Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Явіра Ярослава Романовича*

академічної групи *125-18-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплекс засобів захисту автоматизованої системи*

ТОВ "Аллергік" від низькорівневих DDoS атак на мережевому рівні.

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доцент Сафаров О.О.			
розділів:				
спеціальний	ст. викл. Саксонов Г.М.			
економічний	доцент Пілова Д.П.	90	Відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д. С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Явіру Я. Р.*** **Академічної групи** **125-18-2**

(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплекс засобів захисту автоматизованої системи***

ТОВ "Аллергік" від низькорівневих DDoS атак на мережевому рівні.

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	**Зміст**	**Термін виконання**
Розділ № 1	*Огляд літератури за темою, постановка задачі.*	04.02.2022-25.02.2022
Розділ № 2	*Проведення обстеження інформаційного середовища, виявлення загроз в мережевій системі, наведення методів захисту.*	22.03.2022-08.05.2022
Розділ № 3	*Розрахунок витрат пов'язаними з впровадженням методів захисту інформаційної системи.*	13.05.2022-10.06.2022

Завдання видано_____ Саксонов Г.М.
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Явір Я.Р
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 ст, 9 рис., 5 табл., 4 додатків, 12 джерел

Об’єкт розробки: Інформаційна система товариства з обмеженою відповідальністю “Аллергік”.

Методи дослідження: спостереженн, обстеження, аналіз, опис.

Мета проекту: створити комплекс засобів захисту від низькорівневих DDoS атак на мережевому рівні.

У першому розділі кваліфікаційної роботи наведено опис, що саме підлягає визначенню DoS, DDoS на яких рівнях моделі OSI вони можуть бути реалізовані, як їх класифікують, як вони реалізуються в системі .

У другому розділі представлено основні відомості про підприємство, а саме: персонал, який в ньому працює, які функції виконує, наведений мережевий опис системи, а також представлені основні методи захисту від DDoS атак, та наведені деякі політики безпеки

У третьому розділі розраховано витрати на впровадження методів протидії Ddos атакам, прорахована економічна доцільність створення Комплексу засобів захисту.

Практичне значення полягає в створенні оптимального захисту для ТОВ “Аллергік”.

ІНФОРМАЦІЙНА БЕЗПЕКА, DDoS-АТАКА, ЗАХИСТ, КЗЗ, МЕТОДИ РЕАЛІЗАЦІЇ ДДОС АТАК, МОДЕЛЬ OSI.

РЕФЕРАТ

Пояснительная записка: 68 с., 9 рис., 5 табл., 4 прилож., 12 источ.

Объект разработки: Информационная система общества с ограниченной ответственностью "Аллергик".

Методы исследования: наблюдение, обследование, анализ, описание.

Цель проекта: создать комплекс средств защиты от низкоуровневых DDoS атак на сетевом уровне.

В первой главе квалификационной работы приведено описание подлежащего определению DoS, DDoS на каких уровнях модели OSI они могут быть реализованы, как их классифицируют, как они реализуются в системе.

Во втором разделе представлены основные сведения о предприятии, а именно: персонал, работающий в нем, какие функции выполняет, приведено сетевое описание системы, а также представлены основные методы защиты от DDoS атак, и приведены некоторые политики безопасности

В третьей главе рассчитаны затраты на внедрение методов противодействия Ddos атакам, просчитана экономическая целесообразность создания Комплекса средств защиты.

Практическое значение заключается в создании оптимальной защиты для ООО "Аллергик".

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, DDoS-АТАКА, ЗАЩИТА, КЗЗ, МЕТОДЫ РЕАЛИЗАЦИИ ДДОС АТАК, МОДЕЛЬ OSI.

ABSTRACT

Explonetory note: 66 p., 9 fig., 5 tables, 4 applications, 12 sources.

Object of development: Information system of limited liability company "Allergik".

Research methods: observation, examination, analysis, description.

The goal of the project: to create a set of protection tools against low-level DDoS attacks at the network level.

The first chapter of the qualifying work describes the DoS to be determined, DDoS at what levels of the OSI model they can be implemented, how they are classified, how they are implemented in the system.

The second section provides basic information about the enterprise, namely: the personnel working in it, what functions it performs, a network description of the system, as well as the main methods of protection against DDoS attacks, and some security policies.

In the third chapter, the costs of implementing methods to counteract Ddos attacks are calculated, and the economic feasibility of creating a set of protection tools is calculated.

The practical significance lies in the creation of optimal protection for Allergik LLC.

INFORMATION SECURITY, DDoS ATTACK, PROTECTION, KZZ, METHODS FOR IMPLEMENTING DDoS ATTACKS, OSI MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КЗЗ – комплекс засобів захисту.

DoS – Denial of Service

DdoS – Distributed Denial of Service.

ІС – інформаційна система.

ПЗ – програмне забезпечення.

МЕ – мережевий екран.

ОС – обчислювальна система.

TCP – Transmission Control Protocol.

SYN – флаг протокола TCP (synchronize).

OSI – Open Systems Interconnection.

PDU – Protocol data unit.

MAC – Media Access Control.

LLC – Logical Link Control.

ICMP – Internet Control Message Protocol.

BGP – Border Gateway Protocol.

RTO — Recovery Time Objective

DNS – Domain name system.

DNSSC – Domain name system Security Extensions

ПЗ – програмне забезпечення

ЗМІСТ

С

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Розділ 3 Економічна частина

ВСТУП

Метою кожного підприємства є отримання прибутку та нарощення його виробничих можливостей, щоб забезпечити постійний потік надання послуг, людям які їх потребують. Однак час від часу у підприємства можуть виникнути труднощі з веденням безперервністю бізнесу. Наприклад конкурент, який бачить в новому підприємстві великі перспективи, який не бажає бачити його на ринку або зловмисні треті особи, які бачать, що підприємство має непогану виручку і хочуть отримати вигоду з цього наприклад: шантажем або вимаганням.

В епоху коли Інтернетом користується кожне підприємство, організація, компанія для ведення бізнесу: створюють різноманітні сайти які дозволяють споживачеві ознайомитися з товаром, доставкою, умовами надання послуг, поширюється й інша його сторона – новий плацдарм для нових вразливостей та загроз. DdoS – атаки стали одним з найпопулярнішим видом атак в Інтернеті, тому забезпечення інформаційної безпеки від них є значним пріоритетом кожної компанії.

Мета цієї роботи дослідити DdoS атаки та розібрати основні їх види та напрямки їх реалізації з знаходженням оптимального шлях захисту від них.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1 Стан питання

Перш за все потрібно відповісти на питання що таке DoS атака. DoS атака – це комплекс дій направлений на ОС з метою довести її до такого стану в якому не ОС не здатна надавати доступ до своїх системних ресурсів або максимально сповільнить її здатність до надання ресурсів користувачам системи.

DdoS атака це підвид DoS атаки головна особливість її у тому що на ОС, яку обрали як ціль відбувається атака з великої кількості комп' ютерів. Зібрати таку кількість компьютерів дуже складно, оскільки важко знайти велику кількість людей компетентних в цьому питанні тому чаще за все хакери використовують ботнети. Усі DdoS атаки зав'язані на перевантаження каналу передачі інформації.

При DdoS-атаці, навантаження атакуючого трафіку може бути величезним в порівнянні з ресурсами жертви. Атака може змусити жертву значно знизити продуктивність своїх послуг або навіть припинити їх надання. У порівнянні зі звичайними DoS-атаками, з якими можна боротися, краще захищаючи сервісні системи або забороняючи несанкціонований віддалений або локальний доступ, DdoS-атаки складніші і їх важче запобігти. Оскільки багато мимовільні хости (інші зламані комп'ютери) залучені до DdoS-атак, складно відрізнити атакуючі хости і відреагувати на них.[3]

1.2 Можливі наслідки від DDoS атак

Під час атаки жертва втрачає клієнтів через повільну роботу або повну недоступність сайту, страждає репутація бізнесу. Сервіс-провайдер може заблокувати IP-адресу жертви, щоб мінімізувати шкоду для інших клієнтів. Щоб усе відновити, знадобиться час, а можливо й гроші. Середні збитки від DDoS-атак оцінюються у світі в 50 тис. доларів для невеликих організацій і майже 500 тис. доларів для великих підприємств. Усунення наслідків DDoS-атаки вимагатиме

додаткового робочого часу співробітників, відволікання ресурсів з інших проектів на забезпечення безпеки, розробки плану оновлення ПЗ, модернізації обладнання та ін. персональних даних чи фінансової інформації.

1.3 Мережева модель OSI

Модель OSI є одним із способів багаторівневої організації мереж. Саме на її рівнях реалізовуються усі DdoS атаки тому цю модель вкрай важливо розглянути.

Рисунок 1.1 – Модель OSI

Модель використовується для передачі даних через Інтернет. Вона складається з семи рівнів, які ієрархічно розташовані від більшого до меншого. Тобто, найвищим є сьомий (прикладний), а найнижчим — перший (фізичний).

У процесі передачі даних завжди беруть участь пристрій-відправник, та пристрій-одержувач, а також дані, які повинні бути передані та отримані. Все, що відбувається при надсиланні та прийомі даних, детально описує семирівнева модель OSI рисунок 1.1.

При передачі даних по мережі з пристрій-відправник на пристрій-одержувач здійснюється такий процес: дані виходять з програми, що передаються вниз за рівнями моделі, проходять у вигляді електричного або оптичного сигналу, що представляє окремі логічні нулі і одиниці, після чого піднімаються за рівнями

моделі на іншому кінці з'єднання. У міру виконання цих дій на кожному рівні, який має відповідний протокол, до пакету додається заголовок, що вказує спосіб обробки пакета на іншому кінці з'єднання за допомогою такого ж протоколу. Цей процес називається інкапсуляцією даних.

Після того як пакет був переданий новому комп'ютеру починається зворотній процес, який називається декапсуляцією. Пакет прямує від фізичного рівня до прикладного і на кожному рівні він втрачає заголовок відповідних протоколів, який властивий кожному рівню. В підсумку ми отримаємо дані, які називаються вмістом пакету.

Перший, фізичний рівень (physical layer)

Він відповідає за обмін фізичними сигналами між фізичними пристроями. Комп'ютер не розуміє, що таке зображення або що на ньому зображено, комп'ютеру зображення зрозуміла лише у вигляді набору нулів та одиниць, тобто біт. В даному випадку біти є блоком даних протоколу, скорочено PDU

Кожен рівень мережі OSI має власні PDU, представлений в тій формі, яка буде зрозуміла на даному рівні. Робота з чистими даними відбувається лише на рівнях з п'ятого до сьомого.

Пристрої фізичного рівня оперують бітами. Вони передаються по дротах (наприклад, через оптоволокно).

Другий рівень, канальний (data link layer)

Другий рівень вирішує проблему адресації під час передачі інформації. Канальний рівень отримує біти і перетворює їх в кадри (frame). Його завдання – сформувати кадри з адресою відправника та одержувача, після чого надіслати їх через мережу.

У канального рівня є два підрівні – це MAC та LLC. MAC відповідає за присвоєння фізичних MAC-адрес, а LLC займається перевіркою та виправленням даних, керує їхньою передачею.

На другому рівні OSI працюють комутатори, їхнє завдання — передати сформовані кадри від одного пристрою до іншого, використовуючи як адреси лише фізичні MAC-адреси.

Третій рівень, мережевий (network layer)

Протоколи мережного рівня забезпечують логічну адресацію та визначення маршруту (маршрутизацію). Методи логічної адресації залежать від набору протоколів, але основні засади залишаються однаковими. Адреси мережного рівня застосовуються в основному для вказівки розташування хоста. Це завдання зазвичай вирішується шляхом поділу адресу на дві частини: поле групи та поле хоста. Разом ці поля повністю описують хост, але у контексті групи, до якої він належить. Такий поділ адреси дозволяє кожному хосту враховувати лише наявність інших хостів у його групі та застосовувати передачі пакетів від однієї групи до іншої спеціалізованими пристроями, які називають маршрутизаторами.

