3. *Козаровицкий Л. А*. Бумага и краска в процессе печатания / Л. А. Козаровицкий – М.: Книга. – 1965. – 368 с.
4. *Hongyan Chu*. Analysis of temperature characteristics of ink fluid based on power law model in microchannel / Hongyan Chu, Xuecong Lin, Ligang Cai // Advances in Mechanical Engineering. – 2019. – Vol. 11(3). – P. 1–15. DOI: 10.1177/1687814019833585.
5. *Linlin Liu*. Dynamic simulation modeling of inking system based on elastohydrodynamic lubrication / Linlin Liu, Kaikai Li, Fei Lu // International journal of heat and technology. – 2016. – Vol. 34, № 1. – P. 124–128. DOI: 10.18280/ijht.340118.
6. *Pyr'yev Y.* Analytical solution of thermal conduction in a two-layer cylinder modeling oscillator roller in an offset machine / Y. Pyr'yev // International Journal of Thermal Sciences. – 2019. – Vol. 136. – P. 433–443. DOI: doi.org/10.1016/j.ijthermalsci.2018.11.004.
7. *Верхола М. І.* Моделювання та визначення коефіцієнта передачі фарби передавальним валиком у фарбовій системі з розтиральним циліндром / М. І. Верхола, І. Б. Гук // Комп'ютерні технології друкарства : Збірник наукових праць / УАД. – 2009. – № 21. – С. 39 – 52.
8. *Верхола М. І.* Моделювання та комп'ютерне визначення зонального розподілу товщини шарів фарби на виході фарбодрукарської системи з розтиральним циліндром / М. І. Верхола, І. Б. Гук, Р. М. Споляк // Комп'ютерні технології друкарства : Збірник наукових праць / УАД. – 2010. – № 23. – С. 27 – 34.
9. *Верхола М. І.* Моделювання та аналіз впливу розміщення друкуючих елементів на формі на процес розподілу фарби у фарбових системах / М. І. Верхола, І. Б. Гук, В. М. Бабинець // Комп'ютерні технології друкарства: УАД. – 2007. – № 18. – С. 5 – 21.

http://doi.org/10.5281/zenodo.3860776

Поступила 7.10.2019р.

УДК 009.4

А.Т. Кобевко [1],
О.В. Тимченко [1, 2]

ОСОБЛИВОСТІ DDoS-АТАК НА ХМАРНІ СЕРВІСИ

Abstract. The paper provides a brief description of the features of DDoS attacks on cloud services, the taxonomy of attacks, their types and countermeasures to mitigate the impact. Methods of detection and prevention of attacks are described, the principle of a choice of decisions for protection is defined.

[1] Українська академія друкарства
[2] University of Warmia and Mazury Olsztyn, Poland

Постановки проблеми

Обчислювальні системи використовуються для вирішення великої кількості задач в управлінні та виробництві. Однак, швидкодія та продуктивність одного фізичного серверу у ряді випадків недостатня, тому популярними стають «хмарні» сервери, або середовища, які поєднують ресурси багатьох фізичних серверів. Така потужна віртуальна система має ряд значних переваг при виконанні більшої кількості задач, але її складність призводить до більшої вразливості.

«Відмова в обслуговуванні» (DoS) або «розподілена відмова в обслуговуванні» (DDoS) – це головні загрози доступності до віртуальних серверів хмарних середовищ, що може значно знизити продуктивність хмарних сервісів, пошкодивши віртуальні сервери.

Мета статті. Визначити і класифікувати основні загрози для хмарних середовищ від DDoS-атак та механізми захисту від них.

