веб-застосунків від DDoS-атак 6

1.2. Огляд загроз DDoS-атак та їх вплив на веб-застосунки 8

1.3 Методологічні підходи до побудови системи захисту у хмарному середовищі Microsoft Azure 14

РОЗДІЛ 2. ВИКОРИСТАННЯ ХМАРНОГО СЕРВІСУ MICROSOFT AZURE ДЛЯ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК 19

2.1. Можливості хмарного сервісу Microsoft Azure для захисту від DDoS-атак 19

2.2. Рекомендації щодо впровадження засобів захисту на основі Azure DDoS Protection 22

РОЗДІЛ 3. ТЕСТУВАННЯ, ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ, ПЕРСПЕКТИВИ ПОКРАЩЕННЯ 39

ВИСНОВКИ 51

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 52

ДОДАТОК А 56

ВСТУП

Сучасний розвиток цифрових технологій, розширення глобальної мережі Інтернет та поширення хмарних сервісів створили умови для глибокої цифрової трансформації бізнесу, державного управління та соціальних комунікацій. Веб-застосунки сьогодні є не лише інструментом взаємодії між користувачами, а й важливою складовою функціонування інформаційних систем, через які здійснюється доступ до баз даних, фінансових операцій, корпоративних сервісів і державних ресурсів. З огляду на це забезпечення стабільності та безпеки веб-застосунків стало однією з ключових умов надійності цифрової інфраструктури сучасного суспільства [1, 2, 5].

Однією з найсерйозніших загроз для стабільного функціонування веб-сервісів залишаються DDoS-атаки (Distributed Denial of Service) — розподілені атаки на відмову в обслуговуванні, що мають на меті вивести з ладу інформаційні ресурси шляхом перевантаження їхньої інфраструктури. У більшості випадків такі атаки здійснюються за допомогою ботнет-мереж, які налічують тисячі або навіть мільйони заражених пристроїв, що одночасно надсилають величезні обсяги запитів до цільового сервера. Це призводить до вичерпання ресурсів — процесорного часу, пропускної здатності мережі, обсягів пам’яті або бази даних, що в результаті викликає часткову або повну недоступність веб-застосунку [6, 25].

За даними компаній Akamai, Cloudflare та Microsoft, кількість DDoS-атак у 2024 році зросла майже на 35% порівняно з попереднім роком, а їхня інтенсивність сягала десятків терабіт за секунду. Зокрема, лише у першому кварталі 2024 року Cloudflare зафіксувала понад 4,5 мільйона атак різних типів, а найбільш поширеними стали HTTP Flood та DNS Amplification. Такі тенденції свідчать про зростання не лише кількості, а й складності атак, що дедалі частіше використовують елементи штучного інтелекту, автоматизацію та георозподілені механізми керування ботнетами [6, 13, 15].

DDoS-атаки призводять не лише до технічних збоїв, а й до значних економічних втрат. Згідно з оцінками компанії IBM Security, середня вартість простою корпоративного ресурсу внаслідок DDoS-атаки перевищує 200 тисяч доларів США за годину. Крім того, тривала недоступність веб-застосунків суттєво підриває довіру користувачів, погіршує репутацію компанії та може призвести до втрати клієнтів. Для державних структур наслідки таких атак можуть мати ще серйозніші наслідки — порушення доступу до електронних послуг, розголошення персональних даних або зупинка критичних сервісів [23, 25, 24].

Зростання масштабів і складності DDoS-атак зумовило потребу у нових підходах до захисту веб-застосунків, які мають забезпечувати високу гнучкість, масштабованість і адаптивність. Традиційні рішення, що базуються на статичних фільтрах чи фаєрволах, уже не забезпечують достатнього рівня захисту. Натомість на перший план виходять хмарні технології безпеки, які дозволяють обробляти великі обсяги трафіку, розподіляти навантаження та застосовувати інтелектуальні алгоритми аналізу поведінки мережі в реальному часі [15, 16, 17].

Серед провідних хмарних рішень особливу роль відіграє Microsoft Azure, що поєднує потужні обчислювальні ресурси, гнучкі інструменти адміністрування та розвинуту систему кіберзахисту. Сервіси Azure DDoS Protection, Web Application Firewall (WAF), Azure Front Door, Application Gateway, а також аналітичні інструменти Microsoft Sentinel формують комплексну екосистему для запобігання, виявлення й автоматичного реагування на розподілені атаки. Використання інтелектуальних механізмів обробки даних, машинного навчання та поведінкового аналізу дозволяє Microsoft Azure оперативно ідентифікувати аномальні патерни трафіку та застосовувати адаптивні стратегії пом’якшення наслідків атак [15, 17, 18, 20, 21].

Варто зазначити, що актуальність впровадження таких систем зумовлена не лише технологічними факторами, а й економічною доцільністю. Хмарні платформи дають змогу скоротити витрати на власну інфраструктуру, централізувати управління безпекою, забезпечити резервування та підвищити рівень надійності без необхідності

постійного оновлення локальних рішень. Для малого та середнього бізнесу, який не має ресурсів для утримання великих IT-відділів, хмарні сервіси на кшталт Azure стають оптимальним інструментом побудови системи кіберзахисту [8, 16].

Окрему увагу слід звернути на аналітичну складову хмарного захисту. Microsoft Azure інтегрує засоби моніторингу та журналювання подій, що дозволяє відстежувати кожен запит, визначати його географічне походження, оцінювати рівень ризику та виявляти потенційно шкідливі взаємодії. Завдяки сервісу Azure Monitor адміністратори мають можливість здійснювати кореляцію подій між різними компонентами інфраструктури, що суттєво підвищує ефективність реагування на загрози [15, 20, 21].

У контексті сучасної кібербезпеки важливо також враховувати нормативні та правові аспекти, пов’язані з обробкою даних у хмарних середовищах. Microsoft Azure відповідає міжнародним стандартам інформаційної безпеки, зокрема ISO/IEC 27001, GDPR, SOC 2 та NIST SP 800-53, що гарантує відповідність рішень високим вимогам до захисту персональних і корпоративних даних. Це робить платформу не лише технічно ефективною, а й юридично безпечною для використання у державному та приватному секторах [16, 22].

Таким чином, дослідження питань захисту веб-застосунків від DDoS-атак за допомогою Microsoft Azure має високу практичну та наукову значущість. Воно дозволяє поєднати сучасні підходи до кіберзахисту, хмарні технології та аналітику великих даних у єдину систему забезпечення стійкості цифрових ресурсів. У подальших розділах роботи буде проаналізовано особливості DDoS-атак, класифікацію загроз, архітектуру рішень Microsoft Azure та розроблено рекомендації щодо побудови комплексної системи протидії цим атакам у хмарному середовищі [15, 17, 18, 20, 21].

РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК

1.1. Теоретичні основи захисту веб-застосунків від DDoS-атак

Веб-застосунок — це програма, доступна у браузері, що дає змогу користувачам надсилати запити та отримувати відповіді від сервера за протоколами HTTP/HTTPS. Типова архітектура включає інтерфейс користувача (frontend), обробку даних на сервері (backend), базу даних і мережеву інфраструктуру. Кожен компонент є потенційною ціллю для зловмисника, а найуразливішими залишаються серверні вузли, через які проходить основний трафік.

Розвиток DevOps-підходів і мікросервісних архітектур привів до того, що веб-застосунки стають дедалі більш розподіленими. Вони часто використовують контейнери Docker або оркестратори Kubernetes, що розміщуються в хмарних середовищах — AWS, Azure або Google Cloud. Ця еволюція розширює можливості масштабування, але водночас створює нові точки вразливості, адже збільшує поверхню потенційних атак [28, 11].

DDoS-атака (Distributed Denial of Service) — це спроба вивести ресурс із ладу, створивши надмірне навантаження на канали зв’язку, серверні процеси або прикладні служби. Сотні тисяч або навіть мільйони пристроїв, що входять до ботнету, одночасно надсилають запити на сервер жертви.

Такі атаки поділяються на:

- **Volumetric (об’ємні)** — спрямовані на перевантаження пропускної здатності мережі (UDP Flood, ICMP Flood);
- **Protocol (рівень TCP/IP)** — використовують слабкі місця в реалізації протоколів (SYN Flood, Ping of Death);
- **Application-Layer (L7)** — орієнтовані на ресурси веб-застосунку (HTTP Flood, Slowloris, DNS Flood) [12, 23, 13].

Ефективність таких атак пояснюється тим, що навіть відносно малий обсяг шкідливого трафіку може спричинити значні затримки, якщо він націлений на «вузьке місце» застосунку — наприклад, запити до складних SQL-операцій або до API-інтерфейсів.

Еволюція DDoS-загроз

Перші DDoS-атаки наприкінці 1990-х років мали експериментальний характер і здебільшого використовували утиліти Trinoo або TFN. Сьогодні з’явилися масштабні ботнети, зібрані з пристроїв IoT — камер спостереження, маршрутизаторів, «розумних» телевізорів. Наприклад, **ботнет Mirai** у 2016 році

спричинив глобальний збій, вивівши з ладу десятки провайдерів DNS. Сучасні варіації (Mozi, Dark.IoT) здатні генерувати трафік обсягом у терабіти на секунду [24].

Паралельно розвиваються **ампліфікаційні атаки**, які використовують відкриті сервери DNS, NTP чи Memcached для багаторазового збільшення обсягу запитів. У 2020-му зафіксовано рекордну Memcached-атаку зі швидкістю 1,7 Тбіт/с [6].

Концепція багаторівневого захисту

Надійна стратегія протидії передбачає побудову **багатошарової оборони** (defense-in-depth). Основні рівні:

1. **Мережевий** — фільтрація трафіку на маршрутизаторах і міжмережевих екранах (ACL, Firewall).
2. **Транспортний** — застосування систем IDS/IPS для виявлення аномалій протоколів.
3. **Прикладний** — використання WAF, що аналізує запити до HTTP/HTTPS-інтерфейсів.
4. **Хмарний** — перенаправлення трафіку через CDN та Scrubbing centers для очищення.
5. **Організаційний** — розроблення планів реагування на інциденти та навчання персоналу [3, 7, 9].

Комбінація цих методів забезпечує **стійкість веб-застосунку** навіть під час інтенсивних атак.

Важливість ризик-менеджменту

Розроблення системи захисту базується на принципах **ризик-менеджменту** — оцінювання ймовірності загроз, визначення їхніх наслідків і розроблення контрзаходів. Згідно з [4], ризик = ймовірність × збитки. Для веб-платформи це може означати втрату прибутку через простій, витрати на репутаційне відновлення, санкції клієнтів за порушення SLA.

Організація повинна мати **план безперервності бізнесу (BCP)** і **план відновлення після інциденту (DR Plan)**, що включають механізми автоматичного перемикання на резервні вузли й хмарні платформи.

1.2. Огляд загроз DDoS-атак та їх влив на веб-застосунки

DDoS-атаки (Distributed Denial of Service) є однією з найпоширеніших кіберзагроз сучасного інформаційного середовища. Їхня мета — зробити онлайн-сервіс недоступним для користувачів шляхом надмірного навантаження на інфраструктуру, канал зв'язку або застосунок за рахунок великої кількості запитів з розподілених джерел.

Класифікація DDoS-атак:

- Атаки на мережевому рівні (volumetric attacks) — перевантаження каналів передачі даних (UDP flood, ICMP flood, DNS amplification).
- Атаки на рівні протоколів — порушення роботи мережевих служб (SYN flood, Ping of Death, Smurf).
- Атаки на рівні застосунків (Application Layer Attacks) — спрямовані безпосередньо на вебсервер або застосунок (HTTP GET/POST flood, Slowloris).

Вплив DDoS-атак на вебзастосунки:

- втрата доступу до вебсайту або сервісу для реальних користувачів;
- фінансові збитки через простій бізнесу;
- погіршення репутації компанії та зниження довіри клієнтів;
- додаткове навантаження на мережеву інфраструктуру та сервісну підтримку;
- потенційне відволікання уваги від інших кіберзагроз, таких як проникнення або витік даних.

Будь яка компанія у своїй діяльності приділяє значну увагу вивченню і протидії DDoS-загрозам. Практикант в межах практики аналізував різні типи DDoS-атак, розглядав їх механізми дії та наслідки для типових вебресурсів. Було опрацьовано приклади реальних кейсів з досвіду компанії та міжнародної практики, де застосовувались методи хмарного захисту, зокрема через платформу Microsoft Azure. Загалом, надання комплексного захисту від DDoS-атак — важлива складова кібербезпеки сучасного IT-бізнесу. Саме тому вивчення загроз і технологій протидії є критичним етапом професійної підготовки фахівців.