Четвертый уровень, транспортный (transport layer)

Рисунок 1.2 – Host layers и Media Layers [4]

Усі сім рівнів моделі OSI можна умовно поділити на дві групи:

- Media layers (рівні середовища),
- Host layers (рівні хоста).

Рівні групи Media Layers займаються передачею інформації (кабель або бездротової мережі), використовуються мережними пристроями, такими як комутатори, маршрутизатори і т.п.

Рівні групи Host Layers використовуються безпосередньо на пристроях, чи то стаціонарні комп'ютери, чи портативні мобільні пристрої.

Четвертий рівень – це посередник між Host Layers і Media Layers, що належить швидше до перших, ніж останніх, його головним завданням є транспортування пакетів. Звичайно, при транспортуванні можливі втрати, але деякі типи даних більш чутливі до втрат, ніж інші. Наприклад, якщо в тексті загубляться голосні, то буде складно зрозуміти сенс, а якщо з відеопотоку пропаде пара кадрів, це практично ніяк не позначиться на кінцевому користувачеві. Тому при передачі даних, найбільш чутливих до втрат на транспортному рівні використовується протокол TCP, що контролює цілісність доставленої інформації.

Для мультимедійних файлів невеликі втрати не такі важливі, набагато критичнішою буде затримка. Для передачі даних, найбільш чутливих до затримок, використовується протокол UDP, що дозволяє організувати зв'язок без встановлення з'єднання. При передачі протоколу TCP, дані діляться на сегменти. Сегмент – це частина пакету. Коли надходить пакет даних, який перевищує пропускну здатність мережі, пакет поділяється на сегменти допустимого розміру. Сегментація пакетів також потрібна в ненадійних мережах, коли існує велика ймовірність того, що великий пакет буде втрачений або надісланий тому адресату.

При передачі даних протоколу UDP, пакети даних діляться вже на датаграми. Датаграма (datagram) – це теж частина пакета, але її не можна плутати із сегментом. Головна відмінність датаграм в автономності.

Кожна датаграма містить усі необхідні заголовки, щоб дійти кінцевого адресата, тому вони залежать від мережі, можуть доставлятися різними маршрутами й у різному порядку. Датаграма та сегмент – це два PDU транспортного рівня моделі OSI. При втраті датаграм або сегментів виходять

«биті» шматки даних, які не вдасться коректно обробити. Перші чотири рівні — спеціалізація мережевих інженерів, але з останніми трьома вони не так часто стикаються, бо п’ятим, шостим та сьомим займаються розробники.

П’ятий рівень, сеансовий (session layer)

Сеансовий рівень відповідає за підтримку сеансу чи сесії зв’язку. П’ятий рівень надає послугу наступному: керує взаємодією між програмами, відкриває можливості синхронізації завдань, завершення сеансу, обміну інформацією.

Служби сеансового рівня найчастіше використовуються серед додатків, що вимагають віддаленого виклику процедур, тобто. Щоб вимагати виконання дій на віддалених комп’ютерах або незалежних системах на одному пристрої (за наявності кількох ОС). Прикладом роботи п’ятого рівня може бути відеодзвінок через мережу. Під час відеозв’язку необхідно, щоб два потоки даних (аудіо та відео) йшли синхронно. Коли до розмови двох людей додасться третя — вийде вже конференція. Завдання п’ятого рівня зробити так, щоб співрозмовники могли зрозуміти, хто зараз говорить.

Шостий рівень, представлення даних (presentation layer)

Шостий рівень займається тим, що представляє дані (які все ще є PDU) у зрозумілому людині та машині вигляді. Наприклад, коли один пристрій вміє відображати текст тільки в кодуванні ASCII, а інший тільки в UTF-8, переклад тексту з одного кодування в інше відбувається на шостому рівні.

Шостий рівень також займається представленням картинок (JPEG, GIF і т.д.), а також відео-аудіо (MPEG, QuickTime). Крім перерахованого, шостий рівень займається шифруванням даних, коли під час передачі необхідно захистити.

Сьомий рівень, прикладний (application layer)

Прикладний рівень – це те, з чим взаємодіють користувачі, свого роду графічний інтерфейс усієї моделі OSI, з іншими він взаємодіє як мінімум.

Усі послуги, які отримують сьомий рівень від інших, використовуються для доставки даних до користувача. Протоколам сьомого рівня не потрібно забезпечувати маршрутизацію або гарантувати доставку даних, коли про це вже подбали попередні шість. Завдання сьомого рівня – використовувати свої протоколи, щоб користувач побачив дані у зрозумілому вигляді.

Протоколи тут використовують UDP (наприклад DHCP) або TCP (наприклад, HTTP, HTTPS, SFTP (Simple FTP), DNS).

1.4 Категорії DdoS атак

DdoS атаки можуть реалізовуватися на кожному рівні моделі OSI, але частіше всього їх реалізовують на 3-4 рівнях що об'єднує їх в групу низькорівневих атак, та на 7 рівні що виділяє їх в групу високорівневих атак, також є окрема підгрупа під назвою об'ємні DdoS атак.

Низькорівневі атаки реалізовуються за допомогою недоліків мережевих протоколів таких як TCP, UDP, ICMP. Суть цього виду атак полягає в тому щоб запроси хакерів оброблювалися максимально довго, що перевантажує сервер в результаті чого він не може відповідати на запити інших користувачів системи.

До них відносяться такі DdoS атаки:

- SYN flood
- Icmp smurf flood
- Ping ICMP flood
- Ping of death
- Атака фрагментованими пакетами (TearDrop)

Високорівневі атаки базуються на точковій взаємодії, уражуючи конкретний елемент системи що може значно зменшити швидкість обробки даних завдяки навантаженню на ресурси системи наприклад: процесора або оперативної пам'яті. Також можуть унеможливити функціонування всієї системи. Такі види атак дуже важко відслідковувати, так як вони дуже схожі на звичайний трафік користувачів.

До них відносяться такі DdoS атаки:

- Взлом BGP (Border Gateway Protocol)

- Атака Slowloris (сесіонна атака)
- Slow POST-атака

Об'ємні атаки базуються на великої кількісті запитів до сервера, щоб трафік, що утворився, просто перекрив всю пропускну здатність мережі. Його обсяг може сягати кількох терабіт на секунду.

До них відносять:

- HTTP flood
- UDP flooding
- DNS amplification
- Intermittent Flooding

1.4.1 TCP SYN Flood

Дана DdoS-атака використовує мережевий протокол з відстеження стану свого власного стану (Підтверджений він чи ні), оскільки такі протоколи споживають ресурси для постійного відстежування власного стану. Одним з таких протоколів є протокол під назвою SYN.

Працює він таким чином: Коли клієнт намагається встановити з'єднання з сервером, клієнт спочатку відправляє серверу повідомлення SYN. Потім сервер підтверджує це надсилаючи клієнту повідомлення SYN-ACK. Клієнт завершує інсталяцію, відповідаючи повідомленням ACK. Потім відкривається з'єднання між клієнтом і сервером, між ними може здійснюватися обмін специфічними для служби даними. [1]

Зловживання цим протоком виникає коли він знаходиться напіввідкритому стані і сервер очікує повідомлення ACK від клієнта після надсилання клієнту повідомлення SYN-ACK. Серверу необхідно виділити пам'ять для зберігання інформації про напіввідкрите з'єднання. Пам'ять не буде звільнена доти, доки сервер не отримає остаточне повідомлення ACK або не закінчиться термін дії напіввідкритого з'єднання.

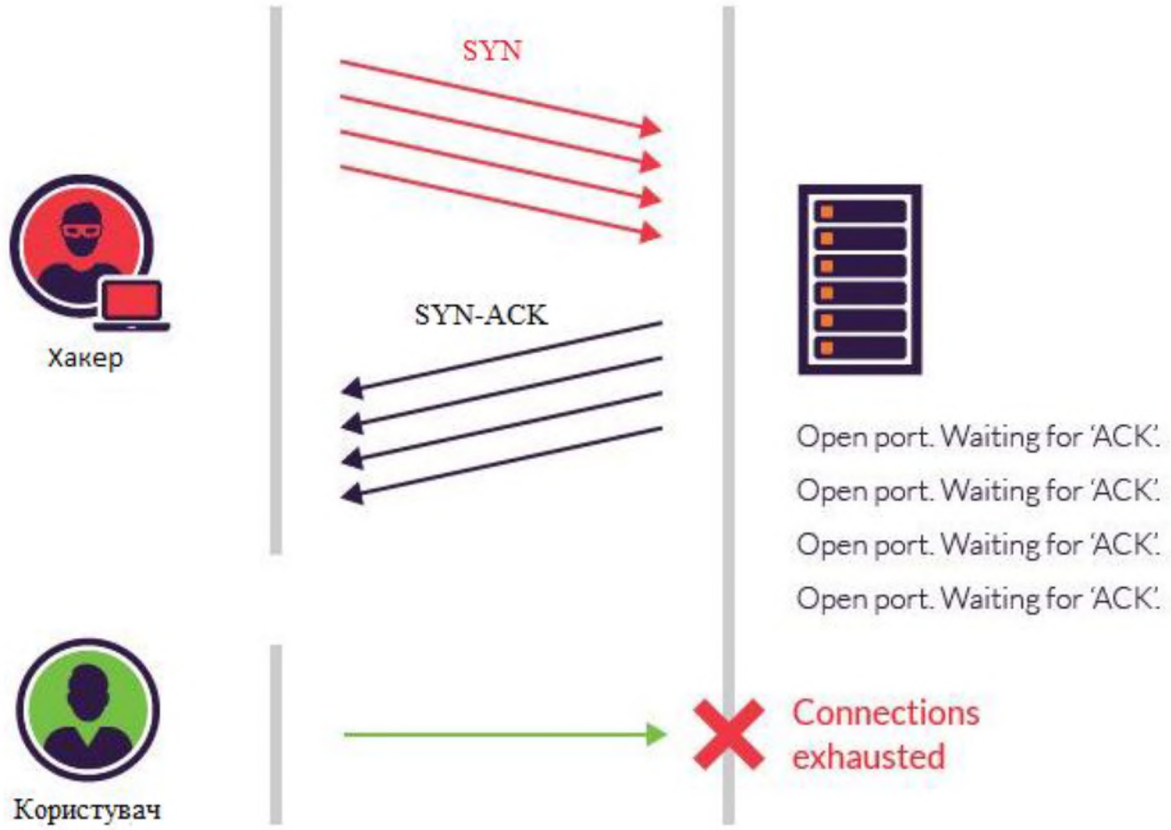

Рисунок 1.3.1 – DdoS за допомогою SYN протоколу [5]

Атакуючі хости можуть легко створювати напіввідкриті з'єднання, підробляючи вихідні IP-адреси в повідомленнях SYN або ігноруючи SYN-ACK. Наслідком є те, що остаточне повідомлення ACK ніколи не буде відправлене жертві. Оскільки жертва зазвичай виділяє обмежений розмір пам'яті у своїй таблиці процесів, тому занадто багато напіввідкритих з'єднань незабаром заповнять простір. Незважаючи на те, що напіввідкриті з'єднання в кінцевому підсумку закінчуються через деякий, ботнет може агресивно відправляти підроблені пакети TCP SYN із запитами на з'єднання зі швидкістю, що набагато перевищує швидкість закінчення терміну дії. Нарешті, жертва не зможе прийняти будь-яке нове вхідне з'єднання і, отже, не зможе надавати послуги.

