УДК 004. 056
DOI: 10.31673/2409-7292.2021.013540

Бородань В.В., Гай Д.О.

ВИБІР ДОЦІЛЬНОЇ АРХІТЕКТУРИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД БАГАТОРІВНЕВИХ DDOS АТАК

В роботі досліджено багаторівневі DDoS-атаки, які являються різновидом атаки відмови в обслуговуванні (DoS), метою яких є заборона мережевих служб шляхом збою цільових серверів або споживання їх ресурсів, так що ці сервери більше не можуть надавати послуги законним користувачам. Виокремлено, що DDoS-атаки розділені на декілька класів, які включають: атаку грубої сили Telnet, SYN flood атаки, ICMP flood атаки, атака Smurf, Ping flood, атаку запиту HTTP Get Flooding та HTTP Post. Зроблено висновок, що для того, щоб створити ефективну архітектуру захисту інформації і, разом з цим, ефективні заходи для боротьби з DDoS-атаками, важливо розуміти різні методи DDoS. Представлено архітектуру захисту інформаційної системи від багаторівневих DDoS-атак, заснованої на SDN та аналізі кореляції трафіку в мережі. Розроблено рекомендації щодо захисту інформаційної системи від багаторівневих DDoS-атак. Зазначено, що окрім технічних заходів, організації також необхідно впровадити процедурні заходи на рівні захисту, виявлення та реагування.

Ключові слова: атака, DDOS, інформаційна безпека, SYN, Flood, модель OSI, багаторівневі атаки.

Вступ

Атаки високої та низької інтенсивності – це дві поширені розподілені атаки відмови в обслуговуванні (DDoS), які порушують працездатність обладнання та атакують користувачів в мережі Інтернет. Виявлення цих атак є важливим та невід'ємним кроком для забезпечення безперебійної роботи IT систему, ділових операцій та навчальних закладів. Раніше було розроблено декілька систем виявлення DDoS-атак, але вони все ще не мають достатньої продуктивності, масштабованості та можливості обміну інформацією для точного та раннього виявлення DDoS-атак високої та низької інтенсивності [1].

Багаторівневі DDoS атаки можуть бути реалізовані на цих трьох площинах архітектури SDN. Виходячи з можливих цілей, багаторівневі DDoS-атаки поділяються на три категорії: DDoS-атаки на рівні додатків, DDoS-атаки на рівні управління та DDoS-атаки на рівні даних. Для протидії таким атакам необхідно побудувати відмовостійку архітектуру системи виявлення DDoS атак у великомасштабних мережах. Вона призначена для виявлення як високих, так і низькоінтенсивних DDoS-атак на ранній стадії [2].

Аналіз найбільш критичних DDoS-атак, направлених на інформаційні системи

За останні декілька років розмір DDoS-атак експоненційно збільшується. Найбільше великих DDoS-атак в 2020-м сталося в кінці року. Зокрема, різко зросла їх кількість зі швидкістю понад 500 Мбіт/с. Крім того, число атак на основі протоколів збільшилася в 3-10 разів у порівнянні з попереднім кварталом. Зловмисники також були більш наполегливі, ніж будь-коли - майже 9% всіх атак, які спостерігалися з жовтня по грудень, тривали понад 24 годин. Відразу необхідно підкреслити, що у четвертому кварталі вперше в 2020 році загальна кількість DDoS-атак на мережевому рівні зменшилася в порівнянні з попереднім кварталом. В 4 кварталі було зафіксовано 15% всіх атак року. Зростання числа великих DDoS-атак – це тривожна тенденція, яка вказує на те, що хакери стають все більш нахабними і використовують інструменти, які дозволяють їм проводити більші нападу. Що ще гірше, такі атаки мають наслідки не тільки для мережі, а й для постачальників послуг [3].