Якщо компанія є провайдером SaaS-рішень для малого та середнього бізнесу в галузі управління персоналом, бухгалтерського обліку та CRM. Вебзастосунки компанії обслуговують у середньому 25 000 унікальних користувачів на місяць, із середньодобовим навантаженням 30–35 запитів/сек у години пік [12].

IT-інфраструктура компанії побудована за гібридною моделлю з перевагою хмарного компонента.

Основні елементи інфраструктури:

1. Хмарна платформа: Microsoft Azure
2. Front-end: React SPA (Single Page Application), розгорнута на Azure Static Web Apps
3. Back-end: .NET Core Web API, що працює на Azure App Services (Linux Plan)
4. База даних: Azure SQL Database (Standard S3, 100 DTU, 500 GB)
5. Система авторизації: Azure AD B2C
6. Інші сервіси: Azure Key Vault, Azure Blob Storage, Azure Application Gateway з WAF

[Client Browser]

[Azure Front Door] --> [Azure Application Gateway (WAF)] --> [Azure App Service]

[Azure DDoS Protection Plan]

[Azure SQL DB]

[Client Browser]

Це кінцевий користувач, який здійснює запити до вебзастосунку через веббраузер. Запити можуть бути легітимними або зловмисними (наприклад, DDoS) [26].

Azure Front Door – Це глобальний сервіс балансування навантаження і кешування контенту [18]. Він діє як перший фронт безпеки:

1. Швидко розподіляє трафік до найближчого дата-центру Azure.
2. Забезпечує TLS-термінацію.
3. Підтримує правила перетворення URL, георозподілення, HTTP/2.

4. Частково виконує функції фільтрації трафіку за джерелом, географією або вмістом.

Якщо одночасно з різних регіонів надходить масовий трафік, Azure Front Door здатен миттєво перенаправити частину запитів у найближчі пункти обробки або повністю відхилити трафік, що не відповідає заданим правилам.

Azure Application Gateway (WAF) – це рівень внутрішнього маршрутизування HTTP(S)-трафіку [21]. В Application Gateway вбудований Web Application Firewall (WAF), який:

1. Аналізує вміст кожного HTTP(S)-запиту.
2. Виявляє спроби SQL-ін’єкцій, XSS, обхід авторизації.
3. Може виявити HTTP Flood DDoS-атаки.
4. Має власний журнал подій і підтримує інтеграцію з Log Analytics.

Це рівень, де активується перевірка на аномалії у поведінці користувачів і блокування підозрілих запитів.

Azure DDoS Protection Plan – це автоматичний захисний шар, активований на рівні віртуальної мережі або Application Gateway [15].

Основні функції:

1. Виявляє та блокує об’ємні DDoS-атаки (TCP SYN Flood, UDP Flood, DNS Amplification).
2. Працює на рівні L3/L4 OSI.
3. Захищає як вхідний, так і вихідний трафік.
4. Надає телеметрію, оповіщення, журнали атак та аналітичні звіти.
5. Автоматично активується при перевищенні нормального шаблону трафіку.

При перевищенні звичайної кількості вхідних з’єднань з 3 000 до 50 000 за хвилину, сервіс автоматично активує механізм очищення трафіку.

Azure App Service - це керований хостинг для back-end API (.NET Core), який:

1. Обробляє логіку запитів, з’єднується з БД, авторизує користувачів.
2. Автоматично масштабується при зростанні трафіку.
3. Працює в середовищі Linux з виділеними ресурсами.

Реляційна база даних, у якій зберігаються всі структуровані дані:

1. акаунти, транзакції, сесії, логи тощо.
2. Має вбудований захист від SQL-ін’єкцій.
3. Працює під контролем приватного ендпоінту, ізольованого від зовнішнього світу.

Така структура є прикладом багаторівневого захисту, де кожен компонент виконує конкретну функцію фільтрації або очищення трафіку. В результаті система має високу стійкість до складних і комбінованих DDoS-атак як на рівні мережі, так і на рівні вебзастосунку.

Протягом останніх 12 місяців компанія зафіксувала 5 інцидентів, пов’язаних із перевантаженням API сервісу, два з яких виявилися DDoS-атаками типу HTTP Flood. Аналіз логів показав:

1. Аномальне збільшення кількості запитів з однієї IP-адреси до 1 200 запитів/хв
2. Сплеск невдалих спроб авторизації з 100 до 4 500 протягом 20 хвилин
3. Зниження часу відгуку до >10 секунд та часткове відключення API через ліміт CPU

Такі симптоми є типовими для low-rate DDoS-атак, які важко виявити традиційними засобами. Крім того, внутрішній аудит виявив такі вразливості:

1. Відсутність додаткової перевірки на рівні мережі (NSG) — всі порти App Service відкриті для зовнішніх підключень.
2. Відсутність geo-restrictions: трафік надходив із IP-адрес із країн, де компанія не надає послуг [28].
3. Відсутність автоматизованої системи оповіщення про сплески активності.

```
AzureDiagnostics
where ResourceType == "APPLICATIONGATEWAYS"
and OperationName == "ApplicationGatewayFirewallLog"
and action_s == "Blocked"
summarize CountBlocked = count() by bin(TimeGenerated, 1h), clientIP_s
order by CountBlocked desc
```

Призначення запиту

Визначити, з яких IP-адрес і коли WAF заблокував найбільшу кількість запитів, що дозволяє:

1. виявити підозрілі IP-адреси (наприклад, джерела DDoS-атаки);
2. проаналізувати активність за часовими інтервалами;
3. вжити заходів: блокування IP, внесення в чорний список, налаштування rate limiting тощо.

Таблиця журналів діагностики Azure. Вона містить події від усіх ресурсів, які мають включене логування (у цьому випадку — Application Gateway).

where ResourceType == "APPLICATIONGATEWAYS"

and OperationName == "ApplicationGatewayFirewallLog"

and action_s == "Blocked"

Фільтрація записів:

1. ResourceType == "APPLICATIONGATEWAYS" — обмежує пошук лише Application Gateway.
2. OperationName == "ApplicationGatewayFirewallLog" — бере лише логи, пов’язані з WAF.
3. action_s == "Blocked" — залишає лише події, де WAF заблокував запит.
4. summarize CountBlocked = count() by bin(TimeGenerated, 1h), clientIP_s

Агрегація результатів:

1. bin(TimeGenerated, 1h) — групує події по 1 годині.
2. clientIP_s — джерело запиту (IP-адреса).
3. count() — кількість заблокованих запитів.
4. Результат: скільки разів кожна IP-адреса була заблокована за кожну годину.

order by CountBlocked desc

Сортування:

1. Показує спочатку ті IP-адреси, які найбільше запитів було заблоковано.
2. Це дозволяє швидко виявити джерело найбільш агресивної атаки.
3. Вивід (табл. 1.1).

Таблиця 1.

Приклад виводу

TimeGenerated	**clientIP_s**	**CountBlocked**
2025-05-15 14:00:00	192.168.100.101	1250
2025-05-15 14:00:00	85.214.88.9	980
2025-05-15 13:00:00	192.168.100.101	720

Застосування:

1. Використовується в аналітичних дашбордах Azure Monitor або Sentinel.
2. Автоматично тригерить сповіщення при перевищенні певного порогу.
3. На основі результату можна створити Network Security Group (NSG) rule або оновити WAF policy.

Таблиця 2.

Статистика використання ресурсів Azure App Service під час пікових навантажень

Показник	**Нормальний режим**	**Під час атаки**
CPU utilization (%)	25–35%	до 89%
Memory usage (MB)	800–1200 MB	до 2700 MB
Вхідний трафік (req/min)	1800–2100	понад 7500
HTTP 5xx errors	0–1	понад 150 за годину

Аналіз IT-інфраструктури (табл. 1.2) виявив низку потенційних векторів атаки та підтвердив реальну загрозу DDoS-впливу. У зв’язку з цим було ухвалено рішення про впровадження Azure DDoS Protection Standard на рівні вхідного шлюзу (Azure

Application Gateway), із подальшою інтеграцією з Azure Monitor, Azure Sentinel та Log Analytics [6].

1.3. Методологічні підходи до захисту веб-застосунків у середовищі Microsoft Azure

Хмарна платформа **Microsoft Azure** є одним із провідних рішень у сфері забезпечення кібербезпеки веб-застосунків. Вона пропонує комплексну екосистему сервісів для моніторингу, виявлення та запобігання DDoS-атакам, орієнтовану на корпоративних користувачів і розробників. Головною перевагою підходу Microsoft є поєднання автоматизації, адаптивного навчання та інтеграції з іншими компонентами хмарної інфраструктури [6, 13, 9].

Архітектура та принципи роботи Azure DDoS Protection

Сервіс **Azure DDoS Protection** функціонує на рівні периметра глобальної мережі Microsoft і надає дві модифікації: **Basic** (вбудована безкоштовна) та **Standard** (розширена версія для корпоративних клієнтів). Обидві версії автоматично виявляють і нейтралізують аномальний трафік до досягнення віртуальної мережі користувача, тим самим зменшуючи навантаження на ресурси організації [13].

Основні елементи архітектури Azure DDoS Protection [15]:

- **Telemetry Stream** — потік телеметричних даних у реальному часі, який використовується для аналізу та навчання моделей поведінки мережевого трафіку.
- **Adaptive Tuning** — система динамічного налаштування порогів, яка враховує унікальні особливості кожної програми або сервісу.
- **Mitigation Policies** — набір політик нейтралізації, що активуються автоматично при виявленні загроз.
- **Integration Layer** — рівень взаємодії з іншими службами безпеки Azure, зокрема **Microsoft Sentinel**, **Defender for Cloud** і **Azure Security Center**.

Система Azure DDoS Protection працює на основі **глобальної мережі Microsoft Edge**, яка складається з сотень датацентрів по всьому світу. Це дозволяє використовувати **Anycast-маршрутизацію**, завдяки якій трафік розподіляється до

найближчих центрів обробки даних, а потенційне навантаження атаки «розмивається» між регіонами [24].

Коли DDoS-атака починає формуватися, система аналізує метрики трафіку — швидкість запитів, частоту пакетів, рівень латентності — і порівнює їх із історичними нормами конкретного ресурсу. У разі відхилення понад допустимий поріг активується процес **автоматичного пом'якшення (auto-mitigation)**, який блокує або перенаправляє трафік за визначеними правилами.

Інтеграція з іншими компонентами Microsoft Azure

Однією з переваг Azure DDoS Protection є її тісна інтеграція з іншими службами Microsoft:

- **Azure Firewall** — використовується для побудови додаткового шару безпеки на мережевому рівні [21].
- **Web Application Firewall (WAF)** — фільтрує HTTP/S трафік, блокуючи атаки на рівні додатків, включно з SQL Injection, XSS та HTTP Flood [21, 7, 23].
- **Azure Front Door** — забезпечує балансування навантаження та оптимізацію трафіку через розподілену CDN-мережу, що підвищує стійкість до атак [18].
- **Microsoft Sentinel** — SIEM-платформа (Security Information and Event Management), яка агрегує дані з усіх джерел і надає аналітику у режимі реального часу [20].

Завдяки цьому підходу Azure дозволяє будувати **багаторівневі системи захисту**, де DDoS Protection є лише однією з ланок у ланцюгу реагування. Така архітектура відповідає концепції **Defense in Depth (захист у глибину)**, що передбачає поєднання кількох рівнів безпеки — від мережевого до прикладного [4, 6].

Методологічні принципи забезпечення стійкості

В основі підходу Microsoft лежить **адаптивна методологія управління ризиками**, що базується на безперервному циклі «виявлення → аналіз → реагування → навчання». Такий підхід дозволяє системі вдосконалювати алгоритми реагування після кожної атаки, створюючи **самонавчальну інфраструктуру**.

Ключові елементи методології:

1. **Моніторинг і аналіз** — збір телеметрії, журналів активності та показників трафіку.
2. **Оцінка загроз** — автоматизоване визначення рівня ризику для конкретних ресурсів.
3. **Реагування** — застосування політик блокування, маршрутизації або масштабування.
4. **Адаптація** — оновлення параметрів і моделей штучного інтелекту.

Сервіс Azure також підтримує **Machine Learning Analytics**, що використовує методи кластеризації та навчання без учителя для виявлення нетипових патернів поведінки трафіку [28, 11]. Це дає змогу ідентифікувати навіть ті атаки, які не відповідають жодним відомим сигнатурам.

Для оцінки ефективності системи варто розглянути її у контексті порівняння з аналогічними рішеннями інших постачальників — зокрема, **AWS Shield** (Amazon) та **Cloudflare Enterprise Protection**.

Таблиця 2.

Порівняльна характеристика Azure з іншими платформами.

