Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

(повне найменування інституту, факультету)

Кафедра телекомунікацій

(повна назва кафедри)

До захисту допущено
В.о. завідувача кафедри
_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)
"04" червня 2020р.

Дипломна робота

на здобуття освітнього ступеня "бакалавр"

(назва ОС)

Спеціальність 172 Телекомунікації та радіотехніка,

(код і назва)

на тему: Розробка рекомендацій щодо забезпечення безпеки в мережі підприємства на основі методів якості обслуговування

Виконав: студент ____4____ курсу, групи _____ТЗ-61_____

(шифр групи)

_____Бондар Олександр Романович_____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник _____к.т.н., професор Романов О.І._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____к.т.н., доцент Созоник Г.Д._____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

(повна назва)

Кафедра телекомунікацій

(повна назва)

Освітній ступінь бакалавр

Спеціальність 172 Телекомунікації та радіотехніка

(код і назва)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

Валерій_ЯВІСЯ

“_22 ”_січня_2020 р.

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

_____Бондару Олександру Романовичу_____

(прізвище, ім’я, по батькові)

1. Тема роботи Розробка рекомендацій щодо забезпечення безпеки в мережі підприємства на основі методів якості обслуговування_____

керівник роботи _____Романов Олександр Іванович, к.т.н., професор_____,

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 30 квітня 2020 р. №924-с

2. Термін подання студентом роботи_____04.06.2020_____

3. Вихідні дані до роботи: , персональний компьютер з операційною системою Windows 10, сервер на базі Ubuntu 18.04, програмний комплекс Fail2ban.

4.Зміст роботи:

1) Основні відомості про мережу підприємства. Обґрунтування важливості забезпечення високого рівня захисту такої мережі.

2) Якість обслуговування в мережі підприємства. Інтеграція якості обслуговування з безпекою в мережі та методи забезпечення безпеки з її допомогою.

3) Програмний комплекс fail2ban. Встановлення та налаштування.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Слайд №1 Актуальність та мета, практична цінність роботи.

Слайд №2 Основні відомості про забезпечення безпеки в мережі підприємства.

Слайд №3 Обгрунтування необхідності забезпечення безпеки в мережі.

Слайд №4 Якість обслуговування в мережі.

Слайд №6 Інтеграція QoS з безпекою.

Слайд №7 Методи забезпечення безпеки з допомогою QoS.

Слайд №8 Програмний комплекс Fail2ban.

Слайд №9 Налаштування та демонстрація роботи Fail2ban.

Слайд №10 Висновки до роботи, напрями подальшого вивчення.

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____01.09.2019_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Збір інформації про мережу підприємства і методи її захисту	17.09.2019-26.09.2019	
2	Написання першого розділу	26.09.2019-13.02.2019	
3	Збір інформації про QoS	13.02.2020-26.02.2020	
4	Збір інформації про методи забезпечення безпеки з допомогою QoS	26.02.2020-26.04.2020	
5	Написання другого розділу	26.04.2020-14.05.2020	
6	Проведення експерименту і написання третього розділу	14.05.2020-29.05.2020	
7	Оформлення результатів	29.05.2020-02.06.2020	

Студент _____ ____Бондар О.Р._____

(підпис) (прізвище та ініціали)

Керівник роботи _____ _ __Романов О.І._____

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи містить 70 сторінок, 32 рисунки, 1 таблицю та 14 джерел.

Метою роботи є формулювання рекомендацій щодо забезпечення безпеки в мережі підприємства методами якості обслуговування.

В роботі розглядаються основні задачі забезпечення безпеки та якості обслуговування в мережі підприємства, а також проводиться експеримент по налаштуванню програмного комплексу Fail2ban на Linux-сервері.

Ключові слова: безпека, якість обслуговування, мережа, IP-пакет, трафік, Fail2ban.

ABSTRACT

The text part of the bachelor's thesis contains 70 pages, 32 figures, 1 table and 14 sources.

The purpose of the work is to formulate recommendations for security in the enterprise network by Quality of Service methods.

The paper considers the main tasks of security and Quality of Service in the enterprise network, as well as an experiment to configure the software package Fail2ban on a Linux server.

Keywords: security, Quality of Service, network, IP packet, traffic, Fail2ban.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

QoS (Quality of Service – якість обслуговування) – якість послуг, що надається мережею, та набір методів управління ресурсами мережі.

Загроза – будь-які події, що можуть бути причиною порушення політики безпеки.

Політика безпеки – сукупність правил та принципів, що регулюють захист і розподіл інформації.

Зловмисник – той хто має намір скоїти протиправну дію.

Мережа – система, що служить для зв’язку двох і більше прикінцевих пристроїв.

IP – протокол маршрутизації мережевого рівня.

TCP/IP – чотирьохрівнева модель передачі даних в мережі. Є практичною реалізацією моделі OSI.

IDS (Intrusion Detection System) – програмний чи апаратний засіб, що виявляє спроби несанкціонованого доступу до мережі.

Кіберзагроза – явища, що створюють потенційну небезпеку у кіберпросторі.

Кібербезпека – захищеність користувача мережі під час використання кіберпростору.

Кіберпростір – інформаційне середовище, що функціонує за допомогою комп’ютерних систем.

ВСТУП

На сьогоднішній день дуже гостро стоїть питання забезпечення безпеки в мережі підприємства. Постійно розвивається технологічна складова, що призводить до вдосконалення старих методів атак на мережу і появи нових. Це викликає необхідність пошуку нових або нетрадиційних методів захисту мережі підприємства.

Об’єктом дослідження є методи забезпечення безпеки в мережі підприємства. Предметом дослідження є забезпечення безпеки в мережі методами якості обслуговування.

Дана тема є недостатньо вивченою. Серед вітчизняної літератури не знайдено жодних матеріалів на дану тематику. Всі дослідження проводяться на основі праць зарубіжних авторів. Дана робота є унікальною працею, оскільки подібних робіт на українській мові не існує. Рівень неграмотності серед спеціалістів по забезпеченню безпеки мереж залишається високим. В роботі піднімаються питання, що є важливими для адміністраторів мереж і допомагають їм підвищити рівень захищеності локальних мереж.

Отримані в роботі результати є корисними для мережевих спеціалістів, і можуть застосовуватись для посилення безпеки в мережі в цілому або на окремих вузлах.

РОЗДІЛ 1. ОСНОВНІ ВІДОМОСТІ ПРО МЕРЕЖУ ПІДПРИЄМСТВА. ОБҐРУНТУВАННЯ ВАЖЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ВИСОКОГО РІВНЯ ЗАХИСТУ ТАКОЇ МЕРЕЖІ

1.1 Характеристика сучасної мережі. Поняття мережі підприємства.

Сучасні мережі, незалежно від їх розміру, вимагають чіткого дотримання норм їх побудови. Вони повинні підтримувати велику кількість додатків і послуг, а також пристроїв з яких складається фізична інфраструктура. Основною функцією мережі є забезпечення доступу до ресурсів всіх пристроїв об’єднаних в мережу. Вимоги до мережі можуть бути різними в залежності від того де саме вона проектується і для кого. Великі підприємства потребують надзвичайно громіздких мереж з максимальним рівнем захисту і безліччю послуг які зменшують вартість обслуговування, полегшують адміністрування, або ж просто необхідні для успішного ведення бізнесу. В той же час для малих підприємств немає дуже суворих вимог до якості виконання мережі. Повільна робота такої мережі не буде мати таких катастрофічних наслідків у порівнянні з мережею великого бізнесу. Однак, можливо сформулювати декілька вимог які повинні бути дотримані в будь-якій мережі, незалежно від її розміру. Для забезпечення вимог користувача, архітектура мережі повинна відповідати чотирьом основним вимогам:

-відмовостійкість

-масштабованість

-якість обслуговування(Quality of Service)(QoS)

-безпека

На рис.1.1. приведена загальна модель архітектури мережі. Термін «архітектура мережі» в даному випадку має на увазі технології, які

підтримують інфраструктуру мережі, а також послуги, правила і протоколи, які служать для передачі даних в мережі.

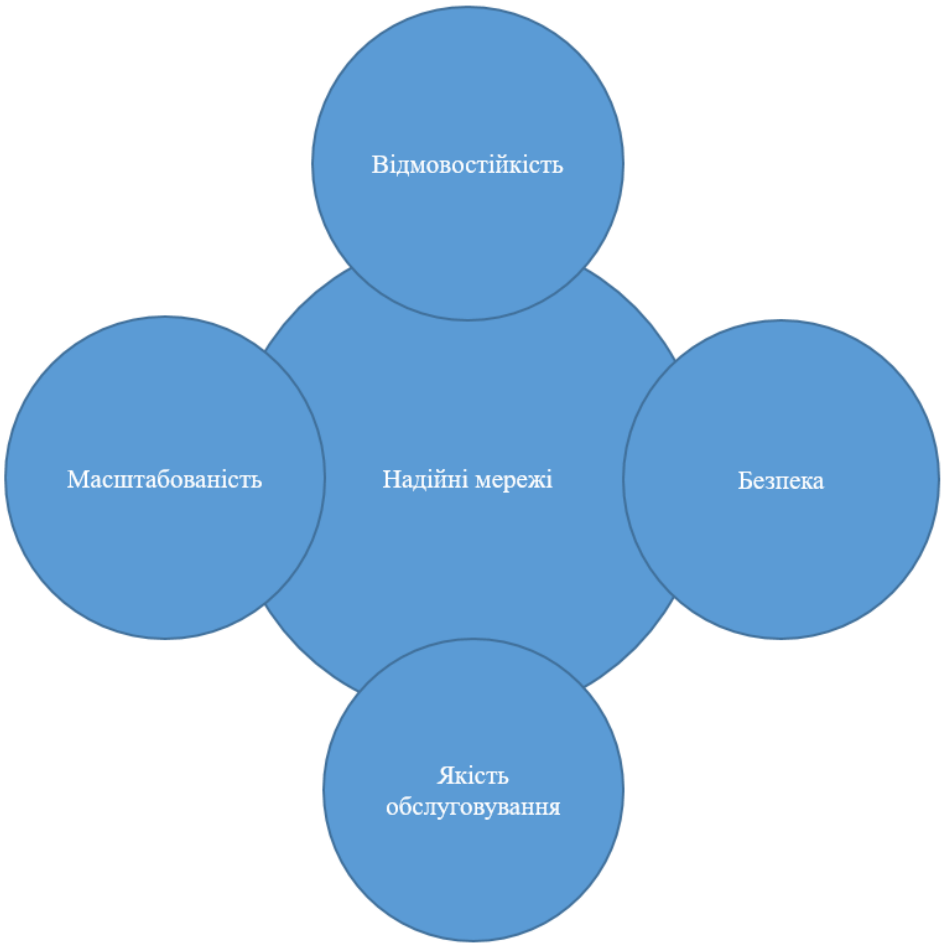

Рис.1.1. Модель архітектури мережі

Необхідно стисло описати, що мається на увазі під цими термінами.

Відмовостійкість означає здатність мережі залишатися працездатною навіть у разі відмови декількох каналів зв'язку. Це означає, що якісно спроектована мережа завжди має декілька шляхів між двома її вузлами. Метод додавання додаткових шляхів передачі даних називається резервуванням.

Під масштабованістю розуміється здатність мережі швидко змінювати свої розміри підключаючи нових користувачів і навіть інші мережі. При цьому існуючи користувачі не помічають зниження продуктивності, і тим

паче не страждають від тимчасової відсутності з’єднання з іншими користувачами.

Якість обслуговування, поруч з безпекою, є основною темою даної роботи. Сам термін може інколи неправильно трактуватися. По суті своїй він означає пріоритизацію трафіку. Тобто певні типи даних мають вищий пріоритет і передаються швидше. Для чого це необхідно? Якщо попит на канали зв’язку перевищує можливості мережі виникає перевантаження каналу. Коли таке трапляється, пакети не можуть одразу потрапити в канал передачі. Пристрої маршрутизації ставлять такі пакети в чергу в буфері пам’яті, до тих пір, доки канал не звільниться. Користувач в цей момент спостерігає велику затримку між запитом, наприклад до серверу, і відповіддю. На практиці це означає, що користувач змушений гаяти час не непотрібне очікування. Для деяких випадків такі затримки допустимі, а от для інших зовсім навпаки. Це не критично, якщо доведеться декілька секунд почекати доки завантажиться поштовий клієнт. Проте такі затримки фатальні при передачі голосового або відео трафіку. Щоб такого не траплялося, якість обслуговування визначає певні типи трафіку які мають вищий пріоритет над іншими. Пакети з голосовим або відео трафіком завжди будуть першими в черзі на передачу, навіть якщо прийшли ну вузол останніми і опинились в кінці довгої черги. Більш детально тема якості обслуговування буде розглянута в наступному розділі.

І нарешті безпека. Найважливіша з вимог до мережі саме для підприємств, особливо для великих. Мережа великої компанії обов’язково повинна бути захищена, так як, вона містить в собі важливу, часто навіть секретну, корпоративну інформацію. Зловмисники легко можуть вдертися в незахищену мережу, викрасти дані, привести мережу в неробочий стан і тим самим зірвати нормальну роботу підприємства, що призведе до значних збитків. Можна виділити два типи проблем з безпекою мережі: безпека мережевої інфраструктури і безпека інформації. Забезпечення безпеки

інфраструктури означає захист всіх пристроїв, що забезпечують підключення до мережі, і попередження несанкціонованого доступу до програмного забезпечення керування, встановленого на них. Безпека інформації означає захист пакетів з даними, що передаються по мережі, а також захист інформації, що зберігається на пристроях користувачів. До захисту інформації існує три основні вимоги: конфіденційність, цілісність і доступність. Інформація повинна бути доступна тільки авторизованим користувачам, інформація не повинна бути змінена або спотворена, до інформації повинен бути своєчасний і надійний доступ відповідно. На рисунку 1.2. представлена так звана тріада інформаційної безпеки, що складається з цих понять.

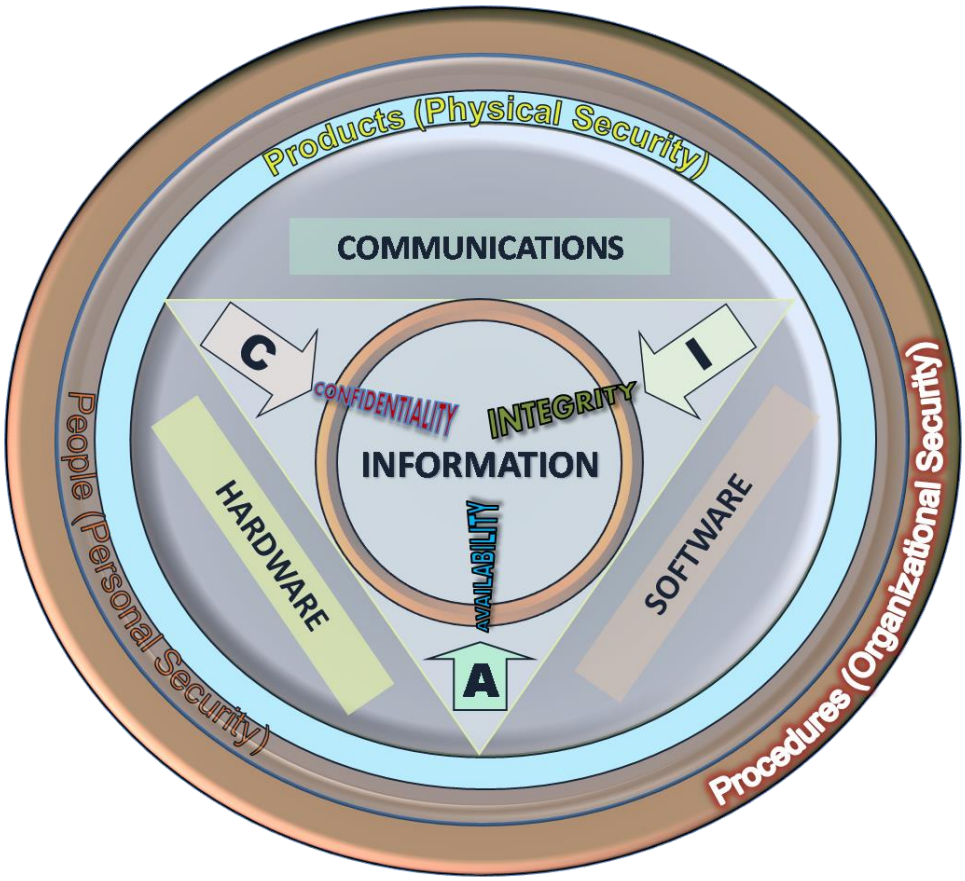

Рис.1.2. Тріада інформаційної безпеки

Тепер слід більш детально розглянути поняття мережі підприємства. Мережа підприємства – це сукупність мереж і служб, призначених для надання захищеного мережного простору користувачам в межах підприємства.[1] Основними особливостями мережі підприємства є:

1) Ті ж самі засоби управління, що використовуються в мережах загального користування.

2) Доступ до інформації надається тільки обмеженій групі користувачів всередині локальної мережі підприємства. Ця локальна мережа відділена від глобальної мережі міжмережевими екранами.

3) Всередині мережі інформація поділяється на три типи. Офіційна (розповсюджується на рівні організації), групова(призначена для використання групою осіб), неофіційна(особиста інформація працівників).

4) Наявність централізованої системи керування мережею.

Биячуев Т.А. в своїй праці[1] надає наступну узагальнену структуру мережі підприємства(рис.1.3.).

