DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-13
УДК 004:338.48
Соняк Софія Олександрівна, студентка
https://orcid.org/0000-0002-3665-3359.
Київський національний університет імені Тараса Шевченка

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК ЗА ДОПОМОГОЮ ЕНТРОПІЇ

Соняк С. О. Виявлення мережевих атак за допомогою Ентропії. Проблема розподіленого відмови в обслуговуванні (DDoS) - це поширена проблема сьогодні. Існує безліч способів виявлення цього типу атак. В статті розглядається метод Ентропії.
Ключові слова: мережеві атаки, DDoS-атаки, ентропія, канали передачі даних, мережевий, кібератаки.

Soniak S.O. Detection of network attacks using Entropy. The problem of distributed denial of service (DDoS) is a common problem today. There are many ways to detect this type of attack. The entropy method is considered in the article.
Keywords: network attacks, DDoS-attacks, entropy, data transmission channels, network, cyberattack.

Соняк С. А. Выявление сетевых атак с помощью Энтропии. Проблема распределенного отказа в обслуживании (DDoS) - это распространенная проблема сегодня. Существует множество способов выявления этого типа атак. В статье рассматривается метод Энтропии.
Ключевые слова: сетевые атаки, DDoS-атаки, энтропия, каналы передачи данных, сетевой, кибератаки.

Постановка проблеми. Глобальна мережа передачі даних Інтернет зайняла міцне місце в сучасному житті. Без цього засобу зв'язку неможливо уявити собі сучасні телекомунікації. Такі засоби, що здавалися екзотикою ще кілька років тому, як відеоконференції, обмін миттєвими повідомленнями, відносно дешевші способи міжміського і міжнародного голосового зв'язку, остаточно увійшли в повсякденне життя. Слід зазначити все більшу конвергенцію мереж: уже зараз багато національних і транснаціональних операторів зв'язку здійснюють передачу міжнародного трафіку через канали глобальної мережі. Мережі з комутацією пакетів поступово витісняють мережі з комутацією каналів, а найбільшою такою мережею і є Інтернет (або просто Мережа).

В основу мережі Інтернет при розробці були покладені принципи децентралізації та самокерованості. Це пов'язано з тим, що мережа розроблялася військовим відомством США як засіб зв'язку на випадок ядерної війни. Однак, аналітики не припускали широкого розповсюдження мережі.

На даний момент все частіше стали виявлятися негативні аспекти такого підходу. Одна з проблем, пов'язаних з таким підходом і розглядається в цій роботі.

Аналіз останніх досліджень і публікацій. В сучасному світі дуже часто зустрічається проблема кібератак, а питання протидії їм є надзвичайно важливим. Особливо протягом останніх років спостерігається збільшення їх кількості, особливе місце серед яких займають саме DoS / DDoS атаки [1, 2, 3, 4]. У роботі О. Купреева [5] відображена статистика, яка показує щорічне збільшення кібератак саме в вересні, коли перевага для атак надається освітній галузі. Яскравим прикладом є DDoS-атака у вересні 2018 року на сайт Единбурзького університету. Так, все частіше для здійснення кібератак використовуються домашні пристрої, зокрема, роутери, веб-камери, принтери та інші IoT пристрої [6]. Найкращим способом боротьби із кібератаками поки що залишається лише їх вчасне виявлення за допомогою різних методів.

Невирішені частини проблеми. Проблема виявлення та захисту від DoS / DDoS атак розглядалась у роботах багатьох вчених, зокрема, О. Смоктюк, Н. Багнюк [7, 8, 9]. На даний момент практично всі виробники мережевого устаткування шукають шляхи вирішення проблем пов'язаних з DDoS атаками та їх відмінністю від простого перевантаження мережі. Це зумовило значне збільшення кількості публікацій на цю тему. Зокрема, у роботі Олени Мірковік та Пігера Райхера [13], висвітлюють повний спектр проблем організацій, пов'язаних із кібератаками. У цій роботі пропонується один з можливих методів, що підвищують ймовірність виявлення такої атаки. Основною проблемою є те, що неможливо передбачити кібератаки, а способи їх реалізації досить різноманітні, що значно уповільнює процес їх виявлення. До того ж, єдиний спосіб швидкого відновлення роботи системи після кібератаки – вчасне виявлення. Одна досі немає методу, який точно би відрізним причину зміни кількості запитів, тобто, чи вона була зумовлена хакерською атакою, чи звичайним збільшенням активності користувачів.