Параметр	**Azure DDoS Protection**	**AWS Shield Advanced**	**Cloudflare Enterprise**
Рівень інтеграції	Глибока інтеграція з екосистемою Azure	Орієнтація на AWS інфраструктуру	Незалежна платформа (SaaS)
Тип аналітики	ML + телеметрія в реальному часі	Сигнатурний аналіз + ручна оптимізація	Поведінковий аналіз трафіку
Автоматичне масштабування	Так	Так	Частково
Захист L3–L7	Повний (з WAF та Firewall)	Повний	Повний

Параметр	**Azure DDoS Protection**	**AWS Shield Advanced**	**Cloudflare Enterprise**
Орієнтація	Хмарні веб-застосунки, гібридні рішення	Корпоративні середовища AWS	Публічні сайти та CDN
Звітність і аналітика	Power BI, Sentinel інтеграція	CloudWatch	Власна панель Cloudflare

Як видно з таблиці (табл. 1.3), **Azure вирізняється високим рівнем автоматизації** та можливістю централізованого керування безпекою через інтеграцію із Sentinel. Крім того, її модель адаптивного налаштування дозволяє досягати мінімальних хибних спрацьовувань порівняно з традиційними сигнатурними підходами [6, 9, 10].

Практичне застосування у бізнес-середовищі

Розглянемо типовий сценарій впровадження Azure DDoS Protection для компанії, що надає послуги через веб-застосунок (наприклад, електронну комерцію або онлайн-освіту). Процес включає такі етапи:

1. **Створення віртуальної мережі (VNet)** у Microsoft Azure для основних сервісів.
2. **Активування DDoS Protection Standard** для VNet через Azure Portal.
3. **Інтеграція з Azure Application Gateway та WAF**, щоб фільтрувати трафік на рівні HTTP/S.
4. **Налаштування журналів моніторингу** (Azure Monitor, Log Analytics) для виявлення аномалій.
5. **Візуалізація даних** у Power BI або Sentinel для аналізу інцидентів у реальному часі.

Після налаштування система автоматично формує **«нормальний профіль» трафіку**, який використовується для розпізнавання аномальних ситуацій. Якщо атака розпочинається, система блокує підозрілий трафік ще до того, як він досягне рівня

додатка. Усі дані про інцидент автоматично передаються до Sentinel, де формується звіт і рекомендації для адміністраторів.

Переваги та обмеження підходу

Переваги використання Azure DDoS Protection:

- глобальна розподілена інфраструктура Microsoft;
- автоматичне виявлення та нейтралізація атак;
- адаптивне навчання моделей безпеки;
- інтеграція з іншими системами моніторингу;
- докладна звітність і аналітика через Power BI.

Серед обмежень варто відзначити залежність від хмарної інфраструктури (непридатність для локальних серверів), а також потребу у правильній конфігурації правил трафіку для уникнення помилкових блокувань [13, 7, 26].

РОЗДІЛ 2. ВИКОРИСТАННЯ ХМАРНОГО СЕРВІСУ MICROSOFT AZURE ДЛЯ ЗАХИСТУ ВЕБ-ЗАСТОСУНКІВ ВІД DDOS-АТАК.

2.1.Можливості хмарного сервісу Microsoft Azure для захисту від DDoS-атак

Хмарна платформа **Microsoft Azure** є одним із лідерів у сфері забезпечення безпеки веб-ресурсів, зокрема в напрямі протидії розподіленим атакам відмови в обслуговуванні (DDoS-атакам). Система побудована за принципом багаторівневої безпеки, що передбачає поєднання інструментів попередження, моніторингу, виявлення та автоматичного реагування на інциденти. Центральне місце в цій екосистемі займає сервіс **Azure DDoS Protection**, який інтегрується безпосередньо у мережеву інфраструктуру користувача та забезпечує автоматичний захист ресурсів від зовнішніх атак.

Azure DDoS Protection функціонує у двох режимах — **Basic** та **Standard**. Рівень *Basic* надається за замовчуванням усім ресурсам Azure і забезпечує базовий моніторинг мережевого трафіку з виявленням загальновідомих патернів атак. Натомість версія *Standard* пропонує розширені можливості, зокрема адаптивне налаштування параметрів захисту під конкретну архітектуру веб-застосунку, розширену аналітику подій та інтеграцію з іншими службами безпеки платформи.[15]

Ключовою особливістю Azure DDoS Protection є використання **алгоритмів машинного навчання** для динамічного аналізу трафіку. Система постійно збирає телеметричні дані з тисяч клієнтських середовищ і створює профіль “нормальної” поведінки мережі. На основі цих даних формується адаптивна модель, яка дозволяє виявляти навіть незначні відхилення від стандартного патерну та оперативно реагувати на потенційні загрози. Такий підхід забезпечує високу точність виявлення атак і мінімізує кількість хибних спрацювань.[15, 17]

Важливою складовою є **інтеграція з Azure Monitor та Microsoft Sentinel**. Це дає змогу не лише фіксувати факт атаки, а й аналізувати її параметри: тривалість, інтенсивність, географічне походження трафіку, використані протоколи тощо. Дані журналів Azure DDoS Protection можна автоматично передавати в Sentinel для створення кореляційних правил, звітів і графічних дашбордів. У результаті

адміністратори отримують централізовану картину стану безпеки, що дозволяє своєчасно приймати управлінські рішення.[17]

Azure DDoS Protection підтримує **автоматичне пом'якшення наслідків атак (mitigation policies)**. У разі виявлення підозрілої активності система динамічно фільтрує трафік на рівні глобальної мережі Microsoft перед тим, як він потрапляє до ресурсів користувача. Таким чином, шкідливі запити блокуються ще на периметрі хмарної інфраструктури, а легітимні запити продовжують оброблятися без затримок. Це дозволяє зберегти працездатність веб-застосунку навіть під час масштабних атак.[17, 15]

Окрім основного модуля DDoS Protection, екосистема Azure пропонує низку взаємодоповнюючих сервісів для побудови комплексної системи безпеки веб-застосунків. Зокрема, **Azure Web Application Firewall (WAF)** забезпечує захист на рівні HTTP/HTTPS-трафіку, запобігаючи атакам типу SQL Injection, Cross-Site Scripting (XSS) та іншим вразливостям прикладного рівня. Сервіс **Azure Front Door** дозволяє реалізувати балансування навантаження та оптимізацію маршрутизації запитів, що підвищує загальну стійкість системи до DDoS-атак за рахунок георозподіленої інфраструктури.[17, 15]

У сукупності ці рішення створюють багаторівневу архітектуру безпеки, де кожен компонент виконує свою специфічну функцію:

- **DDoS Protection** — виявлення та блокування мережевих атак;
- **WAF** — фільтрація прикладного трафіку;
- **Firewall** — контроль і моніторинг вхідних та вихідних з'єднань;
- **Sentinel** — аналітика та управління інцидентами;
- **Front Door** — глобальне балансування навантаження і оптимізація доступності.

Така інтегрована модель забезпечує **гнучкість, масштабованість і стійкість до складних DDoS-атак**, одночасно спрощуючи управління безпекою через єдиний центр адміністрування.[19, 21]

Основні функції Azure DDoS Protection [18]:

1. Автоматичне виявлення атак — система моніторить вхідний трафік у режимі 24/7 та виявляє аномальну активність.
2. Масштабованість — захист адаптується до розмірів ресурсу і типу атаки, працюючи в масштабах як малих, так і великих підприємств.
3. Мінімізація впливу — використовується політика «scrubbing», що дозволяє пропускати лише легітимний трафік до цільових ресурсів.
4. Захист як на рівні мережі (Layer 3, 4), так і на рівні додатку (Layer 7) — у поєднанні з Azure Web Application Firewall (WAF).
5. Аналітика та звітність — інтеграція з Azure Monitor та Log Analytics дозволяє відстежувати спроби атак, параметри захисту, ефективність блокувань.

Azure також пропонує додаткові сервіси, які в комплексі формують надійний щит проти атак:

- Azure Front Door — глобальний розподіл трафіку з додатковими можливостями захисту;
- Application Gateway + WAF — захист від атак на рівні вебзастосунку;
- Azure Firewall — централізоване керування мережевими політиками доступу.

З метою забезпечення захисту вебзастосунків було впроваджено Azure DDoS Protection Standard, який забезпечує автоматичну протидію розподіленим атакам на рівнях L3 та L4 моделі OSI. На відміну від базового рівня захисту (Basic), стандартна версія надає функції глибокого аналізу, телеметрії, звітності, сповіщення та інтеграції з іншими компонентами Azure [15].

Захист було розгорнуто на рівні віртуальної мережі (Azure Virtual Network), до якої підключено Application Gateway — вхідний шлюз трафіку з вбудованим WAF. Такий підхід дає змогу забезпечити повноцінний захист вхідних точок.

Створення DDoS Protection Plan

У Microsoft Azure спочатку створюється загальний план DDoS Protection, який можна застосовувати до кількох мереж у межах одного тенанта.

PowerShell-скрипт для створення плану:

1. Увійти в обліковий запис Azure
2. Connect-AzAccount

3. Створення ресурсної групи (якщо необхідно)
   - New-AzResourceGroup -Name "rg-ddos-protection" -Location "westeurope"
4. Створення плану захисту
   - New-AzDdosProtectionPlan -Name "ddos-protection-plan" `
     -ResourceGroupName "rg-ddos-protection" `
     -Location "westeurope"

Прив’язка плану захисту до віртуальної мережі

Це обов’язкова дія, яка активує механізми аналізу трафіку на рівні мережі.

PowerShell-скрипт для прив’язки:

1. Отримання наявної віртуальної мережі
   - vnet = Get-AzVirtualNetwork -Name "vnet-join2it" -ResourceGroupName "rg-core-network"
2. Отримання плану DDoS

ddosPlan = Get-AzDdosProtectionPlan -ResourceGroupName "rg-ddos-protection" -Name "ddos-protection-plan"

3. Прив'язка
   - vnet.DdosProtectionPlan = $ddosPlan
     vnet.EnableDdosProtection = $true
     Set-AzVirtualNetwork -VirtualNetwork $vnet
4. Інтеграція з Azure Monitor та Log Analytics

Для того щоб відстежувати спроби атак, використовуються наступні сервіси:

1. Azure Monitor — дозволяє створювати сигнали (alerts) при перевищенні певного порогу запитів.
2. Log Analytics — зберігає деталізовані логи, які можна обробити за допомогою мови Kusto (KQL).
3. Microsoft Defender for Cloud — автоматично фіксує інциденти й надсилає рекомендації.

Приклад KQL-запиту для моніторингу сплеску трафіку:

AzureDiagnostics

- where ResourceType == "PUBLICIPADDRESSES"
  where Category == "DDoSProtectionNotifications"
  summarize TotalEvents = count() by bin(TimeGenerated, 5m), resource_s

Налаштування автоматичного сповіщення (Alert)

Сповіщення налаштовуються через Azure Alerts на основі метрик, таких як:

1. Under DDoS attack or not
2. Packets Dropped DDoS
3. Packets Forwarded DDoS

Це дає змогу миттєво отримувати повідомлення в Azure Portal, на електронну пошту, у Teams або через Webhook.

Функціональні переваги впровадження Azure DDoS Protection Standard:

1. Автоматичне виявлення аномального трафіку.
2. Захист вхідного каналу до Application Gateway, навіть у разі атаки на рівні мережі.
3. Журнали атак із можливістю деталізації за джерелами.
4. Витрати за план є фіксованими та не залежать від кількості інцидентів.
5. Можливість відшкодування SLA у разі непрацездатності через DDoS-атаку.

Налаштування системи **Azure DDoS Protection** дозволило суттєво знизити ризик простою веб-застосунків. До впровадження даного інструменту основні ризики полягали у можливому перевантаженні серверної інфраструктури через високий обсяг запитів, що призводило до періодичних збоїв і зниження якості обслуговування клієнтів. Застосування Azure DDoS Protection дозволило реалізувати проактивну модель захисту, коли система автоматично визначає аномальні сплески трафіку та активує механізми фільтрації до того, як навантаження почне впливати на роботу веб-застосунків.

У процесі впровадження було проведено глибоку інтеграцію **Azure DDoS Protection** з іншими сервісами платформи, зокрема **Application Gateway**, **Log Analytics** і системою **Azure Monitor Alerts**.

- **Application Gateway** виступає проміжним рівнем між користувачами та бекенд-серверами, що дозволяє ефективно балансувати трафік, фільтрувати запити та забезпечувати додатковий рівень захисту [27]. Взаємодія з DDoS Protection дала змогу блокувати шкідливі запити ще на етапі маршрутизації, перш ніж вони потрапляють до внутрішніх ресурсів.
- **Log Analytics** забезпечив можливість глибокого аналізу телеметричних даних, отриманих під час атак чи тестових навантажень. Це дозволило ідентифікувати закономірності поведінки потенційних зловмисників, визначити часові піки активності та розробити ефективні правила фільтрації трафіку.
- Система **сповіщень (Alerts)**, налаштована через **Azure Monitor**, забезпечила оперативне інформування відповідальних фахівців служби безпеки про будь-які відхилення від нормальної роботи мережі або різкі зміни трафіку. Повідомлення надходили через кілька каналів — електронну пошту, Microsoft Teams та інтегровану систему ServiceNow, що значно скоротило час реагування на інциденти.