Існують різні способи вимірювання масштабу DDoS. Перший – це обсяг трафіку, що передається або його «бітрейт» (вимірюваний в гігабіта в секунду). Інший – це кількість або швидкість передачі пакетів (вимірюється в пакетах в секунду). Атаки з високою швидкістю передачі даних намагаються перевантажити мережеві канали «останньої милі», а атаки з високою швидкістю передачі пакетів намагаються перевантажити маршрутизатори або інші апаратні пристрої.

DDoS на основі протоколу TCP (такі як SYN і RST-флуд) залишається популярним, а атаки за допомогою NetBIOS і ISAKMP переживають вибухове зростання в порівнянні з попереднім кварталом. NetBIOS – протокол, який дозволяє додаткам на окремих машинах

спілкуватися і отримувати доступ до загальних ресурсів по локальній мережі, а ISAKMP - це протокол, який використовується для налаштувань політик безпеки і криптографічних ключів при налаштуванні IPsec VPN. Структура і організація DDoS-атак стає все складніше, а значить, надійний захист від них стає необхідністю для компаній [4].

Дослідження реалізації та виявлення багаторівневої DDoS-атаки на прикладі мережі SDN

SDN – це мережева архітектура, яка може бути цілью для реалізації багаторівневих DDoS-атак. Через те, що мережа SDN класифікується на три основні функціональні площини: площину програми, площину управління та інформаційну площину (рис. 1) [5].