1.4.1.1 Ботнет

Усі DdoS-атаками запускаються за допомогою розподілених атакуючих хостів. DdoS-атака запускається у два етапи. У першому етапі, зловмисник

створює розподілену атакуючу мережу, іншими словами ботнет, що складається з тисяч скомпрометованих комп'ютерів (так званими ботами, або атакуючими хостами). Потім боти спрямовують величезний обсяг трафіку до жертв або за командою зловмисника, або автоматично.

Щоб побудувати ботнет, зловмисник шукає комп'ютери, які погано захищені, наприклад ті, на які не має встановленого захисту. Як правило,

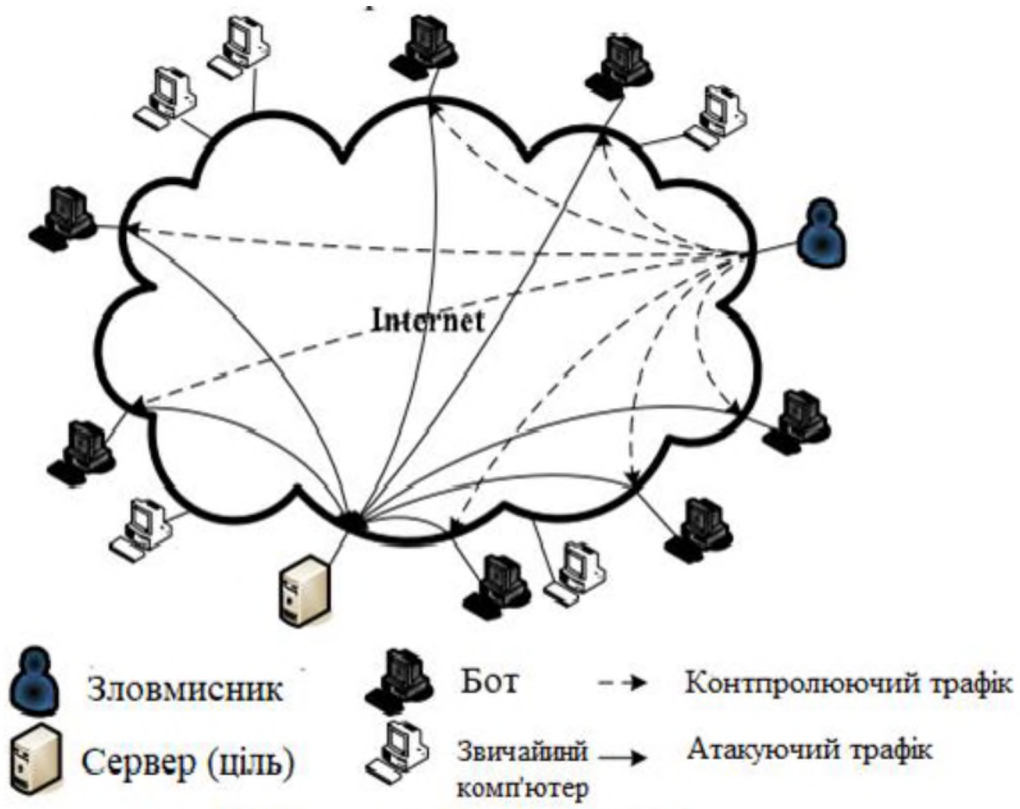

Рисунок 1.3.1.1 - Ботнет [1]

уразливий хост може бути скомпрометований двома способами. Один із них – спонукати користувачів запускати шкідливі програми, такі як віруси, програми-шпигуни або трояни, що містяться у шкідливих електронних листах, файлах чи веб-сторінках. Інший підхід полягає у використанні автоматичних шкідливих програм, таких як хробаки, які можуть автоматично сканувати вразливі віддалені комп'ютери. Потім ця вразливість використовується, зловмисником для того щоб проникнути та встановити програми DdoS-атаки, які додатково сканують інші хости, та розсилають пакети великій кількості.

Зловмисник, таким чином, становиться господарем цих компрометованих комп'ютерів (ботів). Деякі DdoS-програми мають можливість зареєструвати компрометований комп'ютер в якості члена атакуючої мережі, контрольованої зловмисником. Крім того, знову скомпрометовані комп'ютери автоматично повторюватимуть процес сканування та експлуатації для пошуку інших вразливих комп'ютерів. Через таку систему саморозповсюдження можна швидко побудувати велику атакуючу мережу, що включає сотні або тисячі комп'ютерів.[1]

1.4.2 Icmp smurf flood

ICMP використовеють для визначення того, чи комп'ютер має підключення до Інтернет мережі. Для реалізації цієї атаки на комп'ютер надсилається пакет exo-запит ICMP. Якщо комп'ютер отримує пакет запиту, він повинен повернути пакет exo-відповідь.

При smurf-атаці атакуючі хости підробляють exo-запити ICMP, використовуючи адресу жертви (IP) як адресу джерела та широкомовну адресу цих віддалених мереж як адресу призначення.

Як показано на рис. 1.3.2, якщо брандмауер або маршрутизатор віддаленої мережі не фільтрує спеціально створені пакети, вони будуть доставлені (поширені) на всі комп'ютери цієї мережі. Потім ці комп'ютери будуть відправляти пакети ICMP exo-відповідь назад джерелу (тобто жертві), що містяться в пакетах запитів. Таким чином, мережа жертви перевантажена.

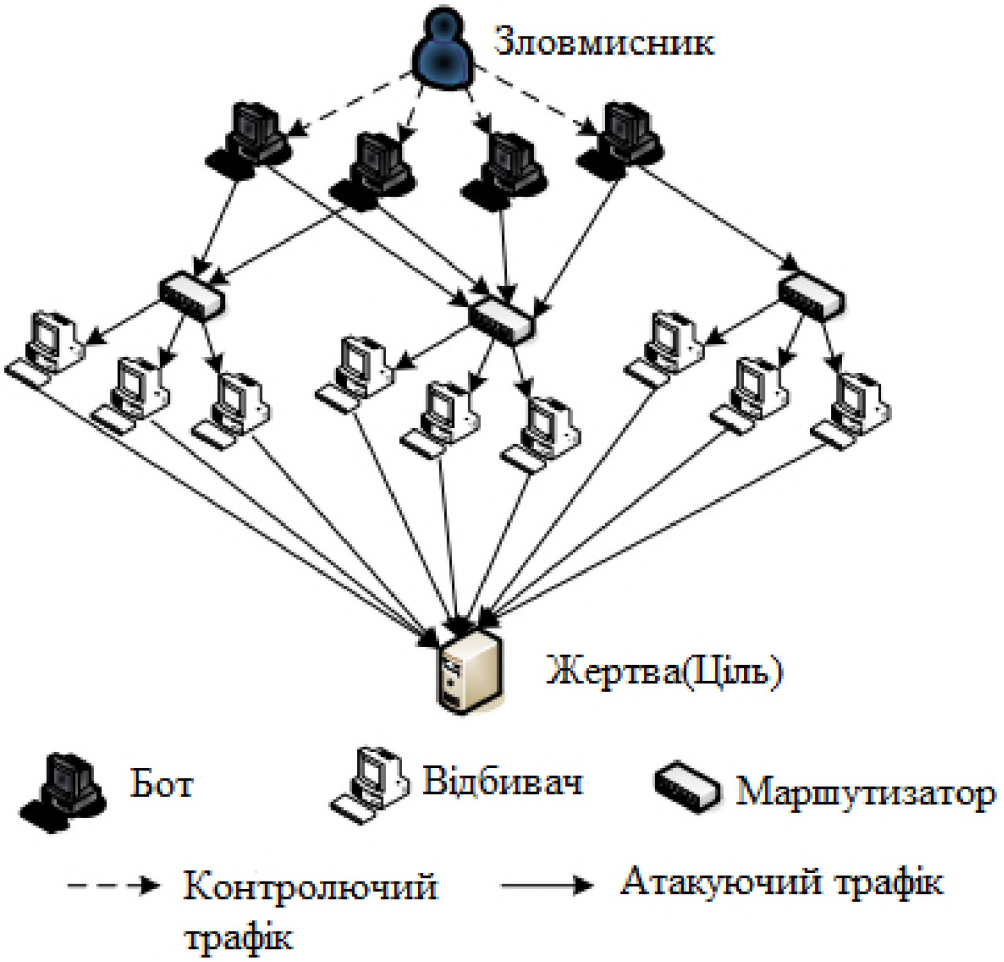

Рисунок. 1.3.2 ICMP Smurf атака [1]

1.4.3 Ping ICMP flood

Зловмисник виводить з ладу комп'ютер жертви, переповнюючи його ICMP exo-запитами, також відомими як ping.

Атака передбачає заповнення мережі жертви пакетами запитів, знаючи, що мережа відповість рівною кількістю пакетів відповіді. Додаткові методи знищення цілі за допомогою запитів ICMP включають використання спеціальних інструментів або коду.

Це напружує як вхідні, так і вихідні канали мережі, споживаючи значну пропускну здатність і призводячи до відмови в обслуговуванні. [11]

Зазвичай запити ping використовуються для перевірки підключення двох комп'ютерів шляхом вимірювання часу зворотного зв'язку від відправлення запиту ICMP до отримання відповіді ICMP. Однак під час атаки вони використовуються для перевантаження цільової мережі пакетами даних.

Виконання ping flood залежить від того, чи знають зловмисники IP-адресу своєї мети. Таким чином, атаки можна розділити на три категорії залежно від цілі та способу розв'язання її IP-адреси.

- Націлений на один комп'ютер у локальній мережі. Зловмиснику потрібен фізичний доступ до комп'ютера, щоб дізнатися його IP-адресу. Успішна атака призведе до зняття цільового комп'ютера.

- Націлений на маршрутизатори, щоб порушити зв'язок між комп'ютерами в мережі. Він залежить від того, що зловмисник знає внутрішню IP-адресу локального маршрутизатора. Успішна атака призведе до зняття всіх комп'ютерів, підключених до маршрутизатора.

- Сліпа атака передбачає використання зовнішньої програми для виявлення IP-адреси цільового комп'ютера або маршрутизатора перед виконанням атаки.

Зауважте, що для підтримки ping flood атакуючий комп'ютер повинен мати доступ до більшої пропускної здатності, ніж жертва. Це обмежує можливість здійснення DoS-атаки, особливо проти великої мережі.

Крім того, атака з розподіленою відмовою в обслуговуванні (DdoS), що виконується за допомогою ботнету, має набагато більше шансів підтримати ping-флуд і перевантажити ресурси цілі.

1.4.4 Атака фрагментованими пакетами

Атаки з фрагментацією IP-адресів є поширеною формою атаки типу «відказу в обслуговуванні», при якому зловмисник контролює мережу, використовуючи механізми фрагментації – датаграми.

Щоб зрозуміти як працює дана атака потрібно зрозуміти процес IP фрагментації, це процедура зв'язку при якій датаграми IP розбиваються на невеликі пакети, передаються по мережі, а потім знову збираються в вихідну інформацію.

Фрагментація необхідна для передачі даних, оскільки кожна мережа може обробляти свій розмір датаграм. Цей розмір відомий як максимальна одиниця передачі (MTU). Якщо відправляється датаграмма перевищує MTU, що приймає сервер, вона повинна бути фрагментована для повної передачі.

Рисунок 1.3.3 – Приклад як працює IP фрагментация [9]

Length – розмір фрагментованої датаграми.

ID – ID датаграми яку фрагментували.

Fragflag – показує чи є ще фрагменти.

Offset – Показує в якому порядку фрагменти повинні розташовані під час сборки.