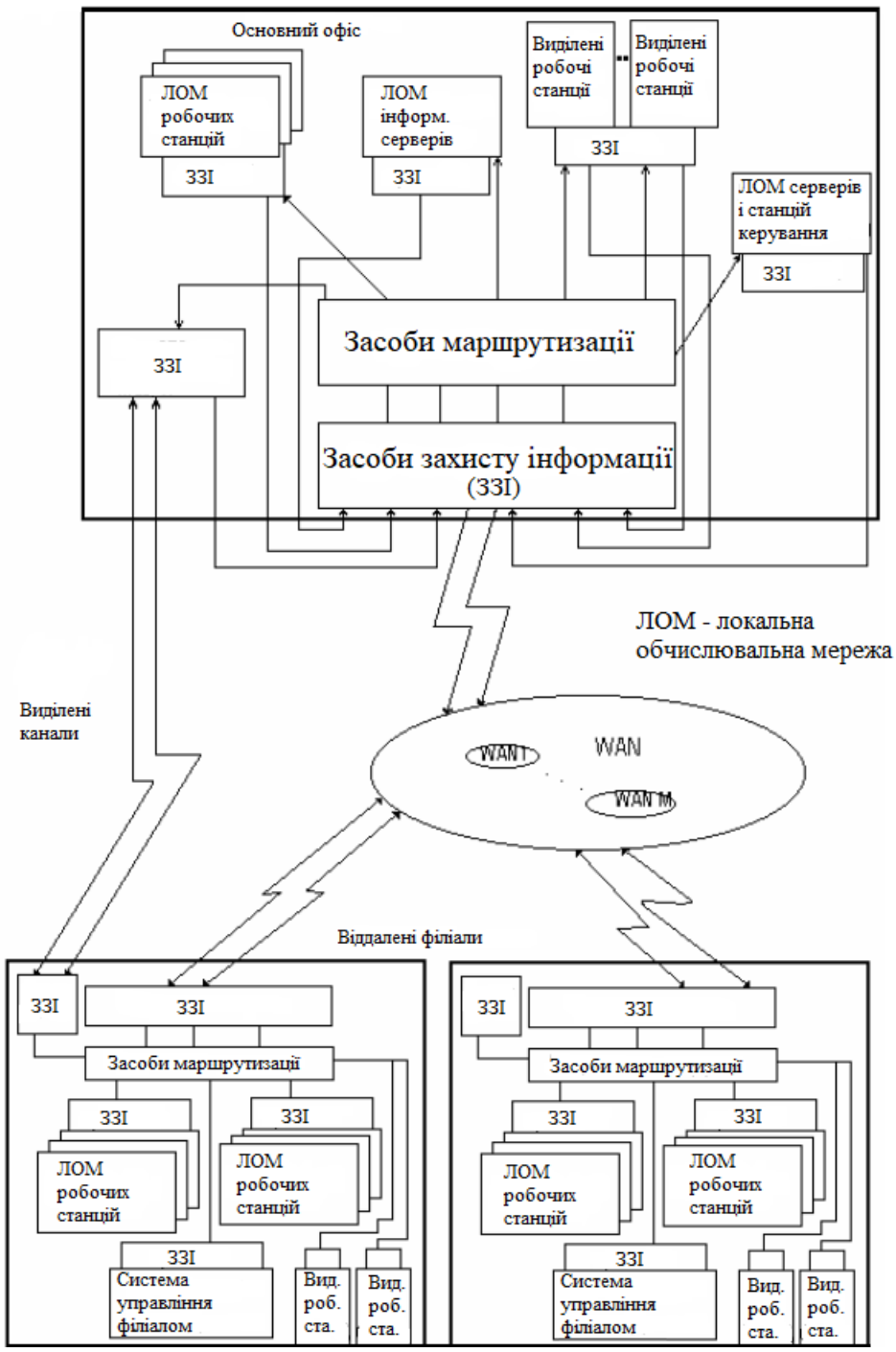

Рис.1.3. Узагальнена структура мережі підприємства

1.2 Законодавство України про безпеку мереж підприємств.

Підприємства бувають різного спрямування. Деякі з них законодавство визначає як «стратегічного значення». Це означає, що зупинка в їх роботі буде мати негативні наслідки для економіки і безпеки держави. До таких належать: електростанції, оборонні заводи, конструкторські бюро і т.д.

Повний список всіх підприємств які мають для України стратегічне значення затверджено в постанові Кабінету Міністрів України від 23 грудня 2004 р. №1734. Зрозуміло, що такі на таких підприємствах безпека мережі повинна бути на найвищому рівні. Так наприклад, 23 грудня 2015 року на енергетичні компанії України з боку Російської Федерація була проведена кібератака, яка паралізувала роботу енергостанцій і перервала енергопостачання для мирних жителів на декілька годин. Детальніше ця подія буде розглянута в розділі 1.4. Наслідки від вимкнення електропостачання взимку можуть бути надзвичайно катастрофічними. Саме тому кожна держава, і в тому числі Україна, на законодавчому рівні закріплює необхідність забезпечення безпеки на підприємствах і урядових установах. В Україні це регулюється законом «Про основні засади забезпечення кібербезпеки України» від 8 липня 2018 р. У цьому законі стаття 5 пункт 4 підпункт 7 визначається необхідність вживання заходів щодо забезпечення безпеки мереж підприємств. В тій же статті пункт 5 наводиться перелік завдань які покладаються на підприємство. Згідно з цим пунктом підприємства повинні[2]:

1) Здійснювати заходи по запобіганню використання кіберпростору у злочинних цілях.

2) Виявляти та реагувати на кібератаки, а також усувати їх наслідки.

3) Обмінюватись інформацією щодо відомих кіберзагроз.

4) Розробляти та реалізовувати відповідні заходи щодо забезпечення безпеки мережі.

На рисунку 1.4. надані вищеперечислені обов’язки підприємств.

Рис.1.4. Обов'язки підприємств по забезпеченню безпеки в мережі

Також в статті 6 пункт 1 детально описано які підприємства відносяться до критичної інфраструктури, а саме[2]:

1) Підприємства енергетичної і хімічної промисловості, транспортні, пов'язані з інформаційно-телекомунікаційними технологіями або ж електронними комунікаціями, крім того, підприємства у банківському та фінансовому секторах.

2) Підприємства, що надають послуги у сфері життєзабезпечення. Постачання електроенергії і газу, водопостачання, виробництво продуктів харчування або медикаментів.

3) Комунальні підприємства, рятувальні служби, та служби екстреної допомоги.

4) Підприємства, яким присвоєно стратегічне значення.

5) Підприємства, що займаються виробництвом небезпечних технологій і продукції.

Детальний розгляд закону «Про основні засади забезпечення кібербезпеки України» не входить до теми даної роботи, але наведеного матеріалу цілком достатньо щоб охарактеризувати підприємства, що мають обов'язково приділяти увагу безпеці локальної мережі, а також, щоб зрозуміти навіщо це робиться і яких саме заходів треба вживати.

1.3 Методи забезпечення безпеки в мережі підприємства. Можливі загрози безпеці такої мережі.

Безпека мережі є не що інше, як набір вимог, які накладаються на інфраструктуру мережі підприємства. Якщо всі вимоги дотримуються, то на виході маємо майже повний захист мережних ресурсів від злому. Тобто, ми попереджуємо несанкціонований доступ зі сторони зловмисників. Звісно захистити мережу повністю не вийде. Технології постійно розвиваються і кожного дня з'являються нові методи злому, що змушує нас шукати нові методи захисту. Та все ж, в наших силах максимізувати рівень безпеки і зробити несанкціонований доступ до мережі надскладним завданням.

Поняття «інформаційна безпека» та «безпека мережі» часто можна вважати ідентичними. Але це не так, розбіжності існують. Безпека мережі – це в першу чергу захист інфраструктури мережі підприємства від зовнішніх загроз. Окрім того, передбачається захист від внутрішніх загроз, тобто необачних або ж навмисних дій працівників[3].

Кіберзлочинці, незадоволені (теперішні і звільнені) працівники, необережні користувачі, всі вони можуть зламати мережу підприємства і поставити під загрозу дані які в ній зберігаються. Мережна безпека складається з обладнання, програмного забезпечення, процедур і політик, які призначені для захисту від зовнішніх і внутрішніх загроз, які потенційно можуть нанести

шкоду мережі. Багаторівневе апаратне і програмне забезпечення може попередити загрози безпеці мережі і унеможливити їх поширення, якщо вони обійдуть ваш захист.

До найбільш поширених кіберзагроз для мереж підприємства можна віднести наступні[3]:

1) Шкідливе програмне забезпечення(ПЗ), віруси, шпигунське ПЗ, рекламне ПЗ, троянські коні.

Це найбільш розповсюджені типи загроз. Їх в мережі Інтернет неймовірна кількість. Неосвічений користувач легко може підхопити вірус на свій комп'ютер з можливістю подальшого зараження всіх вузлів мережі. Їх доволі легко уникнути, проте якщо зараження вже трапилось, то ізолювати його надзвичайно тяжко. Деякі типи вірусів можуть знищити всі дані в мережі повністю паралізувавши його роботу.

2) Атаки нульового дня або ж атаки нульової години(zero hour attack).

Атаками нульового дня називають атаки, що здійснені з використанням вразливості, що не була відома на момент початку атаки. Термін походить від того, що у спеціалістів з безпеки було в розпорядженні нуль днів на усунення вразливості. Це найстрашніша з атак, оскільки проти неї неможливо захиститися. Саме тому всі виробники телекомунікаційного обладнання або ж програмного забезпечення постійно працюють над своїми продуктами, шукають вразливості і виправляють їх. Непомічена виробником вразливість але помічена зловмисником, в результаті призводить до атаки нульового дня.

3) Хакерські атаки.

Будь-які атаки зловмисників, з використанням всіх можливих методів, відомих і невідомих загроз, що направлені на злом мережі з подальшим перехопленням контролю над нею або виведення з ладу.

4) Атаки типу відмова у обслуговуванні(DoS) або розподілені атаки відмови у обслуговуванні(DDoS).

Інколи DoS і DDoS можуть плутати. Хоча абревіатури різняться всього лиш на одну літеру, вони мають різне значення. DoS (Denial of Service) атака являє собою генерацію великої кількості запитів з однієї адреси на певний ресурс (сайт, сервер, тощо) з метою перевантажити його і зробити недоступним для користувачів. Ця атака практично не використовується в наш час оскільки вона надзвичайно легко блокується. Їй на заміну прийшла DDoS (Distributed Denial of Service) атака. Вона проводиться з багатьох мережевих адрес, її потужність надзвичайно велика і її важко заблокувати. Іноді для зупинення такої атаки доводиться забороняти доступ до ресурсу всій країні з якої йдуть атаки. Зазвичай у злочинців є в розпорядженні ціла мережа з інфікованих комп'ютерів(так званий ботнет) які використовуються для генерації запитів. При цьому користувач навіть не підозрює, що його пристрій приймає участь в атаці[4]. Схема атаки на сервер підприємства наведена на рис.1.5.

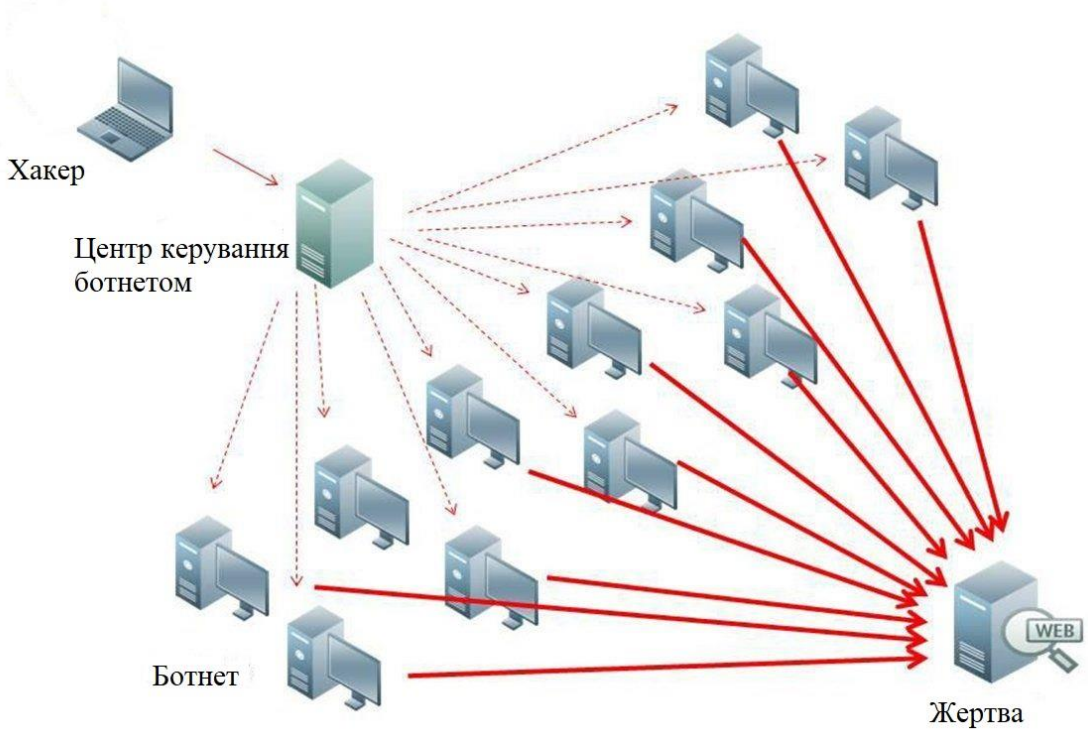

Рис.1.5. Схема DDoS атаки на сервер з використанням ботнету

5) Крадіжка даних.

Атака, ціль якої, заволодіти особистими даними користувачів або секретною корпоративною інформацією. Наносить, тим більше шкоди, чим цінніша інформація була викрадена. Для крадіжки інформації можуть використовуватися всі перераховані вище методи.

На рисунку 1.6. візуально представлені найбільш розповсюджені різновиди кіберзагроз.

Рис.1.6. Різновиди кіберзагроз

Окрім того, працівники підприємства можуть полегшити роботу зловмисникам не дотримуючись норм роботи з мережею(помилки рядових працівників), або не захистивши належним чином мережу(помилка спеціаліста з мережної безпеки). Наступні вразливості можуть стати причиною злому комп'ютерної мережі підприємства[3]:

- незахищені бездротові мережі

- неліцензійне ПЗ

- потенційно небезпечні додатки

- користування незахищеними сайтами

- встановлення слабких паролів

- загублені пристрої які зберегли доступ до мережі підприємства

Можна сформулювати набір загальних правил яких слід дотримуватись як в простих мережах, які не потребують високого рівня надійності, так і в мережах гігантських підприємств, де є нагальна необхідність в найновітніших розробках в сфері безпеки мереж. Ці правила однаково корисні для всіх мереж незалежно від їх розміру, навіть якщо це домашня мережа[3].

1) Завжди слідкувати за оновленнями

Зловмисники використовують вразливості програмного забезпечення для того щоб зламати мережу. Операційні системи та різноманітні додатки постійно оновлюються виправляючи вразливості в безпеці, які можуть бути використані щоб завдати шкоди вашому комп’ютеру, а через нього, і всій мережі. Адміністратор мережі повинен завжди слідкувати за останніми оновленнями і встановлювати їх.

2) Використовувати надійні паролі

Те, що пароль не можна записувати на папірець знає кожен. Але безпека паролів полягає не тільки в тому щоб не тримати їх у всіх на виду. Надійним вважається той пароль, яких складно підібрати, як людям і машинам. Не слід використовувати як пароль загальновідомі слова. Не треба використовувати слова які мають відношення до вас - ім’я, імена домашніх тварин або родичів, назва рідного міста, тощо. Не треба використовувати цифри які мають в собі якусь логіку - дата народження, номер телефону, поштовий код. Найкраще, коли пароль являє собою випадковий набір літер(великих і малих), цифр і символів. Такий пароль надзвичайно складно підібрати і скоріш за все спроби це зробити не залишаться непоміченими. Окрім цього паролі бажано міняти раз в декілька місяців, а адміністратор повинен потурбуватись про те щоб блокувати спроби підбору пароля методом грубої сили. До того треба навчити користувачів розпізнавати методи соціальної

інженерії. Хакер, може видавати себе за інженера технічної підтримки намагаючись визнати пароль у користувача.

3) Обмежити доступ до мережі

Шифрування даних та ідентифікація особи дуже важливі для протидії несанкціонованому доступу. Будь-яке відкрите мережне з'єднання може бути використано кіберзлочинцями для проникнення в мережу. Потрібно впевнитись, що в мережі налаштовані надійні протоколи шифрування і автентифікації. Багатофакторна автентифікація особи є найбільш надійною. Чим більше кроків необхідно для авторизації, тим складніше зловмисникам зламати мережу. Обов'язково слід встановити брандмауер, щоб відділити корпоративну мережу від мережі інтернет.

4) Керувати рівнем доступу користувачів

У кожного користувача повинен бути відповідний рівень доступу. Доступ до критично важливої інформації повинні мати тільки вищі чини. За змінами в ієрархії працівників потрібно слідкувати, своєчасно змінюючи для них рівень доступу. Секретна інформація не в тих руках може мати негативні наслідки для всієї компанії.

Окрім цих основних порад варто згадати ще декілька. Непогано було б вести список дозволених програм які можна завантажувати і заборонити всі інші. Не слід нехтувати політикою безпеки компанії. Політика безпеки - це документ, що визначає сукупність правил і процедур у сфері безпеки, а також задає принципи розподілу цінної інформації. Хорошим способом покращити рівень захищеності важливої інформації є відділення її від основної частини мережі. Постійно відслідковуйте трафік в мережі на предмет наявності незвичайної активності і можливих загроз[3].