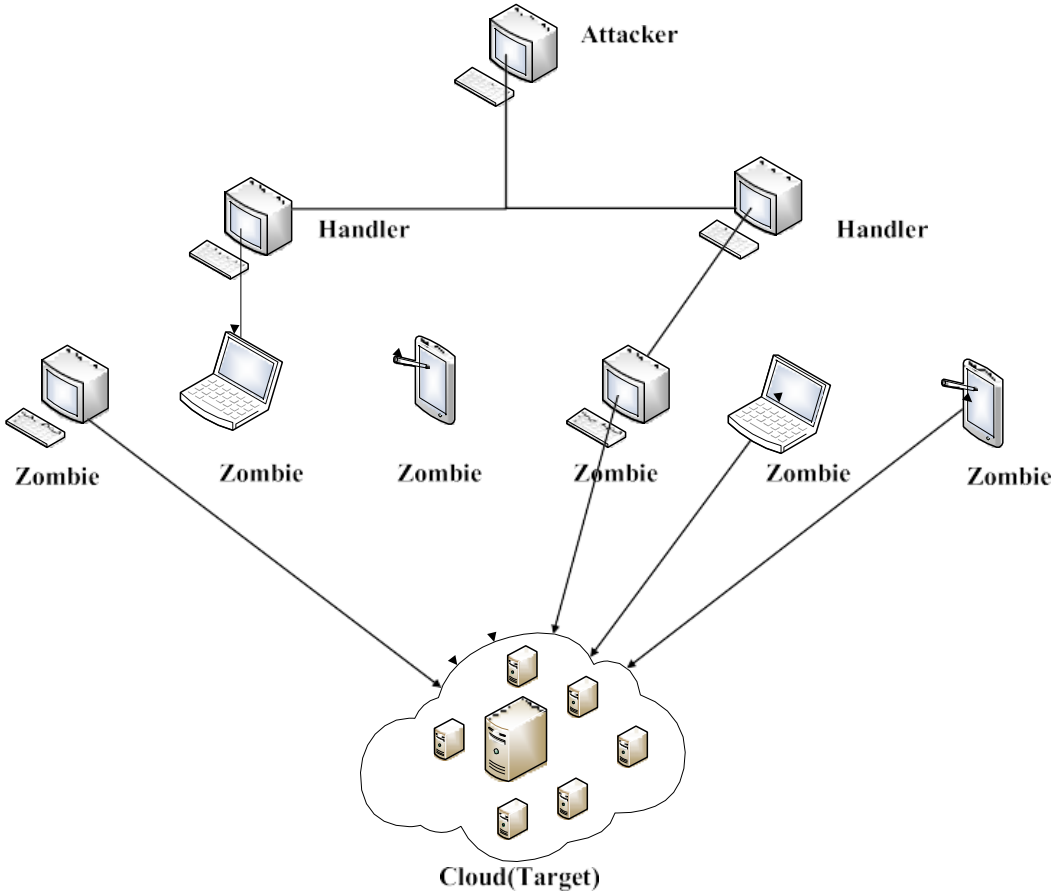

Рис. 1. Приклад багаторівневої DDoS-атаки в хмарний системі

Багаторівневі DDoS атаки можуть бути реалізовані на цих трьох площинах архітектури SDN. Виходячи з можливих цілей, багаторівневі DDoS-атаки поділяються на три категорії: DDoS-атаки на рівні додатків, DDoS-атаки на рівні управління та DDoS-атаки на рівні даних (рис. 2)

Реалізація багаторівневої DDoS-атаки прикладного рівня. Існує два різні способи реалізації DDoS-атак прикладного рівня. Один з них – атаки, зосереджені на деяких додатках SDN; інший - атака, орієнтована на SDN-API. Оскільки розділення програм важко визнати, DDoS-атака на прикладному рівні може вплинути на іншу програму, яка не є ціллю. Такі компрометовані програми можуть спричинити справжні порушення безпеки SDN. Раніше було запропоновано стратегію самоорганізованої карти (SOM) для розрізнення атак на основі DDoS із використанням методів машинного навчання.

У цій стратегії модель SOM навчається шляхом збору фактичної інформації від комутаторів OpenFlow. Особливості навчання SOM - це середні пакети на потік, нормальні байти на потік, середня тривалість на потік, відсоток двонаправлених потоків, ріст одиночного потоку та ріст одиночних портів. Реалізація багаторівневої DDoS-атаки рівня

управління. Рівень управління є центром SDN і, крім того, найслабшим з'єднанням у всій безпеці SDN через одну точку відмови. DDoS-атаки площини управління можуть контролюватися стратегіями, які атакують контролер та API.