Заголовок IP у кожній дейтаграмі містить прапорці, які вказують, чи дозволяється фрагментація. У випадках, коли до IP-заголовка додається прапор «не фрагментувати», пакет відкидається, і сервер надсилає повідомлення про те, що дейтаграма ICMP завелика для передачі.

Атаки фрагментації IP можуть мати кілька форм. Хоча всі вони використовують ділення дейтаграм, щоб пересилати цільові мережі, існують деякі помітні відмінності в тому, як виконуються різні вектори атаки.

- UDP and ICMP fragmentation attacks

Ці атаки включають передачу підроблених пакетів UDP або ICMP, розмір яких перевищує MTU мережі (зазвичай ~ 1500 байт). Оскільки ці пакети є підробленими і не можуть бути повторно зібрані, ресурси цільового сервера швидко споживаються, що призводить до недоступності сервера.

- TCP fragmentation attacks (TearDrop)

Ці атаки націлені на механізми повторного складання TCP/IP, не дозволяючи їм збирати фрагментовані пакети даних. У результаті пакети даних перекриваються та швидко перевантажують сервери жертви, викликаючи їхній збій. Такий ефект досягається через маніпуляцію з полем offset.

1.4.5 Злом протоколу BGP

Протокол прикордонного шлюзу (BGP) використовується для направлення трафіку через Інтернет, дозволяючи мережам обмінюватися інформацією про доступність для полегшення доступу до інших мереж. Перехоплення BGP – це форма DdoS-атаки на рівні додатків, яка дозволяє зловмиснику видати себе за мережу, використовуючи законний мережевий префікс як свій власний. Ідея у тому, щоб скористатися можливістю маршрутизаторів обмінюватися таблицями маршрутизаторів. Зловмисники повідомляють контрольованим маршрутизаторам,

що їхньою метою є маршрутизатор, що запитує обмін таблицею маршрутизації, що призводить до відправки великої кількості вхідних пакетів жертві, тим самим перевантажуючи її.

Крім величезної затримки в мережі, перехоплення BGP може призвести до втрати доходу, оскільки законний сайт втрачає трафік (і, можливо, бізнес) через самозванця. Такі DdoS-атаки можуть використовуватися спамерами або для крадіжки облікових даних, що відкриває можливості для ще більшого шахрайства. Прикладами таких DdoS-атак є захоплення префіксів для фінансових веб-сайтів, коли зловмисник збирає облікові дані користувача та токени автентифікації, надаючи йому інформацію, необхідну для доступу до конфіденційних даних або надання доступу до фінансових послуг користувача.

1.4.6 Атака Slowloris

Ця атака утримує з'єднання відкритими, надсилаючи часткові запити HTTP. Він продовжує надсилати наступні заголовки через рівні проміжки часу, щоб сокети не закривалися. Таким чином, веб-сервери можуть бути швидко підключені. Зокрема, сервери з багатопоточністю будуть уразливі через те, що вони намагаються обмежити допустимий обсяг багато-поточності. Slowloris повинен дочекатися, поки всі сокети стануть доступними, перш ніж він зможе їх використовувати, тому, якщо це веб-сайт з високим трафіком, це може зайняти деякий час. Таким чином, хоча ви не можете бачити веб-сайт зі своєї точки зору, інші все ще можуть його бачити його, поки всі сокети не будуть звільнені і не будуть використані Slowloris. Це пов'язано з тим, що інші користувачі системи повинні завершити свої запити до того, як сокети стануть доступними для використання Slowloris. Якщо інші користувачі повторно ініціюють підключення протягом цього короткого періоду часу, вони все одно зможуть бачити сайт.[8]

У Slowloris також вбудовано декілька прихованих функцій. По-перше, його можна змінити для надсилання різних заголовків хоста, якщо вашою метою є віртуальний хост та журнали зберігаються окремо для кожного віртуального хоста.

Але найголовніше, поки йде атака, лог-файл не записуватиметься доти, доки запит не буде виконано. Таким чином, ви можете відключити сервер протягом декількох хвилин без жодного запису у файлі журналу. Звичайно, як тільки ваша атака припиниться або сеанс буде закрито, у журналах веб-сервера буде приблизно кілька сотень помилок.

1.4.7 Slow Post

Зловмисник надсилає заголовки HTTP POST з легітимним полем «Content-Length», яке дозволяє веб-серверу зрозуміти, який обсяг даних до нього надходить. В цих заголовках правильно вказані розміри тіла повідомлення, яке буде за ним. Як тільки заголовок надіслано, тіло POST повідомлення починає передаватися з дуже повільною швидкістю, що дозволяє використовувати ресурси сервера набагато довше, ніж це необхідно. Швидкість може досягати наприклад один байт кожні дві хвилини.

Оскільки повідомлення обробляється нормально, цільовий сервер зробить все можливе, щоб дотримуватися вказаних правил. Як і при атаці Slowloris, сервер згодом сповільнюється. Що ще гірше, коли зловмисники запускають сотні або навіть тисячі атак Slow POST одночасно, ресурси сервера швидко споживаються, що робить легітимні з'єднання недосяжними.

Оскільки атаки Slow Post DdoS не вимагають широкої смуги пропускання, як це необхідно для інших DdoS-атак методом, їх може бути важко відлічити від звичайного трафіку. Оскільки ці типи DdoS-атак на прикладному рівні не вимагають великої кількості ресурсів, їх можна ініціювати з одного комп'ютера, що робить їх дуже простими для запуску та складними для усунення.

1.4.8 HTTP flood

це тип об'ємної розподіленої атка, яка призначена для перевантаження цільового сервера HTTP-запитами. Після того, як ціль переповнена запитами і не зможе відповідати на звичайний трафік, відмова в обслуговуванні буде

відбуватися для додаткових запитів від реальних користувачів. Існує два різновиди HTTP атак:

1) Атака HTTP GET – у цій формі атаки, кілька комп'ютерів або інших пристроїв координуються для надсилання кількох запитів на зображення чи файли із цільового сервера. Коли ціль переповнена вхідними запитами та відповідями, відмова в обслуговуванні буде відбуватися на додаткові запити від законних джерел трафіку.

2)HTTP POST атака – зазвичай, коли форма надсилається на веб-сайті, сервер повинен обробляти вхідний запит і передавати дані на рівень представлення, найчастіше базу даних. Процес обробки даних форми та виконання необхідних команд бази даних є відносно інтенсивним порівняно з обсягом обчислювальної потужності та пропускної здатності, необхідної для відправки запиту POST. Ця атака використовує нерівність у відносному споживанні ресурсів, надсилаючи багато запитів на пошту безпосередньо на цільовий

1.4.9 UDP Flooding

це тип атаки при якій велика кількість пакетів протоколу датаграм користувача (UDP) надсилається на цільовий сервер з метою переважити здатність цього пристрою обробляти та відповідати. Брандмауер, що захищає сервер, також може бути перевантажений в результаті переповнення UDP, що призведе до відмови в обслуговуванні законного трафіку.

Потік UDP працює насамперед, використовуючи кроки, які виконує сервер, коли відповідає на пакет UDP, надісланий на один із його портів. У звичайних умовах, коли сервер отримує пакет UDP на певному порту, він проходить два кроки у відповідь:

1)Сервер перевіряє, чи запущені програми, які в даний момент прослуховують запити на вказаному порту.

2)Якщо жодна програма не отримує пакети на цьому порту, сервер відповідає пакетом ICMP (ping), щоб повідомити відправника про те, що адресат недоступний.

Оскільки кожен новий пакет UDP отримує сервер, він проходить етапи для обробки запиту, використовуючи ресурси сервера в процесі. Коли пакети UDP передаються, кожен пакет міститиме IP-адресу вихідного пристрою. Під час цього типу DdoS-атаки зловмисник, як правило, не буде використовувати свою власну реальну IP-адресу, а замість цього підробить вихідну IP-адресу пакетів UDP, заважаючи справжньому місцезнаходження зловмисника виявлятися та потенційно насичуватися пакетами відповідей від цільової сервер. У результаті того, що цільовий сервер використовує ресурси для перевірки та відповіді на кожен отриманий UDP-пакет, ресурси цілі можуть швидко вичерпатися при отриманні великого потоку UDP-пакетів, що призведе до відмови в обслуговуванні звичайного трафіку.

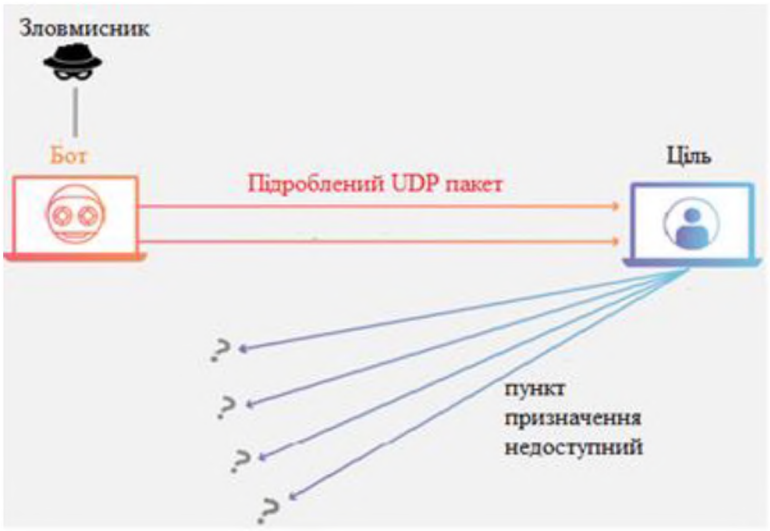

Рисунок 1.3.9 – UDP Flood [10]

1.4.10 DNS amplification

Зловмисник в цій атаці використовує вразливість у серверах системи доменних імен (DNS), щоб перетворити спочатку невеликі запити на набагато більші навантаження, які використовуються для відключення серверів жертви.

Зловмисник в цій атаці маніпулює загальнодоступними системами доменних імен, змушуючи їх заповнювати ціль великою кількістю пакетів UDP. Використовуючи різні методи посилення, зловмисники можуть збільшувати

розмір цих UDP-пакетів, роблячи атаку настільки потужною, що вона може вивести з ладу навіть найнадійнішу інтернет-інфраструктуру.

Посилення DNS, як і інші атаки з посиленням є типом атаки з відображенням. У цьому випадку відображення досягається шляхом отримання відповіді від перетворювачів DNS на підроблену IP-адресу.

Під час атаки з посиленням DNS зловмисник відправляє DNS-запит із підробленою IP-адресою (адресою жертви) на відкритий DNS резолвер, пропонуючи йому відповісти на цю адресу відповіддю DNS. При численних відправлених підроблених запитах і одночасної відповіді кількох перетворювачів DNS мережа жертви може легко перевантажена величезною кількістю відповідей DNS.

Такі є можливість “послювати” і вони стають ще небезпечніші. «Посилення» відноситься до отримання відповіді сервера, яка непропорційна вихідному надісланому запиту пакету.

Для посилення атаки DNS кожен запит DNS можна надіслати за допомогою розширення протоколу EDNS0 DNS, яке дозволяє отримувати великі повідомлення DNS, або за допомогою криптографічної функції розширення безпеки DNS (DNSSEC) для збільшення розміру повідомлення. Також можна використовувати підроблені запити типу «ANY», який повертає всю відому інформацію про зону DNS в одному запиті.

За допомогою цих та інших методів повідомлення запиту DNS розміром приблизно 60 байт можна налаштувати для отримання повідомлення-відповіді розміром понад 4000 байт на цільовий сервер, що призводить до коефіцієнта посилення 70:1. Це помітно збільшує обсяг трафіку, який отримує цільовий сервер, і прискорює швидкість виснаження ресурсів сервера.