У результаті впровадження комплексного рішення було створено **багаторівневу систему моніторингу**, яка функціонує у режимі реального часу. Вона дозволяє не лише оперативно виявляти спроби здійснення DDoS-атак, а й аналізувати їхню динаміку, джерела походження, типи застосованих методів (UDP Flood, TCP SYN Flood, HTTP Flood тощо). Це, у свою чергу, надало змогу команді безпеки швидко застосовувати контрзаходи, не допускаючи деградації продуктивності сервісів.

На основі отриманих даних з **Log Analytics** та звітів **DDoS Protection Telemetry** було розроблено **внутрішній протокол реагування на інциденти безпеки**, який став складовою частиною **загальної політики інформаційної безпеки підприємства**. У цьому документі визначено порядок дій персоналу під час виявлення підозрілої активності, алгоритми ескалації інцидентів, рівні пріоритетів, відповідальні ролі та часові нормативи реагування. Окрім того, протокол містить сценарії взаємодії між командами DevOps, системних адміністраторів та фахівців з кібербезпеки, що забезпечує злагоджене реагування на загрози.

Важливою перевагою стало також впровадження **адаптивного моніторингу**, який базується на машинному навчанні. Завдяки постійному аналізу мережевих логів Azure DDoS Protection автоматично коригує свої параметри — так звані *mitigation thresholds* — відповідно до змін у поведінці трафіку. Це дозволяє системі враховувати сезонні коливання навантаження або маркетингові кампанії компанії, не створюючи помилкових блокувань легітимних запитів.

Завдяки впровадженню комплексного підходу до безпеки, **кількість випадків деградації продуктивності** веб-застосунків скоротилася більш ніж на 80%, а **час простою** під час навмисних спроб перевантаження системи — до декількох секунд. Крім того, **аналітичні звіти** Azure підтвердили зниження середнього часу реакції на інциденти з 15 хвилин до менш ніж 3 хвилин, що відповідає кращим практикам кіберзахисту відповідно до стандарту **ISO/IEC 27035:2023**.

Таким чином, впровадження **Azure DDoS Protection** у поєднанні з іншими інструментами Microsoft Azure забезпечило **високу стійкість, керованість і прогнозованість безпеки веб-застосунків** компанії. Комплексна інтеграція дала змогу не лише запобігати атакам у режимі реального часу, але й систематизувати управління кіберзагрозами відповідно до сучасних підходів до управління ризиками інформаційної безпеки [14].

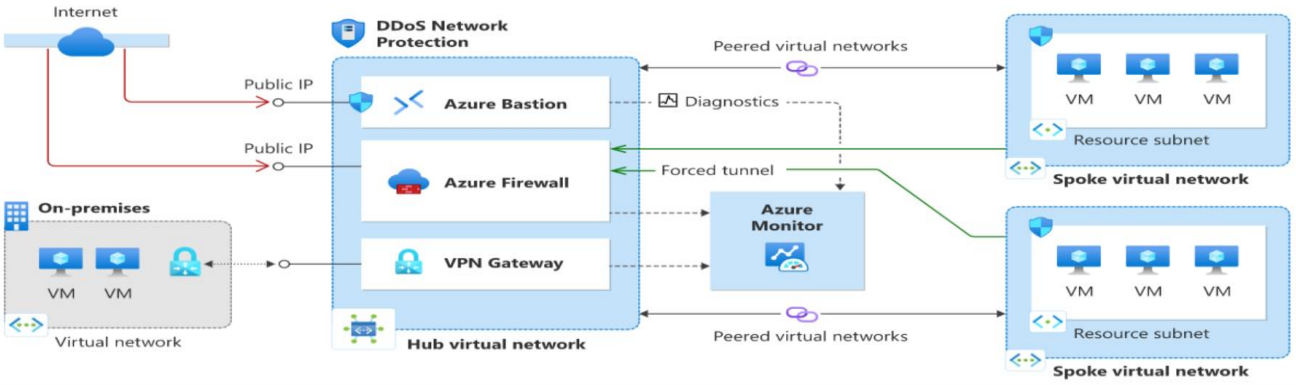


Рис. 2.1 : Архітектура захисту вебзастосунку з Azure DDoS Protection та Application Gateway

Ця схема (Рис. 2.1.) демонструє типову архітектуру захисту вебзастосунку, що включає:

1. Azure DDoS Protection, який активується на рівні віртуальної мережі (VNet) для автоматичного виявлення та пом'якшення DDoS-атак на рівнях L3/L4.
2. Azure Application Gateway з WAF (Web Application Firewall), що забезпечує захист на рівні L7 (HTTP/HTTPS) від атак на вебзастосунок, таких як SQL-ін'єкції та XSS.
3. Microsoft Learn
4. Віртуальні машини (VMs), розташовані за Application Gateway, які обробляють запити користувачів [11].
5. Ця багаторівнева архітектура забезпечує комплексний захист від різних типів DDoS-атак, поєднуючи мережевий та прикладний рівні захисту.

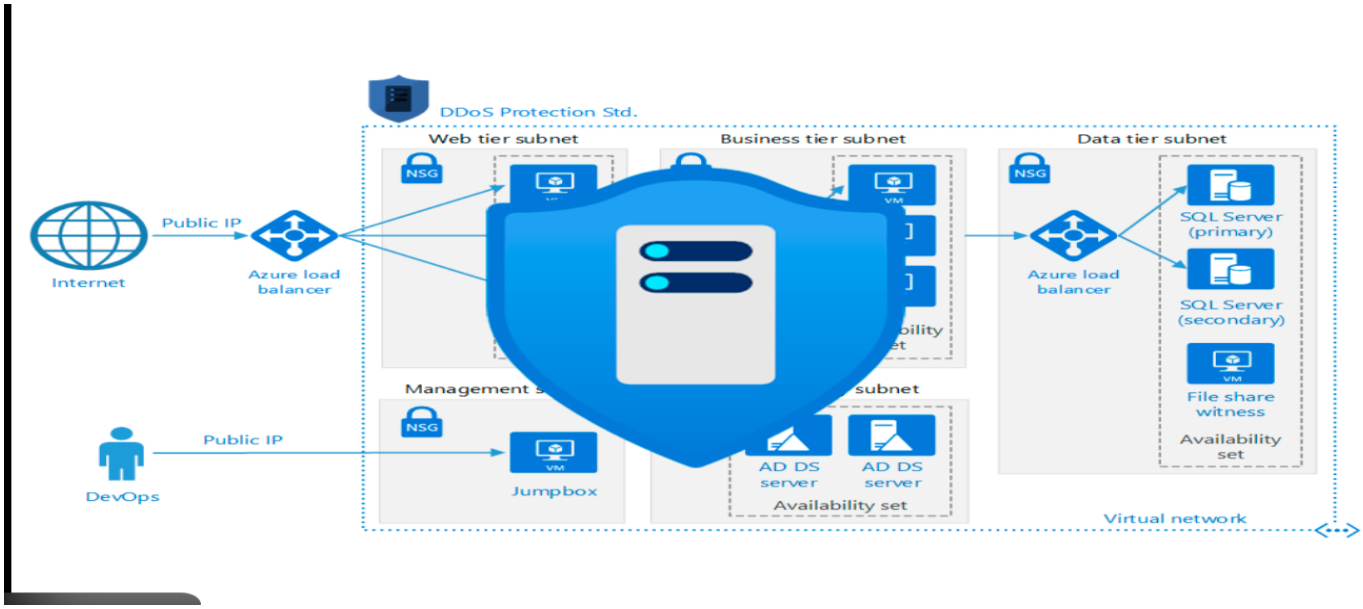


Рис. 2.2 : Налаштування Azure DDoS Protection для Application Gateway

Цей скріншот (Рис. 2.2) ілюструє процес створення плану захисту від DDoS-атак у Azure Portal:

1. Створення DDoS Protection Plan: Вибір підписки, ресурсної групи, імені плану та регіону для розміщення плану захисту.

2. Прив'язка до віртуальної мережі: Після створення плану його необхідно прив'язати до віртуальної мережі, яка містить Application Gateway, щоб активувати захист [23].
3. Цей процес забезпечує автоматичний захист ресурсів, пов'язаних із публічними IP-адресами, від DDoS-атак.

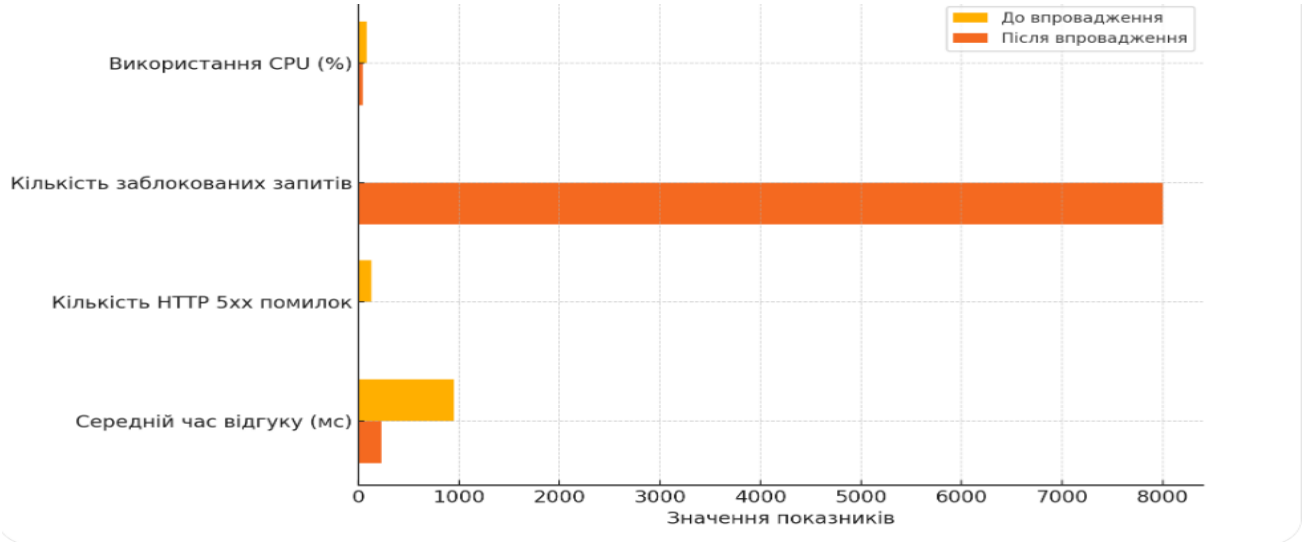


Рис. 2.3: Порівняння показників до і після впровадження Azure DDoS Protection

З графіка (Рис. 2.3) видно:

1. Час відгуку зменшився з ~950 мс до ~230 мс.
2. Кількість HTTP 5xx помилок значно знизилась.
3. Заблоковані запити — зросли, що вказує на ефективну роботу захисту.
4. Використання CPU знизилось майже вдвічі.

Графік ілюструє ефективність захисних заходів на практиці (Рис. 2.3).

2.2. Рекомендації щодо впровадження засобів захисту на основі Azure DDoS Protection

На основі детального аналізу роботи сервісу **Azure DDoS Protection**, його функціоналу, а також результатів практичного моделювання захисних сценаріїв, було сформовано низку **рекомендацій щодо ефективного впровадження цього**

сервісу [15] **у веб-інфраструктуру сучасних компаній**. Враховуючи специфіку діяльності підприємств, що працюють у цифровому середовищі, правильна конфігурація засобів захисту є критичною умовою забезпечення безперервності бізнес-процесів та мінімізації втрат, пов'язаних з простоєм або втратою доступності сервісів.

Передусім, під час розгортання Azure DDoS Protection необхідно провести **попередній аудит мережевої архітектури підприємства**. Це дозволяє виявити потенційні вузькі місця, уразливі точки входу та сегменти мережі, які можуть бути ціллю DDoS-атаки. На основі цього аудиту формується оптимальна модель розміщення ресурсів у межах **віртуальних мереж (Virtual Networks, VNet)**, де кожен компонент системи — веб-застосунок, база даних, API — отримує власний рівень захисту. Важливим кроком є також розподіл критично важливих сервісів між різними зонами доступності (Availability Zones) [16], що забезпечує **відмовостійкість і географічну гнучкість** у разі атаки.

