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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту корпоративних мереж від сучасних DDoS-атак»

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

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

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

_____ Іван МАРКІН
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
МАРКІН Іван
(прізвище, ім'я)

Керівник к.тех.н., доцент БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації бізнес-процесів корпоративні мережі відіграють роль у забезпеченні безперебійного функціонування організацій різних галузей. Проте одночасно з розширенням цифрового простору зростає і рівень кіберзагроз, які стають дедалі витонченими та деструктивними. Серед них особливу небезпеку становлять розподілені атаки типу «відмова в обслуговуванні» (DDoS), які здатні паралізувати роботу сервісів, спричинити значні фінансові втрати, порушити репутацію компанії, а також підірвати довіру з боку клієнтів та партнерів. Ефективна протидія таким загрозам вимагає впровадження інноваційних підходів до моніторингу, виявлення та нейтралізації атак, що обумовлює актуальність дослідження проблеми кіберзахисту корпоративних IT-інфраструктур.

Актуальність проведеного дослідження обумовлена стрімким зростанням кількості, інтенсивності та складності DDoS-атак, які становлять серйозну загрозу для стабільності функціонування корпоративних IT-систем. Сучасні зловмисники активно використовують ботнети, можливості хмарних обчислень, а також технології шифрування трафіку, що істотно ускладнює процес їх виявлення традиційними методами. У таких умовах потрібно розробляти й впроваджувати інноваційні засоби кіберзахисту, здатні оперативно аналізувати аномальну активність у мережі, виявляти потенційні атаки та ефективно нейтралізовувати їх у режимі реального часу. Забезпечення безперервності роботи корпоративних ресурсів та захисту сервісів потребує комплексного підходу, що поєднує новітні технології аналізу даних, штучного інтелекту та автоматизованого управління інформаційною безпекою.

Мета роботи. Аналіз сучасних типів DDoS-атак і дослідження ефективних методів та засобів захисту корпоративних мереж від них.

Завдання дослідження:

проаналізувати типи та механізми DDoS-атак;

розглянути сучасні засоби захисту від DDoS-атак (апаратні, програмні, хмарні рішення);

дослідити алгоритми виявлення та нейтралізації атак на основі штучного інтелекту та машинного навчання;

провести порівняльний аналіз ефективності різних засобів захисту;
запропонувати рекомендації щодо впровадження систем захисту у корпоративних мережах.

Об'єкт дослідження – процеси забезпечення кібербезпеки корпоративних мереж.

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

У процесі роботи використано такі методи: теоретичний аналіз літературних джерел, моделювання DDoS-атак, порівняльний аналіз засобів захисту, аналіз ефективності алгоритмів на основі машинного навчання.

Практичне значення проведеного дослідження: полягає в тому, що його результати можуть бути ефективно використані у сфері інформаційної безпеки для розробки та впровадження систем захисту в рамках корпоративних IT-інфраструктур. Запропоновані в роботі рекомендації орієнтовані на підвищення рівня захищеності мережевих систем від деструктивного впливу DDoS-атак, що, у свою чергу, сприяє забезпеченню безперервності бізнес-процесів, збереженню цілісності даних та стабільності функціонування цифрових сервісів.

Наукова новизна полягає у проведенні комплексного аналізу характеру та еволюції сучасних DDoS-атак з урахуванням їхньої динаміки та технологічної складності. Головною складовою є застосування новітніх методів машинного навчання для виявлення ознак атак та їхнього попередження в режимі реального часу. Окрім цього, в роботі запропоновано оптимізовану архітектуру інтегрованої системи захисту корпоративної мережі, яка враховує як технічні, так і організаційні аспекти кіберзахисту, забезпечуючи гнучке реагування на новітні загрози.

Розділ 1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ВІД DDoS-АТАК

1.1 Аналіз природи та наслідків DDoS-атак

Захист конфіденційної інформації є елементом забезпечення національної, економічної та інформаційної безпеки країни. Для регулювання цього процесу існує низка нормативно-правових актів, які включають міжнародні стандарти, національні закони та підзаконні акти. Вони визначають основи захисту інформації та права і обов'язки осіб, які беруть участь в інформаційних відносинах [1].

Одним із головних нормативних документів у цій сфері є Закон України «Про інформацію». Він регулює визначення поняття інформації, її види, а також правові засади її обробки і збереження. Зокрема, в ньому велика увага приділена інформації з обмеженим доступом, яка включає конфіденційну інформацію. Закон вказує, що доступ до такої інформації може бути обмежено лише в разі, коли це передбачено законом, для захисту прав та інтересів особи, держави або суспільства.

Закон України «Про захист персональних даних» є ще одним актом, який регулює процес обробки, зберігання та передачі персональних даних фізичних осіб. Він чітко визначає, що таке персональні дані, а також права суб'єктів цих даних і обов'язки осіб, які з ними працюють, зокрема забезпечення їх конфіденційності. Закон також встановлює відповідальність за порушення правил обробки персональних даних.

Закон України «Про державну таємницю» регулює порядок надання інформації статусу державної таємниці, організацію доступу до неї та механізми її захисту. Цей акт створює правові основи для функціонування органів, які займаються охороною секретної інформації, а також для процедур доступу до неї.

Закон України «Про електронні довірчі послуги» має значення в умовах сучасної електронної комунікації, оскільки регулює використання електронних підписів, сертифікатів ключів та захищених носіїв інформації, що сприяє забезпеченню безпеки електронних комунікацій.

Не менш важливими є міжнародні стандарти, серед яких особливу увагу заслуговує ISO/IEC 27001. Це міжнародний стандарт, який визначає принципи управління інформаційною безпекою і пропонує комплексний підхід до

забезпечення конфіденційності, цілісності та доступності інформації. В Україні державна політика у сфері захисту інформації поступово адаптується до цих стандартів, що сприяє інтеграції країни до світового інформаційного простору.

До підзаконних актів, які деталізують положення вищезазначених законів, належать постанови Кабінету Міністрів України та накази Держспецзв'язку. Вони визначають технічні аспекти захисту інформації, процедури сертифікації засобів захисту та вимоги до криптографічного захисту.

Нормативно-правова база захисту інформації є багаторівневою системою актів, яка регулює захист на різних рівнях — від загальних принципів до технічних вимог. Подальший розвиток цієї бази та гармонізація з міжнародними стандартами є необхідними для забезпечення ефективного захисту інформації в Україні.

Сучасний розвиток корпоративних і локальних мереж вимагає постійного вдосконалення засобів і методів комплексного захисту інформації. Це передбачає підвищення ефективності організації захисту інформаційних ресурсів шляхом застосування новітніх програмних і технічних рішень.

Комплексна система захисту інформації (КСЗІ) має на меті запобігання кількома типами загроз. Це включає витік інформації через технічні канали, такі як електромагнітні випромінювання чи акустичні впливи, несанкціонований доступ до даних, а також цілеспрямовані впливи, що можуть порушити цілісність інформації. Такі загрози потребують спеціалізованих заходів і засобів для їх попередження [1].

Захист інформації в сучасних інформаційно-комунікаційних системах має враховувати особливості обробки даних, клас автоматизованої системи та умови її експлуатації. Основною метою всіх заходів є забезпечення безпеки інформації на всіх етапах її життєвого циклу.

Інформація в інтегрованих комплексних системах управління (ІКСМ) постійно піддається впливу різних загроз, як з внутрішніх, так і з зовнішніх джерел. До внутрішніх загроз можна віднести помилки персоналу, недоліки кваліфікації співробітників або свідомі дії, такі як крадіжка даних чи саботаж. Зовнішні фактори ризику включають кібератаки, шкідливі програми, несанкціонований доступ та природні катастрофи чи технічні збої в обладнанні.

Такі загрози можуть порушити основні характеристики інформації, включаючи її точність, доступність і конфіденційність. Наприклад, цілісність

інформації може бути порушена через її спотворення чи втрату, доступність – у випадку, коли неможливо отримати доступ до неї в потрібний момент, а конфіденційність – у разі несанкціонованого розкриття або використання даних.

Для зменшення впливу таких ризиків використовуються різноманітні спеціалізовані заходи, що спрямовані на захист інформації на всіх етапах її обробки, передачі та зберігання. Це включає встановлення відповідних нормативно-правових актів, що регламентують правила і стандарти захисту інформаційних ресурсів.

Нормативно-правова база є елементом у захисті інформації, оскільки вона визначає порядок створення та використання захищених ІКСМ, правила обробки та збереження інформації, а також вимоги до побудови комплексних систем захисту інформації (КСЗІ). До того ж, нормативно-правове забезпечення встановлює права та обов’язки персоналу, що працює з інформаційними системами, а також механізми виявлення та усунення загроз безпеці [2].

Захист інформації в сучасних умовах вимагає комплексного підходу, що поєднує технічні, організаційні та правові заходи. Нормативно-правове забезпечення є основою для забезпечення надійного захисту інформаційних ресурсів, враховуючи всі сучасні загрози та виклики в сфері інформаційної безпеки.

Для створення ефективної КСЗІ в ІКСМ необхідно враховувати вимоги численних нормативно-правових актів, які регламентують основи захисту інформаційних ресурсів. Серед основних документів – Закони України «Про інформацію» та «Про захист інформації в автоматизованих системах». Головними є також галузеві нормативні документи, зокрема НД ТЗІ, що визначають термінологію в сфері захисту, класифікацію автоматизованих систем та їх вимоги до безпеки.

Одним із етапів побудови КСЗІ є визначення функціональних профілів захищеності, які містять мінімально необхідні механізми захисту для забезпечення цілісності, доступності та конфіденційності інформації. Це включає процедури ідентифікації та аутентифікації, виявлення порушень цілісності даних та інших заходів, що протидіють несанкціонованим змінам або передачі даних.

Таким чином, побудова захищених інформаційно-комунікаційних систем базується на чіткій нормативно-правовій основі та ефективному впровадженні

методологічних заходів для забезпечення безпеки інформації на всіх етапах її життєвого циклу.

У цифрову епоху розподілені атаки типу відмови в обслуговуванні (DDoS) стали одним з основних інструментів кіберзлочинців. Їх мета — виведення з ладу інформаційних ресурсів організації шляхом перевантаження серверів, каналів зв'язку або програмних сервісів. Особливу небезпеку становлять атаки, які здійснюються з великої кількості джерел (ботнетів), що ускладнює їх блокування. Часто DDoS-атаки супроводжуються інформаційною або фінансовою диверсією.

Щоб краще зрозуміти характер DDoS-атак, їх види та наслідки, розглянемо порівняльну характеристику в таблиці 1.1 нижче [2].

Таблиця 1.1

Типові наслідки для корпоративної мережі

Тип DDoS-атаки	**Принцип дії**	**Типові наслідки для корпоративної мережі**
Volumetric (об'ємні)	Засипають мережу або сервер великою кількістю трафіку для перевантаження	Втрата доступу до вебсайту, перевантаження інтернет-каналу
Protocol-based	Атакують слабкі місця протоколів (TCP, ICMP, DNS)	Зниження продуктивності, падіння серверів, нестабільність з'єднання
Application-layer	Імітують легальні запити до застосунків (HTTP, HTTPS)	Перевантаження веб-додатків, зниження продуктивності, збої в роботі API
Multi-vector	Комбінують кілька типів атак одночасно	Повна відмова сервісу, ускладнення захисту, фінансові та репутаційні втрати

На відміну від традиційних кіберзагроз, таких як крадіжка даних або компрометація систем, DDoS-атаки не завжди мають на меті безпосереднє викрадення інформації. Замість цього вони часто використовуються як інструмент

шантажу, політичного тиску або навіть як відволікання уваги перед серйознішими злочинами, такими як викрадення даних або руйнування критичних систем.

Ransom DDoS (шантаж через DDoS) є одним із небезпечних і підступних видів атак, коли зловмисники вимагають викуп за припинення атаки на сервери або інші компоненти інфраструктури. Вони можуть погрожувати тривалим або масштабним перериванням роботи підприємства, що, у свою чергу, змушує організацію швидко й не завжди вдало реагувати, часто погоджуючись на вимоги зловмисників.

Складність таких атак полягає не лише у їхній потужності, а й у здатності імітувати законну активність. Зловмисники часто використовують техніки, які дозволяють їм маскувати атаки під звичайний користувацький трафік або звичні операції, що робить їх майже непомітними для традиційних систем безпеки, таких як фаєрволи або IDS/IPS. Завдяки цьому атаки можуть тривати довгий час без виявлення, що призводить до великих збитків для організації.

З метою ефективного захисту від таких загроз необхідно впроваджувати багаторівневі системи захисту, які здатні виявляти аномалії навіть у тих випадках, коли атаки імітують звичайний трафік. Використання інтелектуальних систем виявлення аномалій і постійний моніторинг трафіку є критичними для виявлення таких атак на ранніх етапах та попередження їх негативних наслідків.

