Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«18» червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Захист корпоративної електронної пошти»

Виконавець: студент IV курсу, групи КБ-42

_____ **Жаронків Максим Юрійович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Зюбіна Р. В.	

Нормоконтроль	Мирутенко Л. В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«11» листопада 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** **Жаронкін Максим Юрійович**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Захист корпоративної електронної пошти

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Корпоративна електронна пошта, захист інформації

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з нормативно правовою базою у сфері безпеки конфіденційних даних,
Засобами захисту електронної пошти на підприємствах, обрати метод захисту даних та ознайомитися з його використанням, розробити комплексне рішення для забезпечення безпеки корпоративної пошти.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено комплексний метод захисту інформації при використанні корпоративної пошти.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав _____ (підпис) Р.В. Зюбіна (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) М.Ю. Жаронкін (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 30.01.2021	*виконано*
2	Аналіз літератури	31.01.2021 – 12.02.2021	*виконано*
3	Обґрунтування вибору рішення	13.02.2021 – 18.02.2021	*виконано*
4	Вивчення нормативно правової бази у сфері захисту інформації	19.02.2021 – 07.03.2021	*виконано*
5	Аналіз проблем інформаційної безпеки у корпоративній пошті	08.03.2021 – 25.03.2021	*виконано*
6	Дослідження методів та заходів захисту інформації	26.03.2021 – 10.04.2021	*виконано*
7	Розробка власного поштового сервера та розробка вимог до систем безпеки	11.04.2021 – 17.05.2021	*виконано*
8	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.05.2020 – 21.06.2021	*виконано*

Завдання видав _____ (підпис) Р.В. Зюбіна (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) М.Ю. Жаронкін (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 44 сторінок основного тексту, 22 рисунків та 1 схему. Список використаних джерел містить 20 найменування і займає 2 сторінки.

Метою даної роботи є багатокомпонентна оцінка поточного рівня захищеності корпоративної електронної пошти як явища, та розробка загальних універсальних рекомендацій щодо методів захисту від різноманітних загроз при використанні корпоративної пошти на підприємствах, установах та організаціях.

У роботі проаналізовано, які існують основні позиції у літературі з теорії використання електронної пошти, здійснено огляд підходів спеціалістів та науковців щодо захисту корпоративної електронної пошти. Крім цього, виконано аналіз чинної в Україні нормативно-правової бази із застосування електронної пошти в практичному аспекті.

Важливим результатом дипломної роботи є розробка універсальних рекомендацій щодо захисту корпоративної пошти на підприємствах, установах та організаціях. Для досягнення цього результату було розроблено власний поштовий сервіс на програмному забезпеченні CentOS 7. Для перевірки працездатності та функціонування поштового сервісу були проведені тестові дії: його налаштування та відправлення тестових повідомлень.

Наші рекомендації щодо захисту корпоративної пошти на підприємствах, установах та організаціях, розроблені у ході виконання дипломної роботи, є універсальними. Їх перевагою є те, що вони призначені для усіх користувачів, які хочуть забезпечити безпеку своїх персональних даних при застосуванні електронної пошти.

Ключові слова: Захист персональних даних, корпоративна електронна пошта, безпека на підприємстві, захист корпоративної пошти на підприємствах, безпека своїх персональних даних.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

CVV	–	Card Verification Value
(D)DoS	–	(Distributed) Denial-of-Service
BYOD	–	Bring Your Own Device
SBRS	–	Sender Base Reputation Score
IPS	–	Intrusion Prevention System
MTA	–	Mail transfer agent
IT	–	Information Technology
SSL	–	Secure Sockets Layer
SASL	–	Simple Authentication and Security Layer
SMTP	–	Simple Mail Transfer Protocol
POP3	–	Post Office Protocol Version 3
IMAP	–	Internet Message Access Protocol
SaaS	–	Software as a service
DLP	–	Data Leak(Loss) Prevention
TLS	–	Transport Layer Security
VPN	–	Virtual Private Network
MDA	–	Mail Delivery Agent
MUA	–	Mail User Agent
MTA	–	Mail Transport Agent
ПЗ	–	Програмне забезпечення
СБ	–	Служба безпеки