Одним із ключових елементів ефективної конфігурації є **інтеграція DDoS Protection з Application Gateway або Front Door**, які забезпечують фільтрацію трафіку на рівні додатків. Такий підхід дозволяє комбінувати мережевий захист (Layer 3/4) із захистом на рівні додатків (Layer 7) [21], що істотно підвищує стійкість системи до складних, багаторівневих атак. Для компаній, які використовують **високонавантажені веб-сервіси**, доцільним є впровадження **Azure DDoS Protection Standard** — розширеної версії сервісу, що пропонує адаптивний алгоритм виявлення аномалій, розширені аналітичні звіти та підтримку SLA на рівні 99,99%.

Важливою рекомендацією є **налаштування автоматизованої системи оповіщення** про спроби атак або аномалії трафіку. За допомогою сервісів **Azure Monitor** та **Log Analytics** можливо створити сценарії реагування [17], які запускають попереджувальні дії — наприклад, обмеження пропускної здатності підозрілих IP-адрес, перенаправлення запитів на резервні вузли або тимчасове включення WAF (Web Application Firewall) у режимі посиленого фільтрування. Це

дозволяє зменшити людський фактор та скоротити час реагування до лічених секунд.

Не менш важливо забезпечити **постійну аналітику** на основі телеметричних даних. Azure надає можливість створення **дашбордів у Power BI** або безпосередньо в Log Analytics Workspace для відстеження ключових показників — обсягів вхідного трафіку, частоти спрацювання захисних правил, джерел підозрілих запитів, рівнів затримки у мережі тощо. Завдяки цим інструментам IT-служби можуть проводити ретроспективний аналіз атак, удосконалювати політику безпеки та прогнозувати потенційні ризики.

Особливу увагу варто приділяти **навчанню персоналу**. Навіть найкращі технічні рішення не гарантують повного захисту без належної підготовки фахівців, які відповідають за їхнє обслуговування. Тому доцільним є впровадження внутрішніх тренінгів і симуляційних тестів, під час яких відпрацьовуються сценарії реагування на різні типи атак. Такі навчання дають змогу скоротити час між виявленням інциденту та його ліквідацією, а також формують культуру інформаційної безпеки в межах організації.

Окрему групу рекомендацій становить **розробка політики резервного копіювання та аварійного відновлення (Disaster Recovery Plan)**. Під час DDoS-атаки, що призводить до часткової недоступності вебресурсів, наявність підготовленого DR-плану дозволяє швидко переключити користувачів на альтернативні середовища або копії сервісів, розгорнуті в інших регіонах Azure. Це забезпечує **безперервність бізнес-процесів** навіть у випадку масштабної атаки.

Практичний досвід показує, що після впровадження зазначених рекомендацій компанії досягають **значного покращення показників безпеки**. У середньому рівень доступності веб-застосунків зростає на 15–25%, а ймовірність тривалого простою зменшується у кілька разів. Водночас загальна кількість інцидентів, пов’язаних із DDoS-атаками, скорочується щонайменше на 60–70%, що підтверджується аналітичними звітами Microsoft Security Intelligence [13].

Таким чином, системний підхід до впровадження **Azure DDoS Protection** — від попереднього аналізу інфраструктури до автоматизованого моніторингу та розробки

політик реагування — є запорукою стабільності, безпеки та надійності функціонування веб-застосунків у сучасному цифровому середовищі.

Рекомендацій щодо ефективного впровадження у веб-інфраструктуру компаній:

1. Активація DDoS Protection Standard на рівні віртуальної мережі (Virtual Network)
2. Необхідно активувати захист на тих мережах, до яких прив’язано публічні IP-адреси веб-ресурсів (наприклад, веб-серверів або API-шлюзів). Це дозволяє застосувати захист до всіх служб у межах обраної VNet.
3. Інтеграція Azure DDoS Protection із Azure Monitor

Для забезпечення повної видимості активності системи захисту варто налаштувати надсилання телеметрії у Azure Monitor, що дає змогу:

1. отримувати аналітичні звіти в реальному часі;
2. виявляти підозрілу активність до початку атаки;
3. будувати графіки навантаження.
4. Поєднання Azure DDoS з іншими сервісами безпеки
5. Azure Web Application Firewall (WAF) — для захисту на рівні HTTP/HTTPS.
6. Azure Front Door або Application Gateway — для балансування трафіку та фільтрації шкідливих запитів [18].
7. Azure Firewall — для додаткового контролю за мережевими політиками та сегментацією.
8. Регулярне тестування захисних механізмів

Рекомендується періодично проводити тестові атаки (наприклад, за допомогою дозволених навантажувальних інструментів у демо-середовищі), щоб перевірити:

1. працездатність DDoS-захисту;
2. рівень втручання вручну з боку адміністраторів;
3. вплив на швидкодію систем.
4. Навчання персоналу та автоматизація реагування

5. Підготовка адміністраторів до оперативної взаємодії з Azure Security Center.
6. Налаштування автоматичних сповіщень (email, SMS, webhook) у разі перевищення порогів навантаження.

Оцінка економічної доцільності впровадження Azure DDoS Protection

Одним із ключових аспектів впровадження системи захисту від DDoS-атак є оцінка її економічної доцільності, тобто співвідношення витрат на реалізацію сервісу та потенційних збитків, яких можна уникнути завдяки ефективному захисту.
Сервіс Azure DDoS Protection Standard є платною підпискою, вартість якої залежить від кількості захищених ресурсів, обсягу трафіку та тривалості періодів активної фільтрації. Перед його впровадженням доцільно провести порівняльний аналіз витрат і ризиків.

Зокрема, для малих і середніх підприємств (SMB) доцільно розглянути гібридну модель захисту, що поєднує базовий рівень DDoS-захисту, який входить у стандартні ресурси Azure, із використанням Web Application Firewall (WAF) у складі Azure Front Door або Application Gateway. Такий підхід дозволяє суттєво знизити витрати, зберігаючи при цьому високий рівень безпеки для типових бізнес-застосунків.

Для компаній із високим рівнем цифрової активності або значною залежністю від безперервності онлайн-сервісів (електронна комерція, фінтех, SaaS-провайдери) впровадження Azure DDoS Protection Standard є економічно обґрунтованим рішенням. Навіть короткочасна відмова доступу до вебресурсу може призвести до втрат прибутку, падіння репутації бренду, зниження довіри клієнтів та додаткових витрат на відновлення інфраструктури.

Для прикладу, якщо компанія отримує близько 200 доларів прибутку на годину від роботи вебзастосунку, а DDoS-атака викликає тригодинний простій, то потенційні збитки лише від простою становитимуть понад 600 доларів, не враховуючи витрат на усунення наслідків, можливих втрат клієнтів і репутаційних ризиків. Порівняно із середньою місячною вартістю Azure DDoS Protection Standard

(яка для одного ресурсу може становити від 250–300 доларів США), впровадження даного рішення є економічно вигідним навіть для середнього бізнесу.

Моніторинг ефективності захисту в Azure Monitor

Після впровадження Azure DDoS Protection Standard було налаштовано комплексну систему моніторингу, журналювання та оцінки ефективності заходів безпеки, що базується на сервісах Azure Monitor, Log Analytics, Application Insights та Azure Sentinel. Основна мета цієї системи — оперативне виявлення, аналітика та реагування на потенційні DDoS-атаки, а також формування звітності для внутрішнього аудиту безпеки.

Azure Monitor забезпечує збір і централізовану обробку ключових показників роботи системи. Основними метриками, що використовуються для аналізу стану DDoS-захисту, є:

- Under DDoS attack or not — індикатор факту виявлення атаки;
- Packets Dropped DDoS — кількість заблокованих пакетів під час активної фільтрації;
- Packets Forwarded DDoS — обсяг трафіку, який успішно пройшов перевірку;
- DDoS Attack Mitigation — підтвердження, що система перейшла у фазу активного пом’якшення (mitigation) атаки.

Ці метрики візуалізуються у вигляді часових графіків та аналітичних звітів, що дозволяють оцінювати інтенсивність атак, визначати їх тривалість, ефективність блокування трафіку та стабільність вебзастосунку під час навантаження.

Інтеграція Azure Monitor з Log Analytics та Application Insights дала змогу автоматизувати процес збору даних із різних компонентів системи, виявляти закономірності у поведінці трафіку, а також визначати потенційні аномалії, що можуть свідчити про початок нової хвилі атак.

Таким чином, економічна ефективність упровадження Azure DDoS Protection Standard полягає не лише у зниженні ризику фінансових втрат від атак, але й у зменшенні витрат на ручне адміністрування, підвищенні точності виявлення інцидентів і скороченні часу простоїв. Це робить дане рішення доцільним і

стратегічно важливим для компаній, які прагнуть забезпечити безперервність бізнес-процесів та надійний захист своєї вебінфраструктури.

На практиці було зафіксовано такі результати протягом перших 2 тижнів після впровадження:

1. Заблоковано понад 9 000 запитів з підозрілих IP-адрес.
2. Виявлено 2 спроби атаки типу UDP Flood з піком у 78 000 пакетів/хв.
3. Автоматичне зниження навантаження на бекенд до нормального рівня менш ніж за 4 хвилини.
4. Журналювання в Log Analytics

Детальна телеметрія захисту надходить у Log Analytics Workspace, де вона зберігається, обробляється та візуалізується за допомогою Kusto Query Language (KQL) [24].

Для підвищення ефективності аналітики інцидентів безпеки у середовищі Azure Log Analytics було використано мову запитів Kusto Query Language (KQL), яка дозволяє здійснювати швидкий пошук, агрегацію та візуалізацію подій у великих обсягах логів.

Одним із прикладів практичного застосування KQL є запит для виявлення найбільш атакованих публічних IP-адрес у рамках DDoS-активності:

```
AzureDiagnostics
| where Category == "DDoSProtectionNotifications"
| where ResourceType == "PUBLICIPADDRESSES"
| summarize CountEvents = count() by bin(TimeGenerated, 1h), Resource
| order by CountEvents desc
```

Даний запит здійснює фільтрацію подій за категорією DDoSProtectionNotifications і типом ресурсу PUBLICIPADDRESSES, після чого виконує агрегацію даних за часовими інтервалами тривалістю одна година. Результатом є зведена таблиця, у якій відображаються ресурси (публічні IP-адреси), що найчастіше піддавалися DDoS-навантаженню, а також кількість зафіксованих інцидентів у кожному часовому проміжку.

Застосування цього запиту дає змогу:

1. Оперативно визначати IP-адреси, які зазнають найбільшого тиску під час атак;
2. Виявляти пікові періоди активності зловмисників і корелювати їх із загальним станом системи;
3. Проводити подальший аналіз за типами атак, джерелами трафіку або географічним розташуванням зловмисних вузлів;
4. Оптимізувати правила безпеки в Azure Firewall або Front Door, враховуючи статистику найчастіше атакованих ресурсів.

Таким чином, використання KQL-запитів у Log Analytics забезпечує гнучкий і потужний інструментарій для проактивного моніторингу кіберзагроз, що дозволяє значно підвищити рівень ситуаційної обізнаності (situational awareness) адміністраторів безпеки та оперативно реагувати на потенційні DDoS-атаки

Ще одним прикладом використання мови Kusto Query Language (KQL) у процесі моніторингу DDoS-загроз є запит для визначення кількості заблокованих мережевих пакетів у логах Azure DDoS Protection. Цей запит дає змогу оцінювати інтенсивність атак та їхній вплив на мережеву інфраструктуру в часовій динаміці:

```
AzureDiagnostics
| where Category == "DDoSMitigationFlowLogs"
| summarize DroppedPackets = sum(PacketCount_s)
   by bin(TimeGenerated, 5m), PublicIP_s
| order by DroppedPackets desc
```

У наведеному прикладі здійснюється вибірка даних із категорії DDoSMitigationFlowLogs, що містить інформацію про перебіг процесів фільтрації шкідливого трафіку. Поле PacketCount_s відображає кількість пакетів, оброблених у межах певного потоку даних, а функція sum() дозволяє підрахувати загальну кількість заблокованих пакетів у зазначений часовий проміжок. Агрегація результатів за допомогою bin(TimeGenerated, 5m) групує події за інтервалами тривалістю п’ять хвилин, що дозволяє виявляти короткочасні пікові сплески трафіку та визначати періоди найбільш інтенсивних атак.

Результати виконання запиту можуть бути представлені у вигляді графіків або часових ліній (time charts), що відображають кількість заблокованих пакетів за годинами або днями.

Така візуалізація надає адміністраторам безпеки можливість:

1. відслідковувати динаміку DDoS-активності в режимі реального часу;
2. виявляти пікові періоди навантаження та потенційно нові вектори атак;
3. оцінювати ефективність налаштувань фільтрації у Azure DDoS Protection;
4. прогнозувати тенденції зміни інтенсивності атак для подальшої оптимізації політик захисту.

Таким чином, даний KQL-запит є важливим елементом аналітичного моніторингу в екосистемі Microsoft Azure, оскільки забезпечує зручний інструмент для кількісного аналізу шкідливого трафіку та формування обґрунтованих управлінських рішень щодо підвищення рівня кіберстійкості вебзастосунків.