Крім технічних проблем, наслідки DDoS-атак мають глибокий бізнес-аспект, який може мати довгострокові та серйозні наслідки для організацій. Атаки на корпоративні мережі призводять до фінансових збитків через різноманітні фактори, включаючи [4]:

Простій сервісів – зупинка або уповільнення роботи онлайн-платформ, інтернет-магазинів, банківських послуг чи інших систем. Це може призвести до втрат прибутку та порушення надання послуг клієнтам:

Витрати на відновлення – підприємства повинні витратити значні ресурси на відновлення нормальної роботи після атаки. Це може включати в себе оновлення програмного забезпечення, відновлення пошкоджених систем або апаратного забезпечення, а також послуги сторонніх фахівців:

Втрати клієнтів – через перебої в роботі, клієнти можуть втратити довіру до компанії і перейти до конкурентів, що знижує довгострокову лояльність та призводить до втрати ринку:

Погіршення репутації – навіть після того, як атака буде відбита, організація може зазнати значних іміджевих втрат, якщо вона не змогла вчасно відновити доступність своїх послуг. Репутаційні збитки можуть вплинути на майбутні ділові стосунки та довіру до бренду.

Значеннєвими є наслідки DDoS-атак у критичних сферах, таких як [4]:

Банківська справа – атаки можуть призвести до тимчасового припинення фінансових операцій, що може спричинити економічні втрати для компанії, клієнтів та навіть для всієї економіки:

Охорона здоров'я – у медичних установах простій в електронних системах може призвести до затримок у наданні медичних послуг, що в деяких випадках може бути смертельно небезпечним для пацієнтів:

Телекомунікації – атаки на провайдерів інтернет-послуг можуть спричинити серйозні перерви в комунікаціях, що також може мати економічні та соціальні наслідки для ширшого суспільства.

Зважаючи на ці аспекти, потрібно враховувати багатовимірні наслідки DDoS-атак для бізнесу, розробляючи стратегії безпеки, що включають не тільки технічний захист, а й планування кризового реагування, відновлення після атаки та захист репутації.

DDoS-атаки є однією з найбільших загроз для корпоративних мереж, оскільки здатні швидко паралізувати інформаційні системи та спричинити серйозні фінансові та репутаційні збитки. Успішні DDoS-атаки можуть порушити доступність сервісів, що, в свою чергу, позначається на безперервності бізнесу та викликає втрату довіри клієнтів.

Аналіз сучасних типів атак та їх наслідків підтверджує, що традиційні методи захисту стають все менш ефективними, зокрема через появу багатовекторних атак. Ці атаки комбінують кілька методів, що ускладнює їх виявлення та блокування. Наприклад, атаки можуть включати одночасно об'ємне навантаження на мережеві пристрої та атаки на рівні застосунків, що робить навіть найсучасніші фаєрволи та системи виявлення вторгнень малоефективними.

Для протистояння таким складним загрозам потрібно впроваджувати інтелектуальні системи виявлення аномалій, які здатні аналізувати трафік у реальному часі, виявляючи як стандартні, так і нові варіанти атак. Залишаючись

гнучкими і швидкими у виявленні, ці системи можуть блокувати навіть нестандартні техніки атак, замасковані під звичайний трафік.

Головним є також використання мульти-рівневих стратегій захисту, які охоплюють різні шари мережевої інфраструктури. Це дозволяє ефективно блокувати різноманітні види атак, зберігаючи при цьому доступність для легітимних користувачів. Впровадження хмарних сервісів для захисту від DDoS-атак може забезпечити швидке масштабування ресурсів, що дозволяє швидко обробляти величезні обсяги трафіку, зберігаючи працездатність систем.

Зважаючи на стрімкий розвиток DDoS-атак і їх дедалі складнішу природу, питання постійного вдосконалення заходів захисту є надзвичайно актуальним для організацій, які залежать від безперебійної роботи своїх онлайн-сервісів.

1.2 Класифікація та еволюція сучасних DDoS-атак

З моменту появи перших DDoS-атак у кінці 1990-х років вони зазнали суттєвих змін — від примітивних пакетних атак до складних багаторівневих операцій, що використовують шифрування, обхід захисту та навіть елементи штучного інтелекту. Удосконалення інструментів атак пов’язане з розвитком технологій, зростанням пропускної здатності мереж і використанням хмарних сервісів як платформи для атак.

Нижче наведено узагальнену класифікацію DDoS-атак за критеріями методу, рівня впливу, джерела та новітніх форм, що з’явились останніми роками у таблиці 1.2 [4].

Таблиця 1.2

Класифікація DDoS-атак та їх еволюційні ознаки

Критерій	**Класична форма**	**Сучасні модифікації / Тренди**
Механізм атаки	SYN Flood, UDP Flood, ICMP Flood	TCP Connection Exhaustion, DNS Amplification, SSL Exhaustion
Рівень впливу (OSI)	Мережевий (Layer 3), транспортний (Layer 4)	Прикладний рівень (Layer 7) з точковим навантаженням на веб-додатки

Продовження таблиці 1.2

Джерело атаки	Контрольовані ботнети з інфікованих ПК	IoT-ботнети (наприклад, Mirai), хмарні ресурси, використання проксі
Координація	Локальне керування ботами	DDoS-as-a-Service (онлайн платформи), Telegram-боти для запуску атак
Маскування	Відсутність або проста IP-спуфінг	Використання легітимного трафіку, шифрованих з'єднань, CAPTCHA-обхідники
Мотивація	Саботаж, протест, хактивізм	Шантаж (RdoS), корпоративне шпигунство, політична диверсія

З таблиці видно, що сучасні DDoS-атаки стали значно гнучкими, технологічно складними та точними, що ускладнює їх ефективне виявлення та нейтралізацію. Особливу складність становлять Layer 7-атаки, які орієнтовані на імітацію звичайного користувацького трафіку, що робить їх виявлення за допомогою традиційних фаєрволів та систем виявлення та запобігання вторгненням (IDS/IPS) значно важчим. Такі атаки можуть відтворювати поведінку реальних користувачів, що дозволяє їм обходити стандартні механізми захисту, спричиняючи перевантаження веб-сервісів, баз даних чи серверів додатків.

Атаки на рівні застосунків також представляють серйозну загрозу, оскільки вони часто маскуються під автоматизовані звернення до API або операції в системах електронної комерції, таких як запити на продукцію, обробка платежів чи пошук товарів. Ці атаки можуть бути складними для виявлення, оскільки виглядають як звичайний трафік і не викликають підозр у традиційних механізмах моніторингу. В результаті, навіть найсучасніші засоби захисту можуть не відреагувати вчасно, що дозволяє зловмисникам виконувати атаки тривалий час, спричиняючи серйозні збитки для організації.

Щоб успішно протистояти таким складним загрозам, необхідно впроваджувати багаторівневі стратегії захисту, які включають аналіз трафіку на

глибоких рівнях, а також використання новітніх технологій для виявлення аномалій і підозрілого трафіку [4].

Окремо слід виділити комерціалізацію DDoS-атак, яка значно змінила ландшафт кіберзагроз. Сьогодні будь-хто, навіть без спеціальних технічних знань, може замовити DDoS-атаку через онлайн-сервіси типу DDoS-for-Hire, де ціна таких атак може бути дуже низькою — всього кілька доларів. Це дозволяє навіть невеликим зловмисникам або компаніям використовувати DDoS-атаки як конкурентну зброю, щоб спричинити значні порушення в роботі бізнесів, що є небезпечним для середнього бізнесу.

Такий розвиток ситуації значно підвищує загрозу, оскільки дозволяє не лише організованим кіберзлочинцям, але й конкурентам, що можуть використати такі сервіси, щоб нанести шкоду своїм опонентам. Це робить традиційні механізми захисту, які не враховують таку легкість і доступність атак, недостатніми для забезпечення належного рівня безпеки.

Комерціалізація таких атак ставить нові вимоги до безпеки, оскільки зловмисники можуть організувати атакувальні кампанії, навіть не маючи необхідних технічних ресурсів чи навичок. Відповідно, для підприємств потрібно адаптувати свої стратегії захисту, забезпечуючи надійний моніторинг трафіку і використовуючи механізми, здатні виявляти та нейтралізувати атаки незалежно від їхніх джерел чи складності.

Класифікація та аналіз еволюції DDoS-атак свідчать про постійну адаптацію зловмисників до сучасних засобів захисту. Це дозволяє їм постійно удосконалювати методи атаки, знаходити нові способи обходу наявних систем захисту та проникати в слабкі місця корпоративної інфраструктури.

Сучасні DDoS-атаки вже не обмежуються простою перевантаженням сервісів за допомогою великих обсягів трафіку. Зловмисники активно використовують шифрування трафіку, що ускладнює його аналіз та виявлення, а також застосовують методи обходу механізмів фільтрації, таких як фаєрволи або традиційні системи виявлення та запобігання вторгненням (IDS/IPS). Вони можуть спеціально створювати трафік, який виглядає як звичайні користувацькі запити, що утруднює вчасне виявлення атаки.

Ці новітні методи атак часто спрямовані на точкові слабкі місця в інфраструктурі, такі як окремі сервери, порти чи веб-додатки, що дозволяє їм бути

точними та менш помітними для традиційних систем захисту. Вони можуть використовувати специфічні вразливості у програмному забезпеченні або налаштуваннях мережі, що не завжди видно в загальному моніторингу.

Успішне протистояння цим загрозам вимагає комплексного підходу до захисту, який включає постійний моніторинг всіх рівнів мережі, а також впровадження інтелектуальних систем виявлення. Системи, що здатні виявляти аномалії в трафіку, вчасно реагувати на зміни в мережевому середовищі і автоматично адаптуватися до нових загроз, є ключовими для забезпечення ефективного захисту від сучасних DDoS-атак [4].

Застосування таких підходів дозволить своєчасно виявляти навіть складні, зашифровані чи замасковані атаки, що допоможе захистити критичні елементи інфраструктури та забезпечити безперервність бізнес-процесів підприємства.

1.3 Оцінка ризиків для корпоративних мереж від DDoS-атак

У сучасному інформаційному середовищі ризики, пов’язані з DDoS-атаками, стали частиною загального профілю кіберзагроз для бізнесу. Незалежно від галузі, корпоративні мережі можуть постраждати як від прямого впливу атак, так і від непрямих наслідків — фінансових, репутаційних або правових. Варто не лише виявляти факт атаки, а й системно оцінювати потенційні ризики для інфраструктури, бізнес-процесів і стейкхолдерів.

Нижче представлено детальну таблицю 1.3 з категоризацією ризиків за їх природою, можливими втратами та рівнем критичності для підприємства.

Таблиця 1.3

Категоризація ризиків корпоративних мереж унаслідок DDoS-атак

Категорія ризику	**Опис загрози**	**Можливі наслідки**	**Рівень критичності**
Технічний ризик	Перевантаження серверів, збої в роботі мережевого обладнання	Відмова в обслуговуванні, втрата доступу до сервісів, збій бізнес-процесів	Високий

Продовження таблиці 1.3

Фінансовий ризик	Витрати на відновлення систем, втрати прибутку через простої	Прямі фінансові збитки, зниження доходів, штрафи через порушення SLA	Високий
Операційний ризик	Порушення щоденних процесів і автоматизованих систем	Відставання в графіках, збої в обліку, порушення логістичних та виробничих циклів	Середній → високий
Юридичний ризик	Порушення умов контрактів, недотримання вимог збереження даних	Судові позови, регуляторні штрафи, втрати через невиконання зобов'язань	Середній
Репутаційний ризик	Втрата довіри клієнтів і партнерів через недоступність сервісів	Зменшення лояльності, відтік користувачів, зниження конкурентоспроможності	Високий
Інформаційний ризик	Утруднений моніторинг, можливість супутнього злому або витоку даних	Утечка конфіденційної інформації, компрометація внутрішніх систем	Високий
Стратегічний ризик	Вплив на стратегічні цілі, довгострокову стабільність компанії	Зміна бізнес-моделі, перегляд IT-стратегії, вимушене інвестування в кризові рішення	Залежить від масштабів

Як свідчать дані, наведені у таблиці, ризики, пов’язані з DDoS-атаками, мають як негайний, так і відкладений характер. У короткостроковій перспективі вони здатні викликати технічні збої, порушення доступу до сервісів та втрату прибутку. Водночас довготривалі наслідки можуть бути ще серйознішими — це втрата довіри з боку клієнтів, зменшення частки ринку, репутаційні втрати, а в окремих випадках навіть повне згортання бізнес-проєктів. Особливо вразливими є компанії, що не мають доступу до сучасних засобів кіберзахисту: вони можуть стати мішенню повторюваних атак і не мати достатніх ресурсів для своєчасного відновлення та модернізації систем безпеки. Такий стан речей підкреслює значення розробки адаптивних рішень, які враховують обмеження інфраструктури та фінансові можливості різних організацій (рисунок 1.3) [5].