Безпека мережі – це велика тема з багаторівневим підходом. Її можна розглядати на канальному, мережевому та прикладному рівні. До поширених проблем тут можна віднести перехват і шифрування пакетів а також помилки

на рівні користувача. Стек протоколів TCP/IP використовується у всьому світі незалежно від характеру організації, будь-то загальна категорія організацій або організація чутлива до рівня захищеності мережі. Протоколи TCP/IP можуть бути перехоплені. Це викликає необхідність всесторонньо забезпечувати безпеку мережі підприємства. Ця робота покладається на адміністратора мережі. Його задача – забезпечити захист всіх частин мережі а також застосувати необхідні заходи безпеки в мережі TCP/IP. Адміністратор повинен точно визначати основні загрози безпеці мережі. Ці загрози можуть різнитися в залежності від характеру діяльності підприємства. В цьому йому допомагають безліч інструментів для моніторингу стану мережі, володіння якими, також входить в його обов'язки[5].

Основною метою мережі є обмін інформацією між її авторизованими користувачами. Як наслідок, небажаний користувач який виявився підключений до мережі може перехопити інформації яка йому не має бути доступна. Є декілька принципів про які повинен пам'ятати кожен адміністратор[5]:

1. Мережа призначена для обміну інформацією. Отже, вона повинна бути налаштована для ідентифікації інформації загального користування і тої яка не підлягає обміну.

2. В мережі повинно бути чітко встановлено хто має право на перегляд дозволеної інформації.

3. Якщо підвищувати рівень безпеки мережі, то і ціна буде зростати. Тому необхідно знайти необхідне співвідношення в залежності від потреб підприємства.

4. Безпека мережі забезпечується не тільки адміністратором, а й користувачами.

4. Вимоги до безпеки повинні бути описані в політиці мережної безпеки.

1.4 Прогнози розвитку кіберзагроз і методів захисту на 2020 рік.

С появою нових технологій з’являються нові загрози, а старі при цьому еволюціонують до більш ефективних варіантів. Спеціалістам з кібербезпеки важливо передбачати напрямки розвитку загроз, для того, щоб завчасно почати готувати методи захисту проти них. В цьому підрозділі приведені коментарі від декількох провідних компаній в сфері інформаційної безпеки. Всі вони є відповіддю на питання: «Які тенденції розвитку кіберзагроз і методів захисту від них на 2020 рік?».

Дослідники BI.ZONE вважають, що основним завданням в 2020 році стане боротьба з крадіжкою інформації. В 2016 році в Європі був прийнятий загальний регламент про захист персональних даних(GDPR), а в 2019 році, після перехідного періоду, він запрацював на повну силу. Він приніс с собою серйозні штрафи за подібні інциденти. Це змушує великі підприємства приділяти більше уваги захисту корпоративної інформації, оскільки викрасти можуть не тільки персональні дані працівників, а й інформацію, що є комерційною або державною таємницею. Підприємства зосередяться на розробці інструментів превентивного захисту і методології розслідування витоків інформації. Іще одним трендом можна назвати загрози безпеці IoT-пристроїв. Їх кількість зростає, але в цьому сегменті дуже мало пропозицій в сфері кібербезпеки. Це призводить до великої кількості абсолютно незахищених пристроїв, що може в майбутньому зіграти злий жарт[6].

Експерти Check Point Software Technologies думають, що кібератаки почнуть більше впливати на діяльність цілих країн. Кібернапади будуть використовуватись як спроби розв’язати конфлікт між малими країнами, що фінансуються великими країнами. Буде зростати кількість атак на комунальні та інші критичні об’єкти інфраструктури. Експерти також передбачають зростання інтенсивності використання технологій на основі штучного інтелекту. Ще в 2016 році перед виборами президента в США почалось розповсюдження підроблених новин з допомогою штучного інтелекту, таке

повториться і в 2020 році. Окрім цього виділяють ще три тренди: зростання кількості атак на мобільні пристрої, зростання фішингових атак, а також збільшення кількості цільових атак на підприємства[6].

Спеціалісти ESET Software вважають, що в 2020 році збільшиться кількість, потужність і тривалість DDoS-атак. Звичайним явищем стають атаки тривалість в тиждень і потужністю 10 Гбіт/с. В новому році зловмисники почнуть активніше використовувати діпфейки – технології підміни голосу і відео в реальному часі, як для обману користувачів так і систем ідентифікації. В зв'язку з зростанням кількості IoT-пристроїв збільшиться кількість вірусів і експлойтів націлених на них. При цьому слід чекати появи продуктів і послуг націлених на захист IoT-пристроїв. Збережеться тренд на розвиток сегменту аутсорсингу інформаційної безпеки і сегменту Security-as-a-Service. Також продовжиться використання сервісів предиктивної аналітики і машинного навчання[6].

Технічний директор Fortinet каже, що в 2020 році очікується розвиток атак, що опираються на штучний інтелект, машинне навчання, розвиток мереж 5G і підвищення швидкості обміну інформацією. Необхідно бути готовим до того, що інструменти проведення атак стануть автоматизованими і зможуть адаптуватись до ситуації. Це підвищить складність їх виявлення. Майбутні загрози будуть активно маскуватися під легітимний трафік. Їх буде складно виявити звичайними методами захисту, однак тут на допомогу приходять механізми QoS оскільки вони дозволяють глибоко аналізувати пакети і виявляти замаскований небажаний трафік. Найбільш розповсюджений тип атак на сьогоднішній день це DDOS і вони нікуди не дінуться, а будуть тільки розвиватись. Відповідно і засоби захисту проти них також ставатимуть більш ефективними[6].

Експерти компанії Oberon вважають, що в 2020 році збережеться націленість хакерів на великі підприємства, хоча вони й почнуть більш ретельно вибирати жертв, тих хто може заплатити великі суми за

відновлення даних. Максимальну зацікавленість у зловмисників викликають біометричні дані користувачів мережі. Це дозволить їм удосконалити методи соціальної інженерії. Як і багато інших аналітиків в Oberon вважають, що інтерес до машинного навчання і штучного інтелекту зі сторони зловмисників буде зростати. Це змушує спеціалістів з безпеки також приділяти значну увагу до цих методів, але вже з метою протистояння таким атакам. В противагу цим словам експерти Positive Technologies говорять, що хакері будуть націлені більше на малі і середні підприємства оскільки вони менш захищені. Також може набрати популярність схема коли хакери зламують мережу підприємства, але самі нічого з нею не роблять, натомість вони продають доступ до цієї мережі третім особам. Також аналітики компанії відмічають, що атаки на особисті пристрої користувачів не втратять своєї актуальності, і навіть можуть стати на порядок складніше в технічному плані. Хто з них виявиться правий, можна буде дізнатися через рік[6].

Дослідники Group-IB вважають головним трендом використання кіберзброї у відкритих військових операціях. Конфлікт між країнами набув нових форм, і кіберактивність відіграє в ньому не останню роль. Атаки на критичну інфраструктуру і дестабілізація мережі Інтернет в країні дозволяють вести безконтактну війну збитки від якої не менше ніж від реального збройного втручання. Сценарії відключення окремих країн від всесвітньої мережі стають все більш реальними, хоча і потребують багато часу на підготовку, однак технічно це можливо реалізувати. Не слід забувати про скоре запровадження 5G. Збільшення швидкостей в мережі полегшить роботу потенційних зловмисників по проведенню DDoS-атак або маніпуляцій з трафіком[6].

Тут приведена лише незначна кількість коментарів, проте проаналізувавши їх всі, можна скласти деяку загальну картину. Найчастіше згадується тематика «інтернету речей». Це не дарма, оскільки розумні пристрої починають з’являтися в кожному домі і питання їх безпеки

ставатиме все гостріше з кожним роком. Зазвичай мала обчислювальна потужність таких пристроїв не дозволяє інтегрувати в них засоби захисту змушуючи шукати інші способи. На пошуках цих способів і будуть зосереджені спеціалісти з кіберпезпеки в сфері IoT. Також в 2020 році може бути багато нововведень в області законодавства пов'язаного з кібербезпекою. Стрімкий розвиток в цій сфері змусить уряд країн посилювати законодавчу базу, щоб змусити бізнес не жаліти грошей на захист своїх мереж. Багато з аналітиків пов'язують майбутнє мережевої безпеки з машинним навчанням і системами штучного інтелекту. В них є велика необхідність в зв'язку з нестачею спеціалістів в сфері безпеки мереж, а правильно реалізована автоматика легко візьме на себе значний шмат роботи, при цьому володіючи швидкістю реакції набагато більшою ніж у людини.

1.5 Відомі випадки міжнародних кіберзлочинів. Їх вплив на економіку країни.

Щоб належно оцінити негативні наслідки погано захищеної мережі слід звернутися до реальних прикладів. Найкраще буде згадати про ситуацію яка трапилась безпосередньо з Україною. Мова йде про кібератаку на українські енергетичні компанії. Вона відбулась 23 грудня 2015 року на фоні неоголошеної війни з Російською Федерацією. Це перша зареєстрована успішна атака на енергосистему країни з виведенням її з ладу. Російським зловмисникам вдалось зламати мережу трьох українських енергетичних компаній[7].

Спочатку слід описати як взагалі проходять подібні атаки. Це буде актуально як для випадку з українськими енергостанціями, так і частково для наступних прикладів. У всіх сучасних енергокомпаній використовуються складні інформаційні системи управління. Такі системи контролюються через мережу. Це робить їх вразливими до кібератак. В даному випадку мова

ведеться про системи диспетчерського управління і збирання даних(SCADA). Атака на таку систему може здійснюватися в трьох основних точках[7]:

- шлюз між мережею підприємства і мережею SCADA

- зовнішні канали доступу до SCADA

- сторонні сервери підключені до SCADA

Такі кібератаки не проводяться за один день. Підготовка може тривати місяцями. Спочатку необхідно інфікувати комп'ютер жертви програмою яка дозволить отримати доступ до мережі. Після успішного інфікування зловмисник починає вивчати і аналізувати структуру мереж автоматизованого управління. Їх вивчення може тривати місяцями, при цьому жертва і не підозрює, що на неї чекає. Після успішного аналізу складових мережі зловмисники переходять до отримання контролю над системами управління. Їх цілями можуть стати наступні вузли мережі[7]:

- головний диспетчерський блок

- робочі станції інженерів

- людино-машинний інтерфейс

- програмовані логічні контролери

Після вивчення протоколів які задіяні в мережі злочинець також може провести спуфінгову атаку, тобто, відправляти оператору підроблені дані або спотворювати їх. Саме за таким сценарієм проходить злам мереж енергетичних компаній. Це вірно і для підприємств іншого призначення, але зі своїми нюансами притаманними тільки їм.

Всього було дві хвилі атак на українські енергетичні підприємства. Перша хвиля була більш масштабною і нанесла більше шкоди. Про неї і буде далі йти мова. Від неї постраждали «Прикарпаттяобленерго», «Київобленерго» та «Чернівціобленерго». Найгірша ситуація була у «Прикарпаттяобленерго», там без електропостачання залишилось близько 230 тисяч мешканців. Атака

на енергосистеми підприємства проводилась з використанням трояньскої програми BlackEnergy. Нею був інфікований термінал одного із співробітників. Після цього на протязі декількох місяців зловмисники зібрали всю можливу інформацію про мережу: паролі, структуру, дані облікових записів. Це дало їм змогу почати змінювати інформацію в мережі на власний розсуд. Вони переконфігурували пристрої безперебійного живлення, потім замінили мікрокод на конвертерах обробки команд на свій власний. Це не давало можливості операторам заново ввімкнути живлення. І нарешті 23 грудня після місяців підготовки вони скористались викраденими обліковими записами операторів і вимкнули живлення. Окрім цього вони здійснили DDoS атаку на кол-центри підприємств, для того щоб користувачі не змогли повідомити про аварію. Масштаби того що трапилось вражають. Якби не своєчасні дії мережевих спеціалістів, то наслідки були б набагато гіршими. Їм вдалось через декілька годин відновити енергопостачання і на протязі доби встановити контроль над системами[7].

Це не єдиний приклад організованої кіберзлочинності. Відомо і багато інших. В квітні 2007 року Естонія була атакована з допомогою DDoS. Цілями були сайти президента, парламенту, міністерств і агентств новин. Також цілями стали деякі банки. Щоб зупинити безупинні атаки Естонії довелось відключити себе від мережі Інтернет. В 2009 році група хакерів, яку підтримував Кремль, була притягнута до відповідальності[8]. В 2016 році були зламані комп'ютери передвиборного штабу Хіларі Клінтон. Це робилось з метою вплинути на президентські вибори В США. В 2008 році Росія вторгається до Південної Осетії і Абхазії, які були частиною Грузії. При цьому урядові і медійні сайти Грузії піддалися масовим хакерським атакам і були пошкоджені. В лютому 2009 року з'явились повідомлення про те, що троян Conficker пошкодив французькі винищувачі, кораблі і підводні човни. Одним з перших випадків нерозкритого кіберзлочину є запуск мережевого вірусу в космічну програму NASA. Через це вони були змушені відкласти деякі запуски супутників[9].

Це не єдині випадки втручання в роботу мережі. Їх тисячі, і з кожним роком їх кількість буде тільки зростати. Наведені вище приклади показують, що зламавши певні мережі, можна порушити політичний баланс певної країни і навіть вивести з ладу її армію. Це доводить необхідність постійного пошуку нових методів захисту мережі і вдосконалення старих.

1.6 Висновки до розділу.

Загрози інформаційній безпеці стають все складніше, хакери і кіберзлочинці використовують нові прийоми і реалізують все більш витончені атаки з метою злому систем і крадіжки даних. Боротьба з новими атаками вимагає рішень по забезпеченню мережевої безпеки і розробки мережевої стратегії безпеки, що відповідає вимогам надійності, вартості та питань інтеграції з іншими IT-системами. Вироблені рішення повинні бути надійними, забезпечувати захист від атак на рівні додатків і дозволяти ідентифікувати трафік. З усього вищесказаного напрошується простий висновок - в сучасному світі не можна ігнорувати питання інформаційної безпеки. У відповідь на нові загрози потрібно шукати нові підходи до реалізації стратегії захисту інформації і використовувати нові методи і засоби забезпечення мережевої безпеки.

РОЗДІЛ 2. ЯКІСТЬ ОБСЛУГОВУВАННЯ В МЕРЕЖІ ПІДПРИЄМСТВА. ІНТЕГРАЦІЯ ЯКОСТІ ОБСЛУГОВУВАННЯ З БЕЗПЕКОЮ В МЕРЕЖІ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ З ЇЇ ДОПОМОГОЮ

2.1 Якість обслуговування в мережі підприємства.

Раніше постачальникам інтернет послуг, великим бізнес-компаніям і підприємствам доводилось створювати і підтримувати окремі мережі для різних типів трафіку. Голос, відео і пошта повинні були передаватися по різним каналам зв’язку. Сучасні мережі підтримують передачу всього потоку даних через один канал зв’язку. Однак сама по собі така мережа не може забезпечити надійну і вчасну доставку пакетів, оскільки вона не розділяє пакети на більш важливі і менш важливі. Вона передає пакети по принципу «перший прийшов – перший пішов». Це призводить до того, що виникають затримки при передачі, наприклад, відеотрафіку, а оскілки він чутливий до затримок, то користувач буде бачити відео в спотвореному вигляді. Результат таких затримок представлений на рисунку 2.1.

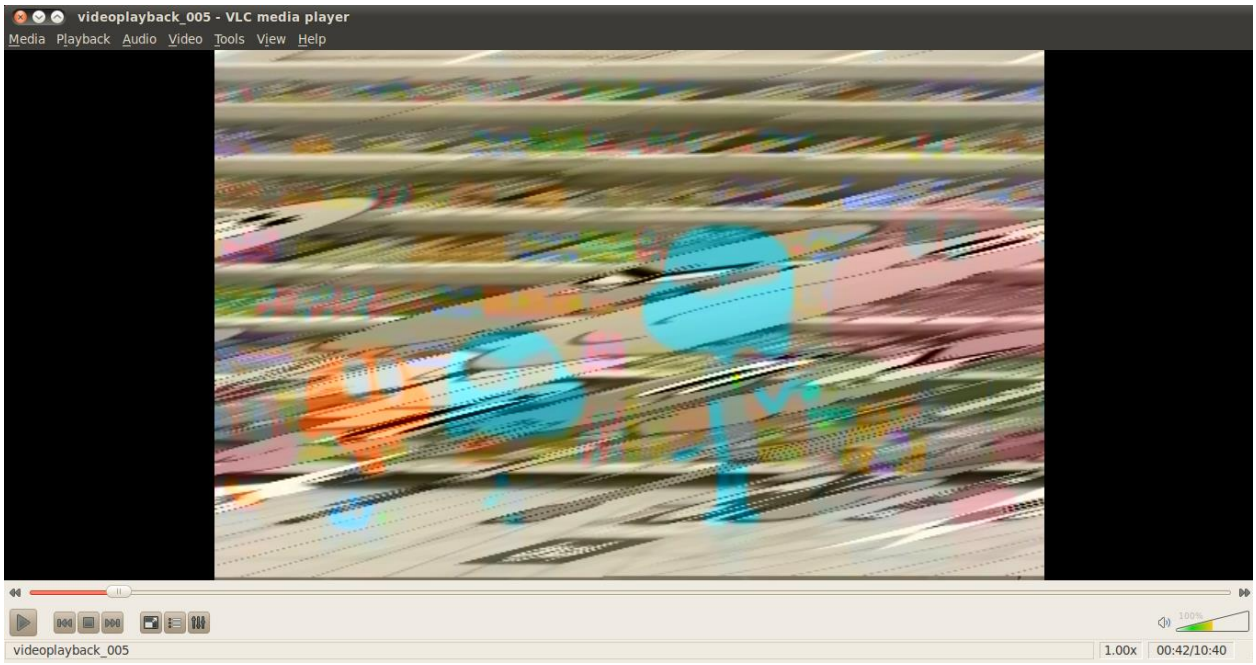

Рис.2.1. Спотворений відеоряд

Для уникнення подібних ситуацій і був розроблений механізм якості обслуговування (Quality of Service, QoS). Функції якості обслуговування в мережі являють собою забезпечення диференційованого і гарантованого обслуговування мережевого трафіку шляхом передачі контролю над використанням ресурсів і завантаженістю мережі її адміністратору. Якість обслуговування є не що інше, як набір вимог до ресурсів мережі при передачі потоку даних. QoS забезпечує гарантію передачі даних, в його основі лежить система правил контролю за засобами підвищення продуктивності мережі, такими як, комутація, маршрутизація, розподіл ресурсів, механізми обслуговування черг і відкидання пакетів[10].