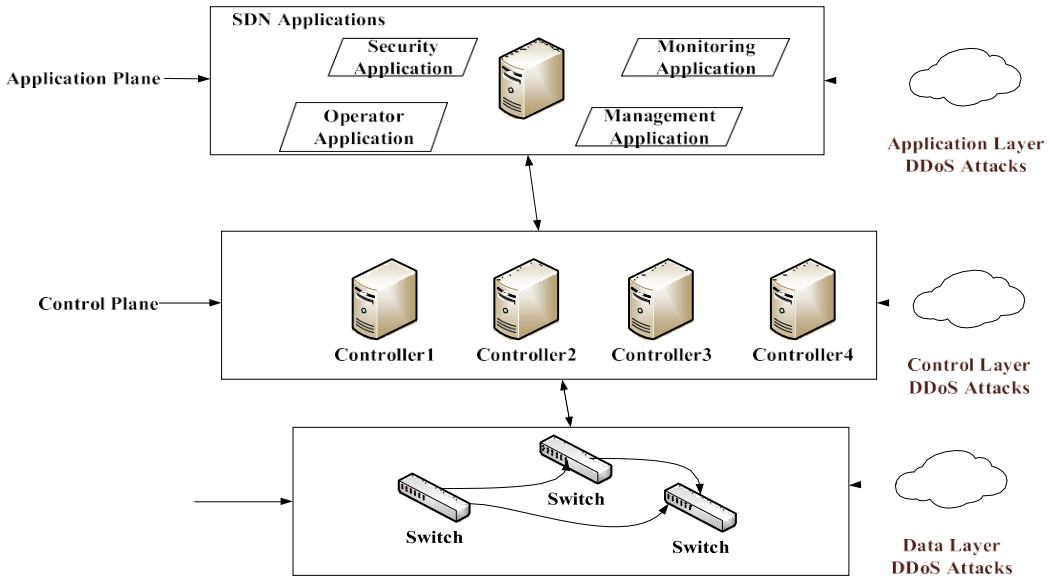

Рис. 2. Приклад багаторівневої DDoS-атаки в SDN

Відмінні програми можуть створювати безліч правил конфлікту, що може спричинити DDoS-атаки на рівні управління. Оскільки контролер приймає рішення про переадресацію потоків відповідно до правил потоку, коли мережевий пристрій знаходить новий мережевий пакет у площині даних, і немає правил потоку, які відповідають існуючій інформації про потоки в таблиці потоків для нових пакетів. Або повний пакет, або частина заголовка пакета надсилається контролеру, щоб вирішити запит. При величезному обсязі мережевого трафіку надсилання загального пакета на контролер може витратити пропускну здатність високих даних. Для цього можна запропонувати використовувати централізоване управління SDN для виявлення DDoS-атак [6].

Реалізація багаторівневої DDoS-атаки канального рівня. Площина даних не повинна бути дозволена будь-яким згубним програмам, які можуть встановлювати, змінювати або коригувати правила потоку, оскільки атака DDoS запускається, коли атакуються маршрутизатори, і атакується API. Дослідники, запропонували, щоб продемонструвати правдоподібність DDoS-атак, SDN влаштовують перевірку моделі пристрою для віддалених мереж. З цією стратегією можна легко працювати, модифікуючи існуючі інструменти перевірки мережі (наприклад, перевірка ICMP та фільтрація TCP SYN). Атака може вестися в мережі SDN віддаленим зловмисником, і це може суттєво зіпсувати виконання механізму SDN, не вимагаючи пристроїв вищої або великої ємності.

Напад багаторівневої DDoS-атаки зазвичай складається з чотирьох кроків. Першим кроком є те, що зловмисник DDoS пише вірус, який надсилатиме пакети пінгу до цільової мережі або веб-сайту. Другий крок – заразити якомога більше систем і перетворити їх на так званих «зомбі». Третій крок – розпочати атаку, пробудивши зомбі-системи, і останній крок полягає в тому, що зомбі-системи атакуватимуть цільовий веб-сайт або мережу до їх дезінфекції.

Базові принципи проектування відмовостійкої архітектури захисту інформаційної системи

Масштабованість при обробці трафіку різного розміру. SCAFE повинен бути масштабованим, щоб обробляти мережі з великою кількістю потоків трафіку та мережевих

зв'язків. Масштабованість SCAFE вимірюється з точки зору часу обробки та складності повідомлення.

Модульність компонентів архітектури системи. Компоненти SCAFE повинні бути модульними в тому сенсі, що кожен компонент в системі виявлення є окремим будівельним блоком системи виявлення з певною функціональністю. Це означає, що кожен із компонентів розроблений з чітко визначеним інтерфейсом і може бути замінений або модернізований при необхідності. Кожен компонент створюється окремо і має окремий функціонал. Наприклад, колектор використовується для збору статистики трафіку, монітор - для моніторингу трафіку, корелятор - для кореляційного аналізу, а база даних - для зберігання статистичної інформації, отриманої від колекторів.

Допуск до несправності та доступність. SCAFE повинен бути стійким до несправностей з високою готовністю, щоб забезпечити постійну функціональність системи виявлення та уникнути єдиної точки відмови. Це означає, що SCAFE повинен бути спроектований таким чином, щоб він міг обробляти як програмні, так і апаратні несправності, такі як збій сервера, збій диска або збій мережі при обробці великих потоків трафіку та мережевих зв'язків. Кожен із компонентів у SCAFE потрібно буде активно тиражувати, щоб забезпечити безперебійну роботу SCAFE та відмовостійкий спосіб.