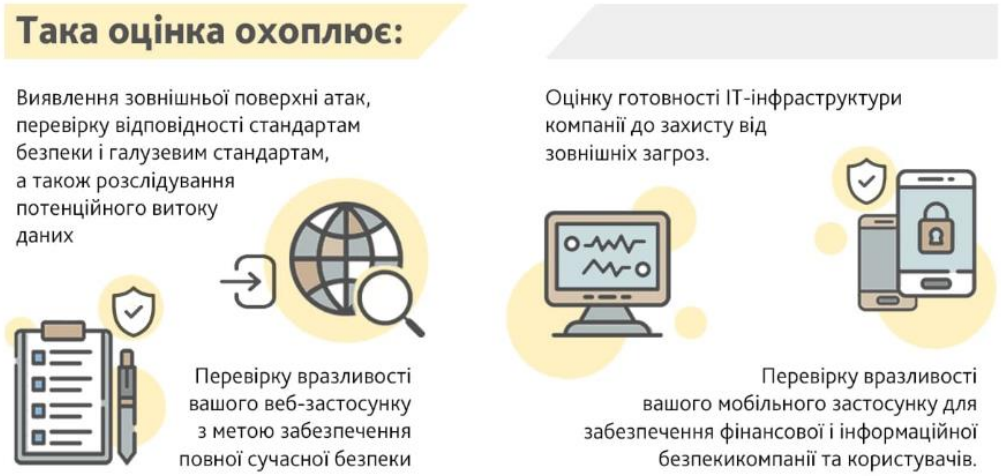


Рис. 1.3. Базові оцінки ризиків [5]

Особливу небезпеку становлять комбіновані атаки, де DDoS-атаки використовуються як «димова завіса» для відволікання уваги від основної мети — реального проникнення в корпоративну мережу. В таких випадках зловмисники можуть скористатися наведеними технічними проблемами, щоб замаскувати інші злочинні дії, такі як викрадення конфіденційних даних, знищення баз даних або руйнування критичної інфраструктури компанії. Оскільки система захисту зазвичай орієнтована на блокування зовнішніх загроз, поява таких комбінованих атак ускладнює виявлення та своєчасне реагування на реальні кіберзагрози. Це

робить необхідним розвиток багаторівневих підходів до захисту, здатних виявляти як DDoS-атаки, так і будь-які інші аномалії в мережевому трафіку [6].

DDoS-атаки представляють собою не лише технічну загрозу, а й можуть бути джерелом багаторівневих ризиків для підприємств, які значно виходять за межі простих технічних збоїв. Їх вплив зачіпає кілька аспектів функціонування організації [4]:

DDoS-атаки можуть призвести до значних фінансових втрат через порушення роботи онлайн-сервісів, зниження продуктивності або втрату клієнтів. Наприклад, через недоступність веб-ресурсів компанія може втратити доходи від онлайн-продажів або послуг. Витрати на відновлення після атаки також можуть бути значними, включаючи витрати на посилення систем безпеки та на ремонт пошкоджених елементів інфраструктури:

Часто наслідки таких атак виходять за межі фінансових втрат і завдають шкоди іміджу компанії. Втрата доступності сервісів або даних може знизити довіру з боку клієнтів і партнерів. У разі повторних атак організація може стати мішенню для негативної уваги медіа, що ще більше погіршить її репутацію:

Атаки можуть порушити безперервність бізнес-процесів, уповільнюючи або повністю зупиняючи операційні системи. Це може негативно вплинути на ефективність виконання поточних завдань і проектів, а також викликати тимчасове зниження продуктивності працівників через неполадки у мережі:

У разі порушення захисту даних або порушення умов договорів з клієнтами чи партнерами, компанія може зазнати юридичних наслідків, включаючи штрафи, компенсаційні виплати або інші санкції згідно з нормативними вимогами. Наприклад, порушення вимог щодо захисту персональних даних може призвести до серйозних юридичних наслідків для компанії.

З огляду на багатогранний характер ризиків, системна оцінка загроз і потенційних наслідків DDoS-атак є етапом у формуванні ефективної стратегії реагування. Така оцінка дозволяє не лише розробити заходи з нейтралізації атак, а й адаптувати політики безпеки організації для посилення захисту на всіх рівнях — від технічного до стратегічного. У результаті, підприємство може ефективно захистити свої критичні елементи інфраструктури та забезпечити їх безперебійну роботу навіть під час кіберзагроз. Наслідки успішної DDoS-атаки можуть бути різноплановими. До прямих втрат належать фінансові збитки через простій систем,

витрати на відновлення працездатності інфраструктури та закупівлю додаткових ресурсів. Важливо також враховувати репутаційні ризики, оскільки тривала недоступність сервісів знижує довіру клієнтів і партнерів. Крім того, порушення роботи інформаційних систем може призвести до невиконання зобов'язань перед контрагентами, що може спричинити юридичні наслідки.

Для оцінки рівня ризику рекомендується застосовувати системний підхід із використанням матриць ризиків, які враховують ймовірність настання атаки та її потенційний вплив. Такий підхід дозволяє ідентифікувати найбільш вразливі елементи корпоративної мережі та пріоритетно впроваджувати заходи захисту.

Оцінка поточного стану системи захисту корпоративної мережі є важливим кроком для визначення готовності організації протидіяти DDoS-атакам. Аналіз повинен включати перевірку засобів виявлення аномального трафіку, наявність політик реагування на інциденти, резервування мережевих каналів і рівень кваліфікації IT-персоналу.

Таким чином, системна та комплексна оцінка ризиків DDoS-атак дозволяє своєчасно виявити вразливі місця в інфраструктурі організації, мінімізувати потенційні збитки і підвищити рівень інформаційної безпеки корпоративної мережі.

Розділ 2 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД DDoS-АТАК НА БАЗІ MICROSOFT AZURE DDoS PROTECTION

2.1 Архітектура та компоненти рішення Microsoft Azure DDoS Protection

Захист від розподілених атак типу відмова в обслуговуванні (DDoS) є критичним елементом забезпечення інформаційної безпеки в корпоративних мережах. Одним із найпоширеніших і ефективних хмарних рішень для протидії таким атакам є платформа Microsoft Azure, Azure DDoS Protection є комплексною службою, призначеною для захисту ресурсів, розгорнутих у віртуальних мережах Azure (VNets). Вона забезпечує посилені можливості пом'якшення DDoS-атак, автоматично налаштовуючись для захисту конкретних ресурсів Azure у VNet. Процес включення захисту є простим для будь-якої нової або існуючої віртуальної мережі та не вимагає внесення змін до додатків або ресурсів, що є значною перевагою для швидкого розгортання та мінімізації операційних складнощів. (рисунок 2.1) [10].

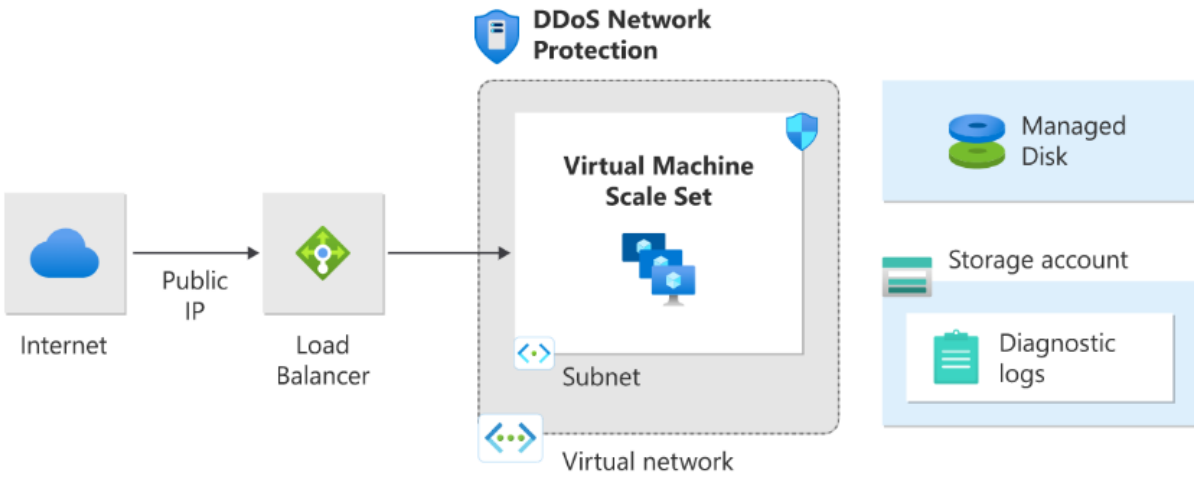


Рис. 2.1. Захист мережі від DDoS-атак увімкнено у віртуальній мережі [10].

Побудова ефективної системи захисту від DDoS-атак є складним багаторівневим завданням, яке охоплює як технічні, так і організаційні аспекти. Рішення повинно не лише фільтрувати шкідливий трафік, а й гарантувати безперервність бізнес-процесів, масштабованість, відповідність нормативним вимогам і оперативне реагування на загрози.

У таблиці 2.1 нижче представлено принципи побудови систем захисту, які лежать в основі сучасних стратегій кібербезпеки, орієнтованих на протидію DDoS-атакам.

Таблиця 2.1

Принципи побудови систем захисту від DDoS-атак

Принцип	**Суть принципу**	**Реалізація на практиці**
Багаторівневий захист	Комбінування кількох рівнів безпеки: мережевий, транспортний, прикладний	Використання міжмережевих екранів, систем IDS/IPS, CDN, WAF, сегментація трафіку
Проактивність	Передбачення та запобігання атакам до їх виникнення	Постійний моніторинг, поведінковий аналіз, виявлення аномалій, сценарії раннього реагування

Продовження таблиці 2.1

Гнучкість і масштабованість	Система повинна адаптуватися до змін у структурі трафіку або масштабах атаки	Хмарні DDoS-сервіси, автоматичне масштабування інфраструктури, еластичне балансування навантаження
Мінімізація часу реакції (RTTM)	Зменшення інтервалу між виявленням загрози та її нейтралізацією	Автоматичні правила фільтрації, тригери для перемикання трафіку на захищені канали
Розмежування доступу	Обмеження прав користувачів і сервісів для запобігання внутрішнім уразливостям	Впровадження політик доступу (RBAC/ABAC), ізоляція критичних сегментів мережі
Аудит і журналювання	Фіксація усіх подій, пов’язаних із трафіком та інцидентами безпеки	Ведення логів, звіти про атаки, подальший аналіз для удосконалення системи
Безперервність сервісу (HA)	Забезпечення високої доступності	Використання резервних ліній, георозподілених

	сервісів навіть під час атаки	центрів обробки даних, систем відновлення
Інтегрованість	Захисна система повинна взаємодіяти з іншими IT-рішеннями	Синхронізація з SIEM, інтеграція з DevOps-процесами, підтримка API
Аналіз після атаки (Post-mortem)	Вивчення природи атаки, її ефективності, вразливих місць у системі	Розслідування інцидентів, оновлення конфігурацій, вдосконалення реагування

Рішення Azure DDoS Protection реалізує багатошаровий підхід до захисту, що є фундаментальним для ефективного протистояння різноманітним векторам атак. Служба працює на мережевих рівнях 3 (мережевий) та 4 (транспортний), забезпечуючи захист від об'ємних та протокольних атак. Однак, для забезпечення повного захисту від атак на рівні 7 (прикладний рівень), які націлені на веб-додатки, таких як HTTP Floods, SQL-ін'єкції або міжсайтовий скриптинг, необхідно додатково використовувати Web Application Firewall (WAF). Ця вимога до інтеграції WAF підкреслює, що підприємства не можуть покладатися виключно на Azure DDoS Protection для всебічної безпеки від усіх типів DDoS-атак, особливо для веб-додатків. Повноцінна стратегія захисту від DDoS повинна обов'язково включати багатошаровий підхід, явно інтегруючи WAF для захисту прикладного рівня. Це означає, що архітектори безпеки повинні планувати розгортання обох служб, що може призвести до більшої складності та витрат, але значно покращить стійкість системи.

Реалізація принципів захисту від DDoS-атак дійсно вимагає комплексного підходу, який включає три основні складові: технічний, організаційний та людський аспекти. Такий підхід дозволяє створити багатошарову систему захисту, що забезпечує надійний захист на всіх етапах взаємодії з мережею.

На технічному рівні захист від DDoS-атак передбачає побудову інфраструктури, яка включає використання різних технологій для фільтрації та розподілу трафіку. Головним елементом є забезпечення масштабованості та гнучкості захисних систем, здатних адаптуватися до змінного характеру атак (рисунок 2.2) [10].