Мережевий трафік складається з багатьох потоків даних згенерованих різними додатками. Ці додатки мають різний набір вимог передачі даних які вони пред’являють до мережі. Здатність мережі забезпечити різні рівні якості обслуговування, що вимагають ті чи інші додатки, може бути класифікована по наступним категоріям:

- Негарантована доставка(best-effort service)

Це означає повну відсутність гарантії доставки. Пакет може бути як доставлений з затримкою, так і взагалі втрачений. Відкидання пакету може трапитись внаслідок переповнення буферу на вхідному чи вихідному інтерфейсі маршрутизатора. Негарантовану доставку не можна вважати частиною якості обслуговування оскільки вона не дає гарантій доставки отже механізми QoS тут не діють[10].

- Диференційоване обслуговування(differentiated service)

Диференційоване обслуговування являє собою розподіл трафіку на класи на основі вимог до якості обслуговування. Кожний тип трафіку обробляється мережею відповідно до заданих до цього класу механізмами QoS. Диференційоване обслуговування саме по собі не передбачає забезпечення гарантій наданих послуг. При цій схемі трафік розподіляється по класам,

кожен з яких має свій власний пріоритет. В зв’язку з цим диференційоване обслуговування іноді називають м’яким QoS[10].

- Гарантоване обслуговування(guaranteed service)

Гарантоване обслуговування передбачає резервування мережевих ресурсів з метою забезпечення вимог до обслуговування потоків трафіку. Виконується завчасне резервування ресурсів на всій дистанції руху трафіку. В зв’язку з такими вимогами гарантоване обслуговування називають жорстким QoS. До додатків, що вимагають гарантованого обслуговування відносять додатки, які передають голосовий і відеотрафік[10].

Рівні якості обслуговування представлені на рисунку 2.2.

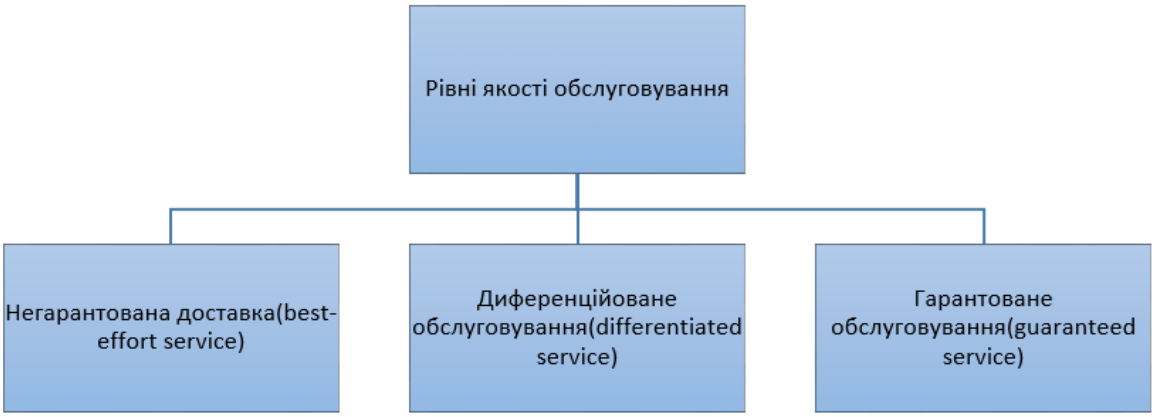

Рис.2.2. Рівні QoS

При керуванні передачею трафіку QoS виконує декілька важливих функцій без яких його робота була б неможлива:

- Класифікація і маркування пакетів

Маршрутизатори виконують функцію класифікації для розпізнавання пакетів, що належать до різних типів трафіку, перевіряючи значення одного або декількох полів в заголовку TCP/IP. Функція маркування пакетів використовується для розмітки класифікованого трафіку шляхом зміни

значення поля IP-пріоритету або поля коду диференційованого обслуговування (Differentiated Services Code Point - DSCP)[10]. Більш детально функція класифікації і маркування буде розглянута далі в розділі.

- Керування інтенсивністю трафіку

Провайдери використовують функцію обмеження мережевого трафіку, що надходить з мережі абонента в залежності від його тарифу. Підприємства використовують функцію вирівнювання для обмеження трафіку, що надходить до інтернет провайдера. Більш детально ця функція буде розглянута далі в розділі.

- Розподіл ресурсів

При відсутності механізмів регулювання QoS обслуговуванням черг займається механізм «перший прийшов – перший пішов» (first-in, first-out - FIFO). Однак, як вже зазначалось раніше, такий підхід має ряд проблем, оскільки не передбачає пріоритетної обробки трафіку чутливого до затримок шляхом переміщення його в чергу з найвищим пріоритетом. Вимога яка пред’являється до алгоритму обслуговування черг – це здатність диференціювати і визначати вимоги до обробки різних пакетів. Алгоритм повинен планувати порядок передачі пакетів в черзі в залежності від їх пріоритету[10]. Приклад розподілу полоси пропускання в мережі без застосування QoS і в мережі де успішно застосовані правила якості обслуговування приведено на рисунку 2.3.

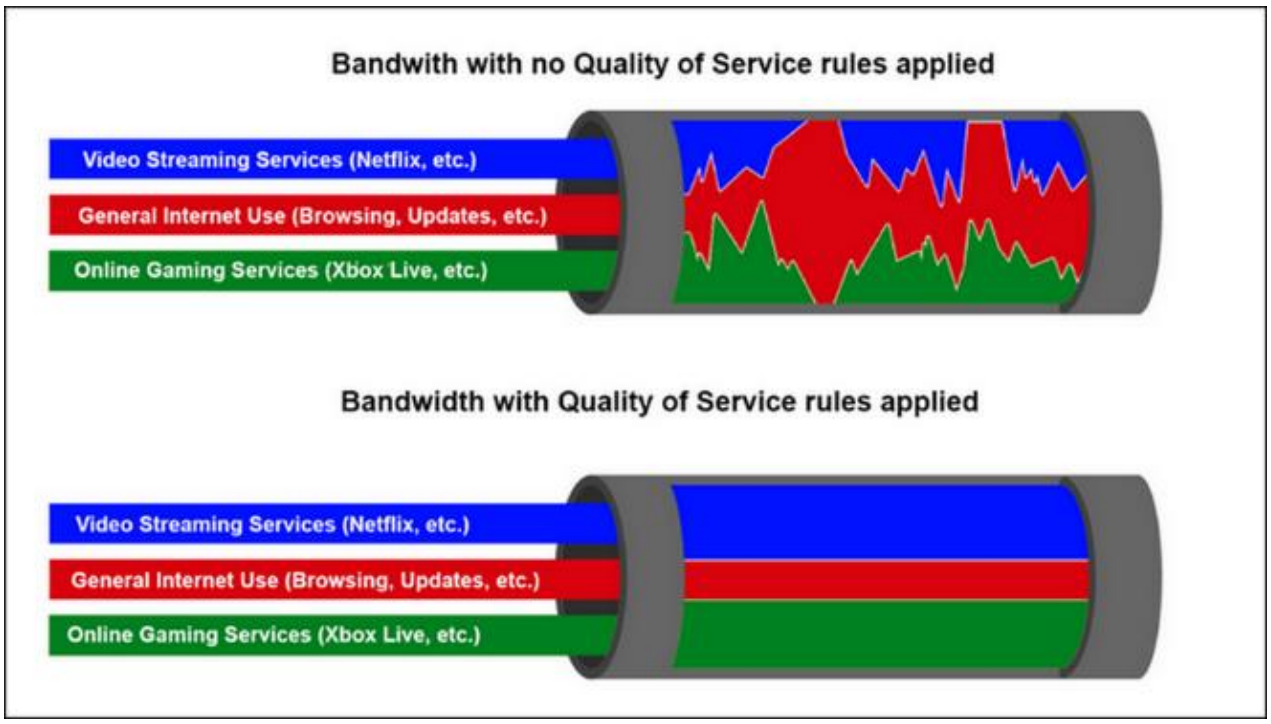

Рис.2.3. Порівняння полоси пропускання каналу зв'язку з QoS і без.

З рисунку видно, що в каналі без QoS весь трафік змішується, і чутливий до затримки трафік передається не достатньо швидко. В свою чергу, якщо механізм QoS застосовано, то полоса частот ділиться між типами трафіку відповідно до вимог, даючи можливість користувачу максимально зручно користуватися мережею.

- Запобігання перевантаженню і політика «відкидання хвоста»

Механізм обслуговування FIFO передбачає відкидання всіх вхідних пакетів після переповнення буферу і перевищення максимальної довжини черги. Такий спосіб керування чергою називається «відкидання хвоста» (tail drop). На жаль даний механізм подає сигнал про перевантаження лише після того як буфер переповнився і не передбачає яких небудь дій по його запобіганню. Однак існують інші активні механізми які в свою чергу здатні це робити і передбачати перевантаження до того як воно трапиться[10].

- Сигнальний протокол QoS

Сигнальний протокол RSVP забезпечує надання наскрізних послуг QoS в масштабах мережі Інтернет. Він дозволяє додаткам сповіщати про вимоги до обслуговування окремих потоків даних.

- Комутація

Одною з функцій маршрутизатора є швидка комутація вхідного трафіку до відповідного вихідного інтерфейсу. Традиційний метод має низьку масштабованість, до того ж його продуктивність може бути дуже низькою при нестабільній роботі мережі. Краще себе показує метод комутації, що враховує топологію мережі. В маршрутизаторах Cisco використовується метод швидкої комутації пакетів (Cisco Express Forwarding - CEF).

- Маршрутизація

Традиційна маршрутизація здійснюється на основі адреси призначення і вибору найбільш короткого маршруту до цілі. Однак іноді цього може бути недостатньо. Маршрутизація на основі політики – це функція якості обслуговування, що дозволяє замінити метод звичайної маршрутизації на метод, що враховує параметри які налаштовує користувач[10].

Функції якості обслуговування представлені на рисунку 2.4.

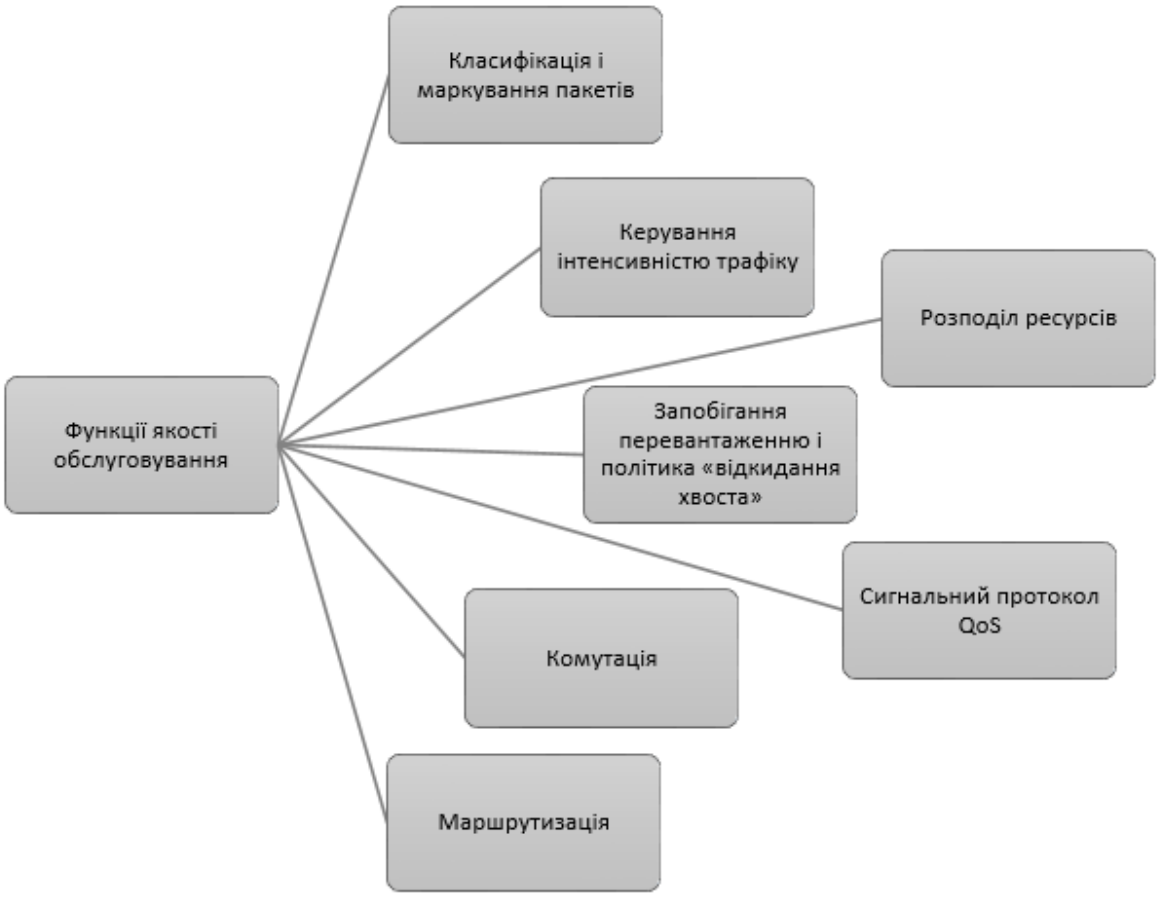

Рис.2.4. Функції QoS

Тепер слід більш детально зупинитись на функціях класифікації та маркування а також керування інтенсивністю трафіку. В загальному їх можна назвати функціями формування трафіку. Вони надзвичайно необхідні для диференційованого обслуговування.

Класифікацією пакетів називається механізм, що дозволяє віднести пакет до того чи іншого типу трафіку на основі одного або декількох полів пакету. Функція розпізнавання може залежати від наступних параметрів[10]:

- адреса джерела, адреса призначення, поля протоколу IP, порт джерела і порт призначення.

- значення поля IP-пріоритету або коду диференційованої послуги(DSCP).

- інші параметри заголовку TCP/IP-пакета, такі як довжина пакету.

- MAC-адреси джерела і призначення пакету.

- номера портів які використовує додаток, адрес URL. В продуктах Cisco це називається методом розпізнання додатків на основі мережевих параметрів(NBAR)

Можна також задати критерії класифікації пакетів на основі списків доступу, їх можна використати для ідентифікації на основі значення поля IP-пріоритету або поля DSCP. Розпізнання додатків на основі мережевих параметрів дозволяє ідентифікувати трафік окремих додатків класифікуючи трафік на основі програмних комплексів, що його генерують. Класифікувати пакети можна також і з допомогою внутрішніх параметрів маршрутизатора, наприклад, ідентифікації на основі вхідного інтерфейсу або поля значення QoS-групи[10].

Маркування пакетів використовується для того, щоб в подальшому такі пакети можна було ідентифікувати. За допомогою маркування в пакет закладаються вимоги які пред’являються до мережі даним типом трафіку. Пакети можна маркувати на основі поля IP-пріоритету, поля DSCP або ж поля QoS-групи.

IP-пріоритет вказує на пріоритет при обробці відповідного пакету. Поле IP-пріоритету складається з трьох бітів одного байту ToS(тип обслуговування – Type of Service). Тобто три з восьми бітів байту ToS відводиться під IP-пріоритет. Структура байту ToS представлена на рис 2.5.

Рис.2.5. Структура байту ToS

P2-P0 це IP-пріоритет, T3-T0 це тип обслуговування, CU – не використовується. В таблиці 2.1 представлені можливі комбінації бітів IP-пріоритету.

Таблиця 2.1

Значення IP-пріоритету	Біти IP-пріоритету	Назва IP-пріоритету
0	000	Стандартний
1	001	Пріоритетний
2	010	Негайний
3	011	Терміновий
4	100	Дуже терміновий
5	101	Критичний
6	110	Міжмережеве управління
7	111	Мережеве управління

Як альтернатива ToS-байту існує DSCP-байт. Структура байту DSCP представлена на рисунку 2.6.

Рис.2.6. Структура байту DSCP

Тут DS5-DS0 це код диференційованої послуги, CU – не використовується.

Маркування за допомогою QoS-групи являє собою поле внутрішньої по відношенню до маршрутизатора структури даних пакету. Воно використовується для маркування пакетів на основі визначених

користувачем критеріїв класифікації. Слід пам’ятати, що воно не входить в заголовок IP-пакету[10].