Топологія мережі

При оцінці використовується проста топологія мережі, яка показана на рис. 3. Мережа складається з шести підмереж, які представляють різні місця розташування мережі. Ці підмережі взаємопов’язані мережею основних комутаторів (E1, E2 та E3) з можливостями маршрутизації. Комутатори в мережі підключені до контролера SDN для збору та моніторингу трафіку. Кожен контролер (C1, C2 та C3) підключений до сервера NFV (MonDB1, MonDB2 та MonDB3), де розташована локальна база даних та локальний механізм моніторингу. Оскільки SCAFE використовує технологію SDN, існує два типи комунікаційних шляхів:

користувацький трафік (лінії передачі даних)

комунікаційний трафік SCAFE (контрольні лінії зв'язку).

Кожен вузол у мережі - це віртуальна машина з встановленою Ubuntu 16.04.1 LTS. Роль кожного компонента в топології мережі описана в табл. 1 [7].

Конфігурації та функціональні можливості вузлів у мережі такі:

1) Локальний та основний комутатори SDN – ці комутатори налаштовані як віртуальні комутатори (Open vSwitch) за протоколом OpenFlow 1.3 і використовуються для переадресації трафіку до відповідного пункту призначення за допомогою таблиць потоків. У кожному комутаторі порт, який приєднаний до виробничого каналу в мережі, налаштований як інтерфейс OpenFlow vSwitch. Тим часом порт, який підключений до каналу зв'язку системи виявлення DDoS, налаштований як звичайний порт зі статичними маршрутами до компонентів системи виявлення DDoS. Усі порти OpenFlow vSwitch налаштовані на підключення до контролера у своїй локальній підмережі. Для простоти перемикачі S1, S2 і S3 підключені до контролера C1, S4 і S5 підключені до C2, а S8 – до C3.

2) Контролер SDN – контролер використовується для управління потоками трафіку в мережі. SDN перемикає вперед невідомі пакети на контролер, і контролер вирішить, куди переслати пакет, та оновить таблиці потоків комутаторів. Контролер також використовується для збору статистики трафіку. Для кожного вузла контролера існують два типи контролерів SDN: POX і FAUCET. POX використовується для управління потоками трафіку та оновлення таблиць потоків у комутаторах, тоді як FAUCET використовується для збору статистики трафіку з використанням його API вимірювального приладу. Кожен комутатор буде підключатися до обох контролерів у вузлі контролера.