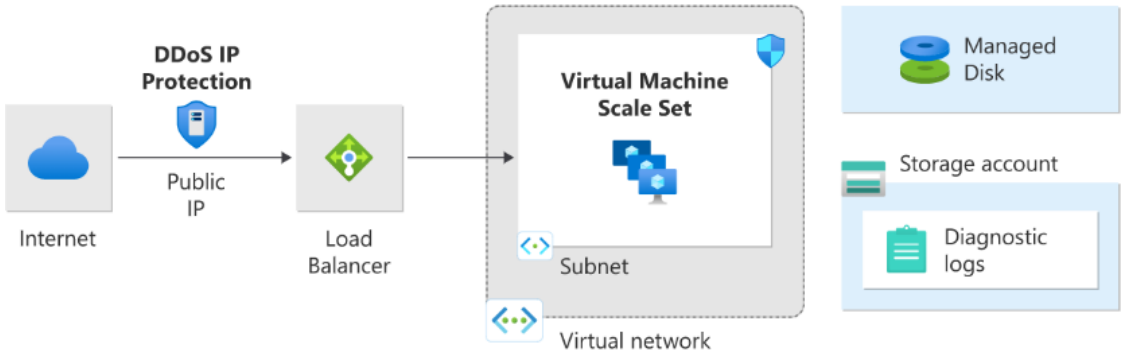


Рис. 2.2. Захист від DDoS-атак увімкнено на публічній IP-адресі, пов'язаній зі шлюзом веб-додатків [10]

Це може бути реалізовано через балансування навантаження, використання систем виявлення та запобігання вторгненням (IDS/IPS), анти-DDoS-рішення на базі хмари, а також інтелектуальні алгоритми аналізу трафіку на основі штучного інтелекту та машинного навчання. Всі ці елементи повинні працювати в єдиній екосистемі, забезпечуючи швидке виявлення і нейтралізацію атак.

Кожен PoP виступає як проксі-сервер, який аналізує, фільтрує та кешує трафік до кінцевого ресурсу. Фактично, увесь вхідний трафік до захищених доменів проходить через вузли, де він перевіряється на наявність ознак шкідливої діяльності. У випадку виявлення підозрілих моделей поведінки чи надмірної активності застосовуються миттєві механізми нейтралізації.

Використовує Anycast-технологію, яка дає змогу одному IP-адресному простору бути оголошеним з різних фізичних розташувань одночасно. Це дозволяє спрямовувати трафік до найближчого географічного PoP, знижуючи навантаження на окремі вузли та забезпечуючи природне масштабування. [28].

Людський аспект полягає в навчанні персоналу та забезпеченні його готовності до дій у разі атаки. Необхідно, щоб співробітники компанії були навчені виявляти потенційні загрози та мали чітке уявлення про свої дії в разі атаки. Навчання персоналу повинно включати в себе як технічні знання щодо конфігурації захисних систем, так і загальні принципи кібербезпеки. Регулярні тренінги, симуляції атак і розробка інструкцій для реагування на інциденти допомагають підвищити ефективність захисту та знижують ймовірність помилок в критичні моменти.

Однією з особливостей сучасних систем захисту від DDoS-атак є здатність до самонавчання. Штучний інтелект та машинне навчання дозволяють системам не лише реагувати на поточні загрози, а й аналізувати попередні атаки для створення точних алгоритмів фільтрації трафіку. Наприклад, якщо система виявила новий тип атаки, вона може автоматично адаптувати свої налаштування або алгоритми виявлення для протидії подібним загрозам у майбутньому. Це дозволяє підвищити ефективність захисту і зменшити час реакції на нові або невідомі типи атак.

Таким чином, комплексний підхід до захисту від DDoS-атак включає технічні рішення, організаційні заходи та навчання персоналу. Системи, що мають здатність до самонавчання, дозволяють постійно удосконалювати алгоритми захисту, підвищуючи ефективність і надійність захисту від нових загроз.

Галузева специфіка дійсно відіграє роль у визначенні вимог до систем захисту від DDoS-атак. В кожній сфері є свої пріоритети, які необхідно враховувати при розробці стратегії безпеки, оскільки різні типи бізнесу можуть по-різному реагувати на кіберзагрози.

У банківському секторі одним із основних пріоритетів є безперервність сервісу та мінімізація часу реакції на будь-які кіберінциденти, в тому числі на DDoS-атаки. Банківські установи зазвичай обробляють величезні обсяги фінансових транзакцій у режимі реального часу, тому навіть короткочасний збій у роботі системи може призвести до значних фінансових втрат, втрати довіри з боку клієнтів та репутаційних ризиків. У цьому випадку необхідно, щоб система захисту мала можливість.

Захист інфраструктури в банківському секторі часто включає використання передових рішень, таких як спеціалізовані анти-DDoS платформи з інтеграцією з іншими компонентами безпеки для оперативного виявлення і блокування атак. Рішення мають бути здатні обробляти атаки на високих швидкостях і масштабах без впливу на кінцевих користувачів або критичні фінансові операції [28].

У сфері онлайн-освіти основним акцентом є масштабованість та гнучкість. Системи для онлайн-курсів і платформ для навчання часто мають короткочасні піки навантаження, наприклад, під час тестувань, семінарів або великих подій, таких як вебінари. У ці періоди трафік може суттєво зростати, тому потрібно, щоб система могла ефективно масштабуватися для обробки додаткового навантаження, не даючи жодного збоїв у доступності сервісу.

До того ж, в цій галузі також потрібно мати систему, яка забезпечує гнучкість у налаштуваннях для швидкої адаптації до різних типів атак, оскільки часто використовуються хмарні рішення, які дозволяють миттєво збільшувати ресурси в разі високих навантажень. У цьому випадку платформи, як Microsoft Azure або AWS Shield, надають необхідні можливості для захисту від DDoS-атак при одночасному забезпеченні стабільної роботи при різних навантаженнях.

Ефективна система захисту від DDoS-атак повинна базуватися на поєднанні технічних інструментів, процедур управління ризиками й безперервного вдосконалення. Застосування перелічених принципів дозволяє зменшити як ймовірність успішної атаки, так і її потенційні наслідки, забезпечуючи стабільну роботу корпоративних сервісів у динамічному кіберсередовищі.

2.2 Призначення та основні функції компонентів Microsoft Azure DDoS Protection

Сучасні технології та рішення для захисту від DDoS-атак включають різноманітні методи та інструменти, що дозволяють як зменшити ймовірність успішної атаки, так і пом'якшити її наслідки. Враховуючи швидкий розвиток технологій і вдосконалення методів атак, компанії повинні застосовувати багаторівневий захист, використовуючи як традиційні, так і новітні рішення.

Нижче наведено у таблиці 2.2 огляд основних технологій захисту, що використовуються для протидії DDoS-атакам [29].

Таблиця 2.2

Технології для захисту від DDoS-атак

Технологія	**Опис**	**Переваги**	**Недоліки**
Міжмережеві екрани (Firewalls)	Фільтрація трафіку на основі визначених правил для блокування шкідливого трафіку.	Простота впровадження, добре відомі технології.	Може бути неефективним проти великих атак, залежить від правильного налаштування.

Продовження таблиці 2.2

Системи виявлення/запобігання вторгнення (IDS/IPS)	Активне виявлення та блокування аномалій трафіку, що характерні для DDoS-атак.	Виявлення та блокування шкідливого трафіку в реальному часі.	Може генерувати багато хибних спрацьовувань, потребує налаштування та моніторингу.
Анти-DDoS рішення на базі хмари	Використання хмарних сервісів для перенаправлення та фільтрації трафіку.	Масштабованість, швидка адаптація до атак.	Залежність від зовнішніх постачальників послуг, ризик втрати контролю над інфраструктурою.
Системи балансування навантаження	Розподілення трафіку між кількома серверами для зниження навантаження на один сервер.	Підвищення доступності сервісів, зменшення ефекту від атак.	Може не допомогти при великих атаках, якщо не використовуються інші заходи захисту.
Фільтрація на рівні DNS	Використання технології DNS для фільтрації запитів до серверів, що допомагає зменшити кількість зловмисних запитів.	Знижує навантаження на основний сервер, ефективний при великій кількості запитів.	Потребує додаткової конфігурації та моніторингу DNS-серверів.

Продовження таблиці 2.2

Інтелектуальні алгоритми аналізу трафіку (AI/ML)	Використання штучного інтелекту та машинного навчання для виявлення та протидії аномаліям у трафіку.	Можливість автоматичного навчання на основі нових загроз, точніше виявлення аномалій.	Потребує значних ресурсів для налаштування та навчання моделей, високі вимоги до інфраструктури.

До основних елементів належать: мережа доставки контенту (CDN), брандмауер веб-застосунків (WAF), механізм захисту від DDoS-атак, засоби обмеження частоти запитів (Rate Limiting), проксі-сервери DNS, шлюз SSL/TLS та балансувальник навантаження (Load Balancer). Кожен з них виконує важливу функцію у виявленні, запобіганні й нейтралізації загроз, а їх синхронна взаємодія формує високоефективну архітектуру захисту. CDN у Microsoft Azure DDoS Protection — це глобально розподілена інфраструктура серверів, яка відповідає за кешування, зберігання та доставку статичного контенту до кінцевих користувачів. Основне призначення CDN — зменшення часу відгуку веб-ресурсів, а також зниження навантаження на основний сервер. У контексті захисту від DDoS-атак CDN виконує також оборонну функцію, оскільки вхідний трафік обробляється спочатку на периферії мережі (у точках PoP), що дозволяє ізолювати оригінальний сервер від шкідливого навантаження.

CDN автоматично кешує ресурси сайту, такі як зображення, скрипти, таблиці стилів та інші статичні об’єкти. У разі атаки типу HTTP flood або надмірного завантаження, CDN дозволяє обробляти більшість запитів без звернення до бекенда, значно знижуючи ймовірність вичерпання обчислювальних ресурсів основного сайту.

Microsoft Azure DDoS Protection — це комплексна хмарна служба, розроблена для захисту додатків та інфраструктури, розгорнутих у віртуальних мережах Azure, від розподілених атак типу "відмова в обслуговуванні" (DDoS). Її основне

призначення — забезпечити доступність та продуктивність онлайн-сервісів, запобігаючи виснаженню ресурсів, спричиненому шкідливим трафіком (рисунок 2.3) [12].

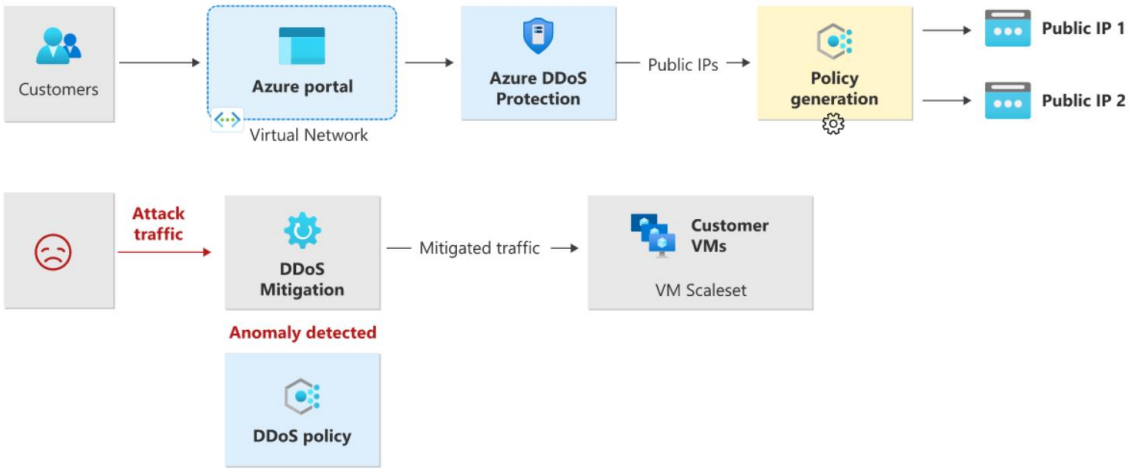


Рис. 2.3. Адаптивне налаштування в режимі реального часу [12]

Основні функції та компоненти Azure DDoS Protection включають:

1. Механізми виявлення атак

Постійний моніторинг трафіку та адаптивне налаштування в реальному часі: Azure DDoS Protection цілодобово моніторить використання трафіку та постійно порівнює його з порогами, визначеними в політиці DDoS. Як тільки поріг трафіку перевищується, пом'якшення DDoS ініціюється автоматично та миттєво. Служба використовує алгоритми машинного навчання для профілювання мережевого трафіку для кожної публічної IP-адреси, що захищається, автоматично налаштовуючи пороги політик для TCP SYN, TCP та UDP. Це забезпечує адаптивну реакцію на атаки в реальному часі. Політики пом'якшення на основі машинного навчання: Для кожної публічної IP-адреси захищеного ресурсу застосовуються три автоматично налаштовані політики пом'якшення: TCP SYN, TCP та UDP. Пом'якшення DDoS відбувається лише тоді, коли поріг політики перевищено.