Основна частина

У 2009 році Національний інститут стандартів і технологій США (NIST) визначив хмарні обчислення як «модель для забезпечення зручного доступу до мережі за запитом до спільного середовища налаштованих обчислювальних ресурсів, які можна швидко забезпечити та випустити з мінімальними зусиллями управління або з взаємодією постачальника послуг». Оплата за час користування, віртуалізація, доступ до запиту, гнучкість та зниження витрат на обладнання та обслуговування – фактори, які сприяють популяризації хмарних обчислень. Віртуальний дата-центр (IaaS – Infrastructure as a Service) – це модель обслуговування, яка надає користувачам можливість розгортати та виконувати довільне програмне забезпечення, до складу якого можуть входити операційні системи та прикладні програми. Віртуалізація відіграє головну роль у хмарних обчисленнях шляхом ефективного та систематичного використання наявного обладнання. Віртуалізація використовується на різних етапах, зокрема мережі, процесор, пам’ять, сховище тощо. Це зменшує вартість та дозволяє створити доступну і гнучку систему.

DDoS-атака – головна загроза доступності. Зловмисник може значно погіршити якість або повністю зруйнувати мережевий зв’язок користувача. Для виконання атаки зловмисник спочатку створює багато агентів або хостів, а потім використовує ці агенти для запуску атаки, навантажуючи цільову мережу. Основний намір DDoS-атаки – зробити так, щоб жертва не могла використовувати свої ресурси. У більшості випадків цілями є веб-сервери, процесор, сховище та інші мережеві ресурси. У хмарному середовищі DDoS також може значно знизити продуктивність хмарних сервісів, пошкодивши віртуальні сервери.

Форми впливу DDoS-атак на жертв:

- Зловмисник виявляє певну помилку або слабкість у програмному забезпеченні та порушує роботу сервісу.

- Деякі напади вичерпують всю пропускну здатність або ресурси системи жертв.

Зловмисники сканують мережу, щоб знайти вразливе обладнання та використовувати його як агента у подальшому. Таке обладнання називають «зомбі». Структура мережі Інтернет має багато особливостей, які дозволяють застосовувати DDoS-атаки. Зловмисники ставлять під загрозу безпеку хостів для запуску DDoS-атак та використовують підроблені IP-адреси, що ускладнює відстеження джерела атаки. В Інтернеті є багато хостів, що дає нападникові широкий вибір цілей для атаки. Основна мета DDoS-атаки - це зробити комп'ютерні ресурси для яких комп'ютерна система була призначена (пропускну здатність, процесор та ресурси, які обмежені мережею) недоступними користувачам. Якщо збільшити ці ресурси, вплив нападу зменшиться. Однак стримування таких атак веде до даремного витрачання наявних ресурсів, і як наслідок – грошових втрат.

DDoS-атаки

DDoS-атаки ініціюються мережею дистанційно керованих, добре структурованих та широко розпорошених хостів - "зомбі". Їх також називають вторинними жертвами. У 2019 році жертвами DDoS-атак стали: китайські веб-сайти, Wikipedia, Telegram, ФБР тощо. Більшість із цих атак були розподіленими, тобто відбувались одночасно з великої кількості IP-адрес.