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 6
ЗМІСТ 7
ВСТУП 8
РОЗДІЛ 1 ОПИС ТЕХНОЛОГІЙ КОРПОРАТИВНОЇ ПОШТИ 10
1.1 Принцип роботи електронної пошти 10
1.2 Характеристика сервісу корпоративної пошти 12
1.3 Нормативно-правова база 13
Висновки до розділу 1 15
РОЗДІЛ 2 ОСНОВНІ ЗАГРОЗИ І МЕТОДИ ЇХ УСУНЕННЯ 16
2.1 Вимоги захисту від загроз для корпоративної пошти 16
2.2 Основні загрози, що походять від корпоративної пошти 18
2.3 Основні заходи захисту корпоративної пошти 21
Висновки до розділу 2 25
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ ПОШТИ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ 27
3.1 Вибір програмних продуктів для створення поштової системи 27
3.2 Програмна реалізація поштової системи 28
3.2.1 Встановлення PostfixAdmin 28
3.2.2 Налаштування Postfix 34
3.2.3 Налаштування Dovecot 37
3.2.4 Перевірка роботи поштового сервера 38
3.3 Рекомендації з захисту корпоративної пошти 39
Висновки до розділу 3 40
ВИСНОВКИ 41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 43

ВСТУП

Актуальність теми дипломної роботи зумовлена сучасними обставинами та умовами роботи підприємств, установ та організацій. На сьогоднішній момент більшість компаній мають свою власну корпоративну електронну пошту, через яку проходить як внутрішній, так і зовнішній зв'язок компанії. Внутрішнім зв'язком ми вважаємо внутрішнє листування співробітників щодо робочих питань та внутрішній документообіг компанії, який утворює велику частку конфіденційної інформації. Щодо зовнішнього зв'язку, він може складатися з наступних елементів: комунікація співробітників компанії з клієнтами або замовниками, листування з партнерами та підрядниками, а також обмін файлами та інформацією з вищеперерахованими суб'єктами.

На даний час, інформація є одним з найбільш важливих ресурсів для більшості людей і компаній по всьому світу. І тому питання захисту такої інформації при її транспортуванні в різні точки призначення стає з кожним роком дедалі гострішим та актуальнішим. Функцію захисту вже багато років виконує і корпоративна електронна пошта, яка як система є одночасно простою, поширеною та ефективною у використанні. Щоправда, останні дослідження підтверджують, що, оскільки в корпоративній пошті наявна велика кількість критично важливої або конфіденційної інформації, цей сервіс інформаційної інфраструктури компанії дедалі частіше стає ціллю для зловмисників та хакерських атак.

Аналіз останніх досліджень та літератури. У ході підготовки дипломної роботи ми визначили наступне коло вчених, які зробили вклад у вивчення поштових технологій: Ніколас Карр, Біл Томсан, Г. Маклеод. Серед вітчизняних науковців, які досліджували поштові технології, не можемо оминути праці: Клементьєва І.П., Устінова В.А., Монахова Д.Н., Кузьмєнкова Д.А.

Отож, *метою роботи* є практична реалізація та тест функціоналу поштового сервера, а також розробка універсальних рекомендацій із захисту корпоративної електронної пошти на підприємствах, установах та організаціях.

Для досягнення поставленої мети нам необхідно вирішити наступні *завдання*:

1) Розглянути та проаналізувати особливості побудови поштових серверів, які використовуються для корпоративної пошти;
2) З'ясувати та визначити головні принципи роботи корпоративної електронної пошти;
3) Дослідити проблематику захисту інформації при використані корпоративної пошти та розглянути існуючі методи захисту інформації при роботі з корпоративною поштою;
4) Визначити, які існують загальні правила при використанні корпоративної електронної пошти на підприємствах, установ та організацій. На основі цього розробити власні універсальні рекомендації із захисту корпоративної електронної пошти.

Об'єктом дослідження у дипломній роботі є процес захисту даних при використанні електронної пошти в компаніях.