Метою дослідження є вивчення методу виявлення аномалій мережевого трафіку на основі інформації про впорядкованості трафіку в каналі передачі даних для виявлення DoS / DDoS атак.

Основні результати дослідження. Атаки типу «відмова в обслуговуванні» (DoS) на пряму впливають на доступ до інформаційних ресурсів. DoS атака вважається успішною за умови, що вона

спонукала до недоступності інформаційного ресурсу. Звісно, вплив від таких атак може бути різним, зокрема, створити загрозу потенційного нанесення фінансових збитків, або ж безпосередньо заподіяти шкоду. Так, напрклад, при атаці інтернет-магазину, така атака може принести величезні фінансові збитки.

У випадку із DDoS атаками, основне завдання зловмисників полягає у тому, щоб зробити із різних місця максимальну кількість запитів. Для цього навіть створюються спеціальні автоматичні бот-мережі, щоб зробити масштабнішою DDoS атаку.

Щодня у світі трапляється безліч кібератак, які різняться за своїм масштабом. Для відстеження цього процесу було створено спеціальний ресурс [12], який зберігає DDoS атаки до архіву, де в режиму інтерактивної карти можна переглянути кожну із атак (див. рис. 1).

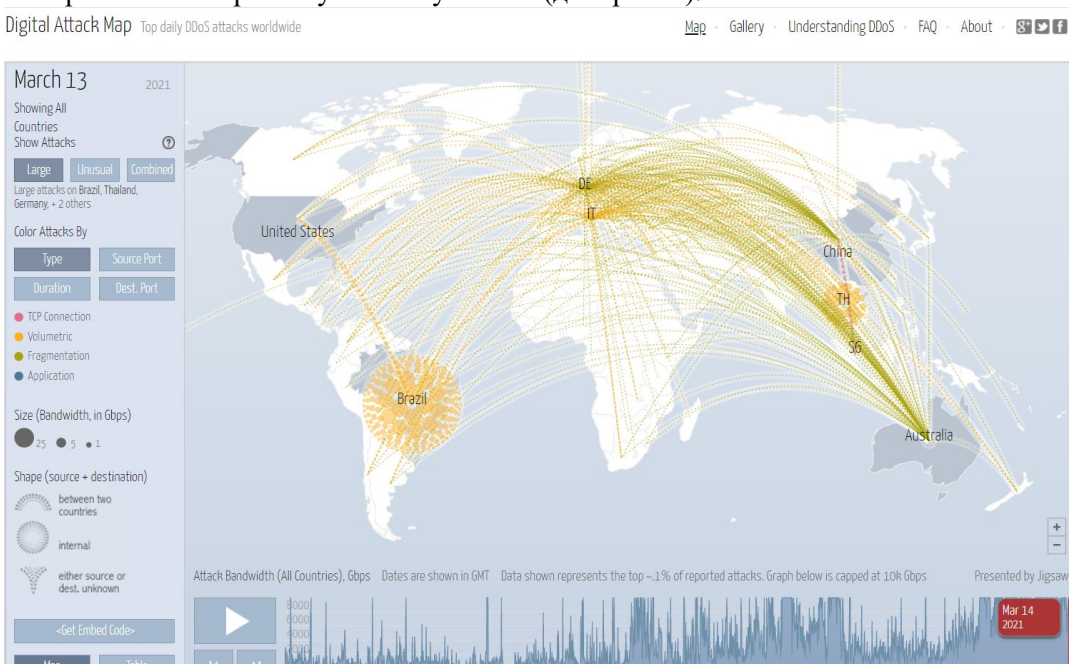

Рис. 1. Цифрова онлайн карта DDoS атак

Цікаво, що на карті чітко видно зростання кібератак із початком вимушених карантинних обмежень на початку березня 2020 року у зв'язку із розвитком коронавірусної хвороби. Скоріше за все це пов'язане із тим, що населення в цілому світі було змушене перейти до онлайн покупок, що зумовило значне збільшення запитів на різноманітних ресурсах.