З метою забезпечення функцій якості обслуговування весь трафік в мережі повинен проходити контроль на її межі, на відповідність його інтенсивності до максимальних можливостей мережі. Якщо інтенсивність буде перевищувати можливості мережі то трапиться перевантаження, що призведе до неможливості забезпечення функцій якості обслуговування для всього трафіка в мережі. Керування інтенсивністю досягається за допомогою функцій обмеження і вирівнювання трафіку. Детальніше вони будуть розглянуті далі в розділі.

Отже, у вузькому технічному значенні, QoS – це набір методів для управління ресурсами мережі: трафіком, канальними ресурсами, буферними ресурсами. Виділимо наступні методи управління ресурсами: TCP – керує швидкістю(flow control), протоколи маршрутизації, засоби керування чергами, засоби обмеження черг, засоби профілювання трафіку. На рисунку 2.7 представлені вище перелічені методи з прикладами технологій які вони використовують.

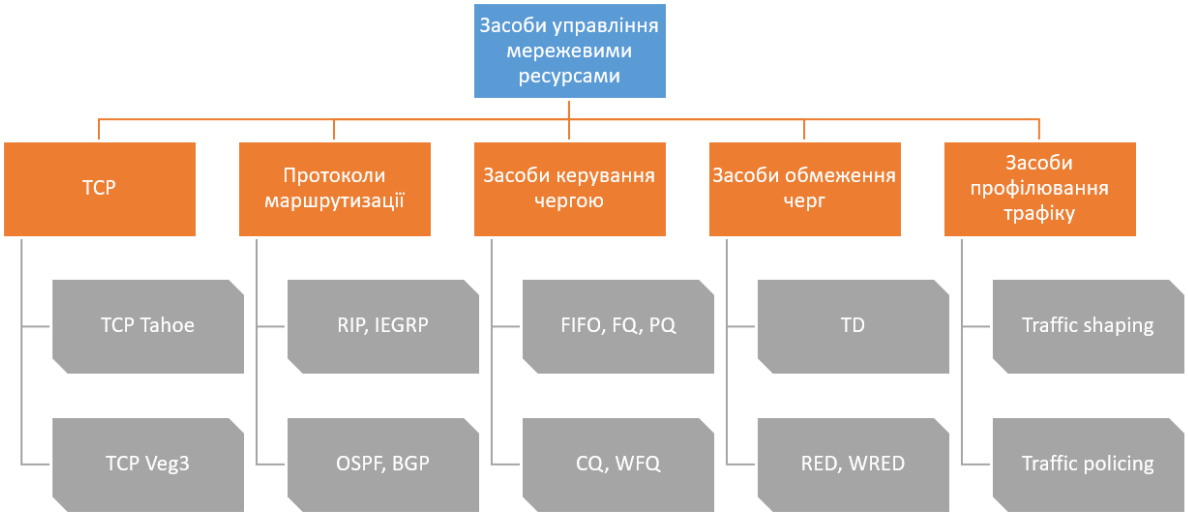

Рис.2.7. Засоби управління мережевими ресурсами

Детальніше зупинимось на засобах керування чергою, обмеження черги і профілювання трафіку.

Частіше за все на мережевих пристроях зустрічаються такі алгоритми обробки черг:

- традиційний алгоритм FIFO

- пріоритетне обслуговування (PQ – Priority Queuing)

- черги з можливістю налаштування (CQ – Custom Queuing)

- зважене справедливе обслуговування (WFQ – Weighted Fair Queuing)

Кожен з цих алгоритмів вирішує свою певну задачу і має місце бути. Алгоритм FIFO вже згадувався раніше. Його принцип полягає в тому, що пакети поміщаються в чергу і передаються в канал зв'язку в тому порядку в якому прийшли. Як вже зазначалось, диференційована обробка пакетів при цьому алгоритмі неможлива. Однак з переваг цього алгоритму можна виділити, що він не потребує конфігурування, оскільки автоматично працює на всіх пристроях маршрутизації і комутації.

Алгоритм PQ розділяє весь трафік в мережі на деяку кількість класів з призначеним їм пріоритетом. Розділення на класи може проводитись різними способами. Деякі способи класифікації розглядались раніше в цьому розділі. Пріоритет який назначається пакету на одному вузлі, може змінюватись під час руху по мережі відповідно до локальних політик. Який би метод класифікації ми не вибрали, на пристрої ми маємо декілька черг відповідно до кількості класів. Трафік потрапляє в ці черги відповідно до свого пріоритету. В першу чергу обробляються пакети, що потрапили в чергу з високим пріоритетом, поки всі пакети в цій черзі не будуть оброблені маршрутизатор не перейде до обробки пакетів з черги з середнім пріоритетом, як тільки закінчиться черга з середнім пріоритетом маршрутизатор почне обробляти чергу з низьким пріоритетом. Такий алгоритм забезпечує високу якість обслуговування для черг з високим

пріоритетом. Трафік в таких чергах завжди отримує ту полосу пропускання, яка йому потрібна. Для інших класів якість обслуговування знижується. Це зниження може бути доволі відчутним, якщо інтенсивність високопріоритетного трафіку велика. Для таких випадків існують інші алгоритми керування чергами, які дають низькопріоритетному трафіку гарантії передачі навіть в періоди великої інтенсивності високопріоритетного трафіку. В зв'язку з цим, пріоритетне обслуговування варто застосовувати в мережах з чутливим до затримок трафіком але невеликої інтенсивності[11].

Алгоритми зважених черг розроблені, щоб для всіх типів трафіку можна було забезпечити необхідний мінімум полоси пропускання. Під вагою мається на увазі доля пропускної спроможності, що виділяється на певний тип трафіку. Якщо ця вага визначається адміністратором, то такий алгоритм називають CQ, а якщо він визначається на основі певної адаптивної стратегії то WFQ. При CQ, як і у випадку з пріоритетним обслуговуванням трафік ділиться на класи з певним пріоритетом. Кожному з них виділяється певний процент від загальної пропускної спроможності каналу зв'язку. Як вже зазначалось мета зваженого алгоритму обслуговування дати низькопріоритетному трафіку гарантії передачі навіть в періоди великої інтенсивності високопріоритетного трафіку. Ця досягається завдяки тому, що черги обслуговуються циклічно і поступово, при кожному циклі з черги забирається число байт, що відповідає вазі черги. В результаті кожен тип трафіку отримує необхідний для нього мінімум[11].

Зважене справедливе обслуговування (WFQ) – це комбінований механізм обслуговування черг який вміщає в себе і пріоритетне обслуговування і зважене. Різні виробники обладнання пропонують свої реалізації WFQ. Найбільш частий випадок, коли існує одна черга, що обслуговується по пріоритетній схемі. Ця черга призначена для системних повідомлень і керування мережею. Всі інші черги обслуговуються алгоритмом зваженого обслуговування. Існують різновиди WFQ, наприклад, в маршрутизаторах

компанії Cisco є CWFQ(class-based) і FWFQ(flow-based). FWFQ створює стільки черг – скільки потоків трафіку існує. Потоки можуть формуватися як по однаковим IP-адресам джерела і призначення, портам, значенням поля ToS. CWFQ має два варіанта реалізації, через класифікацію за допомогою груп QoS, або ж через класифікацію по значенню поля ToS. При першому варіанті адміністратор задає вагу для кожної QoS-групи самостійно, при другому вага класів залишається за замовчуванням[11].

Перед тим, як розглянути засоби обмеження черг слід описати як веде себе протокол передачі TCP при перевантаженні мережі. З метою попередження заторів в мережі TCP використовує «вікно перевантаження», воно представляє собою максимальний розмір даних які може переслати відправник без підтвердження доставки з боку отримувача. З часом розмір цього вікна збільшується, але одразу скидається при виявленні втрати пакетів. Після цього процес поступового збільшення «вікна» починається спочатку, проте більш повільно. Це називається алгоритмом «повільного старту». Традиційна політика обробки пакетів, що не поміщаються в буфер називається tail drop, вона вже розглядалась раніше в розділі. Всі пакети, що не помістились в чергу відкидаються. Це є сигналом для TCP про виникнення перевантаження і розмір «вікна перевантаження» різко скидається до мінімального значення. Оскільки зазвичай пограничні маршрутизатори обробляють одночасно тисячі TCP з’єднань то використання tail drop приводить до втрат пакетів для всіх із них. Це різко зменшує завантаженість черг, проте як ми пам’ятаємо, відповідно до алгоритму «повільного старту» TCP починає знову збільшувати «вікно перевантаження», що врешті-решт призводить до повторного переповнення черг. Це призводить до так званого ефекту глобальної синхронізації, коли розмір черги міняється хвилеподібно[10]. Ефект глобальної синхронізації представлено на рисунку 2.8.

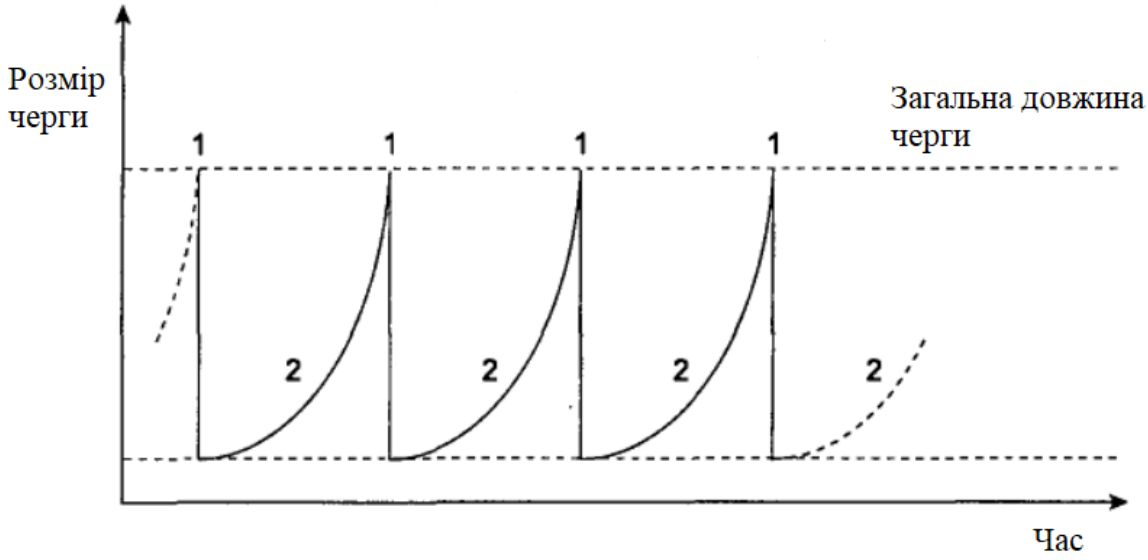

Рис.2.8. Ефект глобальної синхронізації

В момент часу 1 черга переповнюється і розмір «вікна перевантаження» скидається звільняючи чергу. В момент часу 2 алгоритм «повільного старту» починає знову збільшувати завантаженість черги. Це викликає небажану затримку трафіку і зниження пропускної здатності каналу.

Щоб такого не траплялось існують засоби превентивного керування чергами або, як їх було названо, засоби обмеження черг. Вони сигналізують про перевантаження мережі до того як черга переповниться. Мова піде про алгоритм випадково раннього виявлення (RED – Random Early Detection). Механізм RED використовує превентивний підхід для запобігання перевантаженню. Замість того, щоб чекати поки черга переповниться він починає відкидати пакети з певною ймовірністю як тільки середній розмір черги перевищить задане значення. Це означає, що RED відкидає пакети тільки деяких TCP-з'єднань тим самим запобігаючи виникненню ефекту глобальної синхронізації. Якщо розмір черг продовжить збільшуватись, то ймовірність відкидання пакетів продовжить рости. Це мінімізує середній розмір черги, а отже, і загальну затримку трафіку[10].

Алгоритм RED має модифікований варіант під назвою WRED (Weighted Random Early Detection – зважене випадкове раннє виявлення). Алгоритм

WRED має можливість змінювати інтенсивність відкидання трафіку для окремих типів трафіку, наприклад, відкидати менше пакетів голосового трафіку, і більше пакетів http-з'єднань. Окрім цього сам WRED має модифікацію – flow WRED. Оскільки UDP-трафік на відміну від TCP-трафіку не реагує на попередження про перевантаження і не знижує свою інтенсивність. WRED на основі потоку (flow) штрафує потоки, що забирають завелику частину ресурсів[10].

І останнє це засоби профілювання трафіку. Вони керують інтенсивністю передачі даних, тобто швидкістю передачі. Є два види профілювання трафіку – це traffic shaping і traffic policing. Поговоримо спочатку про traffic policing.

Traffic policing обмежує швидкість шляхом відкидання надлишкового трафіку. На рисунку 2.9. показано вплив traffic policing на інтенсивність трафіку.

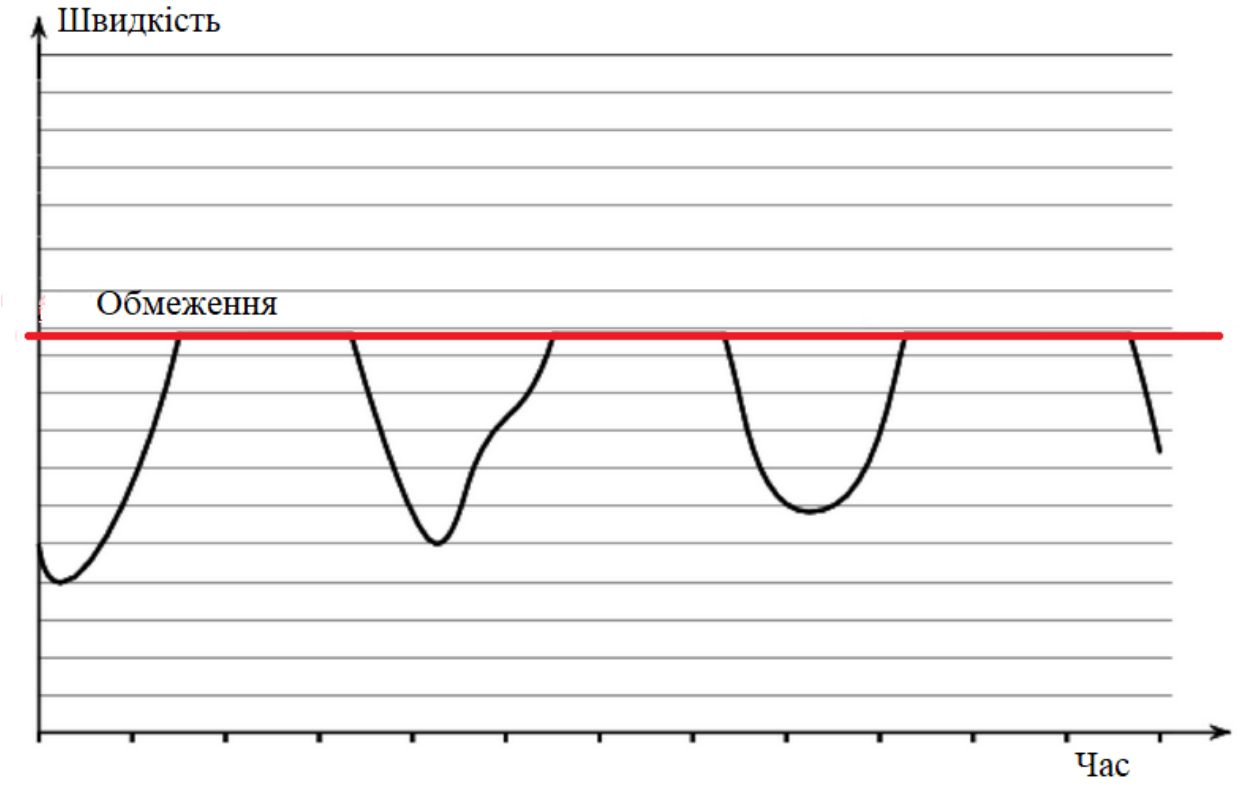

Рис.2.9. Результат застосування політики traffic policing

Це жорсткий варіант traffic policing який називається hard policing. Є також soft policing при якому пакети можуть бути не відкинуті а їм може бути призначений нижчий пріоритет.

Traffic shaping обмежує швидкість шляхом переміщення надлишкових пакетів в буфер з подальшою їх передачею. На рисунку 2.10. показано вплив traffic shaping на інтенсивність трафіку.