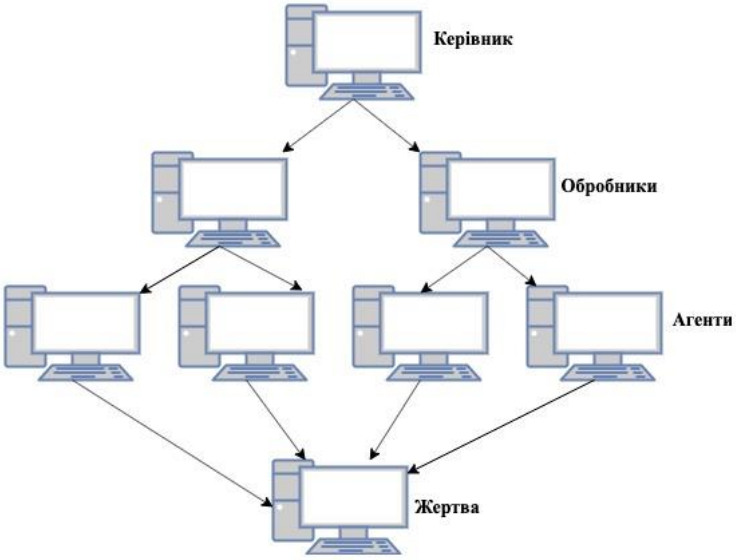

Рис.1. Структура DDoS-атаки

Структура DDOS-атаки

Для здійснення DDoS-атаки широко використовуються інтернет-боти, тобто застосовується технологія «клієнт-сервер» для запуску великої кількості «зазомбованих» хостів. Загалом, DDoS-атака складається з керівника, обробника, агентів та жертви (рис. 1). Зомбі (агенти або боти) використовуються керівником для формування інтернет-ботів. Від їх кількості і залежить сила атаки. Керівник спілкується з агентами через обробників. Обробниками, наприклад, можуть бути програми, встановлені на вражених пристроях (мережевих серверах), з якими зловмисники спілкуються для надсилання команд. Зловмисник відправляє команду та керує своїми агентами через обробників. Боти – пристрої, які запущені обробниками, фактично здійснюють напад на систему жертви.

Зловмисники використовують різні методи сканування для пошуку вразливої машини. Найпростіша стратегія – це випадкове сканування IP-адрес, оскільки вірус не знає, де знаходиться вразливий хост. Метод ефективний лише для IPv4, оскільки адресний простір IPv6 занадто великий. При скануванні за списком зловмисник має перелік заражених IP-адрес.

Коли він робить іншу машину хостом, частина початкового списку звернень буде відправлена на неї. Сканування на основі маршруту зменшує пошукові адреси, використовуючи префікси протоколу маршрутизації BGP (Border Gateway Protocol). Вони скорочують обсяг інформації, у якій відбувається пошук. За допомогою цієї техніки сканування проводиться різними хостами на різних ділянках адресного простору, і таким чином заощаджує ресурси. Часом використовують інші стратегії, такі як сканування перестановки, локальне сканування переваг та топологічне сканування. Після виявлення вразливого хоста знаходять його вразливе місце та отримують контроль над ним.

Класифікація

Різноманітність DDoS-атак дедалі зростає. Найпоширенішими є атаки на основі пропускної здатності та ресурсів. Ці типи споживають всю пропускну здатність та ресурси мережі, що експлуатується. Результати аналізу видів атак подані на рис. 2. Залежно від використаної вразливості, атаки можна розділити на різні типи.

Ураження пропускної здатності:

Цей тип нападу споживає пропускну здатність жертви або цільової системи, навантажуючи небажаним трафіком, щоб запобігти потраплянню легітимного трафіку в мережу жертви. Для здійснення цих атак зазвичай використовуються такі інструменти, як Trinoo. Атаки виснаження пропускної здатності додатково класифікуються як:

Флуд-атака:

Зловмисник надсилає величезний обсяг трафіку жертві за допомогою зомбі, і таким чином перевантажує мережу. Система потерпілого швидко сповільнюється, не даючи легітимному трафіку отримати доступ до мережі.

Це зумовлено пакетами UDP (User Datagram Protocol) та ICMP (Internet Control Protocol). Атака UDP-флуд складається з таких кроків:

1. Зловмисник надсилає велику кількість пакетів UDP у випадкові або вказані порти системи жертви за допомогою зомбі.

2. При отриманні пакетів система жертви шукає порти призначення, щоб ідентифікувати програми, які очікують на порт.

3. Вона не знаходить потрібних програм та генерує пакет ICMP з повідомленням "призначення недоступне".

4. Зворотні пакети від жертви надсилаються на підроблену адресу.

В результаті атаки наявна пропускна здатність системи вичерпується та не може використовуватись жертвою. Це впливає на інтернет підключення та системи, розташовані поблизу жертви. Різновидами цієї атаки є: фрагментація, DNS флуд атака, VoIP флуд атака, флуд медіа даними, тощо.