Карта дозволяє не тільки оцінювати масштаб атак, але й визначати її «напрямок», а також їх типи за різними показниками. Окрім того, можна розглянути й окремі країни (див. рис. 2) для визначення статистичних даних для кожної з них.

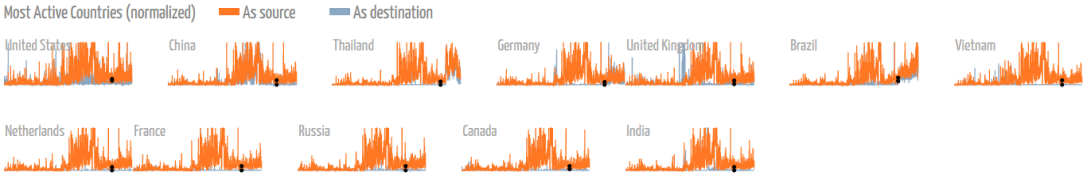

Рис. 2. Цифрова онлайн карта для визначення статистичної інформації для різних країн

Тож, об'єктом дослідження у статті стали виникаючі аномалії трафіку в мережі інтернет. Саме до них і відносяться різке зростання активності користувачів, або ж навмисне атакування якогось із ресурсів.

DoS (DoS - Denial of Service) атака – це тип атаки, який іншими словами називається атакою на відмову в обслуговуванні, завданням якої є напад на комп'ютерну систему, метою якого є бажання зробити недоступними інформаційні ресурси для користувача. Це досягається шляхом зміни структури трафіку так, щоб зійняти усі можливі системні ресурси, які обслуговують справжніх користувачів.

У цій статті розглядається DDoS (DDoS - Distributed Denial of Service) атаки. Це хакерська атака на інформаційну систему з метою довести її до відмови в обслуговуванні користувачів, тобто іншими словами – створити такі умови, за яких доступ до інформаційних ресурсів та в обслуговуванні

користувачів буде обмеженим (частково, або повністю). Варіант такої атаки ґрунтується на принципі, який отримав назву «розподіленої атаки типу відмова в обслуговуванні».

Під час DDoS атаки велика кількість хостів-агентів, або ж хостів-зомбі штучно створюються трафік в мережі, який націлений на хости-жертви (див. рис. 3). При нерівноцінності ресурсів хоста-жертви тв кількості штучних запитів, тобто якщо ресурси, необхідні для обробки згенерованого обсягу трафіку перевищують ресурси хоста-жертви, відбувається відмова в роботі жертви, що і є метою атаки. Така атака може бути спричиненою як звичайними користувачами, так і зловмисниками, які хотіли нанести збитки тій чи іншій інформаційній системі.

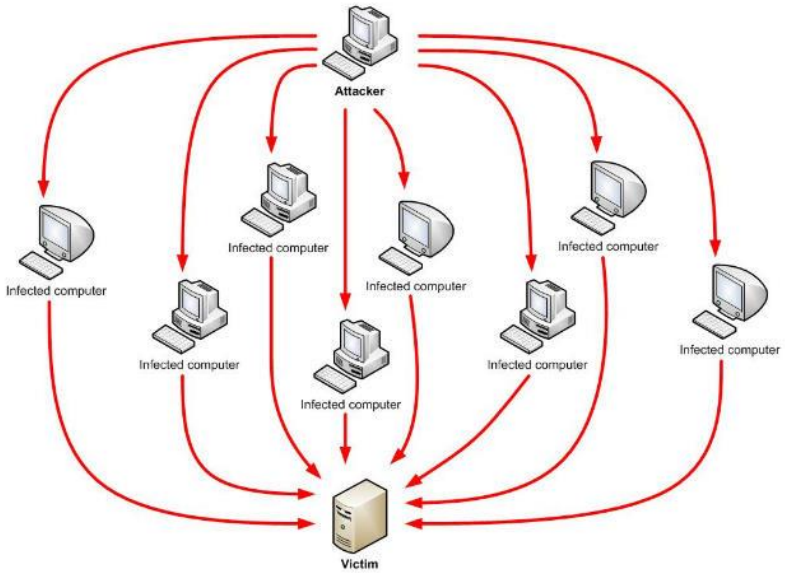

Рис. 3. Схема DDoS-атаки [10]

Основними завданнями дослідження, проведеного для статті, є: ідентифікація DDoS; визначення ознак, які характерні для потоків DDoS атак; ідентифікація потоків трафіку, що викликають перевантаження хостів-жертв, на які націлена атака.