Предмет дослідження у ході дипломної роботи становлять методи, засоби і методики захисту інформації при використанні і налаштуванні корпоративної пошти.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз нормативно-правової бази;
- порівняння існуючих систем захисту корпоративної пошти;
- установка та тестування власного поштового сервера;
- узагальнення здобутих під час практичної реалізації висновків та розробка власних рекомендацій.

РОЗДІЛ 1
ОПИС ТЕХНОЛОГІЙ КОРПОРАТИВНОЇ ПОШТИ

1.1 Принцип роботи електронної пошти

При використанні електронної пошти, ми взаємодіємо з електронними поштовими скринями, це і є основний елемент в роботі цієї системи. При відправленні листа, він переходить між користувачами через так звані поштові вузли, або реле, і після цього воно приходить до одержувача на його поштовий сервер. Поштовий сервер має пряму задачу – переправити повідомлень до серверу електронної пошти одержувача - MTA. Сервери MTA використовують протокол SMTP, який дає їм можливість зв’язатися один з одним, тому вони називаються серверами вхідної пошти, або SMTP-серверами.

Після отримання листа на MTA одержувача, який доставляє електронного листа на сервер вхідної пошти - MDA, який зберігає лист в очікуванні поки користувач його не прийме. Існують два основні протоколи вилучення пошти з MDA:

- POP3, він використовується, аби витягти лист і, в певних випадках, залишити його копію на сервері;
- IMAP, що використовується для координування статусу повідомлень між численними поштовими клієнтами. Протокол IMAP має вбудовану систему резервного копіювання листів прямо на сервері.

Сервери вхідної пошти називаються в залежності від використаного протоколу, POP-сервери і IMAP-сервери. На даний час частіше все ж таки використовують протокол IMAP, бо він набагато зручніший і практичний.

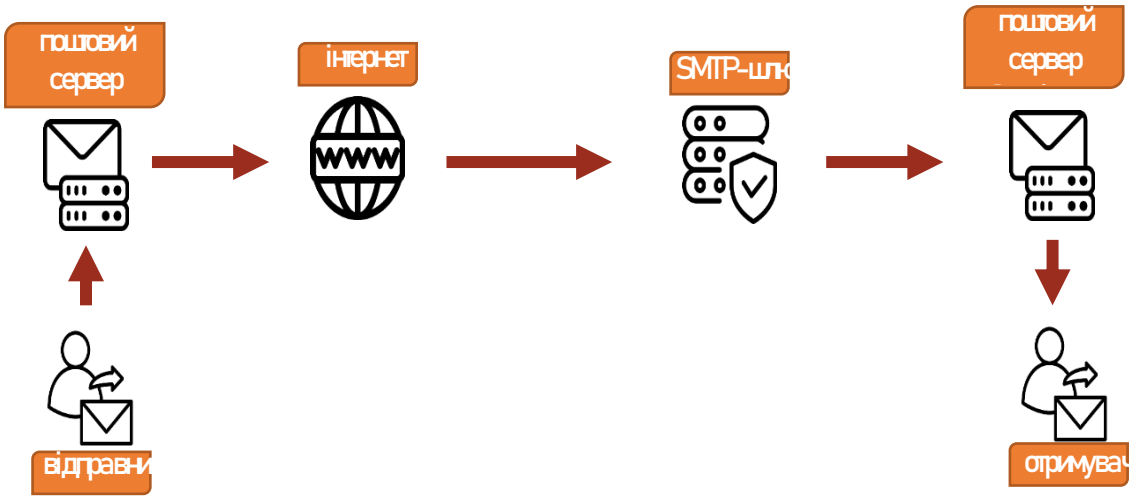

Рисунок 1.1 – Схема роботи електронної пошти

Щоб запобігти доступ до пошти сторонніми особами, MDA використовує автентифікацію користувача завдяки його логіну та паролю.

Витяг пошти здійснюється за допомогою клієнту електронної пошти – MUA.

Якщо MUA встановлений на комп'ютері користувача, або інших його девайсах - це клієнт електронної пошти наприклад Lotus, Microsoft Outlook,

Якщо ж в якості MUA виступає веб-інтерфейс, що використовується для взаємодії з сервером вхідної пошти, він називається веб-поштою.