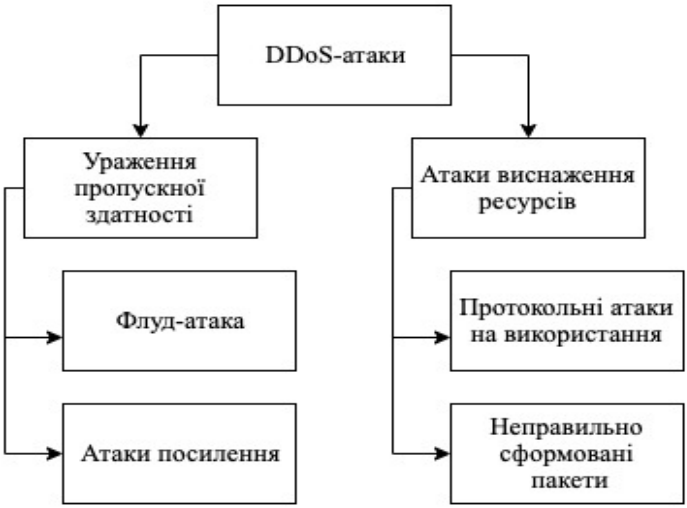

Рис.2. Класифікація DDoS-атак

Флуд атака ICMP складається з таких кроків*:*

1. Зловмисник надсилає велику кількість пінг запитів до системи жертв за допомогою зомбі.

2. Потерпілий надсилає відповіді на отримані запити.

3. Тепер мережа забита трафіком, який надсилає жертва. Відповіді на запити можуть надходити на підроблену IP-адресу, яка зазначається у пакеті ICMP.

Як наслідок, пропускна здатність мережевих підключень швидко вичерпується та не може використовуватись користувачем. Також різновидами атаки ICMP є: фрагментація, DNS флуд та Ping-флуд.

Атака посилення

Зловмисник надсилає велику кількість пакетів на широкомовну IP-адресу. Роутер передає відповіді ці на запити на IP-адресу жертви, що призводить до повного блокування системи. Цей тип атаки використовує широкомовні адреси більшості пристроїв, які мають доступ до інтернету, наприклад роутерів. Цей вид DDoS-атаки може бути запущений безпосередньо зловмисником, або за допомогою зомбі. Найвідомішими атаками цього типу були Smurf та Fraggle.

Атака Smurf складалася з таких кроків:

1. Зловмисник відправляє пакети на мережевий пристрій з широкомовною адресою. Відповідь надсилатиметься або на вигадану адресу, або ж на адресу жертви.

2. Пакети ICMP_ECHO_RESPONSE мережевим підсилювачем надсилаються всім системам широкомовної IP-адреси. Цей пакет передбачає, що приймач відповість ICMP_ECHO_REPLY.

3. Повідомлення ICMP_ECHO_REPLY від усіх систем у діапазоні доходить до жертви.

Атака Fraggle схожа на Smurf, але під час неї UDP надсилаються до портів, що підтримують генерування символів. Вона складається з таких кроків :

1. Зловмисник відправляє пакети UDP на порт, який підтримує генерацію символів. Зворотною адресою в цих пакетах може зазначатись адреса сьомого порта жертви, який генеруватиме символи і таким чином створюватиме нескінченний цикл.

2. Атака орієнтована на порти усіх систем, на які посилається широкомовна адреса.

3. Усі ці системи в діапазоні повторюються назад до порту генератора символів жертви.

4. Цей процес повторюється, оскільки використовуються пакети UDP.

Така атака небезпечніша за Smurf. Її різновидом є рефлекторна атака, яка використовує «відбивачі» (посередницькі хости або пристрої) для виконання завдання. Особливістю відбивача є те, що він постійно реагує на пакети, які надсилає та отримує. Тож зловмисники використовують цей метод для атак, на які потрібні відповіді. Зворотня адреса системі жертви буде підроблена.