Для розв'язання завдань, поданих вище, можна використовувати загальне визначення ентропії заголовків мережевих пакетів, для визначення критичного степеню трафіку в каналі передачі даних, утвореному штучно, або «природньо». При погіршенні стану в каналі передачі даних, тобто при виявленні аномалії в мережі, необхідно виконувати виділення пакетів, а також додавати нові фільтри для них.

Кожна мереж має різний степінь популярності. Під терміном «популярність» будемо приймати не тільки частотність звернень до інформаційної системи, а й частотність відповідей системних ресурсів на запити користувача.

Кожна система володіє деякою статичною популярністю, тобто при нормальній роботі трафіку, рівень його завантаженості буде постійно практично однаковим. Основною причиною цього є те, що у більшості користувачів сформовані деякі вподобання, відносно WEB- ресурсів, серед яких і системи з розважальним контентом, сайтами новин, електронна пошта, тощо. Таким чином при нехарактерному для каналу передачі даних інформаційної системи збільшенню запитів, виникають проблеми із звичним (нормальним) навантаженням трафіку.

Проти, не обов'язково збільшення трафіку це наслідок DDoS атаки, це також може бути зумовлено іншими причинами. Наприклад, в інтернет-магазині такими можна назвати розширення товарного асортименту, поява сезонних акцій, або ж зміною конфігурації мережевих сервісів та ін. Це може спричинити підвищення інтересу користувачів до того чи іншого ресурсу.

Число пакетів в потоці є значущим значенням для відображення витрачених ресурсів маршрутизатора для обробки потоку даних. Тут прослідковується прямий зв'язок, адже чим більше значення числа пакетів, тим більша ймовірність того, що відбудеться відмова в роботі маршрутизатора.

Описані вище показники можуть дати дані на основі яких, будується загальний опис трафіку мережі в каналі передачі даних, яка обслуговується маршрутизатором.

Загальний підхід до виявлення ступеня «нормальності» мережевих потоків викладено далі у статті. Він ґрунтується на застосуванні поняття ентропії до інформації про мережеві потоки, оброблюваних маршрутизатором.

Відповідно до теорії інформації, ентропія служить «мірою невизначеності» повідомлень даного джерела.

В якості такої «міри невизначеності» в теорії інформації приймається число двійкових знаків, необхідне для фіксування (запису) довільного повідомлення даного джерела. Для певного (дискретного) статистичного розподілу ймовірністю інформаційної ентропії називають величину не меншу, ніж:

$$H = -\sum_i p_i log_2 p_i$$

і водночас рівна середньому числу двійкових знаків, необхідних для запису повідомлень.

Пропонований метод базується на припущенні, що ентропія параметрів - випадкова величина, при чому її щільність розподілу підпорядковується якимось законом. А її різку зміну можна розглядати як аномалію, в більшості випадків викликану аномалією трафіку.

Проміжок часу, на основі даних якого будуть будуватися вимірювані параметри, передбачається визначити емпірично. Однак, цей проміжок часу повинен надавати повну інформацію про стан каналу передачі даних. Тому визначимо межі цього проміжку.

Мінімальний час, який проходить між експортом даних в одному й тому ж потоці на маршрутизаторах Cisco за замовчуванням дорівнює 30 секундам. Логічно прийняти цей проміжок часу, як мінімальний можливий, оскільки за 30 секунд маршрутизатор експортує дані про всі мережевих потоках, які проходять через нього. За описаних вище причин, будь-який взятий проміжок часу для аналізу повинен бути кратний 30 секундам. Максимальний проміжок часу, за який доцільно обробляти інформацію, визначимо виходячи з практичних міркувань: DDoS атака виявляється в ручному режимі (в залежності від кваліфікації персоналу) не більше ніж за пів години. Цей час включає в себе час реакції на зниження якості обслуговування або відмову в роботі канального устаткування, комунікації між потерпілим і персоналом провайдера, і час, необхідний на локалізацію та усунення причини неполадки. Таким чином, система виявлення і локалізації DDoS атаки буде корисна, якщо допоможе знизити час виявлення і реакції. Тому встановимо верхнє обмеження проміжку аналізу трафіку в 30 хвилин.