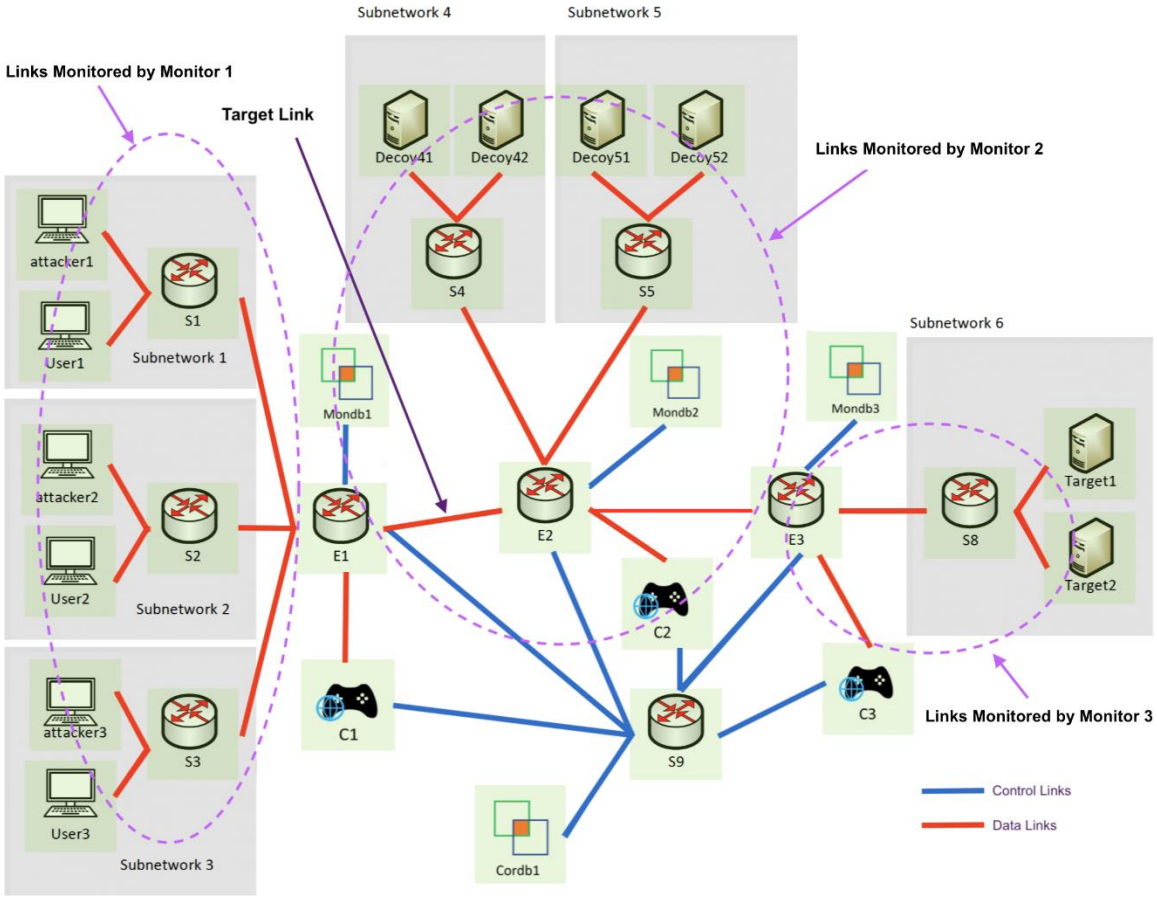

Рис. 3. Налаштування емуляції тестового стенду GENI

Таблиця 1.

Призначення ролей

№	Ролі	Вузли
1	Локальний комутатор SDN	S1, S2, S3, S4, S5, S8, S9
2	Основний комутатор SDN	E1, E2, and E3
3	Контролер SDN	C1, C2, and C3
4	Легітимний хост	User1, User2, and User3
5	Шкідливий хост	Attacker1, Attacker2 and Attacker3
6	Приманковий сервер	Decoy1, Decoy2, and Decoy3
7	Монітор та локальна база даних	MonDb1, MonDb2, and MonDb3
8	Корелятор та глобальна база даних	CorDb1
9	Цільовий господар	Target1, Target 2

3) Легітимний хост – законний хост використовується для надсилання звичайного трафіку (трафік TCP та HTTP) до цільових вузлів у мережі.

4) Зловмисний хост – зловмисний хост діє як зловмисник в мережі. Зловмисник надсилає трафік DDoS-атаки (TCP і HTTP) до своєї цілі в мережі. Ціль може бути або серверами-мановаками (непрямі DDoS-атаки), або цільовими серверами (прямі DDoS-атаки). D-ITG встановлений для генерування трафіку DDoS-атак.

5) Приманковий сервер – приманковий сервер діє як приманка для непрямих нападів. Приманка встановлюється як сервер HTTP Apache для отримання HTTP-запитів у мережі.

6) Монітор та локальна база даних – монітор та локальна база даних - це два компоненти системи виявлення DDoS. Обидва ці компоненти для простоти встановлені в одному вузлі. Вузол діє як сервер NFV, де для моніторингу встановлений сценарій

моніторингу, а для зберігання статистики трафіку - база даних InfluxDB. З нашого дизайну кожна підмережа матиме монітор та локальний вузол бази даних. Щоб подолати обмеження ресурсів, до одного монітора та вузла локальної бази даних підключено кілька підмереж. Однак кожна підмережа матиме у вузлі компонент монітора та локальну базу даних.