Атаки виснаження ресурсів

Атака виснаження ресурсів має на меті вичерпати ресурси системи жертв, щоб унеможливити обслуговування користувачів. Розрізняються наступні типи атак виснаження ресурсів:

Протокольні атаки на використання: мета цих атак – споживання надлишкових ресурсів жертви, використовуючи особливість протоколу, встановленого у системі. Найпоширенішими нападами такого типу є TCP SYN атаки, PUSH + ACK, атака сервера аутентифікації та запитів CGI.

Неправильно сформовані пакети оброблені шкідливою інформацією.

Зловмисник надсилає ці пакети жертві, щоб зламати її систему. Це можна виконати двома способами:

Атака з IP-адресою: пакет складається з однакової IP-адреси джерела та призначення, що створює хаос в операційній системі жертви. Таким чином атака уповільнює та ламає систему.

Атака параметрів IP-пакетів: кожен з IP-пакетів складається з додаткових полів для передачі додаткової інформації. Атака використовує ці поля для формування пакету. Вони заповнюються, встановлюючи всі біти якості обслуговування на один. Тож потерпілий витрачає додатковий час на обробку цього пакету. Ця атака є більш вразливою, коли нападає більше одного "зомбі".

Механізми захисту

Були прийняті різні контрзаходи для запобігання DDoS-атакам. Ініціатором DDOS-атак є зловмисник, який намагається отримати несанкціонований доступ до системи / мережі жертв. Захисні механізми показані на рис. 3.

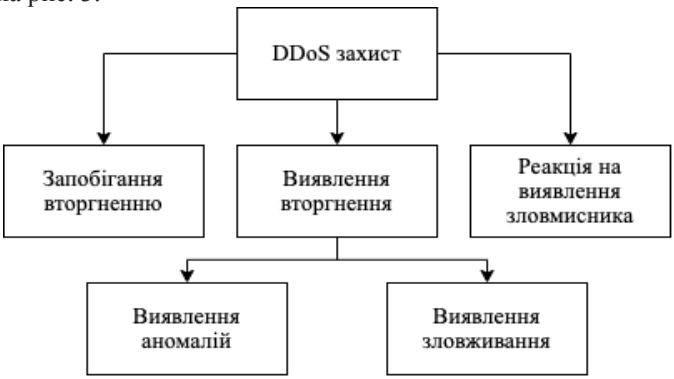

Рис. 3. Механізми захисту від DDoS-атак

Методи профілактики

Найкращою стратегією проти будь-яких атак є запобігання їх виникненню. Однією з таких методик є використання фільтрів:

- *Вхідна фільтрація* – цей процес зупиняє вхідні пакети з неправомірною адресою джерела. Для цього використовуються роутери. Ця методика зупиняє атаки DDoS, викликані підробкою IP-адреси.
- *Вихідна фільтрація* – у цій техніці використовується вихідний фільтр. Ця методика дозволяє пакетам, що мають дійсну IP-адресу в заданому для мережі діапазоні, залишати мережу.
- *Розподіл пакетів на основі маршруту* – фільтр використовує інформацію про маршрут для захоплення або фільтрування підроблених пакетів. Він також використовується, щоб відслідкувати IP-адресу. Але для

цього потрібна глобальна інформація про мережеву топологію.

• *Підвищена безпека з'єднання* – це архітектура з розподіленою функцією, яка передбачає, що вхідний пакет є дійсним, якщо він з законних серверів. Інші пакети блокуються. Клієнт повинен увійти у мережу за допомогою повторного доступу SOAP.

Також можна запобігти атакам за допомогою відключення невикористаних служб, застосування патчів безпеки, зміни IP-адреси, відключення IP-трансляцій, балансування завантаження та пасток. Методи запобігання нападам не гарантують повного захисту від DDoS-атак, але підвищують безпеку.