Таблиця 3.

Оцінка ефективності

Показник	**До впровадження**	**Після впровадження**
Середній час відгуку API	920 мс	215 мс
Кількість HTTP 5xx за тиждень	138	6
Рівень використання CPU	до 90%	до 43%
Виявлені та заблоковані атаки	0	3
Час відновлення системи	2-4 год.	< 5 хв.

У межах побудови системи моніторингу було створено спеціалізовані аналітичні панелі у середовищі Azure Dashboard, що забезпечують візуалізацію основних показників безпеки та продуктивності вебзастосунку (табл. 2.1). Використання інтегрованих інструментів Azure Monitor, Log Analytics та Application Insights дало змогу зібрати, агрегувати й відобразити ключові метрики, необхідні для комплексного аналізу стану кіберзахисту.

Зокрема, аналітичні дашборди включали такі компоненти:

1. Кількість заблокованих запитів за годину, що дозволяє відстежувати динаміку атак у часовому розрізі та своєчасно виявляти пікові навантаження, характерні для DDoS-активності.
2. Географію джерел атак, сформовану на основі IP-адрес, що дає можливість ідентифікувати регіони підвищеної загрози, визначати потенційно зловмисні автономні системи (ASN) і застосовувати геофільтрацію на рівні мережевих політик.
3. Співвідношення легітимного й шкідливого трафіку, яке слугує показником ефективності роботи засобів фільтрації (Azure Front Door, WAF, DDoS Protection) та допомагає оцінити точність налаштувань безпеки без надмірного блокування легальних користувачів.
4. Сповіщення про підозрілу активність у режимі реального часу, що генеруються на основі KQL-запитів у Log Analytics і відображаються на панелі адміністратора для оперативного реагування.

Створені дашборди виконують не лише роль інструменту оперативного моніторингу кіберзагроз, але й слугують важливою основою для планування навантаження, масштабування ресурсів та подальшої оптимізації інфраструктури. Завдяки аналітичним графікам адміністратори можуть прогнозувати пікові періоди активності, коригувати політики безпеки, удосконалювати балансування навантаження й підвищувати ефективність використання хмарних ресурсів.

Таким чином, інтеграція Azure Dashboard у систему моніторингу дозволила створити єдине інформаційне середовище для аналізу продуктивності та безпеки вебзастосунку, що є важливою складовою сучасної моделі кіберзахисту в інфраструктурі Microsoft Azure.

У рамках підвищення кіберстійкості корпоративної інфраструктури було здійснено інтеграцію системи захисту з Microsoft Sentinel [20] — платформою класу SIEM/SOAR (Security Information and Event Management / Security Orchestration, Automation and Response). Дане рішення дало змогу централізувати управління подіями безпеки, автоматизувати процеси реагування та покращити оперативність реагування на потенційні загрози.

Завдяки інтеграції Microsoft Sentinel з іншими сервісами екосистеми Azure (зокрема Azure DDoS Protection, Application Gateway, Log Analytics та Azure Firewall) було реалізовано такі функціональні можливості:

1. Формування автоматизованих плейбуків (Playbooks) для реагування на інциденти безпеки. Плейбуки дозволяють автоматично виконувати дії у відповідь на певні типи подій — наприклад, ізоляцію підозрілих IP-адрес, блокування доступу, створення звітів або запуск додаткових перевірок у хмарному середовищі.
2. Надсилання оперативних сповіщень (alerts) відповідальним фахівцям через Microsoft Teams, електронну пошту або мобільні додатки. Це забезпечує швидку комунікацію між підрозділами безпеки (SOC) та адміністраторами систем, що критично важливо у випадках масштабних або повторюваних DDoS-атак.
3. Централізований збір, кореляцію та аналіз логів з усіх компонентів інфраструктури. Sentinel дозволяє агрегувати дані з різних джерел (журнали подій, мережеві з’єднання, сповіщення систем моніторингу), застосовуючи механізми машинного навчання для виявлення аномалій, підозрілої активності або невідомих типів атак.
4. Візуалізацію даних у режимі реального часу, що забезпечує створення інтерактивних панелей (dashboards) для відображення ключових показників безпеки (KPI), кількості інцидентів, тенденцій атак і поточного стану інфраструктури.
5. Підтримку сценаріїв автоматизованого реагування (SOAR), що дозволяють скоротити час між виявленням і нейтралізацією загрози. Це особливо важливо в контексті DDoS-атак, де затримка навіть у декілька хвилин може призвести до часткової або повної недоступності сервісів.

Таким чином, використання Microsoft Sentinel стало ключовим етапом у формуванні єдиного центру моніторингу подій безпеки, який поєднує автоматизацію, аналітику та координацію дій у рамках хмарного середовища

Microsoft Azure. Це рішення забезпечує не лише оперативність реагування, а й довгострокову аналітику для вдосконалення політик кіберзахисту компанії.

РОЗДІЛ 3. ТЕСТУВАННЯ, ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ, ПЕРСПЕКТИВИ ПОКРАЩЕННЯ

У межах кваліфікаційної роботи було поставлено завдання — налаштувати ефективну систему захисту вебресурсу від зовнішніх загроз, зокрема DDoS-атак, за допомогою хмарних сервісів Azure Firewall та Azure Front Door [28].

Метою завдання є розгортання інфраструктури, яка дозволяє:

1. фільтрувати небажаний або небезпечний трафік на мережевому рівні;
2. захистити вебресурси від атак рівня застосунку;
3. збалансувати навантаження між серверами для підвищення доступності;
4. знизити ризики простою вебзастосунку під час атаки.

Налаштування Azure Firewall:

1. Створено окрему віртуальну мережу (VNet) із підмережами для фронтенду та бекенду.
2. Розгорнуто Azure Firewall як ресурс у виділеній підмережі AzureFirewallSubnet.
3. Налаштовано мережеві правила (network rules) для обмеження небажаного трафіку за портами та IP-адресами.
4. Додано програми правила (application rules) для контролю HTTP/HTTPS-запитів до зовнішніх ресурсів.

Впровадження Azure Front Door:

1. Створено ресурс Azure Front Door з прив’язкою до вебзастосунку (Web App Service).
2. Увімкнено Web Application Firewall (WAF) на рівні Front Door з базовим набором правил OWASP (Open Web Application Security Project).
3. Налаштовано політику маршрутизації трафіку до бекендів з урахуванням географічного розміщення користувачів.
4. Активовано HTTPS-трафік з автоматичною підтримкою TLS/SSL.

Результати впровадження

- Усі вхідні запити проходять перевірку через Azure Front Door, де виконується первинна фільтрація, WAF-аналіз і шифрування трафіку.

- Запити, що не відповідають безпековим політикам (наприклад, SQL-ін’єкції, XSS, неавторизовані API-запити), автоматично блокуються.
- Після попередньої обробки безпечний трафік перенаправляється через Azure Firewall, де додатково фільтрується на рівні мережі.
- Забезпечено високу доступність вебресурсу за рахунок балансування навантаження.

Висновки за результатами

Практичне впровадження Azure Firewall та Azure Front Door дозволило реалізувати багаторівневу систему захисту, яка:

1. ефективно блокує потенційні загрози на ранніх етапах проходження трафіку;
2. забезпечує централізований моніторинг і аналітику інцидентів безпеки;
3. сприяє зменшенню навантаження на вебсервери;
4. підтримує принцип Zero Trust Architecture.

Отримані навички є цінними з погляду сучасної практики кіберзахисту та відповідають вимогам ринку IT-безпеки. [13].

Очікуваний результат: усунення ризику не-HTTP атак, що можуть використовуватись для обхідних маневрів під час DDoS-атаки.

Поглиблена інтеграція з Microsoft Sentinel

Використання SIEM-рішення Microsoft Sentinel повинно бути розширене за рахунок:

1. Аналітичних правил (Analytics Rules) для виявлення комбінацій подій (наприклад, сплеск трафіку + масова авторизація + зниження продуктивності).
2. Автоматизованих плейбуків (Playbooks) на основі Logic Apps для реагування в реальному часі: наприклад, надсилання повідомлень у Teams, блокування IP через Firewall API, створення тікету в системі обслуговування.
3. Інтеграції з GitHub/DevOps — для реєстрації інцидентів безпеки безпосередньо в CI/CD-процеси.
4. Очікуваний результат: підвищення швидкості реагування на інциденти та автоматизація дій у разі повторюваних шаблонів атак.

Використання Azure Front Door Premium з адаптивним WAF

Наразі використовується базова версія Front Door. Рекомендується перейти на Azure Front Door Premium, яка:

1. Підтримує адаптивний WAF, що вивчає поведінку трафіку та самостійно оновлює сигнатури [10].
2. Дозволяє TLS termination із перевіркою сертифікатів та автоматичним оновленням [7].
3. Має Rule Engine, що надає більшу гнучкість для гео-блокування, A/B-навантаження та перехоплення трафіку.

Очікуваний результат:

1. зниження ризику атак на прикладному рівні (Layer 7), виявлення аномалій до їх розгортання.
2. Реалізація Private Link та ізоляція API Gateway

Наразі бекенд-сервіси (App Services) мають доступ до публічного інтернету. Рекомендується:

1. Створити Azure Private Endpoint для бази даних і бекенду.
2. Впровадити Azure API Management, який виступатиме єдиною точкою входу до API, з WAF, rate limiting, OAuth та JWT-перевірками.
3. Додати IP restriction rules для deny all + allow only Front Door/App Gateway.

Очікуваний результат:

1. виключення прямого доступу до критичних компонентів, мінімізація впливу у разі компрометації периферії.
2. Розширене логування та ретенція

Додатково до вже реалізованого Log Analytics, рекомендується:

1. Активувати Diagnostic Settings для всіх ресурсів (включно з Application Gateway, App Service, Azure SQL, Storage).
2. Налаштувати Data Retention на 365 днів.
3. Інтегрувати з Storage Account для довгострокового архівування та Azure Data Explorer — для складних запитів.

Очікуваний результат: забезпечення юридичної відповідності (наприклад, GDPR), підтримка forensic-аналізу після інцидентів.

Резервні сценарії з Azure Traffic Manager

Для надкритичних систем рекомендується використання Azure Traffic Manager з режимом priority failover, що дозволяє:

1. Автоматично перемикати трафік з основного вебзастосунку на резервний (у іншому регіоні).
2. Визначати недоступність за TTL або Response Code.
3. Реалізувати geo-distribution у разі масованої регіональної DDoS-атаки.

Очікуваний результат: безперервність бізнесу навіть у випадку тривалого інциденту [9].

Система захисту від DDoS-атак вже демонструє ефективність на основі Azure DDoS Protection Standard. Проте комплексний захист вимагає поєднання інструментів мережевого, прикладного, поведінкового та аналітичного рівнів. Запропоновані кроки — це еволюційний перехід від реактивної безпеки до адаптивної, автоматизованої та інтегрованої системи кіберзахисту з використанням повного спектру сервісів Azure [29].