2. Механізми пом'якшення атак

Очищення трафіку та перенаправлення легітимного трафіку: Після виявлення атаки Azure DDoS Protection автоматично відкидає шкідливий трафік, який перевищує визначені пороги, і перенаправляє залишковий, легітимний трафік до його цільового призначення. Цей процес відбувається автоматично та швидко,

мінімізуючи вплив атаки на доступність додатків. Захист від об'ємних атак (Layer 3/4): Ці атаки спрямовані на затоплення мережевого рівня значним обсягом трафіку (наприклад, UDP-флуди, атаки підсилення). DDoS Protection пом'якшує їх, автоматично поглинаючи та "очищаючи" їх за допомогою глобальної мережевої інфраструктури Azure. Захист від протокольних атак (Layer 3/4): Ці атаки використовують слабкості в стеку протоколів рівня 3 та 4 (наприклад, SYN-флуд). DDoS Protection пом'якшує їх, розрізняючи шкідливий та легітимний трафік, взаємодіючи з клієнтом та блокуючи шкідливий трафік. Захист від атак на прикладному рівні (Layer 7) за допомогою WAF: Для захисту від атак, націлених на веб-додатки (наприклад, HTTP Floods, SQL-ін'єкції, міжсайтовий скриптинг), необхідно використовувати Web Application Firewall (WAF) у поєднанні з Azure DDoS Protection. Azure надає WAF як функцію Application Gateway та Azure Front Door.

3. Аналітика, метрики та система сповіщень

Телеметрія через Azure Monitor: Azure DDoS Protection надає розширені телеметрії через Azure Monitor, що дозволяє отримувати глибокі уявлення про шаблони атак. Доступні детальні звіти з інтервалом у п'ять хвилин під час атаки та повний підсумок після її завершення. Метричні дані зберігаються в Azure Monitor протягом 30 днів. Важливі метрики включають "Under DDoS attack or not", "Inbound bytes dropped DDoS", "Inbound packets forwarded DDoS", а також тригери пом'якшення (TCP SYN, TCP, UDP). Інтеграція з Microsoft Sentinel: Журнали потоків пом'якшення можуть бути передані до Microsoft Sentinel або інших систем SIEM для моніторингу в майже реальному часі під час атаки. Ця інтеграція дозволяє автоматизувати виявлення та реагування на DDoS-атаки, використовуючи розширену аналітику та можливості машинного навчання Sentinel. Система сповіщень: Можна налаштувати сповіщення про початок та завершення атаки, а також про її тривалість, використовуючи вбудовані метрики атаки. Сповіщення інтегруються з операційним програмним забезпеченням, таким як Azure Monitor logs, Splunk, Azure Storage, Email та Azure portal.

4. Рівні захисту

Azure DDoS Protection пропонує два основні рівні захисту:

DDoS Network Protection: Увімкнений на віртуальній мережі, захищаючи всі публічні IP-адреси в цій VNet на рівнях 3 та 4. DDoS IP Protection: Увімкнений на

окремій публічній IP-адресі. Ці компоненти та функції працюють разом, щоб забезпечити надійний, автоматизований та адаптивний захист від DDoS-атак для ресурсів, розгорнутих в Azure. Компонент Rate Limiting забезпечує можливість гнучкого обмеження кількості запитів до конкретних маршрутів або ресурсів веб-застосунку. Завдяки цьому адміністратор може задати, наприклад, максимальну кількість запитів із певної IP-адреси за одиницю часу. У разі перевищення цього порогу система може ініціювати блокування, тимчасову затримку або іншу дію.Rate Limiting є особливо ефективним у боротьбі з низькоінтенсивними DDoS-атаками (Low-Rate DDoS), які намагаються зімітувати звичайний користувацький трафік. Також цей механізм дозволяє обмежувати доступ до критичних API, сторінок входу або фінансових транзакцій, що захищає від атак автоматизованих ботів.

DNS-проксі забезпечує додатковий рівень захисту, приховуючи реальну IP-адресу сервера від зовнішнього світу. Усі запити до домену клієнта спочатку обробляються, що дає змогу фільтрувати атаки вже на етапі доменного іменування. Крім того, підтримка DNSSEC гарантує цілісність і достовірність відповіді на DNS-запит, запобігаючи кеш-підробці (cache poisoning) і атакам типу spoofing.DNS-проксі функціонує у зв’язці з Anycast-мережею, що дозволяє розподіляти DNS-запити до найближчих PoP, забезпечуючи зниження затримок і підвищення доступності навіть у разі атак на DNS-рівні.

SSL/TLS реалізує повноцінну підтримку шифрування даних між клієнтами та серверами, використовуючи сучасні криптографічні протоколи. Підтримує сертифікати Let’s Encrypt, протоколи TLS 1.2, 1.3, а також забезпечує автоматичне оновлення сертифікатів.

Шифрування трафіку забезпечує конфіденційність та цілісність даних, а також перешкоджає зловмисникам у спробах перехоплення інформації. SSL/TLS Gateway інтегрується з іншими компонентами платформи, включаючи WAF і DDoS Protection, що дозволяє здійснювати фільтрацію навіть зашифрованого трафіку.

Компонент Load Balancer дозволяє розподіляти вхідний трафік між кількома бекенд-серверами відповідно до встановлених політик. Це забезпечує підвищену надійність і масштабованість веб-ресурсів. У разі виявлення недоступності одного із серверів, система автоматично перенаправляє трафік на інші вузли [30].

Іншим інструментом є системи балансування навантаження, які допомагають рівномірно розподіляти трафік між кількома серверами. Це дає можливість зменшити навантаження на окремий сервер і покращити доступність ресурсів у випадку атаки. Однак, ці системи не завжди ефективні при великих атаках, якщо не застосовуються додаткові засоби захисту. В останні роки активно застосовуються інтелектуальні алгоритми аналізу трафіку на основі штучного інтелекту та машинного навчання. Ці технології дозволяють автоматично виявляти аномалії в трафіку та адаптуватися до нових загроз. Однак, вони мають свої недоліки, такі як висока потреба в ресурсах для налаштування та тренування моделей, а також значні вимоги до інфраструктури [1].

2.3 Процеси функціонування рішення Microsoft Azure DDoS Protection у корпоративній мережі

У сучасному світі захист від DDoS-атак є складовою кібербезпеки. Різні постачальники пропонують платформи та інструменти для захисту, які відрізняються функціональними можливостями, ціною, масштабованістю та рівнем інтеграції з іншими рішеннями. є однією з найпопулярніших платформ для захисту від DDoS-атак, і її вибір часто обумовлений здатністю задовольнити потреби малого та середнього бізнесу. Однією з головних переваг є доступність тарифів, що робить її привабливою для компаній, які мають обмежений бюджет на кібербезпеку. До того ж, пропонує простоту інтеграції, що дозволяє швидко налаштувати систему захисту без необхідності в складних технічних знаннях.

Ще одним фактором є масштабованість цієї платформи. Завдяки глобальній мережі дата-центрів здатна ефективно фільтрувати трафік, що забезпечує швидке реагування на атаки навіть при високих навантаженнях. Це є аспектом для веб-додатків та сайтів, які повинні зберігати свою доступність і продуктивність під час DDoS-атак.

Виявлення DDoS-атак. У разі виявлення аномальної активності, яка може вказувати на DDoS-атаку (наприклад, HTTP flood, UDP flood, SYN flood), система активує вбудовані механізми мітингації. До таких належать:

динамічне обмеження частоти запитів (rate limiting); використання CAPTCHA або JavaScript challenge; блокування або ізоляція джерел трафіку за IP або автономною

системою; перенаправлення трафіку на альтернативні вузли або інтерфейси очищення.

Механізми діють незалежно у кожній точці PoP, що забезпечує масштабованість і рівномірний розподіл навантаження на всю інфраструктуру.

Обробка прикладного трафіку за допомогою WAF після проходження первинного фільтра вхідний трафік додатково аналізується модулем WAF цей компонент забезпечує захист від атак на рівні додатків, таких як SQL-ін'єкції, міжсайтове скриптування (XSS), зловживання методами HTTP та інші загрози класу OWASP Top 10. WAF застосовує як стандартні набори правил, так і користувацькі політики, які можуть бути налаштовані відповідно до вимог організації. У разі виявлення небезпечного запиту застосовуються дії, визначені адміністратором: блокування, перенаправлення, логування або сповіщення.

Використання CDN та кешування відповідей якщо трафік визнано безпечним, система перевіряє можливість повернення відповіді з кешу. У випадку наявності відповідного контенту в CDN-пам'яті найближчого PoP, користувач отримує відповідь без звернення до основного сервера. Це зменшує затримку, оптимізує витрати на трафік та підвищує стійкість до повторних звернень. У разі відсутності кешованої відповіді запит перенаправляється до оригінального сервера клієнта через захищений канал із збереженням контрольованого середовища (reverse proxy), що дозволяє зберігати захист навіть під час прямої взаємодії з бекендом.

Аудитом та моніторинг усі дії системи супроводжуються детальним аудитом Інформація про обсяг трафіку, кількість заблокованих запитів, типи виявлених загроз, географію джерел трафіку. Користувач має доступ до візуалізованих звітів, динамічних графіків та журналів подій, що дозволяє проводити оперативний аналіз інцидентів і налаштовувати політики реагування. Крім того, існує можливість інтеграції з SIEM-рішеннями підприємства для централізованого моніторингу.

Адаптація та самонавчання системи підтримує автоматизоване оновлення систем безпеки та самонавчання моделей поведінки. Це дозволяє оперативно враховувати нові типи загроз без необхідності ручного втручання. Система реагує на зміни у структурі трафіку, а також автоматично створює тимчасові правила для фільтрації нових аномальних шаблонів.Додатково можлива інтеграція з внутрішніми політиками доступу підприємства та застосування концепції Zero

Trust, за якої жоден запит не вважається довіреним без перевірки, навіть якщо він ініційований із внутрішньої мережі [32].

Ініціація запиту та маршрутизація усі вхідні запити до веб-ресурсів, захищених, перенаправляються до глобальної Anycast-мережі платформи. Принцип дії полягає у виборі найкоротшого шляху до точки присутності (PoP), розташованої найближче до клієнта, що ініціював запит. Це дозволяє мінімізувати затримки при обробці запиту та зменшити навантаження на основний сервер компанії. DNS-запити обслуговуються через інфраструктуру DNS, яка виконує також функції первинного фільтрування.

Первинна перевірка та аналіз трафіку на етапі початкової обробки кожен вхідний запит піддається перевірці на відповідність налаштованим політикам безпеки. Система виконує перевірку за такими параметрами, як IP-адреса, країна походження, частота запитів, заголовки HTTP/HTTPS, вміст запиту тощо. При цьому запити класифікуються як звичайні, потенційно небезпечні або шкідливі.

Обробка здійснюється модульно, із застосуванням механізмів логічного аналізу, сигнатур загроз та евристичних алгоритмів. Система автоматично адаптується до виявлених аномалій, порівнюючи поточний трафік із базовими моделями нормальної поведінки, сформованими на основі історичних даних[33].

Функціональні процеси, реалізовані у рішенні, забезпечують багаторівневий, адаптивний і безперервний захист корпоративної мережі. Поєднання механізмів маршрутизації, прикладного фільтрування та аналітики дозволяє ефективно протидіяти DDoS-атакам різного типу та інтенсивності. Система функціонує безпосередньо на периферії мережі, ізолюючи внутрішні ресурси компанії від прямого впливу шкідливого трафіку. Це дозволяє забезпечити стійкість до навантажень, високу доступність сервісів і зменшити витрати на підтримку власної інфраструктури захисту.

Розділ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ВІД DDoS-АТАК

3.1 Варіант впровадження системи захисту корпоративної мережі на базі Microsoft Azure DDoS Protection

У сучасних умовах інтенсивного зростання кількості та складності DDoS-атак забезпечення безперервної доступності корпоративних ресурсів є критично важливим завданням для підприємств і організацій. Одним з найбільш раціональних підходів до побудови стійкої системи захисту є використання хмарних сервісів, здатних обробляти значні обсяги вхідного трафіку, забезпечуючи попередню фільтрацію та відсікання шкідливих запитів. У цьому контексті платформу Microsoft Azure DDoS Protection можна розглядати як ефективне рішення, придатне для інтеграції в інфраструктуру середньої або великої організації з метою захисту мережевих ресурсів від DDoS-атак. Що стосується інтеграції, хмарні платформи мають перевагу в тому, що вони легко взаємодіють з іншими інструментами безпеки, такими як фаєрволи, VPN, антивірусне програмне забезпечення та інші рішення, що дає змогу створити комплексну стратегію захисту [29].