Для визначення ентропії впливу потоків в каналі на маршрутизатор нам необхідні повідомлення та ймовірності їх виникнення в каналі. Будемо вважати, що крім існуючих повідомлень, ніяких інших в каналі передачі даних бути не може. Як повідомлення візьмемо інформацію про потік. Як ймовірності повідомлення вважатимемо кількість ресурсів маршрутизатора, використовуваних потоком, виділених на загальну кількість використовуваних маршрутизатором ресурсів:

$$p_i = \frac{\frac{F_{5i}}{F_{8i}} - F_{7i}}{\sum_k \frac{F_{5k}}{F_{8k}} - F_{7k}}$$

На основі цих даних обчислюється ентропія мережевого потоку в каналі передачі даних:

$$H = -\sum_i p_i log_2 p_i$$

Приймемо ентропію каналу передачі даних за випадкову величину. На основі реальних даних виберемо закон розподілу. Припустимо, що вона підпорядковується обраному закону розподілу. У разі різкої її зміни, тобто збурення, визначатимемо, які саме поля вносять найбільший вплив на трафік. Одним з можливих методів визначення потоків, що вносять збурення, може бути обчислення ентропії по різному кількості полів. Кожне поле, включаючи додаткове - випадкова величина з певною ймовірністю виникнення. Додатковим полем, які беруть участь в обчисленні ентропії, будемо вважати частину ширини пропускання каналу, яка використовується потоком, поділене на всю використовувану смугу пропускання каналу:

$$V_i = \frac{\frac{F_{5i}}{F_{8i}} - F_{7i}}{\sum_k \frac{F_{5k}}{F_{8k}} - F_{7k}}$$

Полями в цьому випадку є початкові значення полів.

За повідомлення приймемо складову випадкову величину, ймовірність виникнення якої розраховується як добуток ймовірностей значень кожного складового її поля.

За ймовірність приймемо сумарні ресурси маршрутизатора, що використовуються потоками з рівними значенням поля поділені на загальні зайняті ресурси маршрутизатора.

Розрахуємо ентропію для кожної комбінації полів.

Знову приймемо кожне обчислене значення ентропії за випадкову величину. Найбільший збурює фактор вносять ті поля, ентропія комбінації яких максимально обурена.

Ще один пропонований метод полягає в зберіганні сигнатур законів розподілу значень ентропії в момент атак. В даний час, у зв'язку зі зниженням кваліфікації інтернет-порушників (назвемо їх «хакерами»), більшість DDoS атак проводиться дилетантами з низьким рівнем підготовки. Для цього ними використовується доступне в Мережі програмне забезпечення. Атаки, які генеруються одним і тим же ПЗ аналогічні один одному. Таким чином, отримавши величину ентропії, яка значно відрізняється від нормальної, але підходящої під одну з сигнатур можна з більшою впевненістю говорити про наявність шкідливого трафіку в каналі передачі даних.

Висновки. Через значене збільшення DDoS-атак у сучасному світі було гостро поставлене питання про їх попереднє виявлення. У статті був запропонований метод виявлення аномалій мережевого трафіку на основі інформації про впорядкованості трафіку в каналі передачі даних. У подальшому цей метод можна покращувати та збільшувати його ефективність, беручи за основу роботу Т. Бабенка [11].