Крім того, атаки посилення DNS зазвичай передають запити DNS через один або кілька бот-мереж, що різко збільшує обсяг трафіку, спрямованого на цільовий сервер або сервери, і значно ускладнює відстеження особи зловмисника.

1.4.11 Intermittent Flooding

Зловмисники можуть налаштувати свої дії так, щоб зменшити середню швидкість розсилки пакетів до дуже низького рівня, але не втратити свою ефективність атаки як при звичайній розсилці пакетів, на за допомогою TCP з'єднаннь. При таких атаках хости розсилають пакети, щоб перевантажити та порушити існуючі TCP-з'єднання. Оскільки всі перервані з'єднання TCP будуть очікувати повторної передачі втрачених пакетів протягом певного періоду часу (названого тайм-аутом повторної передачі (RTO)), атакуючі вузли можуть залити пакети при наступному RTO, щоб перервати повторну передачу.

Таким чином, атакуючі хости можуть синхронізувати свою атаку з наступними RTO та відключати законні TCP-з'єднання, як показано на рисунку 1.3.10. Така атака атакуючими хостами не лише знижує загальний обсяг лавинного трафіку, а й допомагає уникнути виявлення.

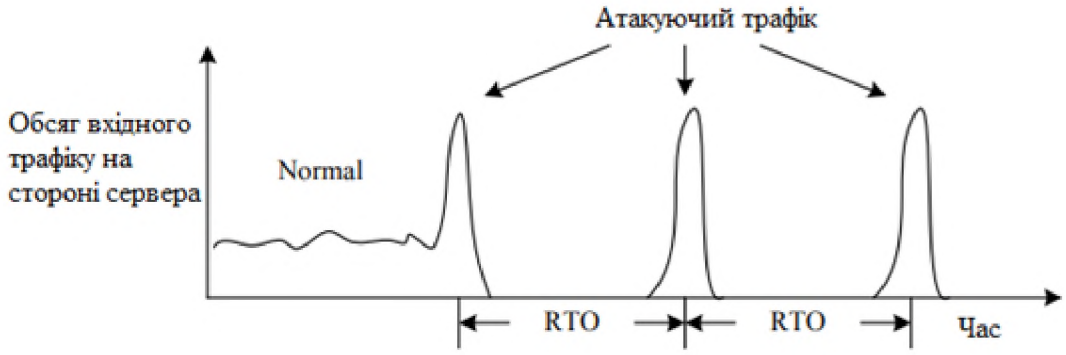

Рисунок 1.3.10 – схема роботи короткочасної об'ємної атаки

Подібні методи атак націлені на послуги з механізмами керування навантаженням Quality of Service (QoS). Коли сервер з підтримкою QoS отримує пакет запитів на обслуговування, він тимчасово блокує вхідні запити на період, доки не будуть оброблені попередні запити. Таким чином, зловмисники можуть лавинно розсилати запити з такою швидкістю, щоб сервер обмежував вхідні запити та досягав ефекту DoS.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА.

2.1 Характеристика Об’єкту

ТОВ “Аллергік” – це підприємство яке займається постачанням, рекламою медичного товару. Підприємство нещодавно створене, тому кількість людей в ньому не велика. У підприємства виділений офіс в якому є створений сервер на якому зберігається бази даних: замовників, медичного товару, адресу доставки товару та інше. Ця вся інформація використовується на спеціальному веб-ресурсі підприємства, а саме на його сайті. Сайт в свою чергу представляє деяку кількість послуг, а саме освітлює свій товар, характеристику товару (з чого зроблений, в якій кількості постачається), а також сайті надає можливість створення замовлення на медичний товар, які доставляються аптекам.

Таблиця 2.1 – Штат робітники головного офісу “Аллергік”:

№	Посада	Роль в системі	Кількість працівників на посаді	Рівень кваліфікації
1	Директор	Користувач	1	Висококваліфікований користувач
2	Бухгалтер	Користувач	2	Висококваліфікований користувач
3	Системний адміністратор	Адміністратор	1	Висококваліфікований користувач
4	Менеджер	Користувач	2	Середньо кваліфікований користувач
6	Фармацевт	Користувач	1	Середньо кваліфікований користувач
7	Охоронець	-	3	Низькокваліфікований користувач
8	Прибиральниця	-	1	Низькокваліфікований користувач

Робочий день:

Робочий день для працівників підприємства починається з 9:00 до 18:00. Охорона працює цілодобово, у сенсі 1 охоронець замінює іншого через кожні 8 годин. Для прибиральниці робочий день з 9:30 до 10:00 та з 17:30 до 18:00

Основні завдання працівників:

- Директор – проводить аналіз маркетингу підприємства, наскільки ефективно підприємство виконує свою функцію, заохочує нові кошти на розширення списку товарів підприємства, заохочує інвесторів в підприємство, проводить особисті зустрічі з клієнтами при необхідності.

- Бухгалтер – ведення документообігу, ведення та контролю обліку господарської діяльності, складання та подання звітності.

- Фармацевт – займається відбором нових фармацевтичних препаратів для магазину підприємства та виробами медичного призначення.

- Системний адміністратор – Займається наглядом з сайту, переглядає весь трафік, введенням нових методів, які зможуть підвищити безпеку підприємства, створює політики безпеки.

- Прибиральниця – займається підтримкою чистоти в приміщенні.

- Менеджер – організовує роботу, видає вузько спеціалізовані завдання, та відповідає за їх виконання, проводить аналіз якості виконаної праці.

- Охоронець - запобігання і протидіє небезпеці по відношенню до осіб, які працюють на підприємстві.

2.2 Характеристика серверу і ПК підприємства

На підприємстві знаходиться сервер DELL T620 (16x2.5) SFF, його характеристика:

Процесор: Intel Core i5-12600K 3.7(4.9)GHz.

Материнська плата: Asus ProArt B660-CREATOR

Оперативна пам’ять: DDR4 3 X 16GB 3200Mhz Aegis (F4-3200C16S-8GIS)

Слоти PCI: PCI-E 16x v3.0, PCI-E 16x v4.0, PCI-E 16x v5.0

Жорсткі диски: HDD: 2 x 1 ТБ, SSD: 2 X 250 ГБ

Мережевий контролер: Dell Intel X520-DA2 2x10 Ethernet SFP + PCI-e;

RAID контролер:

Сстандартні порти виводу/введення: порт RJ-45, 2 x USB 2.0 2 x USB 3.0 2 x USB 3.1;

Корпус: Vinga CS311W

Джерела живлення: DELL R720 / R620 / R520 / R820

У кожного робітника в офісі свій комп’ютер. Усі 7 комп’ютерів мають однакову характеристику, а саме:

Екран: 23.8" IPS (1920x1080) Full HD;

Процесор: Intel Core i3 - 4170 (3.1 ГГц);

Материнська плата: ASUS Q87M-E/SI RTL

Оперативна пам’ять: 8 ГБ DDR3-3.7 МГц;

Жорсткі диски: HDD 500 ГБ SSD 120;

Відео: Intel HD Graphics 4400;

Пристрої: DVD+/-RW / Wi-Fi / ;

Клавиатура: Ergo KB-960;

Миша: Dell MS116 Black (570-AAIS).

2.3 Встановлене ПЗ на компоненти мережі системи

Таблиця 2.2 – ПЗ встановлене на комп’ютери користувачів

№	Програмне забезпечення	На яких машинах встановлена	Строк роботи ліцензійного забезпечення	Користувачі
1	Windows 10 Pro Build-20H2 64bit version	Pc-1, Pc-2, Pc-3, Pc-4, Pc-5, Pc-6, Pc-7	Дата придбання: 30.10.2021	Директор, бухгалтер, фармацевт, менеджер, системний адміністратор
2	Microsoft Office 2021 Build - 2109.16.0.14430.20234 64bit version	Pc-1, Pc-2 Pc-3, Pc-4, Pc-5, Pc-6, Pc-7, Pc-8	Дата придбання: 30.10.2021	Директор, бухгалтер, фармацевт, менеджер, системний адміністратор
3	Adobe Photoshop 20 Build- 21.2.0 64bit version	Pc-1, Pc-2, Pc-3, Pc-4, Pc-5, Pc-6, Pc-7, Pc-8	Дата придбання: 30.10.2021 Діє До: 30.10.2022	Директор, бухгалтер, фармацевт, менеджер, системний адміністратор
4	WinRAR Build 1.25.3 64bit version	Pc-1, Pc-2, Pc-3, Pc-4, Pc-5, Pc-6, Pc-7	Freeware	Директор, бухгалтер, фармацевт, менеджер, системний адміністратор
6	Adobe Reader	Pc-1, Pc-2, Pc-3, Pc-4, Pc-5, Pc-6, Pc-7	Freeware	Директор, бухгалтер, фармацевт, менеджер, системний

				адміністратор

Продовження таблиці 2.2 - ПЗ встановлене на комп’ютери користувачів

7	бухгалтерія 1С	Pc-5, PC-4	Дата придбання: 30.10.2021 Діє До: 30.10.2023	Бухгалтер

2.4 Характеристика комп’ютерної мережі підприємства

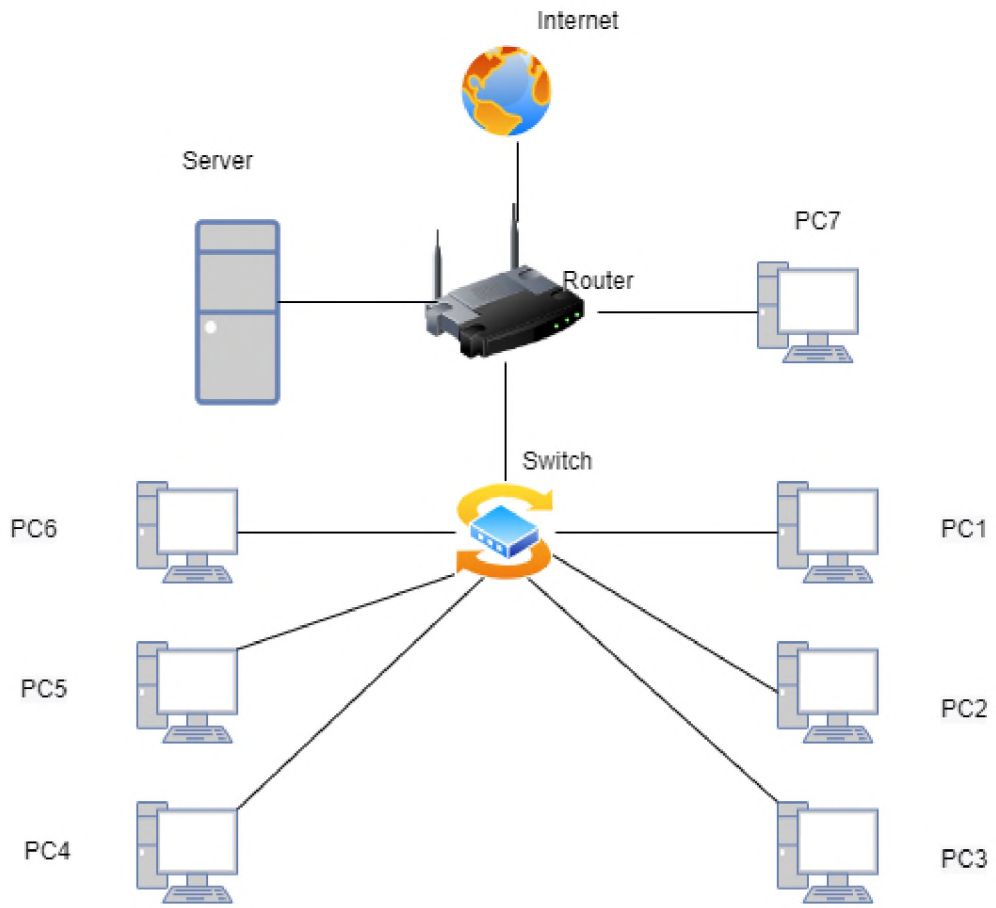

Рисунок 2.3 – Вигляд Комп’ютерної мережі підприємства

Комп'ютерна мережа представлена топологією типу "зірка". Кожна робоча станція під'єднується кабелем до концентратора. Концентратор забезпечує паралельне з'єднання ПК і, таким чином, всі комп'ютери, підключені до мережі, можуть спілкуватися один з одним. Інформація надходить на всі робочі станції, але приймається тільки тими станціями, яким вона призначається.