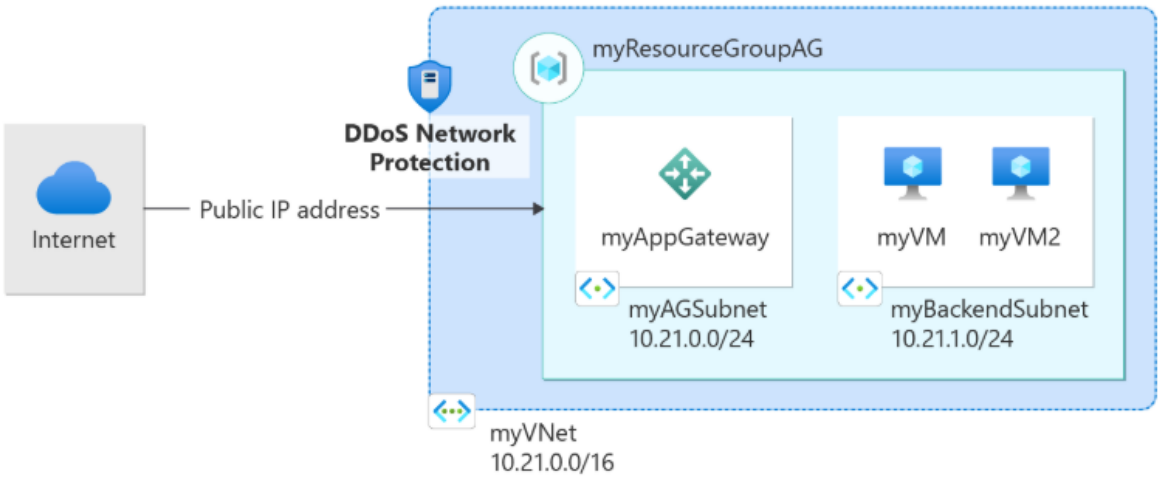
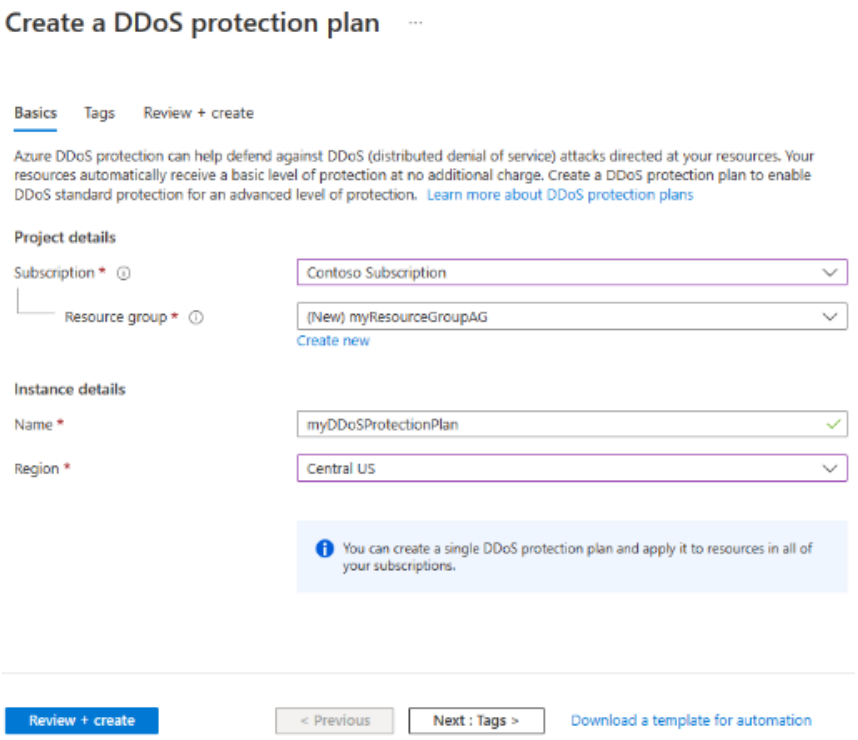


Рис. 3.1. Захист шлюза застосунків за допомогою захисту мережі Azure DDoS [29]

Однак є й деякі недоліки, пов’язані з використанням хмарних сервісів. Одним із головних є залежність від третьої сторони та її інфраструктури. Якщо постачальник послуг стикається з технічними проблемами в своїй мережі, це може вплинути на доступність вашої платформи, і компанія втратить контроль над певними аспектами безпеки. Додатково, зберігання даних та обробка трафіку через хмару може породити питання щодо безпеки даних якщо йдеться про чутливу інформацію, яка передається або зберігається на сторонніх серверах.

Ще одним аспектом є висока вартість хмарних рішень для великих компаній, що може бути суттєвим бар’єром для малого і середнього бізнесу. Хоча для малих підприємств такі платформи можуть бути економічно вигідними завдяки гнучким тарифам і можливості вибору потрібних послуг, для великих організацій, які потребують масштабованих рішень, ціни можуть стати значним фактором при виборі.

Таким чином, хоча хмарні сервіси пропонують значні переваги в плані ефективності та масштабованості, необхідно уважно оцінювати їхні недоліки, зокрема залежність від постачальника і потенційні ризики збереження даних. Локальні рішення для захисту від DDoS-атак є оптимальним вибором для великих компаній, які мають власні дата-центри або сервери, оскільки ці рішення забезпечують максимальний контроль над безпекою. Вони дозволяють компаніям безпосередньо контролювати трафік і налаштовувати системи безпеки відповідно до конкретних потреб та специфіки інфраструктури. Основною перевагою локальних рішень є повний контроль над системою захисту. Оскільки ці рішення розміщуються на власних серверах або в дата-центрах компанії, вона може безпосередньо контролювати всі аспекти безпеки. Це потрібно для організацій, які працюють із конфіденційними даними або мають вимоги до суворого дотримання стандартів безпеки. Локальне рішення також забезпечує відсутність залежності від сторонніх постачальників послуг, що дає змогу уникнути проблем, пов’язаних із можливими збої у роботі постачальника або зростанням витрат на хмарні сервіси. Це дозволяє компанії зберігати більший контроль над своїми даними та інфраструктурою.



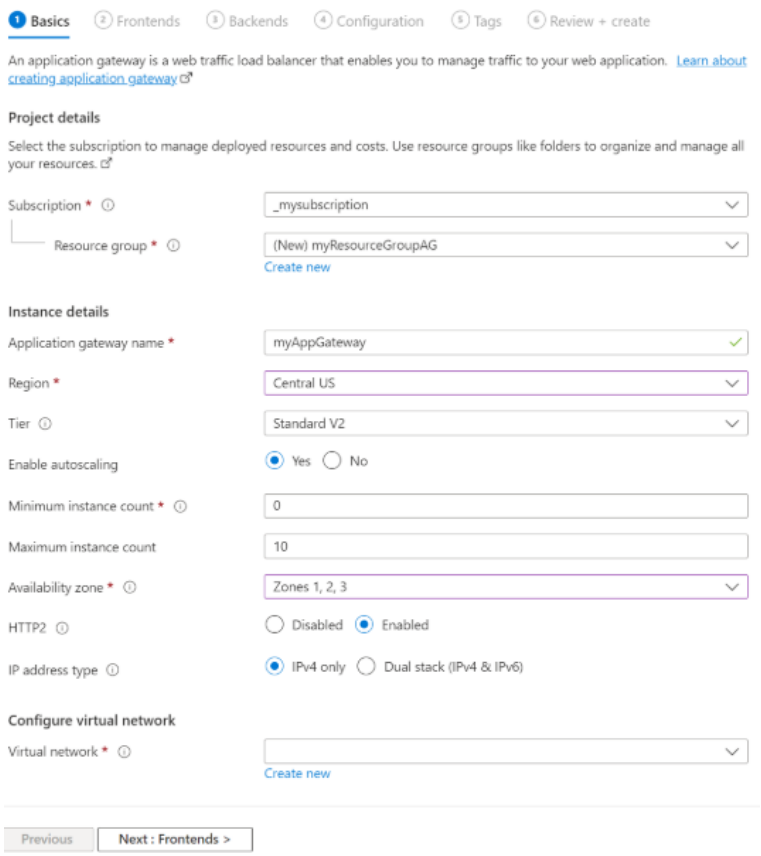
Ще однією перевагою є можливість налаштування під специфічні потреби організації. Локальні рішення дають змогу точно адаптувати систему захисту до особливостей конкретної інфраструктури та вимог бізнесу, що дозволяє створити ефективну стратегію безпеки.

Однак є і суттєві недоліки при впровадженні локальних рішень. Одним із основних є висока вартість придбання та обслуговування. Локальні рішення вимагають значних капітальних вкладень на придбання обладнання, а також постійних витрат на обслуговування та оновлення систем. Ці витрати можуть бути значними для малих і середніх підприємств. Додатково, для налаштування і моніторингу таких рішень потрібен спеціалізований персонал, що також веде до додаткових витрат на навчання та утримання фахівців [28].

Іншим недоліком є обмежена масштабованість. Локальні рішення не можуть так швидко адаптуватися до великих обсягів трафіку, як хмарні сервіси. Якщо обсяг атак або трафіку різко збільшується, компанії, які використовують локальні рішення, можуть зіткнутися з проблемами швидкої адаптації або необхідністю значних інвестицій в додаткове обладнання. Хмарні платформи, в свою чергу, можуть забезпечити гнучке та автоматичне масштабування.

Таким чином, локальні рішення для захисту від DDoS-атак є ефективними для великих компаній, які мають власні ресурси і потребують високого рівня контролю

над безпекою. Однак вони вимагають значних інвестицій і можуть мати обмеження в масштабованості та складності налаштування.



Гібридний підхід до захисту від DDoS-атак поєднує переваги як хмарних, так і локальних рішень, що дозволяє забезпечити високий рівень безпеки та ефективності. Замість того, щоб обирати між одним з варіантів, цей підхід дає змогу комбінувати їх, використовуючи сильні сторони кожного з них для досягнення оптимального результату.

Основною перевагою гібридного підходу є можливість комбінувати найкращі властивості обох типів рішень. Наприклад, трафік спочатку фільтрується через хмарні сервіси, що дозволяє масштабувати захист і миттєво реагувати на масові атаки, не навантажуючи при цьому внутрішню інфраструктуру. Локальні пристрої та системи можуть обробляти вже очищений трафік, що дає змогу підтримувати контроль над критичними частинами мережі та даними, зберігаючи при цьому високу ефективність фільтрації на рівні хмарного сервісу.

Такий підхід також дозволяє зберігати гнучкість і масштабованість. Хмарні платформи автоматично масштабуються відповідно до навантаження, що дає змогу

ефективно справлятися з великими обсягами трафіку, одночасно залишаючи можливість для локальних рішень забезпечувати глибшу безпеку та спеціалізовану обробку даних для чутливих елементів інфраструктури.

Ще однією перевагою є детальний контроль над критичними частинами мережі. Локальні рішення дають змогу організації зберігати повний контроль над безпекою внутрішніх даних, що може бути потрібно для компаній з особливими вимогами до конфіденційності чи регулювання. Це дозволяє краще адаптувати систему захисту до внутрішніх потреб організації, зберігаючи гнучкість у разі необхідності.

Проте, гібридний підхід має й деякі недоліки. Перший з них — складність інтеграції та адміністрування. Поєднання двох різних рішень вимагає чіткої інтеграції між хмарними платформами та локальними пристроями, що може вимагати значних зусиль для налаштування і підтримки системи. Це також може створити додаткову складність для команди адміністраторів, оскільки доведеться працювати з двома різними технологіями, що можуть вимагати окремих знань та вмінь.

Іншим недоліком є вищі витрати на підтримку та управління системою. Гібридний підхід потребує як інвестицій у хмарні рішення, так і в локальне обладнання, а також складного моніторингу і управління цією інфраструктурою. Зважаючи на це, організації можуть зіткнутися з більшими фінансовими витратами на обслуговування та оновлення таких систем.

В цілому, гібридний підхід є оптимальним варіантом для організацій, які прагнуть поєднати масштабованість і гнучкість хмарних рішень з контролем над критичними даними, що зберігаються на локальних пристроях. Однак цей підхід потребує ретельної інтеграції та додаткових витрат на підтримку, що може бути викликом для деяких компаній.

Системи, які використовують інтелектуальні алгоритми для виявлення аномалій у трафіку, є потужним інструментом у боротьбі з DDoS-атаками. Такі системи здатні здійснювати глибокий аналіз трафіку, застосовуючи методи машинного навчання та аналізу поведінки для виявлення аномальних патернів, які можуть свідчити про атаки. Оскільки атаки DDoS можуть постійно змінювати свої характеристики, ці системи дозволяють адаптуватися до нових типів загроз, зменшуючи ймовірність успішних атак.