Методи виявлення

Система виявлення вторгнень допомагає жертві уникнути розповсюдження DDoS-атак та запобігає зупинці системи. Серед таких методів:

• *Виявлення аномалій***:** Цей метод виявляє напади, розпізнаючи аномалії в роботі системи. Це робиться шляхом порівняння поточних значень із раніше виявленими нормальними робочими характеристиками системи. Цей метод визначає помилкові значення в поведінці системи. Найпоширенішими методами виявлення аномалій є:

– NOMAD – система моніторингу мережі, яка виявляє мережеві аномалії шляхом аналізу інформації заголовка IP-пакета.

– *Техніка відбору та фільтрування пакетів із перевантаженістю***.** З підмножини скинутих пакетів було проведено статистичний аналіз, і як тільки виявлено аномалію, на роутер подається сигнал для фільтрації шкідливих пакетів.

– D-WARD – виявляє DDoS-атаку у першої жертви. Це запобігає поширенню нападу на інших користувачів мережі. D-WARD встановлюється на роутері для виявлення вхідного та вихідного мережевого трафіку.

– MULTOPS- MULTOPS – це структура даних, розроблена для виявлення DDoS-атак. Вона виявляє атакуючі або атаковані системи, функціонуючи в режимі, орієнтованому на напад та його жертву відповідно. Це багаторівнева структура, яка визначає швидкість пакетів на різних рівнях агрегації. Але для цього потрібна конфігурація маршрутизатора та додаткові схеми управління пам'яттю.

• *Виявлення зловживань***:** Цей метод виявляє DDoS-атаки, підтримуючи базу даних адрес або шаблонів експлойтів. Коли такий зразок виявлено, система повідомляє про атаки DDoS.

Відповідь на виявлення

У разі виявлення DDoS-атаки її слід заблокувати та визначити особу зловмисника. Це можна зробити, наприклад за допомогою списку управління доступом ACL (Access Control List) або автоматично.

Окремі методи, що використовуються для відстеження та ідентифікації зловмисника, подано у табл. 2. Зауважимо, що існує багато методів для зупинки DDoS-атак, проте не всі напади можна виявити та запобігти, можна лише зменшити вплив нападу.

Таблиця 2

Методи відстеження DDoS-атак

Метод	Опис
Відстеження ICMP	Механізм стосується переадресації пакетів з низькою ймовірністю до кожного маршрутизатора, а також відправки повідомлення про зворотний зв'язок ICMP до місця призначення. Якщо основна кількість повідомлень ICMP, які використовуються для ідентифікації нападника, стикається з такими проблемами як додатковий трафік, перевірка цих пакетів і виявлення накладних даних інформації з карти маршрутів є складним.
IP-відслідковування	Цей метод відстежує шлях зловмисника, щоб знайти походження атаки. У цій техніці шлях нападника прослідковується назад, щоб знайти своє джерело. Але це стає важким завданням, якщо звітність джерел у протоколі TCP / IP відключена.
Послідовність зворотного тестування зв'язків	Цей механізм перевіряє кожне з вхідних посилань, щоб визначити чи не є воно атакою. Для цього створюється великий потік трафіку та відслідковується наявність порушень у мережі. Щоб застосувати цей механізм, потрібна система, яка зможе генерувати великий потік трафіку, а також інформація про розташування та спосіб з'єднання комп'ютерів мережі.
Імовірнісне маркування пакетів	Ця методика долає недоліки тестування зворотних зв'язків, оскільки вона не вимагає попередніх знань про топологію мережі, розміру трафіку тощо. Ця перевага також накладає додаткові витрати на системи, але існує багато методів, щоб уникнути додаткових витрат.