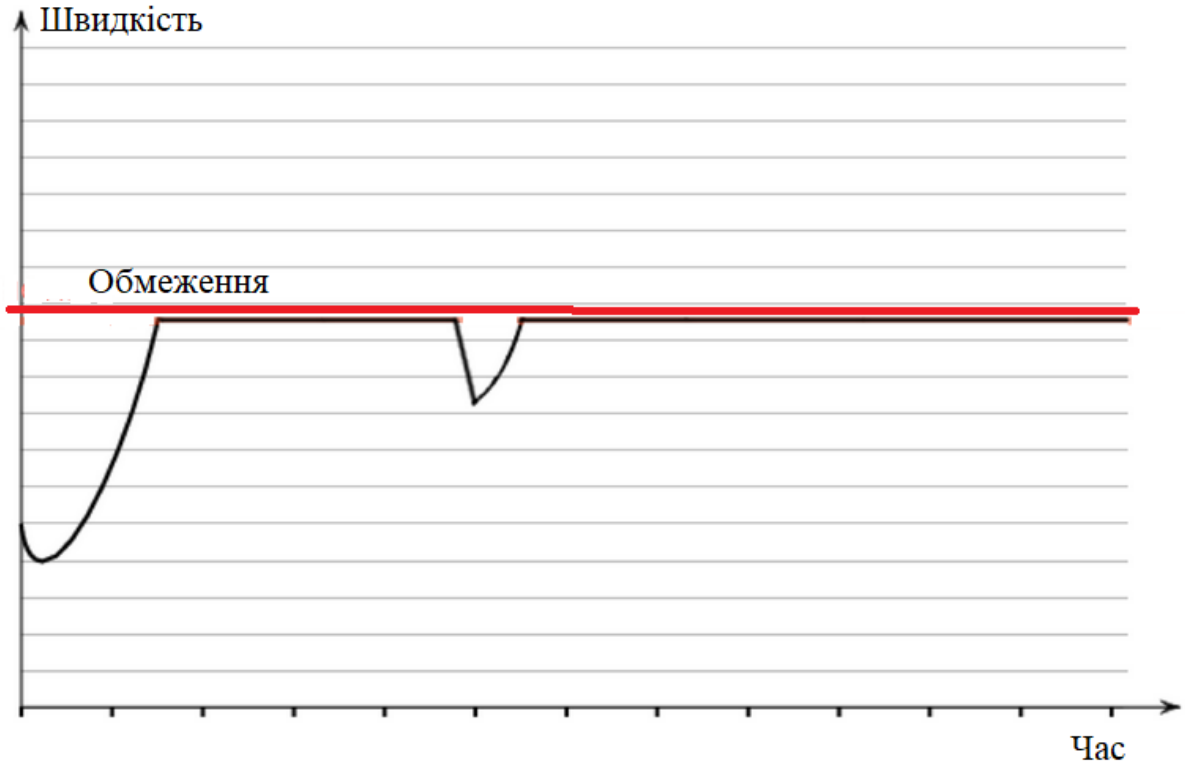

Рис.2.10. Результат застосування політики traffic shaping

Тобто, замість того щоб відкидати надлишкові пакети, ми переміщуємо їх в буфер де вони чекають своєї черги на передачу. Таким чином ми нівелюємо періодичне перевищення допустимої межі інтенсивності трафіку передаючи надлишкові пакети в період коли інтенсивність трафіку низька, гарантуючи при цьому доставку всіх пакетів. Порівняння traffic shaping і traffic policing показано на рисунку 2.11.

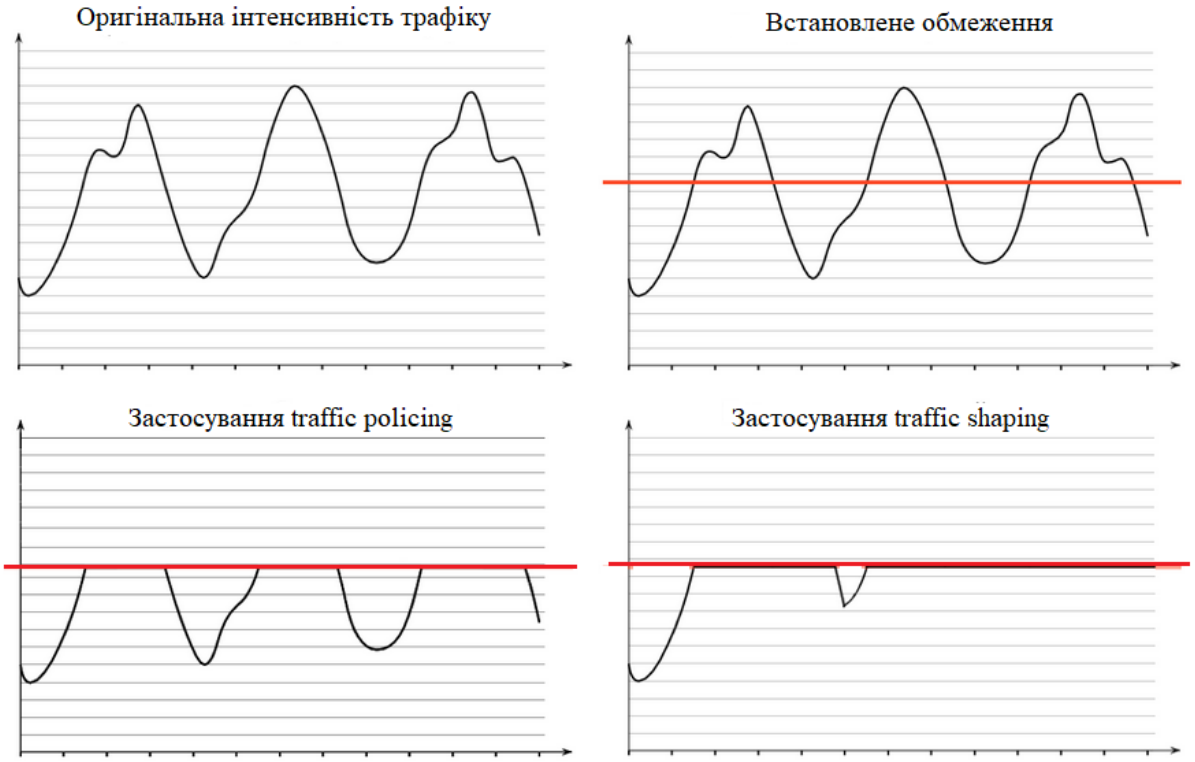

Рис.2.11. Порівняння traffic shaping і traffic policing

Обидва методи мають свою область застосування. Додатки, які нечутливі до затримок, але для яких небажані втрати пакетів краще обмежувати з допомогою traffic shaping. Додатки які чутливі до затримок краще обмежувати з допомогою traffic policing оскільки передати відкинутий пакет заново може бути швидше ніж чекати доки пакет буде переданий з великою затримкою.

2.2 Інтеграція QoS з засобами забезпечення безпеки.

Історично, налаштування параметрів безпеки та якості обслуговування в мережі велось окремо. Однак механізми захисту вимагають додаткових ресурсів мережі, часто впливаючи на загальний рівень QoS. Під час спроб інтеграції QoS з безпекою почали вводити термін «Quality of Protection» - якість захисту, що означає забезпечення належного рівня захисту в мережі

при мінімальному впливі на якість обслуговування. Далі буде розглядатися робота [13], в якій пропонується новий підхід до безпеки та QoS в мережі, так званий QoS^2. Його ідея полягає в налаштуванні такого механізму який керує одночасно і якістю обслуговування і безпекою. Якщо рівень загрози високий то заходи з безпеки посилюються, якщо ж мережі нічого не загрожує, більше ресурсів виділяється на забезпечення якості обслуговування. Механізм визначає рівень загрози мережі на основі брандмауера і системи виявлення вторгнень (IDS – intrusion-detection systems). Він постійно повідомлення вузлів мережі і оновлює рівень загрози. Відповідно до цього рівня механізм встановлює необхідну комбінацію якості обслуговування і безпеки. Якщо для певного рівня безпеки вимоги QoS не можуть бути задоволені, блок управління політикою безпеки / QoS дає запит на ослаблення безпеки. Навпаки, якщо мережа під загрозою потенційної атаки, і система рекомендацій з безпеки рекомендує найвищий рівень безпеки, система повинна дотримуватися рекомендованого рівня, хоча це рішення може поставити під загрозу необхідний рівень забезпечення QoS. Таким чином, ослаблення QoS (наприклад, адаптація швидкості передачі) стає обов'язковим в такому випадку[13].

В тій же праці[13] надається пояснення яким самим чином вибираються і комбінуються рівні безпеки та QoS, а також проводиться моделювання для оцінки ефективності QoS^2. При цьому порівнюються статичне налаштування параметрів безпеки з динамічним налаштуванням за допомогою QoS^2. Для прикладу, при імітації по мережі передавався відеотрафік. Повний опис експерименту також наведено в праці[13]. Однак зазначимо тут результат дослідження. Найкращий рівень якості обслуговування забезпечується при найнижчому рівні безпеки. Однак це може бути недопустимо з точки зору безпеки. Коли рівень безпеки відповідає найвищому, то продуктивність передачі відеотрафіку значно зменшується, оскільки в буфері не вистачає місця, і відповідно, швидкість передачі даних є дуже низькою. У порівнянні з цими двома підходами, представлений QoS^2 забезпечує прийнятний рівень

безпеки і одночасно надає високу якість QoS, аналогічну або близьку тій, яка досягається при найнижчому рівні безпеки. Приведені результати моделювання показують, як система QoS^2 вирішує конфліктні вимоги QoS і безпеки, і демонструє, що адаптація рівня безпеки у відповідності з вимогами QoS дає задовільні результати. Хоча для більш високого рівню загрози механізм може рекомендувати більш високий рівень безпеки, навіть якщо при цьому не забезпечується достатній рівень QoS[13].

2.3 Роль якості обслуговування в забезпеченні безпеки мережі.

До недавнього часу якість обслуговування ніяк не відносилась до забезпечення безпеки в мережі. Але вони мають деякі спільні риси. Певні типи атак на мережу впливають на продуктивність додатків, а забезпечення їх продуктивності це задача QoS. Таким чином, механізмам QoS потрібно відповідним чином реагувати на такі загрози, щоб забезпечити прийнятну якість обслуговування. Віруси, троянські програми або DDoS-атаки, всі ці види загроз швидко реплікують фрагменти коду або ж запити додатків до точки в мережі, де вони перевантажують певний вузол. Міжмережеві екрани і системи виявлення вторгнень (IDS – intrusion-detection systems) зазвичай ідентифікують шкідливий трафік на основі фрагментів коду або деяких параметрів в заголовку IP-пакету. В той же час складні засоби керування трафіком які доступні QoS, як програмно так і апаратно, розпізнають трафік на основі додатків, користувачів, протоколів, адрес керування доступом до середовища, IP-адрес та інших гранулярних складових. Продукти безпеки і QoS вже використовують спільні списки контролю доступу (ACL), щоб обробляти трафік по одним правилам. І якщо продовжувати інтеграцію то IDS, як тільки буде виявляти небажане втручання, буде попереджувати механізми QoS про те, що цей потік даних потрібно обробляти відповідно до політики обробки небажаного трафіку. Об’єднання брандмауерів, IDS і QoS дає додаткові методи пошуку загроз і боротьби з ними. Основною метою QoS

є керування продуктивністю додатків, і виділення їм певної полоси пропускання. Для цього продукти QoS класифікують і обробляють трафік відповідно до політик, що діють в мережі. Наприклад, можна налаштувати мережу так, що деякому додатку 1 виділяти тільки 128 Кбіт/с, голосовому трафіку виділити 512 Кбіт/с, в додаток 2 взагалі заблокувати. Маючи такі можливості можна виявляти аномальні потоки трафіку, а потім застосовувати політики для автоматичного пом'якшення їх впливу на мережу. Брандмауер зазвичай розгортають на границі мережі, щоб контролювати доступ на основі ACL. В свою чергу IDS сканує потоки трафіку на предмет шаблонів, що вже були ідентифіковані як шкідливі. QoS же може виконувати частину кожної з цих функцій, забезпечуючи при цьому відповідну обробку підозрілого трафіку[14].

За допомогою певних програмних засобів, наприклад PacketShaper QoS, можна виявляти з яких IP-адрес надходить небажаний трафік а потім блокувати ці адреси, або ж, виділяти їм мінімальну полосу пропускання, щоб мінімізувати їх вплив на мережеві ресурси. Схожим чином можна встановити правила для порту на який надходять пакети від шкідливого додатку. Для порту можна мінімізувати трафік який він може використовувати, тим самим зменшивши вплив додатку на мережу. Політики QoS можна використовувати як тимчасовий захист. Доки загроза не стане вивчена, а відповідні системи захисту не запрограмують на її усунення, QoS може ідентифікувати шкідливі потоки трафіку і заблокувати їх, або зменшити їм полосу пропускання[14].

Якщо взяти для прикладу вже розглянуті засоби керування чергою, такі як PQ або CQ, то можна запропонувати наступну методику захисту мережі. Спочатку налаштовуємо потрібний нам механізм керування чергою. Визначаєм для кожного типу трафіку його пріоритет. У нас буде існувати високопріоритетний трафік і низькопріоритетний трафік. Слід пам'ятати, що адміністратор мережі може самостійно налаштувати які типи трафіку який пріоритет матимуть. В умовах відсутності загроз наша мережа буде

працювати в звичайному режимі. Як тільки певна загроза з’явиться, будь-то DDoS-атака, силовий підбір паролів на вузли мережі, або ж, поява додатків які буде заборонено політикою підприємства, адміністратор може швидко змінити політику керування чергами в мережі. Можна виявити і згрупувати IP-адреси з яких проводиться DDoS-атака чи силовий підбір паролів, або ідентифікувати порт на який надходить трафік від небажаного додатку, і помістити трафік який надходить з цих адрес або портів в чергу з низьким пріоритетом. Таким чином ми мінімізуємо вплив шкідливого трафіку на мережу. DDoS-атака просто не буде ефективною оскільки виділена їй полоса пропускання буде мізерною. Як радикальний варіант можна взагалі заблокувати трафік, що надходить з цих адрес та портів, але такий метод не завжди може бути використаний, оскільки сучасна мережа Інтернет побудована таким чином, що одну адресу можуть використовувати безліч людей. Адреса з якої надходить небажаний трафік використовується не тільки зловмисником. Це можливо завдяки технології NAT (Network Address Translation) яка дозволяє на границі мережі перетворювати всі приватні IP-адреси в одну публічну. Заблокувавши її, ми залишимо багато людей без доступу до нашої мережі, інколи цілі регіони країн. Саме тому просте зменшення пріоритету трафіку, що призводить до зменшення полоси пропускання для нього, є гарним варіантом боротьби зі зловмисниками. Поки спеціалізований захист, ще не був налаштований для протидії певному додатку чи атаці, ми можемо зменшити їх вплив на мережу і дочекатись поки захист не буде реалізований на брандмауерах чи IDS. Таким чином додання QoS в арсенал безпеки створює іще одну лінію захисту мережі від вторгнень.

2.4 Висновки до розділу.

В розділі були розглянуті механізми якості обслуговування в мережі. Була обґрунтована необхідність застосування механізмів QoS поруч з механізмами забезпечення безпеки. Загрози стрімко розвиваються, це викликає нагальну

необхідність в додаткових способах захисту мережі. Інструменти якості обслуговування чудово підходять на цю роль. Можливість QoS проводити глибокий аналіз трафіку і широкий набір способів керування трафіком, дозволяють QoS виступати як один із можливих засобів захисту мережі від потенційних зловмисників. QoS можна налаштувати для захисту мережі від невивченої загрози, ще до того, як звичайні інструменти забезпечення безпеки будуть налаштовані для її виявлення. Все перелічене робить QoS, в інтеграції з традиційними засобами безпеки, надзвичайно потужним інструментом протидії вторгненням в мережу.

РОЗДІЛ 3. ПРОГРАМНИЙ КОМПЛЕКС FAIL2BAN. ВСТАНОВЛЕННЯ ТА НАЛАШТУВАННЯ

3.1 Встановлення та налаштування Fail2ban. Опис принципу роботи.

Будь-який сервіс підключений до Інтернету може бути атакований зловмисниками. Якщо до нього потрібна автентифікація то неавторизовані користувачі і боти будуть намагатись проникнути в систему шляхом підбору даних автентифікації. Поширений приклад – SSH. Він є ціллю ботових атак, завдання яких, підібрати логін і пароль. Fail2ban пом’якшує такі атаки. Fail2ban – це програмний комплекс, що працює в середовищі Linux, призначений для виявлення і запобігання спробам вторгнення в систему, підключену до мережі. Він динамічно змінює правила брандмауера, щоб заборонити адреси які намагаються підібрати дані для входу. Основна ідея Fail2ban – це відслідковування журналів певних сервісів з метою виявлення шаблонів в збоях автентифікації. Коли Fail2ban налаштовано він переглядає фільтр для конкретної служби. Фільтр призначений для виявлення збоїв автентифікації для конкретного сервісу за допомогою набору правил. Fail2ban має фільтри для всіх поширених служб. Але навіть якщо якийсь фільтр відсутній, його можна створити самому. Коли рядок у файлі журналу збігається з правилом в фільтрі, то виконується певна дія (action), визначена для цієї послуги. Action – це змінна, яка може бути налаштована на виконання певної дії, в залежності від уподобань адміністратора. За замовчуванням action забороняє IP-адресу зловмисника шляхом зміни правил брандмауера iptables. Action можна модифікувати для роботи з іншими брандмауерами. При стандартній конфігурації IP-адресу буде заблоковано при трьох невдалих спробах автентифікації на протязі 10 хвилин. Всі ці параметри можна змінювати, при чому окремо для кожної служби. Для забезпечення такого функціоналу Fail2ban використовує інструмент QoS, керування чергами. Як тільки Fail2ban запущено і налаштовано на захист

певної служби, наприклад SSH, він створює нову чергу. Він додає нове правило до вхідної черги, що пересилає весь TCP трафік спрямований на порт 22 до нової черги. В свою чергу в новій черзі він додає правило яке пересилає трафік назад до вхідної черги. Це змушує трафік, перед тим як пройти далі, спочатку пройти через чергу створену Fail2ban. Це не впливає на нормальне переміщення потоків трафіку, але як тільки фіксується спроба силового підбору даних автентифікації, Fail2ban додає правило в нову чергу, що заборонить трафік від певної IP-адреси. З точки зору архітектури Fail2ban представляє єдину систему "кліент-сервер". Серверна частина - fail2ban-server – це багатопотокова програма, яка прослуховує Unix-сокети, очікуючи надходження команду та відправляючи клієнту необхідну інформацію. Це все відбувається в режимі реального часу. Сам сервер не має жодної інформації про поточний статус файлів конфігурації, тому при запуску знаходиться в стані "за замовчуванням". Клієнтська частина - fail2ban-client - це інтерфейсний компонент для всіх підсистем. Клієнт встановлює з'єднання через сокет сервера і відображає через нього команди для конфігурації сервера і виконання необхідних операцій. Клієнт може зчитувати та передавати вміст конфігураційних файлів або просто надсилати на сервер одну команду, використовуючи для цього командну строку.