Однією з основних переваг таких систем є автоматичне виявлення нових типів атак. Завдяки машинному навчанню та алгоритмам аналізу поведінки, ці системи можуть виявляти не тільки відомі атаки, але й нові, які раніше не були зафіксовані. Це дозволяє знижувати час реакції на загрози та підвищувати загальний рівень захисту мережі.

До того ж, системи, що використовують інтелектуальні алгоритми, здатні адаптуватися до змінюваних умов і нових загроз. Вони не просто реагують на попередньо задані шаблони, а й вчаться з нових даних, коригуючи свої стратегії виявлення і блокування атак. Це дозволяє системі бути гнучкою і ефективною навіть у умовах змінних типів загроз.

Завдяки можливості самонавчання, такі системи також знижують кількість фальшивих спрацювань (false positives). Традиційні методи фільтрації трафіку можуть час від часу блокувати легітимний трафік, однак інтелектуальні алгоритми здатні точніше визначити, чи є запит аномальним, зменшуючи ймовірність помилкових спрацьовувань.

Основні етапи впровадження

Початковий аудит інфраструктури. Перед початком інтеграції виконується аудит поточної мережевої конфігурації, аналіз публічних IP-адрес, доменних імен, хостинг-платформ, наявності TLS-сертифікатів. Це дозволяє уникнути конфліктів при перенаправленні трафіку.

Реєстрація облікового запису та додавання домену. Адміністратор створює обліковий запис у та додає основний домен компанії. Система автоматично імпортує поточні DNS-записи.

Перенесення DNS Адміністратор змінює DNS-сервери домену на ті, які надає. Відтепер весь DNS-трафік буде оброблятись через платформу, що забезпечує як оптимізацію, так і фільтрацію.

Активація захисних модулів дозволяє активувати DDoS Protection за замовчуванням. Також адміністратор може включити WAF з базовими або розширеними наборами правил, увімкнути TLS-з’єднання та задати обмеження частоти запитів.

Налаштування політик хешування та доступу у рамках оптимізації використовується хешування статичного контенту на PoP-серверах. Також

можливо вказати правила доступу для географічних регіонів, IP-діапазонів, типів пристроїв.

Тестування і моніторинг проходить після завершення налаштування проводиться тестування працездатності ресурсів та перевірка наявності помилок при доступі. Запити збираються у реальному часі, що дозволяє швидко виявити проблеми або потенційні загрози. Проте, є і кілька недоліків, які варто враховувати. Одним із них є потреба в значному часі на налаштування та тренування моделей. Щоб алгоритми працювали ефективно, вони повинні пройти етап навчання на великій кількості даних. Це може бути тривалим процесом в умовах постійно змінюваних загроз.

Також системи, що використовують машинне навчання, можуть бути складними для впровадження в існуючу інфраструктуру без значних змін. Оскільки для роботи таких систем потрібні спеціалізовані алгоритми та інфраструктура, впровадження може вимагати додаткових ресурсів для інтеграції та налаштування, що може бути викликом для деяких компаній.

Загалом, системи з інтелектуальними алгоритмами є дуже ефективними для виявлення DDoS-атак, але вони вимагають певних ресурсів і часу на впровадження та налаштування, а також можуть бути складними для інтеграції з наявними системами без значних змін наведені у таблиці 3.1.

Таблиця 3.1

Порівняння варіантів побудови системи захисту від DDoS-атак

Тип рішення	**Переваги**	**Недоліки**	**Приклад платформи**
Хмарне рішення	Масштабованість, швидка реакція, доступність з будь-якої точки	Залежність від постачальника, можливі питання безпеки даних	Cloudflare, AWS Shield, Akamai
Локальні рішення	Повний контроль, безпосередня інтеграція в інфраструктуру	Висока вартість, складність адміністрування	Radware DefensePro, Arbor Networks APS

Продовження таблиці 3.1

Гібридний підхід	Поєднання переваг хмарного та локального рішень, висока масштабованість	Складність у налаштуванні та інтеграції	Radware, Arbor, Cloudflare
Інтелектуальні системи моніторингу	Автоматичне виявлення атак, адаптивність до нових загроз	Потребує часу для навчання, складність впровадження	Darktrace, Vectra AI

Хмарні рішення - найкращий вибір для середніх компаній, які прагнуть знизити витрати на інфраструктуру і забезпечити захист без значних витрат часу на налаштування. Такі рішення ідеально підходять для стартапів або організацій, що хочуть швидко запровадити захист для своїх онлайн-сервісів. Хмарні платформи, як-от Cloudflare або AWS Shield, надають необхідну гнучкість та масштабованість для ефективного боротьби з DDoS-атаками при мінімальних капіталовкладеннях у власну інфраструктуру.

Для великих компаній із високими вимогами до безпеки та контролю за даними найбільш підходять локальні рішення, такі як Radware або Arbor Networks. Вони дають змогу детально налаштувати систему захисту, однак вимагають значних фінансових витрат на придбання, установку та обслуговування обладнання. Ці рішення підходять для організацій, які не хочуть залежати від сторонніх постачальників і мають необхідні ресурси для постійного моніторингу та підтримки систем.

Поєднання хмарних і локальних рішень дозволяє забезпечити найкращий рівень захисту при збереженні контролю над частинами інфраструктури. Цей підхід дозволяє комбінувати переваги обох варіантів, забезпечуючи масштабованість і гнучкість хмарних рішень з високим рівнем контролю та налаштування локальних систем. Однак цей підхід вимагає складного адміністрування та додаткових витрат на інтеграцію та підтримку.

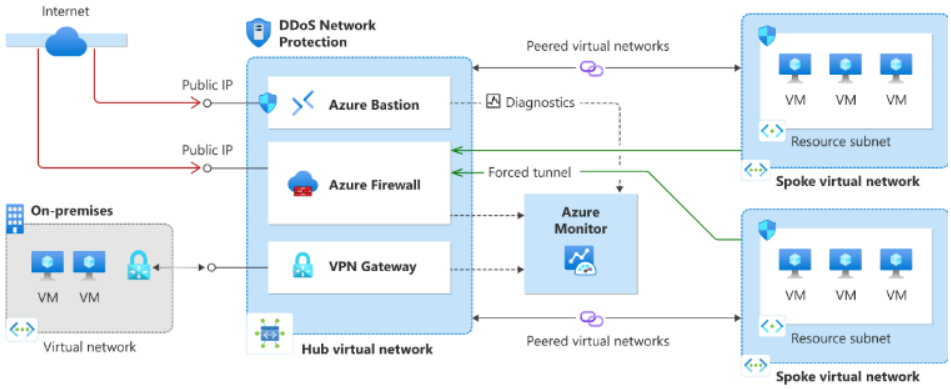
Системи, що використовують машинне навчання та інтелектуальні алгоритми для виявлення аномалій у трафіку, є перспективними для забезпечення високого рівня захисту від нових і складних типів атак. Однак їх впровадження може бути дорогою і складною задачею для організацій, які не мають досвіду в роботі з такими технологіями. Потрібно буде інвестувати в навчання моделей, що може зайняти багато часу, а також потребує спеціалізованих ресурсів для інтеграції в існуючу інфраструктуру.

Загалом, вибір найефективнішого рішення для захисту від DDoS-атак залежить від конкретних потреб організації, її бюджету, а також вимог до безпеки та контролю над інфраструктурою.

3.2 Послідовність реагування на DDoS-атаки в архітектурі Microsoft Azure DDoS Protection

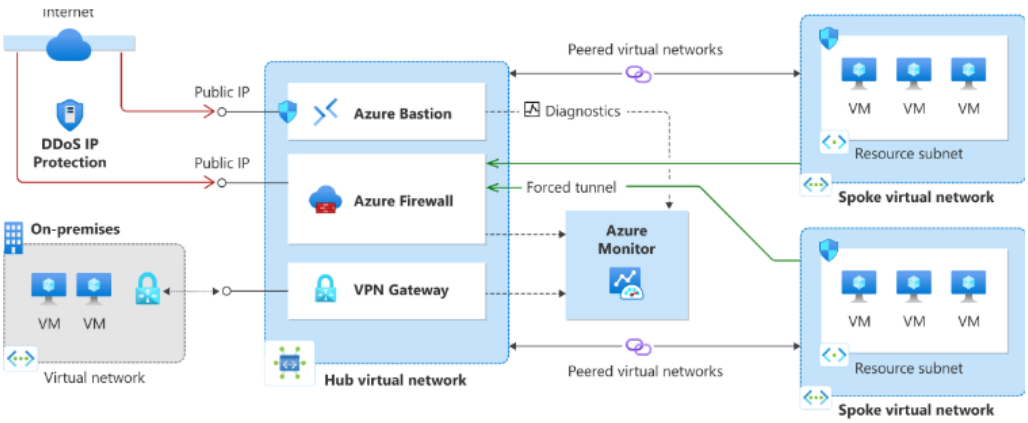
Для ефективного реагування на DDoS-атаки в корпоративних мережах необхідно розробити чітку стратегію, яка дозволяє швидко виявляти загрози, блокувати атакуючий трафік, знижувати ризики та мінімізувати час простоїв. Алгоритм реагування має включати кілька етапів, які взаємодіють і забезпечують максимальний захист. Цей процес можна поділити на кілька етапів: виявлення, аналіз, реагування та відновлення.

На першому етапі потрібно швидко виявити, що відбувається DDoS-атака. Для цього використовуються різноманітні методи моніторингу трафіку, які дозволяють виявити аномалії у поведінці мережі. Це може бути різке збільшення трафіку, незвичайний характер запитів або інші ознаки аномальної активності. Для цього застосовуються як традиційні засоби моніторингу (системи виявлення вторгнень, мережеві монітори), так і новітні рішення, засновані на машинному навчанні, здатні прогнозувати атаки [21].



Як тільки атака виявлена, необхідно оцінити її масштаби. Це включає в себе кількісне визначення трафіку, що надходить до мережі, аналіз джерел атакуючих запитів, а також визначення типу DDoS-атаки. Оцінка загрози дозволяє вирішити, як саме реагувати на атаку — чи потрібно залучати додаткові ресурси (наприклад, хмарний захист), чи достатньо локальних засобів захисту.

Якщо атаку було виявлено і її масштаби оцінено, наступним кроком є вжиття заходів для блокування атакуючого трафіку. Для цього можуть бути використані різноманітні методи, такі як фільтрація трафіку за IP-адресами, використання "чорних списків" для небезпечних IP-адрес, фільтрація за типом пакету або запитом, а також залучення додаткових інструментів, таких як CDN або хмарні платформи захисту, здатні знешкодити шкідливий трафік до того, як він потрапить в мережу підприємства.



На цьому етапі потрібно забезпечити адаптивність захисту. Якщо атакуючий трафік продовжує зростати, система повинна мати змогу масштабуватися,

підключаючи додаткові ресурси для обробки великого потоку запитів. Це може включати використання розподілених хмарних рішень, таких як Azure, для масштабування в режимі реального часу. Адаптивні системи повинні автоматично реагувати на зміни в характері атаки, ефективно розподіляючи навантаження та блокуючи небезпечні запити.

Під час атаки потрібно забезпечити чітку комунікацію між технічними спеціалістами та керівництвом компанії. Всі дії, вжиті для нейтралізації атаки, повинні бути задокументовані та передані до відповідних осіб для подальшого аналізу та звітності. Це також необхідно для належного реагування на інциденти безпеки та проведення подальших внутрішніх розслідувань.

Після відбиття атаки необхідно провести детальний аналіз її результатів. Оцінка ефективності вжитих заходів дозволить зробити висновки щодо вдосконалення системи захисту. На цьому етапі вивчаються лог-файли, дані з мережевих моніторів, а також робота використовуваних фільтрів. Ці дані допоможуть поліпшити систему виявлення атак, оптимізувати стратегії реагування та запобігти подібним атакам у майбутньому.

Після того як атака була зупинена і всі критичні уразливості усунуті, необхідно відновити нормальну роботу корпоративної мережі. Це включає в себе перевірку інфраструктури на наявність пошкоджень, відновлення можливості доступу до сервісів та ресурсів і підтвердження відсутності подальших загроз [20].

Завершальний етап алгоритму полягає в оновленні стратегій захисту та підготовці до можливих майбутніх атак. Це включає в себе удосконалення інфраструктури захисту, навчання персоналу та створення планів дій для швидкого реагування на атаки. Також потрібно постійно стежити за новими методами атак, що дозволить підтримувати високий рівень готовності до нових загроз.

Алгоритм реагування на DDoS-атаки є багатоступінчастим процесом, що вимагає інтеграції різноманітних технологій і стратегій. Головними складовими цього процесу є виявлення загроз на ранніх етапах, швидка реакція на атаки, адаптивне масштабування захисту та постійний моніторинг інфраструктури. Після відбиття атаки особливу увагу слід приділити вдосконаленню системи захисту та підготовці до можливих майбутніх атак.