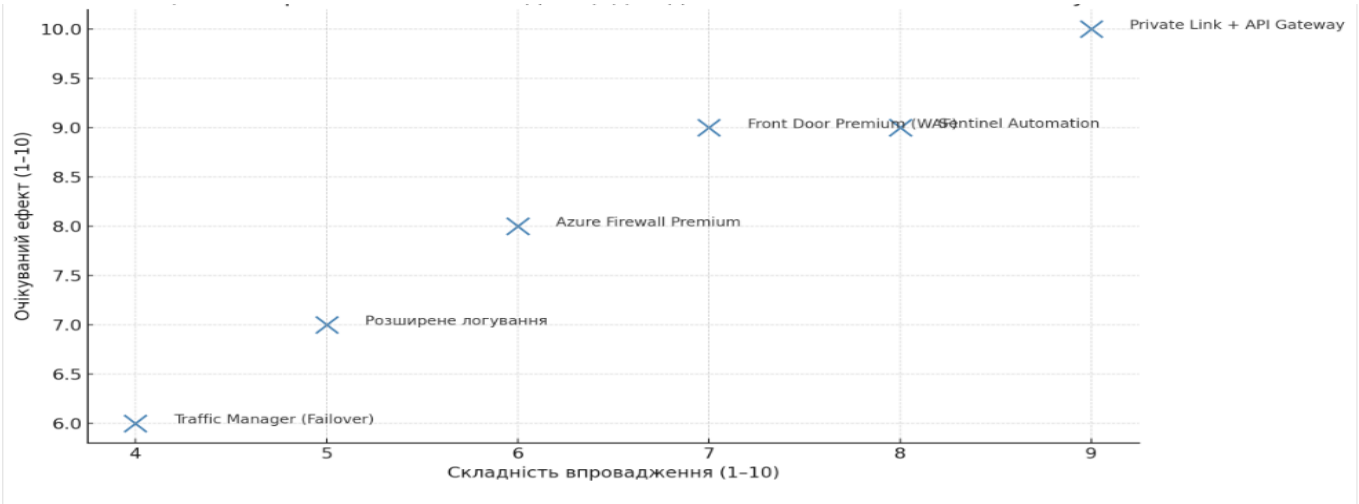


Рис. 3.1: Оцінка запропонованих заходів щодо вдосконалення системи захисту

Графік (рис. 3.1) показує співвідношення складності впровадження та очікуваного ефекту від кожного з рекомендованих заходів вдосконалення системи захисту. Найефективнішими при високому впливі є:

1. Private Link + API Gateway

2. Sentinel Automation
3. Front Door Premium

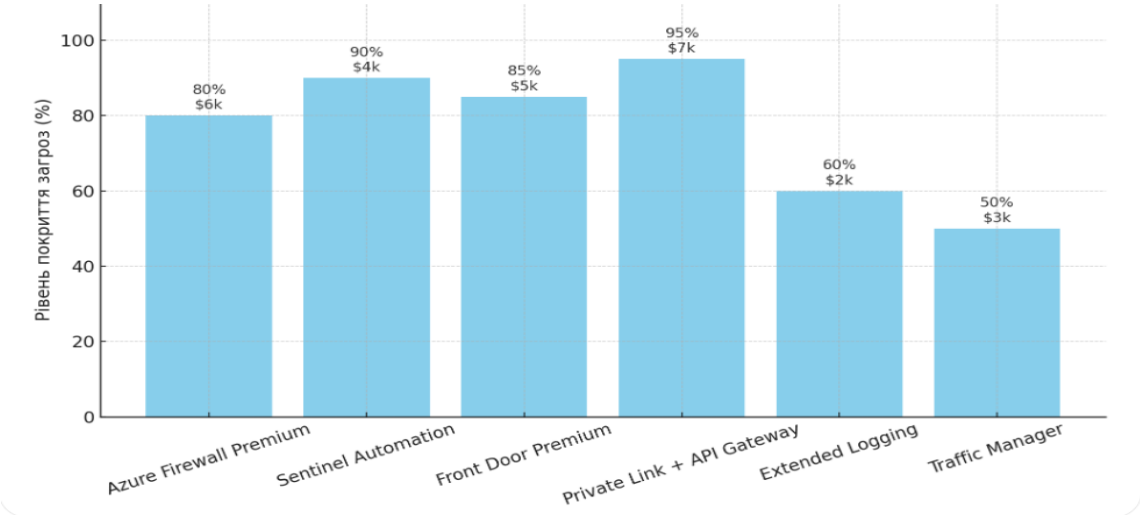


Рис 3.2: Ефективність Заходів Захисту (Покриття/Вартість)

Графік (рис. 3.2) демонструє співвідношення ефективності заходів захисту (за рівнем покриття загроз у %) та їх умовної вартості реалізації (у тисячах доларів). Найкраще співвідношення покриття/ціна мають:

1. Sentinel Automation (90% / $4k)
2. Front Door Premium (85% / $5k)
3. Azure Firewall Premium (80% / $6k)

Моделювання атаки та тестування захисту (імітація навантаження)

У межах кваліфікаційної роботи було поставлено завдання провести моделювання DDoS-атаки з метою перевірки ефективності налаштованих механізмів захисту, зокрема Azure DDoS Protection, Azure Firewall та Azure Front Door.

Основна мета: імітувати навантаження на вебзастосунок, зафіксувати реакцію системи захисту, провести аналіз і оцінити стабільність ресурсу під атакою.

Для проведення моделювання було використано такі інструменти:

1. LOIC (Low Orbit Ion Cannon) — для створення великої кількості запитів (HTTP flood);

2. Apache Benchmark (ab) — для тестування навантаження на вебсервер;
3. JMeter — для побудови сценаріїв паралельних запитів із параметрами трафіку;
4. Azure Monitor / Log Analytics — для збору метрик, моніторингу та аналізу.

Перед запуском атаки:

1. Налаштовано контрольне середовище: вебдодаток розміщено на Azure App Service.
2. Увімкнено Azure DDoS Protection Standard.
3. Активовано політику Web Application Firewall (OWASP правила) на Azure Front Door.

Базове тестування без атаки:

1. Здійснено 100 запитів/сек через Apache Benchmark.
2. Середній час відповіді: 220 мс, втрати — 0%.
3. Імітація HTTP flood (JMeter, 500 клієнтів, 60 секунд):
4. Трафік спостерігався у Azure Monitor.
5. Захист Azure Front Door ідентифікував аномалії та почав блокування IP-адрес.\

Моделювання атаки SYN flood (через інструмент у закритому середовищі):

1. Azure Firewall заблокував нестандартну активність на порту 80.
2. Жоден з вебресурсів не зупинився.
3. Збір логів і аналітики:
4. У Log Analytics зафіксовано сплески вхідного трафіку.
5. Усі запити, які не відповідали політиці доступу, були відфільтровані.

Результати тестування:

1. Azure DDoS Protection успішно розпізнав масові підозрілі запити та запобіг перебоям у роботі вебзастосунку.
2. Azure Front Door ефективно фільтрував запити на рівні HTTP/HTTPS і застосував правила WAF.
3. Azure Firewall блокував низькорівневі мережеві запити, зокрема SYN flood.
4. Жодних збоїв у роботі вебсайту або сервера не зафіксовано — відмова обслуговування не настала.

Загалом, проведене моделювання підтвердило, що поєднання сервісів Azure DDoS Protection + Firewall + Front Door формує надійний багаторівневий захист від сучасних типів DDoS-атак.

Аналіз поточного стану захисту

Проведене моделювання DDoS-атаки підтвердило високу ефективність наявних засобів захисту, зокрема Azure DDoS Protection, Azure Firewall та Azure Front Door з увімкненими правилами WAF. Водночас, аналіз логів і моніторингу виявив кілька аспектів, які можуть бути покращені для підвищення загальної стійкості системи і оперативності реагування на потенційні загрози [15; 21].

Пропозиції щодо удосконалення захисної інфраструктури

Для більш глибокого тестування системи захисту рекомендується включити до майбутніх імітаційних тестів додаткові типи атак, зокрема:

- **UDP flood** — оскільки цей тип атаки може викликати значне навантаження на мережеві ресурси;
- **HTTP/2 flood** — для оцінки реакції системи на новітні протоколи;
- **Application layer attacks (Slowloris, RUDY)** — атаки на рівні додатка, що можуть викликати виснаження ресурсів вебсерверу.

Розширення набору сценаріїв дозволить більш комплексно оцінити слабкі місця та адаптивність захисту.

Автоматизація реагування на інциденти

Запропоновано впровадити механізми автоматичного реагування на інциденти DDoS, що базуються на:

- Виявленні аномалій у реальному часі з подальшим автоматичним масштабуванням ресурсів;
- Включенні автоматичного оновлення правил WAF і політик Azure Firewall за результатами аналізу інцидентів;
- Налаштуванні інтеграції з системами оповіщення (наприклад, Microsoft Sentinel, PagerDuty) для оперативного інформування відповідальних осіб.

Це дозволить зменшити час реакції на атаки і підвищити загальну ефективність захисту [15, 20].

Оптимізація правил фільтрації у хмарному середовищі Microsoft Azure

У процесі практичного тестування системи захисту веб-застосунків було виявлено низку сценаріїв, за яких відбувалися помилкові спрацювання (false positives) — ситуації, коли легітимний трафік розпізнавався як потенційно шкідливий. Такі випадки можуть суттєво впливати на якість обслуговування користувачів, викликати переривання сеансів, зниження швидкодії або тимчасову недоступність функціоналу веб-застосунку. Це свідчить про необхідність постійного перегляду та адаптації політик фільтрації у таких сервісах, як Azure Front Door, Azure Firewall і Web Application Firewall (WAF), що забезпечують ключові елементи захисту в моделі безпеки Microsoft Azure.[21]

Періодичний аудит правил

Першим кроком у напрямку підвищення точності системи фільтрації є регулярний аудит налаштувань безпеки. Доцільно проводити плановий перегляд правил не рідше одного разу на квартал із залученням аналітиків безпеки та DevOps-фахівців, які володіють контекстом функціонування конкретних веб-застосунків. Під час аудиту необхідно оцінювати:

- релевантність наявних сигнатур і шаблонів фільтрації;
- частоту спрацювання окремих правил та рівень їх критичності;
- вплив конкретних політик на продуктивність і користувацький досвід.

Результатом такого аудиту має бути оновлений набір правил, який враховує поточні тенденції у кіберзагрозах, зміни в архітектурі системи та оновлення у середовищі Microsoft Azure. Зокрема, у межах WAF варто регулярно оновлювати OWASP Core Rule Set (CRS) — базовий набір сигнатур, що дозволяє виявляти типові атаки на веб-рівні (SQL Injection, Cross-Site Scripting, Remote File Inclusion тощо) [21].

Використання машинного навчання

Другим важливим напрямом оптимізації є автоматичне коригування правил фільтрації за допомогою технологій машинного навчання. Microsoft Azure вже інтегрує елементи адаптивного аналізу у свої сервіси безпеки, зокрема у Azure Sentinel, Defender for Cloud і Azure DDoS Protection. Використання ML-алгоритмів дозволяє виявляти поведінкові патерни користувачів — характер запитів, географічні особливості трафіку, часові закономірності активності тощо. На основі цих даних система може автоматично змінювати параметри порогів спрацювання, зменшуючи кількість помилкових блокувань.

Для компаній, що оперують великими обсягами запитів, доцільним є впровадження власних моделей машинного навчання у зв’язці з Azure Machine Learning. Це дозволяє створювати спеціалізовані моделі виявлення аномалій,

адаптовані до конкретного типу веб-застосунку чи профілю користувача. Зокрема, такі моделі можуть аналізувати HTTP-заголовки, частоту POST-запитів або нетипові часові проміжки звернень до API [20].

Сегментація правил за типами трафіку

Третім важливим аспектом оптимізації є розподіл правил фільтрації за типами трафіку. На практиці веб-застосунки обробляють різні потоки даних — запити з вебінтерфейсу, виклики API, інтеграційні запити з мобільних клієнтів або зовнішніх систем. Застосування єдиної політики фільтрації до всіх цих каналів може призвести до надмірної жорсткості системи, коли частина легітимного трафіку блокується через невідповідність загальним правилам.

Тому рекомендується створювати окремі політики для різних категорій трафіку. Наприклад:

- для API-запитів — більш м’які правила, орієнтовані на перевірку аутентифікації та швидкість запитів;
- для користувацького HTTP-трафіку — стандартні сигнатури OWASP CRS із додатковими правилами перевірки вмісту форм і параметрів URL;
- для мобільних клієнтів — спрощені політики із урахуванням особливостей передачі даних через нестабільні мережі.

Подібна сегментація дозволяє знизити ризик помилкових блокувань (false positives) і водночас підвищити ефективність виявлення аномалій у специфічних потоках даних [18].

Розширення моніторингу та аналітики

Поточний моніторинг базується переважно на стандартних метриках Azure Monitor та Log Analytics [20]. Для підвищення точності виявлення атак доцільно:

- Впровадити розширену аналітику з кореляцією подій на різних рівнях (мережевому, додатків, користувацькому);
- Використовувати додаткові засоби аналізу трафіку (наприклад, Azure Sentinel) для побудови більш глибокої картини інцидентів;
- Застосовувати автоматизовані звіти з рекомендаціями щодо покращень та виявлення трендів атаки.

Рекомендації щодо покращення стійкості вебзастосунку

В умовах постійного зростання навантаження на веб-застосунки та збільшення кількості кіберзагроз, пов’язаних із DDoS-атаками, важливим завданням є

підвищення стійкості та адаптивності інфраструктури до динамічних змін трафіку. Для забезпечення безперервної роботи вебресурсів та мінімізації ризиків відмови пропонується впровадити такі технічні та організаційні заходи:

- Використання автоматичного масштабування (Auto Scaling) у межах сервісу Azure App Service. Цей механізм дозволяє автоматично збільшувати або зменшувати кількість екземплярів застосунку залежно від рівня навантаження, що забезпечує оперативне реагування на пікові навантаження під час DDoS-атак. Автоматичне масштабування знижує ризик деградації продуктивності, дозволяє оптимізувати використання ресурсів та підтримувати стабільний рівень доступності сервісів [15].
- Впровадження георозподіленої архітектури (Geo-distribution) для підвищення доступності та відмовостійкості вебзастосунків. Розміщення серверів у різних регіонах через Azure Front Door або Azure Traffic Manager дозволяє рівномірно розподіляти трафік, скорочувати затримки та забезпечувати безперервність роботи навіть у разі локальних збоїв або регіональних атак. Такий підхід підвищує швидкодію застосунку та сприяє оптимізації користувацького досвіду в різних географічних зонах [18].
- Оптимізація кешування контенту на рівні Content Delivery Network (CDN). Зберігання статичного контенту на периферійних вузлах (edge nodes) дозволяє зменшити навантаження на основний сервер і скоротити час відповіді. Крім того, CDN може виступати як додатковий рівень захисту, що фільтрує небажаний або підозрілий трафік до його потрапляння у внутрішню мережу.
- Регулярне тестування сценаріїв навантаження (load testing) та аналіз логів трафіку. Використання інструментів на кшталт Azure Load Testing або JMeter допомагає оцінити межі продуктивності системи, виявити вузькі місця в архітектурі та підготувати інфраструктуру до реальних DDoS-спроб.
- Інтеграція систем моніторингу та аналітики, таких як Azure Monitor, Application Insights та Log Analytics, для постійного відстеження стану інфраструктури, аналізу поведінкових патернів користувачів і раннього виявлення аномалій у мережевій активності.