Проведемо експеримент по встановленню і налаштуванню Fail2ban. Для цього змоделюємо ситуацію. Ми системний адміністратор одного з філіалів підприємства. Нещодавно в нашій мережі було розгорнуто сервер на базі Linux. Сервер підключений до мережі Інтернет, що робить його вразливим до атак ззовні. Наша задача захистити підключення до серверу за допомогою SSH, щоб зловмисники не могли зайти на наш сервер. На рисунку 3.1. представлена схема локальної мережі філіалу.

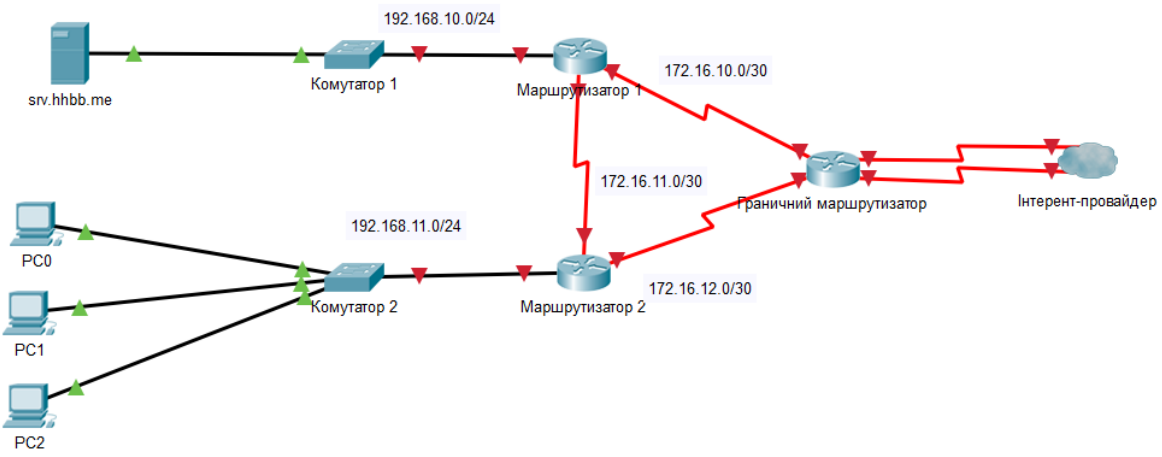

Рис.3.1. Схема локальної мережі філіалу підприємства

Сервер знаходиться в мережі 192.168.10.0/24. Його доменне ім’я srv.hhbb.me. Це реальний сервер, він може бути знайдений в мережі. На момент написання роботи він увімкнений і функціонує. Приступимо до захисту нашого сервера. Перш за все підключимось до нього за допомогою SSH.

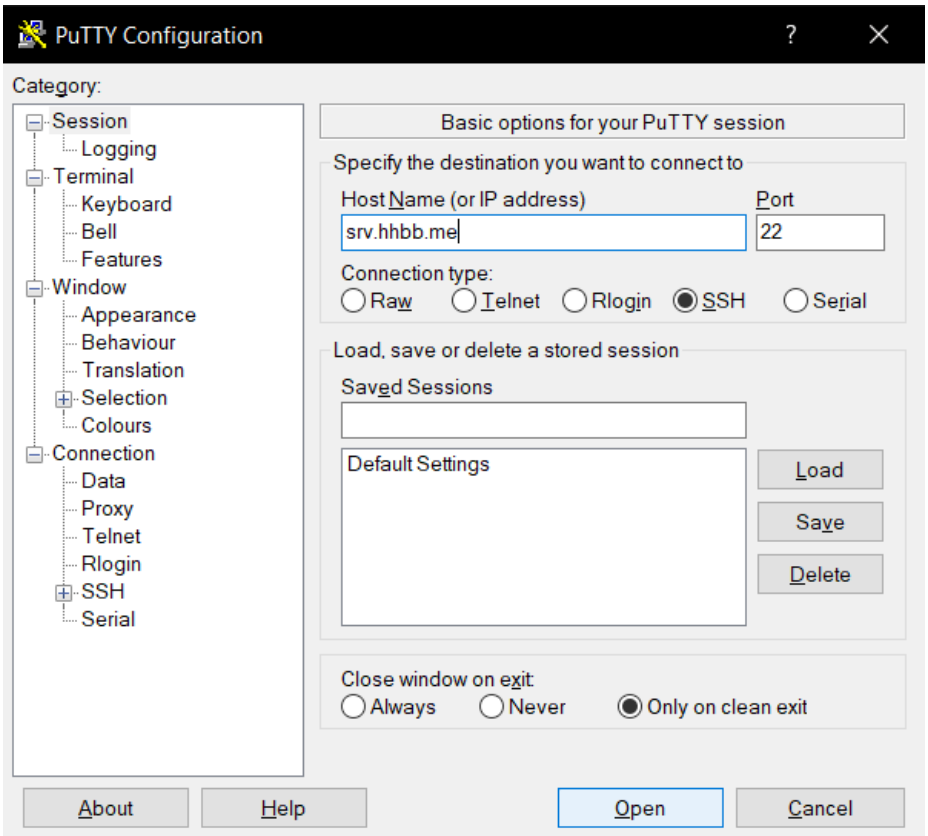

Рис.3.2. Підключення до серверу

Отримаємо запит для вводу логіну і паролю.

Рис.3.3. Вікно автентифікації

Як адміністратору, нам відомий необхідний логін і пароль. Однак зловмисники за допомогою бот-програм можуть спробувати підібрати його. Щоб цього уникнути необхідно налаштувати проти них захист. Встановимо Fail2ban.

Рис.3.4. Команда для встановлення fail2ban

Перевіримо чи правильно встановилась програма за допомогою команди **systemctl status fail2ban.**

```
root@srv:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset:
   Active: active (running) since Tue 2020-06-02 09:38:40 UTC; 5min ago
     Docs: man:fail2ban(1)
 Main PID: 1545 (fail2ban-server)
    Tasks: 3 (limit: 1151)
   CGroup: /system.slice/fail2ban.service
           └─1545 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jun 02 09:38:40 srv systemd[1]: Starting Fail2Ban Service...
Jun 02 09:38:40 srv systemd[1]: Started Fail2Ban Service.
Jun 02 09:38:40 srv fail2ban-server[1545]: Server ready
```

Рис.3.5. Перевірка встановлення fail2ban

Як можна бачити інсталяція пройшла успішно. Fail2ban знаходиться в стані active. Перейдемо безпосередньо до конфігурування Fail2ban. Перейдемо в директорію, де він знаходиться і відобразимо її вміст.

```
root@srv: /etc/fail2ban

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.


Last login: Tue Jun  2 09:34:31 2020 from 94.158.95.225
root@srv:~# cd /etc/fail2ban/
root@srv:/etc/fail2ban# ls -l
total 60
drwxr-xr-x 2 root root  4096 Jun  2 09:38 action.d
-rw-r--r-- 1 root root  2334 Jan 18  2018 fail2ban.conf
drwxr-xr-x 2 root root  4096 Apr  4  2018 fail2ban.d
drwxr-xr-x 3 root root  4096 Jun  2 09:38 filter.d
-rw-r--r-- 1 root root 22897 Jan 18  2018 jail.conf
drwxr-xr-x 2 root root  4096 Jun  2 09:38 jail.d
-rw-r--r-- 1 root root   645 Jan 18  2018 paths-arch.conf
-rw-r--r-- 1 root root  2827 Jan 18  2018 paths-common.conf
-rw-r--r-- 1 root root   573 Jan 18  2018 paths-debian.conf
-rw-r--r-- 1 root root   738 Jan 18  2018 paths-opensuse.conf
root@srv:/etc/fail2ban#
```

Рис.3.6. Вміст директорії fail2ban

Можна помітити файли fail2ban.conf і jail.conf. Це основні файли з якими ми будемо працювати. Їх не рекомендується змінювати оскільки вони можуть бути переписані під час оновлень, тому необхідно скопіювати їх в .local і змінювати вже копії. Наприклад jail.conf можна скопіювати за

допомогою команди **cp jail.conf jail.local**. Переглянемо вміст fail2ban.local. Він представлений на рисунках 3.7. – 3.9.

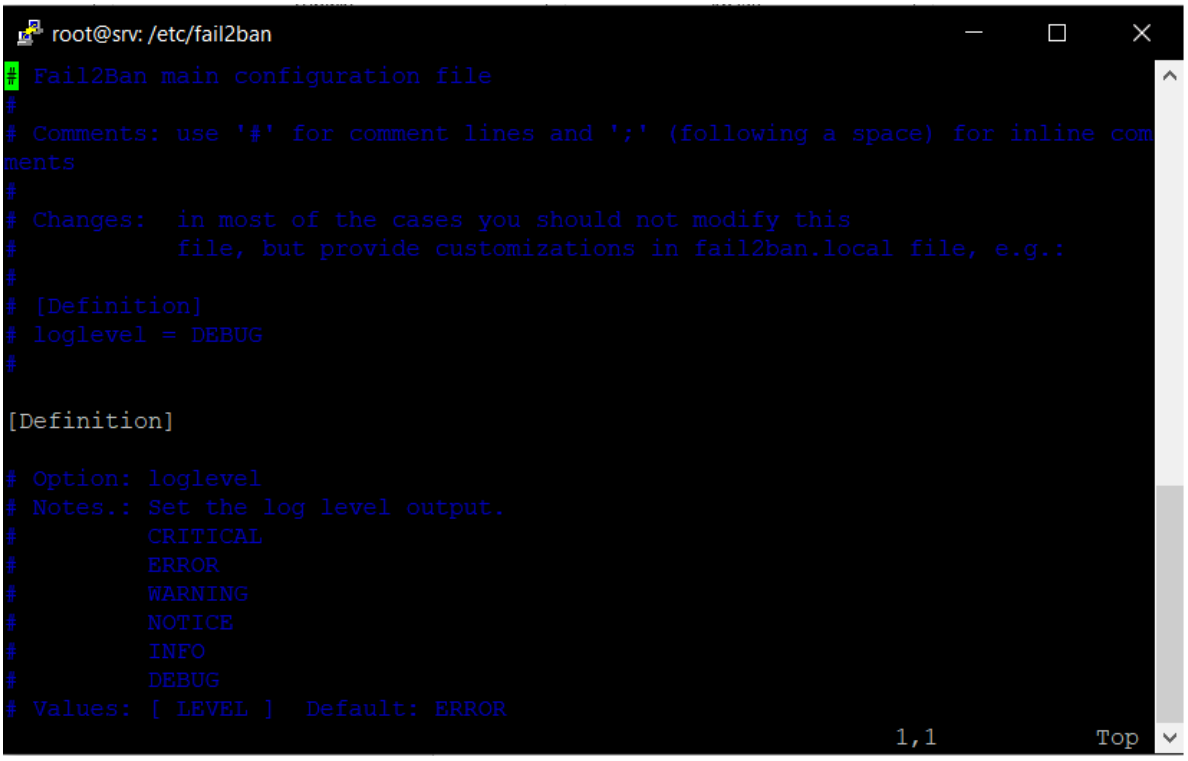

Рис.3.7.

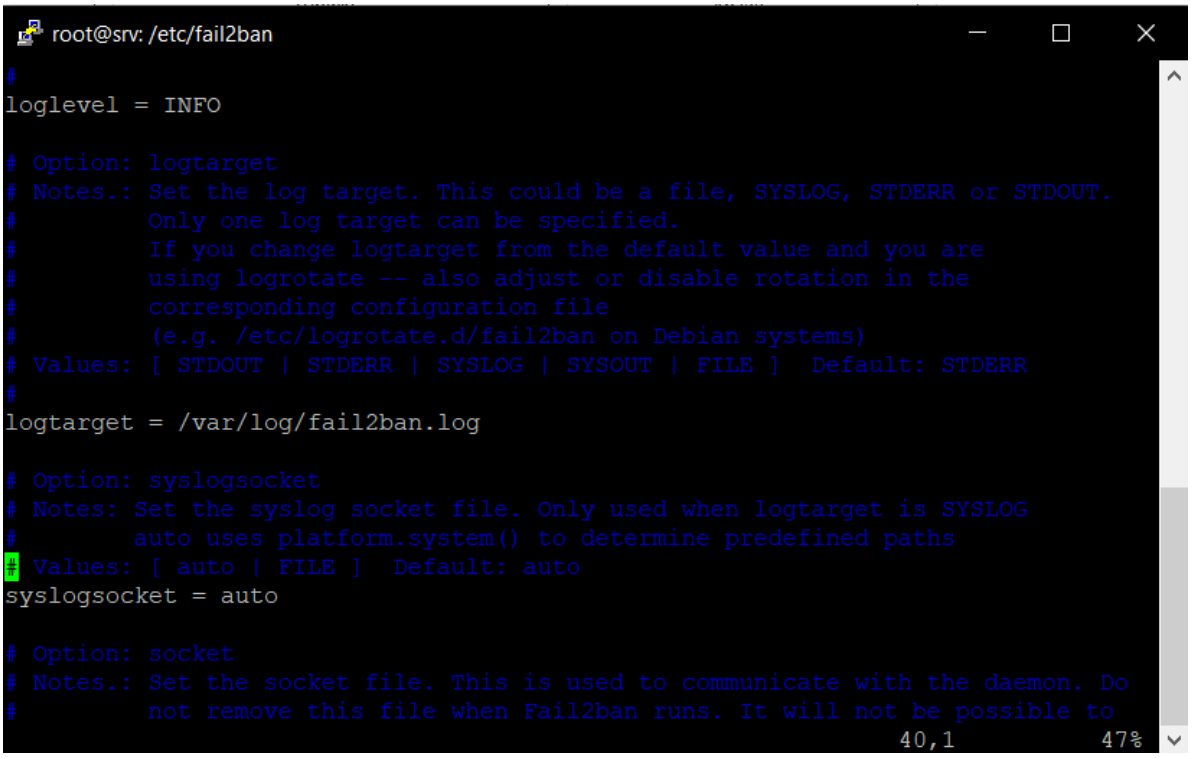

Рис.3.8.

Рис.3.9.

Параметр loglevel визначає наскільки детально буде виводитись інформація про роботу fail2ban. За замовчуванням заданий рівень 3 - INFO. Можливі значення:

- ERROR (тільки інформація про помилки);

- WARN (інформація про помилки і попереджувальні повідомлення);

- INFO (повна інформація про роботу);

- DEBUG (показ більш докладних описів всіх дій, станів, помилок, необхідних для налагодження підсистеми).

logtarget - задає напрямок потоку для виведення інформації про роботу fail2ban. Цей параметр може мати одне з наступних значень: STDOUT, STDERR, SYSLOG або ім'я файлу. За замовчуванням (якщо цей параметр не визначений) присвоюється ім'я файлу /var/log/fail2ban.log.

Ще один параметр, що визначає функціональність Fail2ban, - це socket, який задає ім'я файлу, використовуваного для обміну інформацією між

клієнтом і сервером. За замовчуванням цьому параметру присвоюється ім'я файлу /var/run/fail2ban/fail2ban.sock. В fail2ban.local налаштовуються загальні параметри програми. Тепер перейдемо до розгляду файлу jail.local. Він доволі об’ємний, тому весь вміст приводитися не буде, лише окремі фрагменти про які буде йти мова.(Рис. 3.10. – 3.11.)

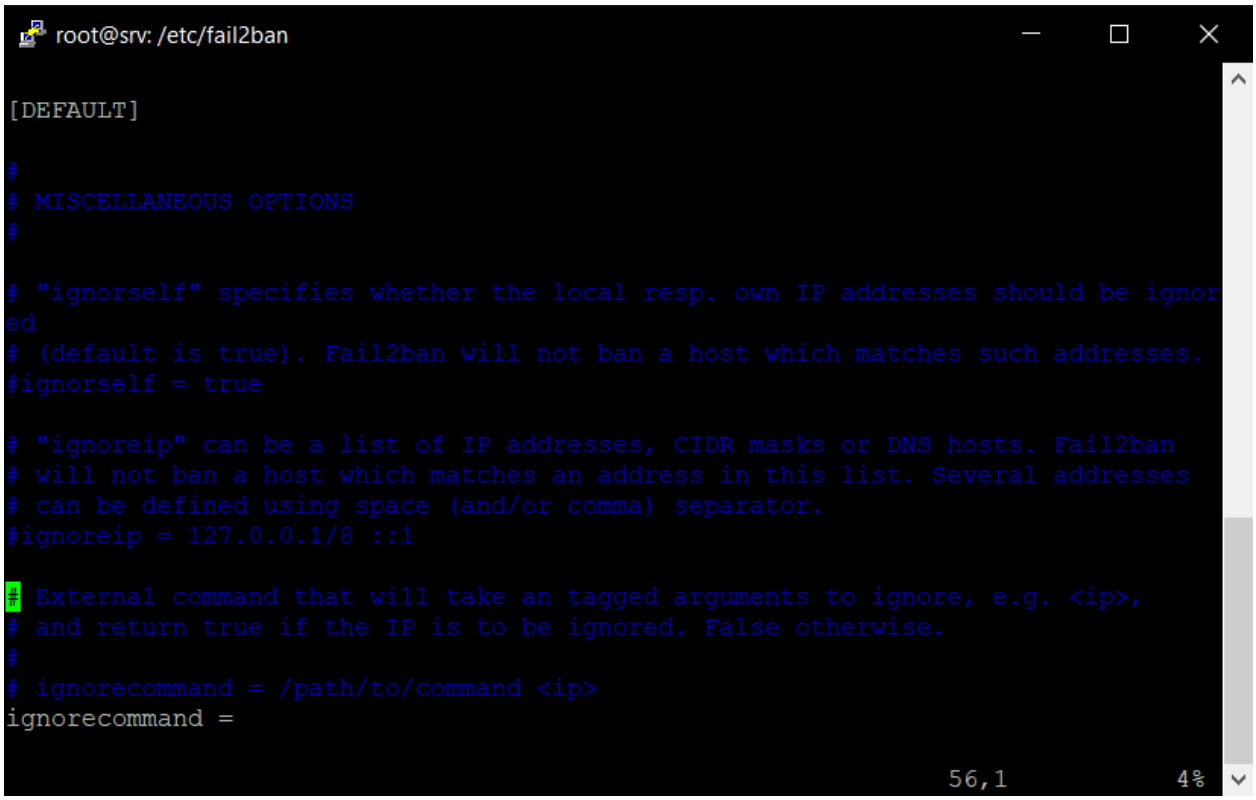

Рис.3.10.