Список бібліографічного опису

1. SAM COOK DDoS attack statistics and facts for 2018-2019 [Електронний ресурс] // - Режим доступа: https://www.comparitech.com/blog/information-security/dDoS-statistics-facts/
2. Актуальные киберугрозы — 2018. Тренды и прогнозы Дата публикации 12 марта 2019 [Електронний ресурс] // - Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
3. Купреев О. DDoS-атаки во втором квартале 2019 года [Електронний ресурс] О. Купреев, Е. Бадовская, А. Гутников // - Режим доступа: https://securelist.ru/dDoS-report-q2-2019/94452/
4. Купреев О. DDoS-атаки в третьем квартале 2018 года [Електронний ресурс] / О. Купреев, Е. Бадовская, А. Гутников // - Режим доступа: https://securelist.ru/dDoS-report-in-q3-2018/92512/
5. DoS-атака на сервер [Електронний ресурс] // - Режим доступа: https://i-exam.ru/node/542
6. Гресько А.О. Загальний комплексний опис проблем інформаційної безпеки в "Інтернеті речей" / А.О. Гресько, Ю.М. Щебланін // Сучасний захист інформації. - 2016. - № 1. - с. 69-73.
7. Смоктій О.Д. Анализ механизма и последствий воздействия DDoS-атак на эталонную модель взаимодействия открытых систем OSI / О.Д. Смоктій, К.В. Смоктій, О.В. Іванченко // Системи управління, навігації та зв'язку. - 2017. - № 1. - с.33-37.
8. Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack / [Н.В. Багнюк, В.М. Мельник, О.В. Клеха, І.А. Невідомський] // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. - 2015. - № 18. - С.6-12.
9. Защита от DDoS атак своими руками [Електронний ресурс] // - Режим доступа: https://geekelectronics.org/linux/zashhita-ot-dDoS-atak-svoimi-rukami.html
10. DOS и DDoS-атаки: понятие, разновидности, методы выявления и защиты [Електронний ресурс] – Режим доступу до ресурсу: https://compconfig.ru/net/dos-i-ddos-ataki.html.
11. Бабенко Т. В. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак / Т. В. Бабенко.
12. Digital Attack MapTop [Електронний ресурс] – Режим доступу до ресурсу: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18348&view=map
13. Reiher P. A taxonomy of DDoS attack and DDoS Defense mechanisms [Електронний ресурс] / P. Reiher, J. Mirkovic – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.879.9772&rep=rep1&type=pdf.

Reference

1. SAM COOK DDoS attack statistics and facts for 2018-2019 [Electronic resource] // - Access mode: https://www.comparitech.com/blog/information-security/dDoS-statistics-facts/
2. Current cyber threats - 2018. Trends and forecasts Date of publication March 12, 2019 [Electronic resource] // - Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
3. Kupreev O. DDoS-attacks in the second quarter of 2019 [Electronic resource] O. Kupreev, E. Badovskaya, A. Gutnikov // - Access mode: https://securelist.ru/dDoS-report-q2-2019/ 94452 /
4. Kupreev O. DDoS-attacks in the third quarter of 2018 [Electronic resource] / O. Kupreev, E. Badovskaya, A. Gutnikov // - Access mode: https://securelist.ru/dDoS-report-in-q3 -2018 / 92512 /
5. DoS-attack on the server [Electronic resource] // - Access mode: https://i-exam.ru/node/542
6. Gresko A. General comprehensive description of information security problems in the "Internet of Things" / A. Gresko, Y. Shcheblanin // Modern information security. - 2016. - № 1. - p. 69-73.
7. Smoktiy O. Analysis of the mechanism and consequences of the impact of DDoS-attacks on the reference model of interaction of open OSI systems / O. Smoktiy, K. Smoktiy, O. Ivanchenko // Control, navigation and communication systems. - 2017. - № 1. - p.33-37.
8. Types of DDoS-attacks and algorithm for detecting DDoS-attacks of flood-attack type / [N. Bagniuk, V. Melnyk, O. Klekha, I. Nevidomsky] // Computer-integrated technologies: education, science, production. - 2015. - № 18. - P.6-12.

9. Protection against DDoS attacks with your own hands [Electronic resource] // - Access mode: https://geekelectronics.org/linux/zashhita-ot-dDoS-atak-svoimi-rukami.html
10. DOS and DDoS-attacks: the concept, types, methods of detection and protection [Electronic resource] - Mode of access to the resource: https://compconfig.ru/net/dos-i-ddos-ataki.html.
11. Babenko T. Investigation of entropy of network traffic as an indicator of DDOS-attacks / TV Babenko
12. Digital Attack MapTop [Electronic resource] - Mode of access to the resource: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18348&view=map.
13. Reiher P. A taxonomy of DDoS attack and DDoS Defense mechanisms [Electronic resource] / P. Reiher, J. Mirkovic - Mode of access to the resource: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.879.9772&rep=rep1&type=pdf.