3.3 Рекомендації щодо оптимального застосування засобів Microsoft Azure DDoS Protection для захисту корпоративної інфраструктури

У сучасних умовах цифрової трансформації корпоративні інформаційні системи все частіше стають мішенню для DDoS-атак, які можуть паралізувати роботу організації, зупинити надання послуг і спричинити значні репутаційні та фінансові втрати. Одним із ефективних рішень для протидії цим загрозам у хмарному середовищі є служба Microsoft Azure DDoS Protection, яка забезпечує активний мережевий захист на рівнях L3 та L4 моделі OSI.

Щоб використання цього інструменту було максимально ефективним, доцільно дотримуватись низки рекомендацій, що стосуються як проектування інфраструктури, так і налаштування засобів безпеки, реагування на інциденти та аналізу подій.Вибір та впровадження засобів захисту від DDoS-атак є етапом у забезпеченні безпеки корпоративних мереж. Правильний підхід дозволяє ефективно захищати інфраструктуру та знижувати ризики впливу атак на роботу компанії. Ось кілька рекомендацій, які допоможуть організаціям правильно вибрати та впровадити засоби захисту від DDoS-атак.

Перш ніж обирати рішення для захисту від DDoS-атак, необхідно провести детальний аналіз ризиків та виявити особливості корпоративної мережі, які можуть бути вразливими до таких атак. Це включає в себе:

- Визначення критичних точок доступу до мережі та сервісів.
- Оцінка обсягу трафіку, що проходить через мережу.
- Аналіз бізнес-процесів, які можуть бути порушені в разі успішної атаки.

Існує два основних типи рішень для захисту від DDoS-атак: хмарні та локальні. Кожне з них має свої переваги. Хмарні рішення (наприклад, Cloudflare, AWS Shield, Azure) забезпечують захист на зовнішньому рівні та можуть масштабувати ресурси в реальному часі. Це зручне рішення для компаній, які мають обмежені ресурси або потребують високої масштабованості. Локальні рішення (наприклад, Arbor Networks, Radware) дозволяють контролювати трафік безпосередньо на рівні корпоративної інфраструктури і можуть бути ефективними для великих компаній з власною мережею. Вони також можуть бути інтегровані з іншими системами безпеки підприємства.

Технології атак постійно змінюються, тому вибрані засоби захисту повинні бути адаптивними до нових типів DDoS-атак. Система повинна мати можливість [20]:

– Регулярно оновлюватися і вчасно адаптуватися до нових методів атак.

– Використовувати механізми машинного навчання для виявлення нових, раніше невідомих загроз.

Засоби захисту від DDoS-атак повинні бути сумісні з іншими компонентами корпоративної системи безпеки, такими як системи виявлення вторгнень (IDS/IPS), фаєрволи, VPN, антивірусні програми та інші. Сумісність дозволить забезпечити комплексний підхід до захисту корпоративної інфраструктури.

Необхідно вибирати між профілактичними (попередження атаки до її початку) та реактивними (реагування на атаку в реальному часі) засобами захисту. Профілактичні засоби (наприклад, розподілені мережі контенту (CDN), системи кешування) допомагають зменшити ймовірність успішного виконання атаки. Реактивні засоби забезпечують швидку нейтралізацію атаки після її виявлення, наприклад, автоматичне блокування IP-адрес атакуючих.

При виборі засобів захисту від DDoS-атак потрібно звертати увагу на підтримувані протоколи, оскільки вони визначають, як система буде реагувати на різні типи атак [20]:

TCP/UDP-фільтрація: Цей тип фільтрації працює на рівні транспортного протоколу і дозволяє блокувати або обмежувати атаки ще до того, як вони потраплять до мережі. Він ефективний при блокуванні великих атак, що використовують TCP або UDP трафік для переповнення мережевих ресурсів:

DNS фільтрація: Використовується для захисту серверів від атак, спрямованих на систему доменних імен (DNS). Така фільтрація дозволяє відсіяти шкідливі запити на рівні DNS, що допомагає запобігти DDoS-атакам, які намагаються перевантажити DNS-сервери:

HTTP/S фільтрація: Це фільтрація, яка застосовується для захисту веб-додатків і сервісів. Вона дозволяє аналізувати і фільтрувати запити на основі параметрів HTTP або HTTPS, щоб запобігти атакам, які спрямовані на веб-сайти, наприклад, атак з великим обсягом запитів або на рівні додатків.

Ці протоколи дозволяють забезпечити ефективний захист на різних рівнях мережі, від транспорту до додатків, і допомагають організаціям вибрати оптимальне рішення в залежності від їхніх потреб та інфраструктури.

Засіб захисту має відповідати розмірам та потребам компанії. Якщо компанія швидко розвивається або має велику кількість клієнтів, потрібно вибирати рішення, яке дозволяє ефективно масштабувати ресурси. Більшість сучасних рішень пропонують можливості для масштабування, дозволяючи адаптувати захист під зростаючі потреби.

Вартість рішень для захисту від DDoS-атак може варіюватися в залежності від їх функціональності, масштабованості та інфраструктури. Варто проводити оцінку витрат на впровадження та підтримку рішення, а також порівнювати їх з потенційними втратами від успішних атак. Це дозволить вибрати оптимальне рішення з точки зору ефективності витрат.

Не менш значеннєвим аспектом є наявність технічної підтримки від постачальника рішення. Потрібно переконатися, що компанія має можливість оперативно отримувати допомогу в разі виникнення проблем, а також проводити регулярне обслуговування та оновлення програмного забезпечення. Невід'ємною частиною впровадження засобів захисту є навчання співробітників. Всі працівники, які працюють з мережами та безпекою, повинні бути навчені основним принципам захисту від DDoS-атак, методам виявлення загроз і реагування на інциденти. Це дозволяє оперативно виявляти проблеми та мінімізувати їх вплив.

Вибір і впровадження засобів захисту від DDoS-атак є значеннєвим етапом для забезпечення безпеки корпоративних мереж. Необхідно оцінювати не тільки технічні характеристики рішень, але й їхню адаптивність до змінюваних умов, інтеграцію з іншими засобами безпеки, а також рентабельність та масштабованість. Правильний підхід до вибору дозволить зменшити ризики і ефективно захистити мережі від DDoS-атак.

ВИСНОВКИ

В результаті проведеного аналізу було виявлено, що DDoS-атаки можуть мати різні форми, зокрема атаки на виснаження ресурсів, атаки на рівні мережевих та прикладних протоколів. Кожен тип атаки має свої унікальні характеристики і вимагає специфічних методів захисту. Механізми, що використовуються для проведення цих атак, є дуже різноманітними, включаючи ботнети, інструменти для зміни джерела трафіку, а також складні методи маскування. Це робитDDoS-атаки складними для виявлення і нейтралізації.

В результаті огляду різноманітних засобів захисту було встановлено, що на сьогоднішній день існує велика кількість рішень для захисту від DDoS-атак, які включають апаратні, програмні та хмарні рішення. Апаратні рішення є ефективними для захисту на рівні мережі, забезпечуючи швидкий аналіз трафіку та блокування шкідливих запитів. Програмні рішення дають змогу гнучко адаптувати захист до специфічних потреб організацій. Хмарні рішення надають масштабовані платформи для забезпечення безпеки, здатні протистояти великим атакам без суттєвих втрат в ефективності мережі.

Штучний інтелект і машинне навчання мають великий потенціал для підвищення ефективності захисту від DDoS-атак, оскільки ці технології дозволяють створювати адаптивні системи, які здатні виявляти та нейтралізувати загрози на основі аналізу трафіку. Одна з головних переваг таких систем полягає в їх здатності адаптуватися до нових типів атак. Алгоритми машинного навчання здатні навчатися на історичних даних та виявлених аномаліях у трафіку, що дозволяє їм з часом покращувати свої можливості в розпізнаванні шкідливого трафіку, навіть якщо атака використовує нові методи.

Іншою особливістю є здатність ШІ прогнозувати нові загрози. Машинне навчання дозволяє системам передбачити зміни в поведінці атак, навіть якщо вони ще не були зафіксовані раніше, що знижує ймовірність успішного нападу. Це дає змогу значно підвищити рівень безпеки мережі та швидкість реагування на нові типи атак.

Технології ШІ також значно прискорюють процес виявлення загроз, обробляючи великі обсяги даних в реальному часі. Це дозволяє швидко виявляти

аномалії та запобігати атакам, мінімізуючи час, коли система може бути вразливою до зовнішніх загроз. Це є значеннєвим для компаній, де безперервність роботи є потрібною.

Водночас, завдяки автоматизації процесу виявлення атак, технології на основі ШІ знижують потребу у постійному людському втручанні. Система сама адаптується до нових умов і атак, що робить її ефективною та стійкою без необхідності постійного оновлення або участі фахівців у процесі захисту.

Таким чином, штучний інтелект та машинне навчання значно підвищують рівень кібербезпеки, дозволяючи швидко реагувати на зміни в умовах загроз і знижуючи ймовірність успішних DDoS-атак.

Порівняння ефективності різних засобів захисту від DDoS-атак показало, що жодне з рішень не є універсальним для всіх ситуацій. Кожен підхід має свої переваги і недоліки в залежності від масштабів організації та специфіки атак. Хмарні рішення забезпечують високу масштабованість та швидкість реагування на великий обсяг трафіку, тоді як апаратні рішення можуть бути ефективними для менших організацій, які мають обмежені ресурси для захисту.

Враховуючи отримані результати, можна рекомендувати організаціям використовувати комбінований підхід до захисту від DDoS-атак, поєднуючи апаратні, програмні та хмарні рішення для забезпечення максимальної ефективності. Варто враховувати специфіку організації та її потреби при виборі відповідних засобів захисту. Для великих компаній оптимальним буде використання хмарних рішень з інтеграцією в корпоративні системи безпеки, тоді як для малих і середніх організацій доцільно використовувати економічно вигідні програмні або апаратні рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.

2. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)

3. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект: монографія. Київ: Видавничий дім «Гельветика», 2017. 700 с.

4. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

5. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)

6. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації)

7. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.

8. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. Публічне урядування. 2016. № 4. С. 154–161.

9. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук: 12.00.01. Київ, 2007. 236 с.

10. Довідкові архітектури захисту від DDoS-атак Azure https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-reference-architectures

11. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства / Наше право. 2016. № 1. С. 17–23.

12. Адаптивне налаштування в режимі реального часу https://learn.microsoft.com/ru-ru/azure/ddos-protection/ddos-protection-features

13. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.

14. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".

15. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".

16. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".

17. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис.… канд. юрид. наук: 12.00.07. Львів, 2019. 268 с.

18. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.

19. Положення про організацію освітнього процесу в Тернопільському національному технічному університеті імені Івана Пулюя - наказ №4/7-340 від 21.05.2015 із змінами від 25.06.2019 - наказ №4/7-622 від 27.06.2019 та від 14.04.2020 - наказ №4/7-243 від 15.04.2020.

20. Положення про кваліфікаційні роботи студентів Тернопільського національного технічного університету імені Івана Пулюя - наказ №4/7-241 від 15.04.2020.

21. Положення про екзаменаційну комісію з атестації здобувачів вищої освіти ТНТУ ім.І.Пулюя - наказ №4/7-339 від 21.05.2015.

22. Положення про оцінювання здобувачів вищої освіти ТНТУ ім.І.Пулюя - наказ №4/7-542 від 11.07. 2016 зі змінами від 21.05.2019 - наказ №4/7-524 від 05.06.2019 та зі змінами від 31.10.2019 - наказ №4/7-970 від 01.11.2019.

23. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. — [Чинний від 2000.12.04]. — К. : ДСТСЗІ СБУ, 2000. — № 53.— (Нормативний документ системи технічного захисту інформації).

24. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах інтеграції України : дис. док. юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

25. Хом'яков Д. О. Нормативно-правове регулювання інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави: збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.). Київ: НА СБУ, 2018. С. 182–184.

26. Юдін О.К. Інформаційна безпека.Нормативно-правове-забезпечення: Підручник. – К.: Вид-во Видавництво Національного авіаційного університету «НАУ-друк», 2011. – 640 с

27. Gupta, N., Jain, A., Saini, P., & Gupta, V. (2016, March). DDoS attack algorithm using ICMP flood. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 4082-4084). IEEE.

28. Kirichenko, L., Radivilova, T., & Bulakh, V. (2019). Machine Learning in Classification Time Series with Fractal Properties. Data, 4(5), 1-13.

29. Посібник: Захистіть свій шлюз застосунків за допомогою захисту мережі Azure DDoS https://learn.microsoft.com/en-us/azure/application-gateway/tutorial-protect-application-gateway-ddos?toc=%2Fazure%2Fddos-protection%2FTOC.json

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)