Особливості DDoS-атак у хмарному середовищі

DDoS – одна з загроз безпеки, яка кидає виклик доступності хмарним обчисленням. З багатьох атак у хмарному середовищі за даними Cloud Security Alliance, 14% – це DDoS-атаки. У березні 2009 року VeriSign уклала контракт з Forrester Consulting для проведення дослідження щодо загроз та захисту від DDoS-атак. Опитування проводилось серед 400 респондентів із США та Європи. 74% зазнали однієї або декількох DDoS-атак у своїх

організаціях. Із них 31% напади спричинили зрив служби, але 43% – не призводять до зриву послуг (рис. 4). Опитування говорить про те, що при збільшенні використання хмарного середовища швидкість DDoS-атак також швидко зростає. У хмарному середовищі, коли навантаження на послугу росте, вона почне надавати додаткову обчислювальну потужність, щоб протистояти додатковому навантаженню. Це означає, що хмарна система працює проти зловмисника, але певною мірою підтримує зловмисника, дозволяючи йому наносити найбільш можливий збиток за доступністю сервісу, починаючи з єдиної точки входу атаки.

Рис. 4. Розподіл статистики DDoS-атак в організаціях

Хмарний сервіс складається з інших послуг, що надаються на тих же апаратних серверах, які можуть зазнати навантаження, спричиненого флудом. Таким чином, якщо служба намагається запустити на одному сервері з іншою навантаженою службою, це може вплинути на її власну доступність. Ще одним ефектом від повені є різке підвищення рахунків за користування хмарою. Проблема полягає в тому, що не існує «верхньої межі» для використання і однією з потенційних атак на хмарне середовище є атаки сусідів, тобто віртуальна машина може атакувати свого сусіда в тій же фізичній інфраструктурі і тим самим заважати йому надавати свої послуги. Ці атаки можуть вплинути на продуктивність та можуть призвести до фінансових втрат і спричинити шкідливий вплив на інших серверах у тій самій хмарній інфраструктурі.

Фактори вибору рішень захисту хмарного середовища

Рішення для запобігання DDoS-атак має бути:

• *Функціональне*: рішення повинно бути достатньо функціональним, а це означає, що воно повинне бути здатним зменшити вплив атаки незалежно від того, наскільки потужною є атака.

• *Прозоре*: рішення має бути простим у здійсненні, тобто не повинно вимагати змін існуючої мережі та її інфраструктури.

• *Легке*: рішення не повинно перекривати систему.

• *Точне*. Вибране рішення не повинно видавати помилкові результати. Ряд методів вимагають зменшення трафіку, але рішення для захисту від DDoS-атак не має впливати на трафік.

Висновок

Оскільки кількість DDoS-атак у хмарних сервісах зростає, подано короткий опис DDoS-атак, таксономію атак, їх види та заходи протидії пом'якшенню впливу. Описані методи виявлення і запобігання атак, визначені принципу вибору рішень для захисту.

1. Denial of Service Attack, http://en.wikipedia.org/wiki/Denial-of-serviceattack
2. DDoS attack tool time line, http://staff.washington.edu/dittrich/talks/sec2000/timeline.html
3. History of DDoS, http://www.timetoast.com/timelines/history-of-ddos
4. DoS and DdoS Evolution, http://users.atw.hu/denialofservice/ch03lev1sec3.html
5. CERT Coordination Center, Over view of attack trends, Feb.2002. http://www.cert.org/archive/pdf/attacktrends.pdf.

http://doi.org/10.5281/zenodo.3860778

Поступила 3.10.2019р.

УДК 009.4

Б.М. Гавриш [1], к.т.н., доцент
Б.В. Дурняк [1], д.т.н., професор
О.Б. Полусин [1], аспірант
О.Є. Семенова [2], асистент

ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Abstract. Methods of protection by encryption, implementation of authentication system and use of electronic signature algorithms are considered and compared. The structural division of encryption algorithms is given.

[1], Українська академія друкарства, Львів

[2] Національний університет «Львівська політехніка»