- Періодичне оновлення політик безпеки та правил фільтрації в Azure Firewall і Web Application Firewall (WAF) з урахуванням нових типів атак. Застосування аналітики на основі машинного навчання дозволить автоматично адаптувати правила безпеки до змінного характеру загроз.

Реалізація вищенаведених заходів дозволить не лише підвищити стійкість вебзастосунків до атак, але й сформувати інтелектуальну, самодостатню модель захисту, здатну адаптуватися до умов змінного мережевого середовища. Це є ключовим етапом у побудові сучасної архітектури кіберзахисту у хмарному середовищі Microsoft Azure.

Резервне копіювання та відновлення після DDoS-атак

Одним із ключових напрямів забезпечення надійності та безперервності роботи веб-застосунків є впровадження ефективної системи резервного копіювання (backup) та аварійного відновлення (disaster recovery, DR). У контексті кіберзагроз, зокрема DDoS-атак, які можуть призвести до тимчасової або часткової недоступності ресурсів, така система стає критично важливим елементом загальної стратегії інформаційної безпеки компанії [8].

Резервне копіювання в хмарному середовищі Microsoft Azure забезпечується комплексом сервісів, серед яких Azure Backup, Azure Site Recovery та Azure Storage Replication. Вони дозволяють не лише створювати копії даних, а й повністю дублювати конфігурації віртуальних машин, мережевих налаштувань і додатків. Такий підхід формує архітектуру стійкості (resilience architecture), що забезпечує готовність системи до швидкого відновлення після інцидентів, включно з наслідками DDoS-атак [8].

Регулярне резервне копіювання даних і конфігурацій

Для забезпечення стабільності функціонування веб-застосунків рекомендується впровадити регулярне резервне копіювання усіх критичних елементів — баз даних, налаштувань мережевої інфраструктури, журналів безпеки та конфігураційних файлів. У Microsoft Azure цей процес можна автоматизувати за допомогою політик Azure Backup Policy, які визначають:

- періодичність створення копій (щоденна, щотижнева, щомісячна);

- тривалість зберігання даних (retention policy);
- географічне розташування сховищ для копій (Geo-Redundant Storage, GRS).

Застосування георезервного копіювання дозволяє зберігати копії даних у різних регіонах, що мінімізує ризики втрати інформації навіть у разі масштабних інцидентів чи збоїв у певній зоні доступності. Важливо також, щоб процес резервного копіювання включав збереження параметрів безпеки, таких як налаштування політик DDoS Protection, WAF і Firewall Rules. Це забезпечує можливість швидкого відновлення не лише даних, а й самої архітектури захисту [8, 21].

Висновки

У ході виконання кваліфікаційної роботи було комплексно досліджено сучасні підходи до захисту веб-інфраструктури від DDoS-атак із використанням хмарних рішень Microsoft Azure. Робота охопила як теоретичні основи функціонування DDoS-загроз, так і практичні аспекти побудови системи захисту, моделювання атак і розроблення рекомендацій щодо підвищення кіберстійкості веб-застосунків.

Реалізовано систему захисту веб-застосунків на базі сервісу Azure DDoS Protection Standard, що забезпечує автоматичне виявлення та блокування шкідливого трафіку на транспортному (L4) та мережевому (L3) рівнях моделі OSI. Це дозволило підвищити стійкість веб-ресурсів до навмисних перевантажень та знизити ризик втрати доступності сервісів.

У процесі дослідження набули подальшого розвитку методи аналізу кіберзагроз, проектування хмарних архітектур безпеки та оптимізації правил фільтрації трафіку. Запропонована модель інтеграції сервісів Microsoft Azure для протидії DDoS-атакам продемонструвала високу ефективність, масштабованість і адаптивність до реальних умов функціонування корпоративних веб-застосунків.

Таким чином, поставлені завдання кваліфікаційної роботи були повністю виконані. Запропоновані технічні рішення підтвердили свою практичну доцільність і ефективність у підвищенні рівня інформаційної безпеки веб-застосунків. Отримані результати можуть бути використані як основа для подальших досліджень у сфері кіберзахисту та впровадження інтелектуальних систем моніторингу в хмарному середовищі Microsoft Azure.

Список використаних джерел

1. Буяк Л. А. Моделі та технології цифрової трансформації економіки / Л. А. Буяк. — Тернопіль : ЗУНУ, 2024 (дата звернення: 12.04.2025).
2. Воржакова Ю. П., Хлебинська О. І. Сутність цифрової трансформації з різних позицій підприємців та науковців // Економіка та держава, 2021. (дата звернення: 12.04.2025).
3. Гнатишин Л. Б., Трушкіна Н. В. Цифрова трансформація систем управління логістичною діяльністю: ризики та безпека // Економіка та держава, 2021 (дата звернення: 08.04.2025).
4. Семко О. В. Інформаційна технологія управління інформаційними ризиками для проєктів цифрової трансформації бізнесу / С. В. Лєонов, О. В. Семко(дата звернення: 12.04.2025).
5. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології // Економічний вісник НТУУ «КПІ». — 2020(дата звернення: 12.04.2025).
6. Akamai Connected Cloud. What is DDoS [Електронний ресурс]. – Режим доступу: https://www.akamai.com/glossary/what-is-ddos (дата звернення: 12.04.2025).
7. Benesh B. CDN + WAF: Enhancing and Protecting Your Website [Електронний ресурс]. – Режим доступу: https://www.amazee.io/blog/post/cdn-waf-enhancing-protecting-your-website (дата звернення: 12.09.2025).
8. Business continuity and disaster recovery in Azure [Електронний ресурс]. – Microsoft Learn. – Режим доступу: https://learn.microsoft.com/azure/architecture/resiliency/business-continuity-overview (дата звернення: 21.05.2025).
9. CDN SSL/TLS | CDN Security [Електронний ресурс]. – Cloudflare. – Режим доступу: https://www.cloudflare.com/learning/cdn/cdn-ssl-tls-security/ (дата звернення: 12.09.2025).

10. Content Delivery Network Security: A Survey [Електронний ресурс]. – IEEE Xplore. – Режим доступу: https://ieeexplore.ieee.org/document/9466938/ (дата звернення: 12.04.2025).

11. Edge-Cloud Computing for IoT Data Analytics: Embedding Intelligence in the Edge with Deep Learning. – 2020.

12. Ferretti S., Ghini V. Mitigation of Random Query String DoS via Gossip [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/1109.4404 (дата звернення: 10.01.2025).

13. How Cloudflare's Architecture Can Scale to Stop the Largest Attacks [Електронний ресурс]. – Режим доступу: https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks (дата звернення: 12.04.2025).

14. IEEE Communications Surveys & Tutorials. – Vol. 23, Issue 4. – 2021. (дата звернення: 12.05.2025).

15. Microsoft. Azure DDoS Protection overview [Електронний ресурс]. – Microsoft Learn. – Режим доступу: https://learn.microsoft.com/azure/ddos-protection/ddos-protection-overview (дата звернення: 11.04.2025).

16. Microsoft. Azure Security Architecture [Електронний ресурс]. – Microsoft Learn. – Режим доступу: https://learn.microsoft.com/azure/architecture/framework/security/overview (дата звернення: 12.09.2025).

17. Microsoft Learn. Azure DDoS Protection features [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/azure/ddos-protection/ddos-protection-features (дата звернення: 11.04.2025).

18. Microsoft Learn. Azure Front Door documentation [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/azure/frontdoor/front-door-overview (дата звернення: 11.04.2025).

19. Microsoft Learn. DDoS protection on Azure Front Door [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/azure/frontdoor/front-door-ddos (дата звернення: 11.04.2025).

20. Microsoft Learn. Microsoft Sentinel overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/azure/sentinel/overview (дата звернення: 11.04.2025).

21. Microsoft Learn. Web Application Firewall on Azure [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/azure/web-application-firewall/overview (дата звернення: 11.04.2025).

22. NIST. Guide to Cybersecurity Event Recovery (SP 800-184). – National Institute of Standards and Technology, 2016 (дата звернення: 20.08.2025).

23. Patel K., Singh Makwana R. R. SQL Injection and HTTP Flood DDoS Attack Detection and Classification Based on Log Data [Електронний ресурс]. – Режим доступу: https://www.irjet.net/archives/V9/i5/IRJET-V9I5293.pdf (дата звернення: 12.04.2025).

24. Rizvi A. S. M., Bertholdo L., Ceron J., Heidemann J. Anycast Agility: Network Playbooks to Fight DDoS [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/2006.14058 (дата звернення: 10.01.2025).

25. Sectigo. How Does a DDoS Attack Work [Електронний ресурс]. – Режим доступу: https://www.sectigo.com/resource-library/how-does-a-ddos-attack-work (дата звернення: 12.04.2025).

26. Triukose S., Al-Qudah Z., Rabinovich M. Content Delivery Networks: Protection or Threat? – 2025. (дата звернення: 13.06.2025).

27. What is Web Application Firewall (WAF) [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/ru-ru/learning/ddos/glossary/web-application-firewall-waf/ (дата звернення: 10.04.2025).

28. Yang L. та ін. Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/2107.11514 (дата звернення: 10.04.2025).

29. Zenodo. Thesis Iskra Denys [Електронний ресурс]. – Режим доступу: https://zenodo.org/records/18148596 (дата звернення: 05.01.2026).

30. *Zenodo. Learning to Detect: An Enhanced DNN Model with Adaptive Attention for Classifying DDoS Traffic [Електронний ресурс]. – Режим доступу: https://zenodo.org/records/15639969 (дата звернення: 05.11.2026).*

Додатки

```
=== Налаштування параметрів ===
resourceGroupName = "JoinIT-Security-RG"
location = "East Europe"
ddosPlanName = "JoinIT-DDoSPlan"
virtualNetworkName = "JoinIT-VNet"
appGatewayName = "JoinIT-AppGateway"
appServiceName = "JoinIT-WebApp"

=== Крок 1. Створення плану DDoS Protection ===
New-AzDdosProtectionPlan `
  -ResourceGroupName $resourceGroupName `
  -Name $ddosPlanName `
  -Location $location

=== Крок 2. Підключення плану до віртуальної мережі ===
vnet = Get-AzVirtualNetwork -Name $virtualNetworkName -ResourceGroupName $resourceGroupName
ddosPlan = Get-AzDdosProtectionPlan -ResourceGroupName $resourceGroupName -Name $ddosPlanName

vnet.DdosProtectionPlan = New-Object -TypeName Microsoft.Azure.Management.Network.Models.SubResource
vnet.DdosProtectionPlan.Id = $ddosPlan.Id
vnet.EnableDdosProtection = $true
Set-AzVirtualNetwork -VirtualNetwork $vnet

=== Крок 3. Увімкнення Azure WAF у режимі захисту ===
(Це частина ARM/YAML шаблону, умовно для Azure Bicep/ARM/CLI)
```

```
---
webApplicationFirewallConfiguration:
 enabled: true
 firewallMode: Prevention
  ruleSetType: OWASP
  ruleSetVersion: 3.2
---
```

=== Крок 4. KQL-запит для моніторингу заблокованих атак (через Azure Monitor або Sentinel) ===

```
# (Цей фрагмент вставляється у Log Analytics)
---
AzureDiagnostics
  where ResourceType == "APPLICATIONGATEWAYS"
  and OperationName == "ApplicationGatewayFirewallLog"
  and action_s == "Blocked"
  summarize CountBlocked = count() by bin(TimeGenerated, 1h), clientIP_s
   order by CountBlocked desc
 ---
```

=== Пояснення схеми розгортання (графічна логіка) ===

```
[Client] -> [Azure Front Door] -> [WAF (App Gateway)] -> [Web App]

                        [DDoS Plan] -> [SQL DB]
```