Аналізуючи комп'ютерну мережу компанії можна сказати, що основними загрозами є відсутність мережевих екранів, в

2.5 Загальні методи захисту від DDoS атак

У відповідь на DDoS-атаки виробники мереж та систем безпеки розробили та впровадили безліч комерційних продуктів, в основному в тому числі системи виявлення вторгнень (IDS), брандмауери та маршрутизатори з підвищеною безпекою. Ці пристрої зазвичай розгортаються між Інтернетом та серверами, щоб вони могли відслідковувати вхідний та вихідний трафік та вдаватися до відповідних заходів для захисту серверів. Фундаментальні технології всередині цих пристроїв включають аналіз трафіку, контроль доступу, фільтрацію пакетів, блокування адрес, резервування тощо.

2.5.1 IDS система.

Ця система зазвичай реєструє вхідний трафік і становлять статистику на основі трасування трафіку. Наприклад, CISCO IOS NetFlow може вести облік мережевого трафіку та використання та надавати цінну інформацію про мережевих користувачів та додатки, пікові періоди використання та маршрутизації трафіку. Трасування та статистику трафіку можна порівняти з базовими профілями трафіку, щоб виявити потенційні DoS-атаки.

2.5.2 Класифікація IDS систем.

- Мережеві IDS зазвичай класифікуються на основі методу виявлення, що використовується: метод на основі сигнатур або на основі виявлення аномалій. Перший метод, також відомий як грунтований на правилах неправильного використання , дозволяє виявити атаку, порівнюючи відомі сигнатури атак або

шаблони з трафіком, що відстежується. Збіг сигналізує про потенційну атаку. Цей метод має малий час роботи, що дозволяє виявляти більшість відомих атак, і, як правило, має низьку частоту помилкових спрацьовувань, тобто не створює сигнал тривоги для легального трафіку.

IDS на основі аномалій, також відомі як засновані на поведінці, працюють, порівнюючи поведінку мережевого трафіку з попередньою «нормальною» поведінкою трафіку. Будь-яке відхилення вважається ознакою атаки. Система отримує нормальний профіль трафіку зазвичай за допомогою навчання і відстежує трафік на предмет будь-яких відмінностей з нормальним профілем. Навчений трафік використовується визначення порогового значення для майбутнього виявлення. Виявлені аномалії допомагають виявити невідомі атаки; проте застосування цього методу призводить до більш частих хибним спрацьовуванням, ніж сигнатурні системи. Насправді системи можуть поєднувати як сигнатурні, і аномальні методи.

2.5.3 Методи виявлення DDoS-атак.

Одним із ключових параметрів методики виявлення DDoS є час виявлення. Механізм виявлення повинен виявити DoS-атаку, перш ніж сервіс почне деградувати. Однак пакети DDoS-трафіку часто не відрізняються від пакетів користувачів. Це ускладнює виявлення і збільшує шанси помилкового спрацьовування, що є критичною проблемою у виявленні DoS. Якісний метод виявлення повинен реагувати швидко і мати низьку частоту помилкових спрацьовувань.

Виявлення атак з урахуванням сигнатур. Ідентифікація на основі сигналатур зазвичай використовується для ідентифікації відомих типів атак. Для виявлення атаки не потрібно будь-який опис типових дій при ній, проте для виявлення цих видів атак необхідна база даних з відомими сигнатурами атак. Для виявлення вірусу чи хробака не потрібно докладний опис його дій: як хробак знаходить ціль, як він поширює себе або які ділянки пам'яті він використовує. При виявленні на основі сигнатур корисне навантаження досліджується та

обробляється незалежно від того, чи містить вона черв'яка. Один величезний тест системи виявлення вторгнень на основі сигнатур полягає в тому, що для кожної сигнатури потрібен розділ у базі даних, тому вся база даних може містити сотні або навіть тисячі сигнатур. Кожен пакет має бути зіставлений з ідентичним у базі даних. Цей процес може бути дуже ресурсномістким, він може використовувати всю пропускну здатність і зробить даний тип виявлення вразливим для DoS-атак.

Виявлення атак на основі аномалій.

Методи виявлення вторгнень, засновані на суперечливості, розпізнають незвичайну активність та створюють попередження аномалій у діях системи чи діях додатків [7]. Звичайні специфічні дії, які можуть бути перехоплені, включають: 1) зловживання системними угодами, наприклад, приховування інтервалу IP-адрес і виконання стандартної угоди на прихованому порту; 2) унікальні патерни трафіку, наприклад, більше UDP-пакетів у порівнянні з TCP; 3) підозрілі приклади в корисних даних програми. Найбільші труднощі у використанні методів виявлення на основі аномалій полягають у визначенні типової поведінки системи, виборі межі для спрацьовування попередження та запобігання хибним попередженням. Користувачі системи, як правило, люди, та їх поведінка важко передбачати. У тому випадку, якщо звичайна модель не буде охарактеризована докладним чином, виникне безліч помилкових спрацьовувань, і система виявлення відчуватиме негативні наслідки невірного виконання. У зв'язку з розвитком засобів машинного навчання на сьогоднішній день багато дослідників вважають за краще застосовувати алгоритми машинного навчання та штучні нейронні мережі для виявлення різних загроз.

2.6. Класифікація архітектур запобігання DDoS-атак відповідно до місця їх розгортання.

При виявленні DDoS-атаки не можна зробити нічого іншого, крім вручну усунути проблему і відключити систему-жертву від мережі. DDoS-атаки блокують багато ресурсів, наприклад, обмежують потужність процесора і пропускну здатність мережі, пам'ять, час обробки і т. д. Основна мета будь-якого

механізму захисту від DDoS-атак - якнайшвидше виявити DDoS-атаки і зупинити їх як можна ближче до джерел. Схеми захисту від DDoS поділяють на чотири класи залежно від місця розгортання: джерело, жертва, проміжні маршрутизатори і розподілений або гібридний захисний механізм [7]. Переваги та недоліки всіх цих підходів наведені у таблиці.

Механізми захисту, що встановлюються за джерела атаки. У цьому типі механізмів захисту від DDoS засоби розгорнуті на стороні джерела атаки, щоб запобігти створенню DDoS-атак користувачами мережі. При такому підході пристрої-джерела ідентифікують шкідливі пакети у вихідному трафіку та фільтрують або обмежують трафік. Виявлення та запобігання DDoS-атаки на джерелі є найкращим можливим захистом, оскільки легальному трафіку завдається мінімальний збиток [9].

Механізми захисту, встановлювані за жертви атаки. У цьому типі механізмів захисту від DDoS жертва виявляє, фільтрує або обмежує швидкість шкідливого вхідного трафіку на маршрутизаторах мереж жертви, тобто мереж, що надають веб-служби. Легальний і атакуючий трафік можна чітко визначити, використовуючи або виявлення вторгнень на основі неправильного використання, або виявлення вторгнень на основі аномалій [10]. Однак трафік атаки, що досягає жертви, може відмовити або погіршити якість послуг і різко скоротити ширину смуги пропускання [8].

Механізми захисту, що встановлюються на проміжних маршрутах-заторах. Будь-який маршрутизатор в мережі може незалежно спробувати визначити шкідливий трафік і фільтрувати або обмежити швидкість трафіку. Він також може налаштовувати баланс між точністю виявлення та споживанням смуги пропускання атаки [6]. Виявлення та відстеження джерел атак стає простим завдяки спільній роботі кількох маршрутизаторів мережі. У цій точці захисту весь трафік об'єднується, тобто і атакуючі, і легітимні пакети прибувають у маршрутизатор, і це місце для обмеження швидкості всього трафіку [8].

Розподілені чи гібридні механізми захисту. Даний тип захисту може бути найкращою стратегією проти DDoS-атак. Механізми гібридного захисту розгортаються (або їх компоненти розподіляються) у кількох місцях, таких як джерело атаки, жертви або проміжні мережі, і зазвичай між точками розгортання здійснюється взаємодія [10]. Механізми маршрутизаторів найкраще підходять для обмеження швидкості всіх видів трафіку, тоді як механізми на стороні жертви можуть точно виявити трафік атаки в комбінації легітимних та атакуючих пакетів. Тому використання даної стратегії захисту від DDoS може бути вигіднішим

2.7 Міжмережевий екран

Міжмережевий екран широко використовуються для захисту від DoS-атак. У разі правильної конфігурації брандмауери використовуються для перевірки вхідних та вихідних пакетів та фільтрації небажаних пакетів. Брандмауери дозволяють або забороняють певні пакети відповідно до протоколів, портів, IP-адрес, корисного навантаження, стану підключення і т. д. Інформація зазвичай визначається в списках контролю доступу і правилах фільтрації в брандмауерах. Деякі брандмауери та можуть перевірити стан, щоб у мережі могли передаватися лише законні пакети для поточних з'єднань, а також могли встановлюватися та підтримуватись лише законні TCP-з'єднання.

Брандмауери також можуть створювати профілі (тривалість бездіяльності, швидкість передачі даних тощо) для з'єднань та проводити аналіз у реальному часі для виявлення та заборони зловмисних спроб (Thomas et al. 2003).

Деякі продукти об'єднують функції виявлення вторгнень та брандмауера, а також надають адміністративним засобам повнішу видимість мережі для DDoS-атак.

2.8. Безпека за допомогою маршутизаторів

Заходи безпеки в маршрутизаторах можуть відсунути лінію оборони далі від цілі атакуючих, тому внутрішні мережі не будуть безпосередньо порушені DDoS-трафіком. Подібно до брандмауерів, багато маршрутизаторів мають списки

контролю доступу і можуть фільтрувати або обмежувати трафік. Маршрутизатори можуть швидко фільтрувати пакети з підробленими та небажаними IP-адресами, тоді як брандмауери можуть ретельніше перевіряти корисне навантаження пакетів.

2.9 Підтримання безпеки за допомогою додаткових ресурсів.

Постачальники послуг також можуть підвищити надмірність мережі та інфраструктури обслуговування. Контент служби може бути зарезервований на резервних серверах. Коли сервер виходить з ладу, його можуть взяти він резервні сервери. Збій через DoS-атак у цьому випадку аналогічний звичайному збою. Точки доступу до послуг також можуть бути розподілені через мережу. Оскільки DoS-атаки можуть бути націлені лише на одне мережеве з'єднання, надлишкові мережеві доступи можуть як альтернативу надавати послуги. Проте рішення з резервуванням може виявитися неефективним проти DoS-атак, як очікується. По-перше, надмірність вимагає додаткових обчислювальних ресурсів для обробки вхідного трафіку. Постачальникам послуг можливо дорого підтримувати достатню кількість обчислювальних ресурсів. По-друге, зловмисники можуть легко знайти велику кількість атакуючих агентів в Інтернеті (див. розділ II.A), щоб придушити можливості надлишкового обладнання.

Незважаючи на те, що було впроваджено кілька практичних рішень та продуктів, багато проблем досі існують.