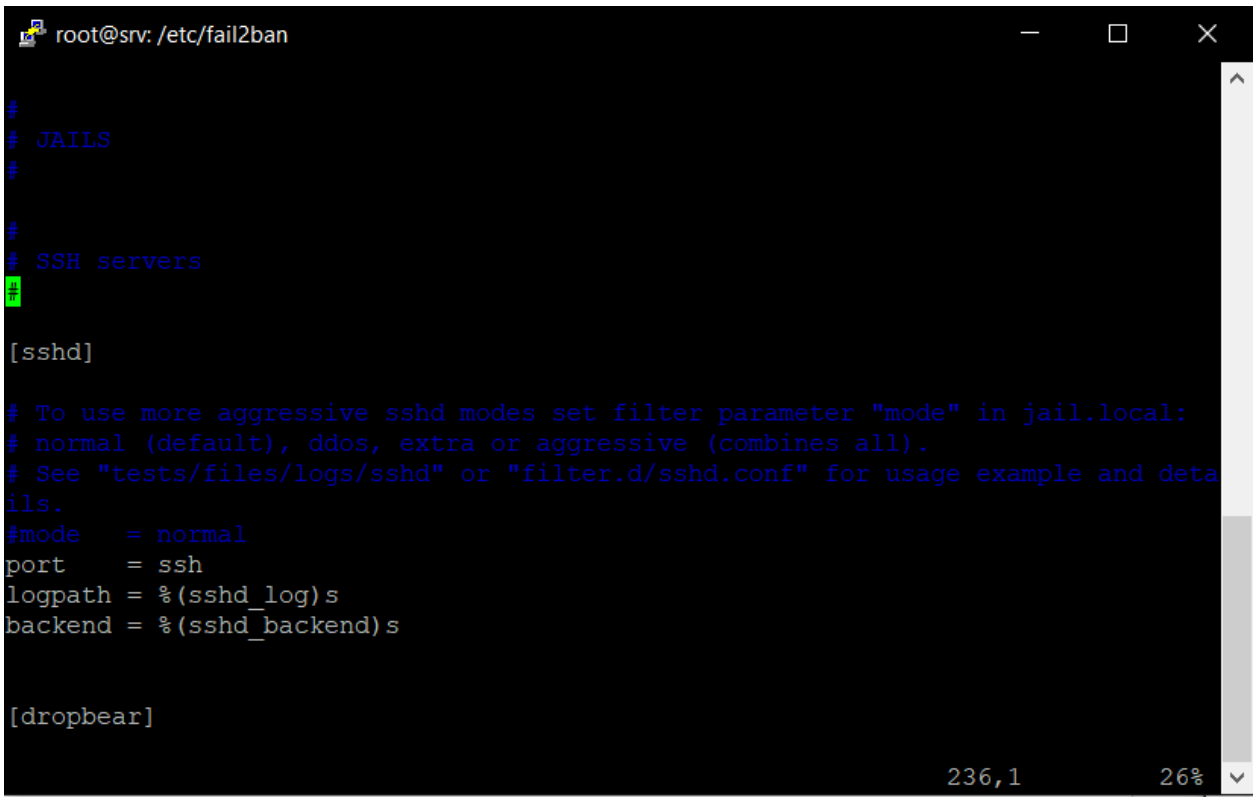

Рис.3.11.

Перша частина файлу визначатиме параметри за замовчуванням для політики fail2ban. Ці параметри можна змінити в розділі конфігурації кожного окремого сервісу. Давайте розберемо, деякі з наявних параметрів:

- ignoreip: Цей параметр ідентифікує IP-адресу, яку система повинна ігнорувати. За замовчуванням встановлено Loopback адресу.

- bantime: Цей параметр встановлює тривалість заборони в секундах. За замовчуванням - 600 секунд або 10 хвилин.

- findtime: Цей параметр встановлює вікно, в межах якого fail2ban буде рахувати максимальну кількість спроб автентифікації. За замовчуванням встановлено 600 секунд (знову 10 хвилин).

- maxretry: Визначає кількість невдалих спроб, які будуть допущені у вікні автентифікації, перш ніж буде встановлено заборону.

- backend: Цей запис визначає, як fail2ban буде контролювати файли журналів. Налаштування auto означає, що fail2ban спробує pyinotify, а потім gamin, а потім алгоритм опитування на основі того, що доступно.

- usedns: визначає, чи використовується зворотний DNS, щоб допомогти виконувати заборони. Якщо встановити "no", то будуть блокуватись IP-адреси замість імен хостів. Параметр "попередження" намагатиметься використовувати зворотний DNS для пошуку імені хоста і його заборони.

- destemail: Це адреса, на яку буде надіслано сповіщення, якщо така функція налаштована.

- sendername: буде використано в електронній пошті в полі відправника.

- banaction: встановлює дію, яка буде використана при досягненні максимальної кількості спроб автентифікації. За замовчуванням це ім'я файлу, розташованого в /etc/fail2ban/action.d/, який називається iptables-multiport.conf. Він проводить маніпуляції з iptables, щоб заборонити IP-адресу.

- mta: Це поштовий агент, який буде використовуватися для надсилання повідомлень електронної пошти.

- protocol: Це тип трафіку, який буде скинутий при застосуванні заборони IP. Це також тип трафіку, який надсилається до нової черги iptables.

- chain: це черга, яка буде налаштована для передачі трафіку до fail2ban.

Під розділом за замовчуванням є розділ JAILS, який використовується для зміни параметрів служб і їх активації. Кожен заголовок розділу вказаний так:

[ім'я служби]

Будь-який розділ можна увімкнути додавши наступний рядок до служби:

enabled = true

У кожному розділі налаштовуються параметри, включаючи файл фільтру, який слід використовувати для моніторингу журналів та розташування самого файлу журналу. За замовчуванням в fail2ban доступний захист для SSH серверів, HTTP серверів таких як apache і nginx, web-додатків таких як drupal, HTTP-proxy серверів, FTP серверів, поштових серверів, DNS серверів.

З оглядом основних параметрів закінчено. Тепер перейдемо до встановлення захисту для нашого SSH з'єднання. Активуємо jail для sshd.

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and deta
ils.
#mode   = normal
enabled = true
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Рис.3.12.

Перезавантажимо службу fail2ban і перевіримо чи наші налаштування було прийнято.

```
root@srv:/etc/fail2ban# systemctl stop fail2ban
root@srv:/etc/fail2ban# systemctl start fail2ban
root@srv:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
root@srv:/etc/fail2ban#
```

Рис.3.13.

Все успішно працює, захист для SSH активовано. Тепер перевіримо як він буде працювати. Спробуємо підібрати пароль для віддаленого доступу до серверу.

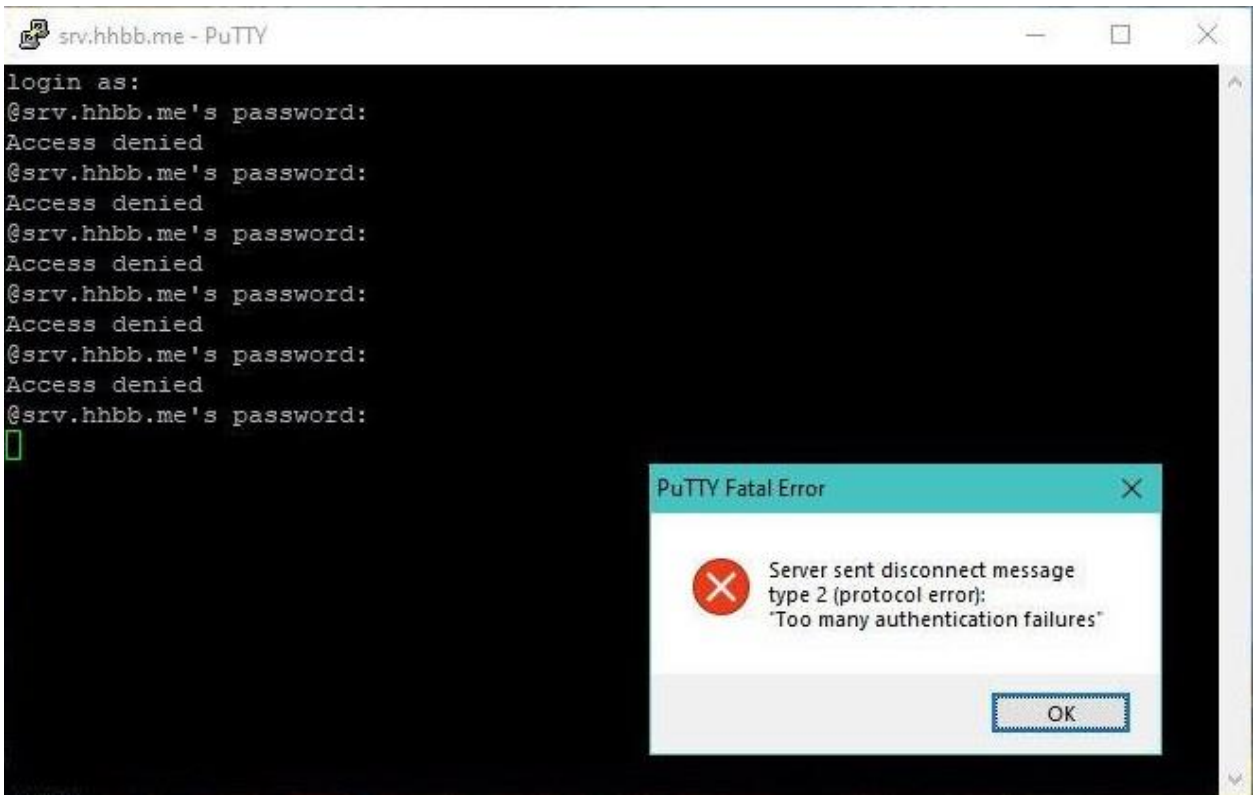

Рис.3.14.

Як видно, на шостій спробі, сервер заборонив нам доступ. Давайте перевіримо статус служби sshd.

```
root@srv:/etc/fail2ban# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 9
|  |- Total failed:     259
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 6
   |- Total banned:     39
   `- Banned IP list:   125.212.207.205 222.186.52.39 87.251.74.30 218.92.0.211
49.234.45.241 14.18.62.124
root@srv:/etc/fail2ban#
```

Рис.3.15.

IP-адреса з якої ми намагались отримати несанкціонований доступ до мережі остання в списку. Отже захист успішно встановлений. Тепер віддалений доступ до нашого серверу захищено. Як можна бачити, окрім нашої адреси там вже є багато інших. Оскільки сервер має доступ до глобальної мережі, звідти йдуть постійні спроби його зламу. На сьогоднішній день в Інтернеті діє велика кількість ботів які в автоматичному режимі

намагаються проникнути на сервери, що доступні в мережі Інтернет. За час проведення експерименту було заблоковано 39 адрес, 6 із них заблоковано на момент перевірки статусу служби. Оскільки час блокування обмежено то адреси поступово видаляються зі списку заблокованих. Можна налаштувати блокування назавжди, якщо виникне така потреба, у відповідному полі, вказавши від'ємне число.

Це був приклад налаштування служби захисту sshd. Однак це далеко не всі можливості fail2ban. Як вже зазначалось раніше в розділі, коли fail2ban приймає рішення про блокування адреси він звертається до змінної action. В ній прописано, що саме має зробити fail2ban з цією адресою. Змінна action являє собою посилання на файл, у якому записаний скрипт. Ми можемо написати свій власний скрипт і змусити fail2ban не блокувати IP-адреси, а наприклад, створювати для них окрему чергу, обробка якої займатиме тривалий час, оскільки буде повільною. Таким чином ми сповільнимо підбір паролю. Але чому не заблокувати цю адресу взагалі? Інколи, повне блокування адреси нас може не влаштовувати. В попередньому розділі зазначалось, що з однієї адреси, в мережу може виходити безліч людей. Заблокувавши її, ми заблокуємо доступ для всіх них. Але обмеживши швидкість з'єднання ми збережемо доступ, хоча й повільний, а зловмиснику доведеться підбирати пароль при низькій швидкості дуже довго.

3.2 Висновки до розділу.

В розділі було детально розглянуто програмний комплекс Fail2ban. Описано його можливості, принцип роботи і структуру. В ході написання розділу була змодельована ситуація при якій виникає необхідність налаштування Fail2ban і проведено експеримент по встановленню захисту для служби віддаленого доступу. Експеримент виявився успішним, SSH було захищено, а результат блокування адрес – продемонстровано.

ВИСНОВКИ

В роботі було розглянуто основні засади забезпечення безпеки в мережі підприємства. Доведено необхідність вдосконалення систем захисту мереж. Сформовано загальні рекомендації, щодо забезпечення безпеки в мережі підприємства, загальновідомими методами. Також були проаналізовані перспективи розвитку кіберзлочинності на 2020 рік. Приведена законодавча база, і приклади світової кіберзлочинності доводять необхідність серйозно ставитись до безпеки мережі.

Були розглянуті механізми якості обслуговування в мережі. Описано основні принципи і особливості QoS. Обґрунтовано необхідність застосування механізмів QoS поруч з механізмами забезпечення безпеки. Показано як саме інструменти якості обслуговування допомагають захистити мережу. Окрім цього, сформовано рекомендації по застосуванню такого методу захисту. Доведено ефективність застосування методу захисту за допомогою QoS, особливо, поруч з традиційними інструментами захисту мережі.

В ході виконання експерименту була змодельована ситуація при якій виникає необхідність налаштування Fail2ban і проведено експеримент по встановленню захисту для служби віддаленого доступу. Було розглянуто основні особливості Fail2ban. Наглядно показано діяльність зловмисників і вплив роботи Fail2ban на їх спроби зламу мережі. Експеримент дав задовільний результат, його можна вважати успішним, оскільки основне завдання по захисту служби SSH, було виконано.

СПИСОК ЛІТЕРАТУРИ

1. Биячуев Т.А. / под ред. Л.Г.Осовецкого. Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 08.07.2018 №2163-VIII. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 05.03.2020)

3. Network Security: Top 5 Fundamentals by Megan Berry. URL: http://www.itmanagerdaily.com/network-security-fundamentals/ (дата звернення 12.03.2020)

4. DoS и DDoS-атаки: значение и различия. URL: https://ddos-guard.net/ru/info/blog-detail/dos-i-ddos-ataki-znachenie-i-razlichiya (дата звернення 12.03.2020)

5. What is Network Security? Explain Basic Requirements of Network Security by Dinesh Thakur. URL: http://ecomputernotes.com/computernetworkingnotes/security/requirements-of-network-security (дата звернення 12.03.2020)

6. Прогноз развития киберугроз и средств защиты информации 2020. Автор: Николай Головко. URL: https://www.antimalware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast (дата звернення 20.04.2020)

7. Кібератака на енергетичні компанії України. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%B5%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D1%87%D0%BD%D1%96_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8 (дата звернення 18.03.2020)

8. 20 самых громких киберпреступлений XXI века. Автор: Лев Шевченко. https://ubr.ua/ukraine-and-world/technology/20-samyh-gromkih-kiberprestuplenii-xxi-veka-356485 (дата звернення 18.03.2020)

9. Самые известные киберпреступления. URL: https://datbaze.ru/article/kiberprestupleniya.html (дата звернення 18.03.2020)

10. Качество обслуживания в сетях IP. Шринивас Вегешна. : Пер. с англ. – М. : Издательский дом «Вильямс», 2003. – 368с.

11. Алгоритмы управления очередями. Автор: Дмитрий Федодеев. URL: https://www.osp.ru/lan/2007/12/4659316/ (дата звернення 29.03.2020)

12. Traffic shaping and traffic policing. URL: https://linkmeup.gitbook.io/sdsm/15.-qos/7.-ogranichenie-skorosti/0-traffic-policing (дата звернення 05.04.2020)

13. Integrating Security with QoS in Next Generation Networks. Tarik Taleb, Yassine Hadjadj, Abderrahim Benslimane. DOI:10.1109/GLOCOM.2010.5683321

14. Security and QoS Unite by Joanie Wexler. URL: https://www.computerworld.com/article/2574473/security-and-qos-unite.html (дата звернення 15.04.2020)