7) Корелятор та глобальна база даних – як і монітор та локальна база даних, корелятор та глобальна база даних встановлюються в одному вузлі на сервері NFV. Однак корелятор і глобальна база даних є централізованим компонентом, де всі підмережі підключені до них. Вузол містить скрипт кореляції для загальномережного аналізу кореляції, а база даних InfluxDB встановлена для зберігання статистичних даних про потоки [8].

Для того, щоб створити ефективну структуру та, як частину цієї основи, ефективні заходи для боротьби з DDoS-атакою, також важливо розуміти різні методи DDoS. В даний час зловмисники використовують широкий спектр DDoS-атак. Ці DDoS-атаки можна розділити на три типи, які відбуваються на рівнях 3, 4 та 7 моделі рівня OSI. Для ефективної боротьби з DDoS-атаками ключовим для організації є здійснення технічних заходів, які не тільки запобігають або мінімізують ризики на одному з цих шарів, але й запобігають або мінімізують ризики на рівнях 3, 4 та 7. Ось чому система контролю безпеки DDoS охоплює ці три шари.

Окрім технічних заходів, організації також необхідно впровадити процедурні заходи на рівні захисту, виявлення та реагування. Метою цих процедурних заходів є ініціювання дій та підвищення обізнаності. Поєднання обох типів заходів є ключовим для створення ефективного функціонуючого середовища зменшення наслідків DDoS.

Висновки

Представлено архітектуру захисту інформаційної системи від багаторівневих DDoS-атак, заснованої на SDN та аналізі кореляції трафіку в мережі. Дана архітектура має на меті покращити масштабованість шляхом звуження обсягу трафіку, необхідного для аналізу, щоб розрізнити атакуючий та звичайний транспортні потоки. Розроблено рекомендації щодо захисту інформаційної системи від багаторівневих DDoS-атак. Зазначено, що окрім технічних заходів, організації також необхідно впровадити процедурні заходи на рівні захисту, виявлення та реагування. Метою цих процедурних заходів є ініціювання дій та підвищення обізнаності. Поєднання обох типів заходів є ключовим для створення ефективного функціонуючого середовища зменшення наслідків DDoS.

Перелік посилань

1. Shui Yu. An Overview of DDoS Attacks. In Distributed Denial of Service Attack and Defense, pages 1–14. Springer, 2014.
2. Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Analysis of DDoS-Capable IoT Malwares. In Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), pages 807–816. IEEE, 2017.
3. Обзор киберугроз 2020. https://techexpert.ua/ru/cybersecurity-covid/
4. Какими были DDoS-атаки сетевого уровня в 4-м квартале 2020-го. https://vasexperts.ru/blog/bezopasnost/ddos-ataki-2020-go/
5. Mahjabin, Tasnuva & Xiao, Yang & Sun, Guang & Jiang, Wangdong. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. 13. 155014771774146. 10.1177/1550147717741463.
6. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and Ren Ping Liu. A System for Denial-of-Service Attack Detection based on Multivariate Correlation Analysis. IEEE Transactions on Parallel and Distributed Systems, 25(2):447–456, 2014.
7. Ying-Dar Lin, Po-Ching Lin, Chih-Hung Yeh, Yao-Chun Wang, and Yuan-Cheng Lai. An Extended SDN Architecture for Network Func- tion Virtualization with a Case Study on Intrusion Prevention. IEEE Network, 29(3):48–53, 2015.
1. Bing Wang, Yao Zheng, Wenjing Lou, and Y Thomas Hou. DDoS Attack Protection in the Era of Cloud Computing and Software- Defined Networking. Computer Networks, 81:308–319, 2015.

Надійшла: 13.02.2021 Рецензент: д.т.н., професор Вишнівський В.В.