- По-перше, важко відрізнити миттєвий натовп від повені. Наприклад, брандмауери можуть не запобігти атакам на порт 80 (веб-служба) серверів, тому що багато пакетів на цьому порті це просто трафік веб-серфінгу на веб-сайти, розміщений на цільових серверах.

- По-друге, коли лавинний трафік пригнічується за допомогою механізмів фільтрації та обмеження швидкості, деяка частина законного трафіку також може постраждати.

- По-третє Списки керування доступом також можуть бути налаштовані на неправильну інформацію, оскільки лавинні пакети можуть підробляти адреси. По-третє, брандмауери та маршрутизатори можуть бути легко перевантажені DDoS-атакою. Вони можуть бути уповільнені або перевантажені. Якщо вони не можуть надсилати вхідні пакети на сервери, зловмисники також досягають ефекту DoS.

- По-четверте, існуючі продукти діють власними силами, не контролюючи інші маршрутизатори. Навіть якщо прикордонний маршрутизатор або брандмауер ідентифікував висхідні маршрутизатори, на які приходять лавинні пакети, непросто попросити власників висхідних маршрутизаторів (наприклад, телекомунікаційних компаній або інтернет-провайдерів) обмежити певні потоки трафіку.

2.10 Методи захисту від DDoS атак типу ICMP smurf flood та Ping ICMP flood

- Одним із способів захисту від таких видів DDoS атак є заборона ICMP на прикордонному маршрутизаторі, але тоді буде заблоковано легітимний трафік, у тому числі пакети ICMP ECHO. Зважаючи на службові функції протоколу ICMP, його блокування може стати причиною втрат інших пакетів, порушення зв'язності та зниження пропускної спроможності каналів.

- Другим методом є створення спеціалізованого алгоритма на основі фільтрації вихідних IP-адрес. В цьому методі, граничний маршрутизатор граничний маршрутизатор зберігає історію всіх правомірних адрес IP, які раніше з'являлися в мережі. Коли граничний маршрутизатор перевантажений, ця історія використовується для рішення, чи слід приймати пакети від конкретного IP. На відміну від інших алгоритмів для захисту від DDoS атак, цей метод працює добре при високорівневій розподіленій DDoS атаці, тобто з великої кількості джерел.

- Третім методом є залучення стороннього сервісу для вирішення проблеми відносно DDoS атаки наприклад: CloudFLARE. Воно надає функцію Magic Transit що забезпечує переваги підключення, безпеки та продуктивності, будучи

«вхідними дверима» у вашу IP-мережу. Це означає, що він приймає IP-пакети, призначені для вашої мережі, обробляє їх, а потім виводить їх до вашої вихідної інфраструктури.

Як тільки пакети потрапляють у мережу Cloudflare, трафік перевіряється на предмет атак, фільтрується, спрямовується, прискорюється та надсилається до вашого джерела. Magic Transit підключається до вашої вихідної інфраструктури за допомогою тунелів Anycast Generic Routing Encapsulation (GRE) через Інтернет або, за допомогою Cloudflare Network Interconnect (CNI), через фізичне або віртуальне з'єднання.

Користувачі Magic Transit мають два варіанти їх реалізації: вхідний трафік або вхідний і вихідний трафік. Користувачам із вихідною реалізацією потрібно буде налаштувати маршрутизацію на основі політики (PBR) або забезпечити маршрутизацію за замовчуванням на їх кінці, щоб перенаправляти трафік до Cloudflare через тунелі.

Підводячи підсумок під усим вище сказаним у нас є декілька рішень як можна підвищити захист мережі підприємство, такими засобами як IDS фільтр протоколів, встановленням між-мережевого Firewall-у, написати своє власне правило фільтрації, а також віддати весь трафік на інший ресурс, який його буде фільтрувати. У кожного рішення щодо вибору захисту є свої плюси та мінуси.

Також ми можемо підвищити захищеність системи політиками безпеки.

2.11 Організаційні заходи щодо забезпечення інформаційної безпеки мережі.

Впровадити моніторинг та фільтрацію використання Інтернету співробітниками

Завдяки цій політиці буде здійснюватися моніторинг та обмеження використання Інтернету з будь-якого хосту в мережі компанії. Ця політика покликана забезпечити безпечне використання Інтернету, а також зменшити можливість створення бот-нету в рамках мережі підприємства.

Ця політика розповсюджується на: працівників, підрядників, агентів видавництва наряду з належними видавництву персональними комп'ютерами або робочими станціями підключеними до мережі. Ця політика застосовується до всіх повідомлень, між мережею видавництва та Інтернету, включаючи веб -перегляд, миттєві повідомлення, передачу файлів, спільний доступ до файлів та інші стандартні та фірмові протоколи. Комунікація типу "Сервер--Сервер" така як: трафік SMTP, резервне копіювання, автоматична передача даних або зв'язок із базами даних не входять до цієї політики.

2.11.1 Веб-сайт моніторинг

Департамент інформаційних технологій повинен моніторити (відсідковувати) використання Інтернету з усіх комп'ютерів та пристроїв, підключених до корпоративної мережі. Для всього трафіку система моніторингу повинна записувати IP -адресу джерела, дату, час, протокол та місце знаходження сайту або сервера. По можливості, система повинна записувати ідентифікатор користувача облікового запису, що ініціює трафік. Записи використання Інтернету повинні зберігатися протягом 180 днів.

2.11.2 Доступ до записів веб-сайт моніторингу

Загальні звіти по діяльності будуть надані будь -якому працівнику у разі потреби за запитом до Департаменту інформаційних технологій. Члени Команди реагування на інциденти комп'ютерної безпеки (КРНІКБ) можуть отримати доступ до всіх звітів та даних, якщо це необхідно для реагування на інцидент із безпекою. Звіти про використання Інтернету, що ідентифікують конкретних користувачів, сайти, команди чи пристрої, стануть доступними лише для співробітників за межами (КРНІКБ) за письмовим запитом або електронним листом до Команди реагування на інциденти комп'ютерної безпеки

2.11.3 Система фільтрації використання Інтернету

Департамент інформаційних технологій повинен блокувати доступ до веб-сайтів та протоколів Інтернету, які вважаються неприйнятними для

корпоративного середовища видавництва. Такі протоколи та категорії веб -сайтів слід заблокувати:

- Матеріал для дорослих/явного сексуально характеру.

- Реклама та спливаючі вікна.

- Чат та миттєві повідомлення.

- Азартні ігри.

- Злом системи.

- Незаконні наркотики.

- Інтимний одяг та купальники.

- Спільний доступ до файлів.

- Послуги соціальних мереж.

-Спам, фішинг та шахрайство.

-Шпигунське програмне забезпечення.

-Образливий зміст.

-Насильство, нетерпимість та ненависть.

- Веб-електорнна пошта.

2.11.4 Зміна правил фільтрації Інтернету

Департамент інформаційних технологій повинен періодично переглядати та рекомендувати зміни до правил фільтрації мереж та протоколів. Керівництво повинно переглянути ці рекомендації та вирішити, чи потрібно вносити якісь зміни. Зміни до правил фільтрації Інтернету та протоколів будуть записані в політику моніторингу та фільтрації використання Інтернету.

2.11.5 Винятки використання Інтернет фільтрації

Якщо сайт неправильно класифіковано, співробітники можуть подати запит на його розблокування, подавши заявку до служби підтримки інформаційних технологій. ІТ-працівник розгляне запит і розблокує сайт, якщо він неправильно класифікований.

Працівники можуть отримувати доступ до заблокованих сайтів з дозволу, якщо це доречно та необхідно для комерційних цілей. Якщо працівник потребує доступу до веб -сайту, який заблоковано, він повинен подати запит своєму керівництву. Керівництво надасть усі затверджені запити в письмовій формі або електронною поштою. ІТ-працівник розблокує цей сайт лише для цього працівника. ІТ-працівник відстежуватиме весь трафік від працівника та звітуватиме за нього.

Команда інформаційного захисту перевіряє відповідність цій політиці різними методами і не обмежує себе, періодичними проходами, відео-моніторингом, звітами бізнес-інструментів, внутрішніми та зовнішніми аудитами та зворотнім зв'язком з власником поліса.

Будь-які винятки з політики повинні бути затверджені командою інформаційного захисту заздалегідь.

Працівник, який виявив, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, і аж до припинення трудових відносин.

2.12.1 Впровадити моніторинг Інтернет трафіка системним адміністратором

Завдяки цій політиці буде проводитися перехоплення усього Інтернет трафіку через програму WideShark, що дозволить відслідковувати підозрілий трафік у реальному часі та швидко протидіяти йому.

Ця політика розповсюджується на: системних адміністраторів підприємства наряду з належними підприємству персональними комп'ютерами або робочими станціями підключеними до мережі. Ця політика застосовується до всіх повідомлень, між мережею підприємства та Інтернету.

2.12.2 Ведення логування

Після кожного виявлення підозрілого трафіку повинен формуватися спеціальний лог за допомогою якого, буде надана можливість його заблокувати підозрілий трафік.

Логи періодично перевіряються та досліджуються, на наявність якщо нових видів використання ДДоС атак на базі логів можуть бути створені нові методи захисту підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА.

Створення комплексу засобів захисту на підприємстві від DDoS атак є край важливою, оскільки від нього залежить наскільки підприємство буде знаходитися в стані простою, а отже не буде отримувати прибуток, але потрібно не забувати про економічну доцільність створення захисту, щоб витрати на захист були доцільними.

3.1 Розрахунок витрат

Нормування праці в процесі КЗЗ істотно ускладнено через творчий характер праці спеціалістів з інформаційної безпеки. Проте трудомісткість розробки КЗЗ може бути розрахована на основі трудомісткості робіт, які виконуються.

3.1.1 Трудомісткість

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста): Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{б}\text{, годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритма;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_б$ – тривалість підготовки технічної документації на ПЗ.

Підрахуємо трудомісткість:

$t_{тз}$ = 20 годин, $t_в$ = 32 годин, $t_а$ = 15 годин, $t_{пр}$ = 17 годин, $t_{опр}$ = 8 годин, $t_б$ = 20 годин.

Т = 20 + 32 + 15 +17 +8 + 20 = 112 годин.

3.2 Розрахунок витрат на створення захисту від DdoS атак

Витрати на розробку КЗЗ від DdoS-атак $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки системи захисту $З_{мч}$

$$К_{рп} = З_{зп} + З_{мч} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t * З_{іб}, грн \quad (3.3)$$

де *t* – загальна тривалість розробки КЗЗ, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{зп} = 112 * 140 = 15\,680 \text{ грн.}$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t * С_{мч}, \text{ грн} \quad (3.4)$$

де *t* – трудомісткість розробки політики безпеки інформації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч}= Р * t_{нал} *С_е + \frac{Фзал*На}{Fp} + \frac{Клпз*Напз}{Fp}, грн \quad (3.5)$$

де P – встановлена потужність ПК, кВт;

C_e – тариф на електричну енергію, грн/кВт година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ — річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання

$С_{мч}$ = 0.7 * 1 *1.68 + ((8900*0.462)/1920) + ((7062*0.2)/1920) = 4 грн

$З_{мч}$= 4* 112 =448 грн

$К_{рп}$ = 448+15680=16128 грн

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість розробки політики безпеки *Крп* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К= К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. гри. Зовнішні консультанти не наймалися ($К_{пр}$=0)

$К_{зпз}$ — вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

Таблиця 3.2.1 – Перелік придбаного Пз

№	Назва	Кількість	Вартість за 1 шт
1	Microsoft Windows 10	7	1050 грн
2	Eset Nod 32	7	122 грн
Всього: $К_{зпз}$ = 8204 грн			

$К_{рп}$ – вартість розробку КЗЗ від ДДоС атак, тис. гри; ($К_{рп}$=16128)

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. гри;

Таблиця 3.2.2 – Перелік придбаного апаратного забезпечення.

№	Назва	Кількість	Вартість за 1 шт
1	Cisco IDS Network Sensor IPS-4255-K9 – IDS система	1	20050 грн
2	CISCO ASA5505-K8 – мережевий екран	1	9222 грн
Всього: $К_{зпз}$ = 29 272 грн			

$К_{навч}$ — витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. гри; ($К_{навч}$ = 800грн)

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. гри. ($К_{н}$ = 900)

К =8204+16128+29272+800+900 = 55304 грн

3.2.1 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

$$С = С_в + С_к + С_{ак}, \text{ тис. Грн} \quad (3.7)$$

Де $С_в$ – Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки. ($С_в$=10248 грн)

$С_к$ – витрати на керування системою в цілому;

Витрати на керування системою інформаційної безпеки **($С_к$)** складають:

$$С_к = С_н + С_а + С_З + С_{єв} + С_{ел} + с_о + С_{тос}, \text{ грн.} \quad (3.8)$$

Витрати на навчання адміністративного персоналу и кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо (Сн=2500 грн).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ); Вартість купівлі ліцензійного ПЗ - 8204 грн., мінімальний срок дії користування - 2 роки

$$С_{а1} = 8204/2 = 4102 \text{ грн}$$

амортизаційні відрахування для апаратного забезпечення

$$С_{а2} = 29272/5 = 5855 \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_З$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.9)$$

Де $З_{осн}$ $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

$$З_{дод} = 87840 * 9\% = 7906 \text{ грн}$$

Основна заробітна плата системного адміністратора персоналу безпеки – ($З_{осн}$ = 7320 грн/місяць)

$$С_з = 87840 + 7906 = 95746 \text{ грн}$$

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати (за узгодженням з консультантом економічної частини дипломного проекту)

$$Сэв=22\%* С_з \quad (3.10)$$

$$0.22*95746 = 21064.12$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р * F_Р * Це \text{ , грн}, \quad (3.11)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$$Р = 0,6 \text{ кВТ} * 7 \text{ комп'ютерів} + 0,9 * 1 \text{ сервер} = 5.1 \text{ кВт}$$

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (працює кожен день с 9:00 до 18:00 10 годин на добу);

FP = 365 днів * 10 годин * 2 (сервер та комп'ютер) + 107 днів * 10 годин *6 = 13 720 год.

Це – тариф на електроенергію, грн/кВт-годин. (Це = 1.68)

$$C_{ел} = 5.1 * 1.68 * 13720 = 117\ 553$$

Витрати на залучення сторонніх *організацій* для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу визначаються за даними організації. ($C_o = 0$)

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($C_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$$K = 55304 \text{ грн}$$

$$C_{тос} = 55304 * 1\ \% = 553.04 \text{ грн}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($C_{ак}$) можна орієнтовно визначити, користуючись даними табл. 1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

C = 10248 + 2500 + 2940 + 4102+ 5855 + 95746 + 117553 + 553.04 +21064.12 = 260 561,16 грн

У кожному конкретному випадку можуть бути враховані й інші види поточних витрат, що визначаються специфікою експлуатації проектованої системи інформаційної безпеки.

3.3 Оцінка Величини збитку

Таблиця 3.3.1 – Заробітна плата працівників

Посада	Кількість працівників	Заробітна плата в місяць, грн	Заробітна плата помножена на кількість працівників
Директор	1	30 000 грн	30 000 грн

Системний адміністратор	1	20 000 грн	20 000 грн
Бухгалтер	2	15 000 грн	30 000 грн
Менеджер	2	14 000 грн	28 000 грн
Фармацевт	1	23000 грн	23 000 грн
Прибиральниця	1	5000 грн	5000 грн
Охоронець	3	8000 грн	24 000 грн

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \quad (3.3.1)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн,

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$Пп = (Зс/F)*tп, \text{ грн} \quad (3.3.2)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

tп — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 24 годин;

$$Пп= (160000/176)*24= 21818 \text{ грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.3.3)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі,

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$: ($t_{ви}$ = 10)

$$Пви = \frac{Зс}{F} * t_{ви} \quad (3.3.4)$$

$$Пви = (20000/176)*10 = 1136 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки $t_В$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів): ($t_В$ = 25)

$$П_{пв} = \frac{Зо}{F} * тв \quad (3.5)$$

$$П_{пв} = (20000/176)*25 = 2840 \text{ грн}$$

$$П_в = 2840 + 1136 + 21818 = 25794 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі: (О=315000)

$$V = \frac{О}{Fr} * (tп + tв + tви) \quad (3.6)$$

$$V = (315000/176) *(25+10+24) = 87698 \text{ грн}$$

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

$$U = 21818 + 25794 + 87698 = 135\ 310 \text{ грн}$$

Таким чином загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$U = \sum i \sum n U \qquad (3.7)$$

Де і – число атакованих вузлів, 1;

N – середнє число атак на рік 4 рази;

$$U = 135\ 310 * 1 * 4 = 541240 \text{ грн.}$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B*R - C \qquad (3.8)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. гри;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 541240 * 0.74 - 174210 = 226\ 307{,}6$$

3.4 Визначення та аналіз показників економічної ефективності

Показник сукупної вартості володіння (TCO) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

У цьому випадку необхідно порівняти сукупну вартість володіння, розраховану для двох варіантів проектного рішення щодо створення або

удосконалення системи інформаційної безпеки, і вибрати варіант із найменшою з них.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$\text{ROSI} = \frac{E}{K}, \text{ частка одиниці.} \quad (3.4.1)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки (розділ 3.2 методичних вказівок, формула 3.8), 226 307,6 грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. гри.

Якщо порівнюється два варіанти системи інформаційної безпеки, то обирається варіант з більшим значенням ROSI.

$$\text{Rosi} = 226307{,}6/55304 = 4{,}09$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності Ен.

Проект системи інформаційної безпеки визнається доцільним за умови

$$\text{ROSI} > E_H \quad (3.4.2)$$

При $\text{ROSI} < E_H$ варіант є збитковим і більш економічним визнається відмова від його реалізації.

Розрахунок бажаного значення коефіцієнта ефективності виконується за узгодженням з консультантом економічної частини.

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій $T_р$.

Термін окупності капітальних інвестицій $T_р$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_о = \frac{E}{K} = \frac{1}{ROSI} \text{ років} \quad (3.4.3)$$

Якщо варіанти економічно рівноцінні, то приймається варіант, що забезпечує більш високу надійність, поліпшення умов праці.

$T_о$ = 55304/226 307,6= 0.244 (приблизно за 3 місяця)

3.5 Висновки

- Капітальні витрати складають: 55304 грн

- Експлуатаційні витрати на впровадження інформаційної безпеки складають: 260 561,16 грн

- Можливий збиток від атаки на вузол складають: 541 240 грн

- Загальний ефект від впровадження системи інформаційної безпеки складає -

Термін окупності капітальних інвестицій - приблизно за 3 місяця

Тому економічна доцільність впровадження політики інформаційної безпеки обґрунтована і може піти на користь підприємству.

ВИСНОВКИ

Об’єктом розробки кваліфікаційної роботи є Автоматизована система ТОВ “Аллергік”.

Під час виконання першого розділу кваліфікайної роботи було висвітлене питання необхідності створення спеціальних умов захисту інформації на підприємстві від DDoS атак, оскільки цей вид атак з великою можливістю можуть використати зловмисники щоб нашкодити будь-якому підприємству в зв’язку з тим що цей вид атак можливо легко реалізувати і не потребує глибоких знань та вмінь.

В ході виконання другого розділу було виконане обстеження об’єкту автоматизованої системи, була проаналізована комп’ютерна мережа компанії, а також розглянуто особливості оброблювальної інформації. Проаналізувавши комп’ютерну мережу та програмне забезпечення були сформульовані основні DDoS атаки які можуть вплинути на мережу, в зв’язку з чим були представлені основні апаратні та організаційні заходи, які допоможуть уникнути DoS-у.

В ході виконання третього розділу підтвердилась доцільність впровадження даних апаратних засобів та програмного забезпечення через отримані дані. В ці дані входить капітальні витрати на введення апаратних засобів та ПЗ, загальний

ефект після впровадження Апаратних засобів та ПЗ, а також період окупності даних інвестицій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Denial of Service Attacks Qijun Gu, PhD. Assistant Professor Department of Computer Science Texas State University – San Marcos San Marcos, TX, 78666 Peng Liu, PhD. Associate Professor School of Information Sciences and Technology Pennsylvania State University University Park, PA, 16802 URL: http://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

2. Основы организации сетей CISCO: Модель OSI URL: http://www.williamspublishing.com/PDF/5-8459-0589-3/part.pdf (дата звернення: 16.06.2021)

3. Orange-business services: Какие бывают DDoS-атаки и почему защищаться сложнее из года в год [Електронний ресурс] URL:https://www.orange-business.com/ru/blogs/kakie-bivayut-ddos-ataki-i-pochemu-zaschischatsya-slozhnee-iz-goda-v-god (дата звернення: 16.06.2021)

4. Selectel.ru: Простое пособие по сетевой модели OSI для начинающих [Електронний ресурс] URL: https://selectel.ru/blog/osi-for-beginners/ (дата звернення: 16.06.2021)

5. Imperva:TCP SYN Flood [Електронний ресурс] URL: https://www.imperva.com/learn/ddos/syn-flood/

6. Netscout IP/ICMP Fragmentation DDoS Attacks [Електронний ресурс] URL: https://www.netscout.com/what-is-ddos/ip-icmp-fragmentation#:~:text=UDP%20and%20ICMP%20fragm entation%20DDoS,the%20packets%20are%20actually%20sent. (дата звернення: 16.06.2021)

7. Netsoout BGP Hijacking DdoS Attacks [Електронний ресурс] URL: https://www.netscout.com/what-is-ddos/bgp-hijacking (дата звернення: 16.06.2021)

8. Hackers.org Slowloris [Електронний ресурс] URL: http://ha.ckers.org/slowloris/

9. Imeprva IP Fragmentation Attack URL: https://www.imperva.com/learn/ddos/ip-fragmentation-attack-teardrop/ (дата звернення: 16.06.2021)

10. Cloudflare UDP flooding attack URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (дата звернення: 16.06.2021)

11. Imperva Ping flood (ICMP flood) URL: https://www.imperva.com/learn/ddos/ping-icmp-flood/ (дата звернення: 16.06.2021)

12. МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ DDOS-АТАК URL: http://ptsj.ru/articles/507/507.pdf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кіль кість	При мітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	Стан Питання. Постановка задачі	21	
6	А4	Спеціальна частина	17	
7	А4	Економічний розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

- Явір 125-18-2.docx
- Явір 125-18-2.pptx
- Явір 125-18-2.pdf
- Явір_125-18-2.pdf (1).p7s

Додаток В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-18-2 Явіра Я.Р.

на тему: «Комплекс засобів захисту автоматизованої системи ТОВ “Аллергік” від низькорівневих DDoS атак на мережевому рівні.»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 80 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення освітлення проблем захисту підприємств які можуть знаходитися під впливом dos, Ddos атак які є великою проблемою сьогодення особливо для багатьох інтернет додатків.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу різноманітних методик виявлення цих типів атак був сформульований найбільш відповідний метод захисту від атак на мережевому рівні.

Практична цінність роботи полягає у тому, що представлений метод захисту є повноцінною можливістю уникнення атак на мережевому рівні та забезпечення доступності інформації підприємства.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Явір Я. Р. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

ДОДАТОК Г. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)