Історично так склалося, що аби відправити листа, нам не потрібно ідентифікуватися, і ще може привести до того, що підробити свій власний адресу при відправленні повідомлення дуже легко.

Через це всі Інтернет-провайдери ставлять шлюзи на свої SMTP-сервери, щоб тільки їх користувачі могли використовувати саме їх, або, точніше, тільки машини, чий IP-адреса належить домену Інтернет-провайдера. З цієї причини користувачі повинні змінювати налаштування вихідного сервера в своїх поштових клієнтів кожен раз, коли вони переїжджають жити або працювати в інше місце.

Якщо поштовий сервер (релей) не має такого захисту, треті особи можуть відправляти листи. Такий сервер називається відкритим реле.

Відкриті релеї, як правило, використовуються спамерами, оскільки вони дозволяють замаскувати справжнє походження повідомлень. Щоб захистити своїх користувачів від отримання листів з таких серверів, багато Інтернет-провайдери ведуть постійно оновлювані чорні списки відкритих реле.

1.2 Характеристика сервісу корпоративної пошти

Корпоративна електрона пошта – це група поштових скриньок в адресі (назві) яких присутній домен компанії. Наприклад в нас є компанія “company” яка хоче створити свою власну корпоративну пошту, в такому випадку вона може назвати її так: info@company.ua, kate@company.ua, ceo@company.ua.

Як правило, такі почтові сервери розгортаються на власних обчислювальних потужностях, що має багато плюсів порівняно з хостингом на сторонніх сервісах. І зі сторони забезпечення безпекою цієї інфраструктури, так і з обслуговуванням.

Таблиця 1.1

Порівняльна таблиця видів розгортання почтових сервісів

Порівняльні характеристики	***Корпоративна пошта на власному обладненні***	***Корпоративна пошта на сторонніх сервісах***
Повний контроль над адмініструванням сервісу	+	-
Безкоштовний хостинг	+	-
Захист від спаму та вірусів	Більш потужні можливості	Обмежені можливості зі сторони сервісу
Розгортання внутрішнього документообігу	+	-
Впевненість у технічному обслуговуванні поштового сервера	+	-

Тому на самому початку будування власної мережі треба розуміти, який з методів розгортання саме ваша компанія хоче використовувати і відштовхуючись від цього вже розробляти політики безпеки і будувати безпечний периметр мережі.

У наш час кожна компанія має мати власну корпоративну пошту. Адже завдяки цьому програмному продукту компанії можуть організувати як внутрішню так і зовнішню комунікаційну функцію, і використовувати його як інструмент для внутрішнього документообігу компанії. А це означає, що через цей об’єкт буде проходити велика кількість конфіденційної інформації, такої, як: комерційна інформація про компанію та її партнерів, приватні данні про всіх робітників, цінні папери, та ще багато різних критичних даних.

Через це спеціалістам з інформаційної безпеки треба дуже ретельно віднестись до впровадження всіх необхідних заходів, аби забезпечити цілісність та конфіденційність всієї інформації, яка проходить через корпоративну електронну пошту.

1.3 Нормативно-правова база

Питання захисту інформації при використанні корпоративної електронної пошти в Україні на пряму не регламентується, але якщо підійти більш ретельно до цього питання, то стає можливим знайти потрібні законодавчі документи. В наступних документах можливо знайти потрібні висловлювання:

- Стаття 505 Цивільного Кодексу України «Поняття комерційної таємниці»;
- Закон України «Про інформацію» (Сфера діяльності та основні положення, які стосуються розвитку інформаційних технологій та систем в Україні);

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (Питання захисту інформації криптографічним методом);
- Постанова КМУ №611 від 09.08.1993 (Перелік відомостей, які не можуть бути ніким зараховані до комерційної таємниці).

Стаття 505 Цивільного Кодексу України «Поняття комерційної таємниці» регламентує роботу з конфіденційною інформацією, як вона має бути захищена, яку інформацію можна та потрібно відносити до комерційної таємниці.

Закон України «Про інформацію» має в собі розгорнуту відповідь на питання «Що таке інформація?». У цьому законі перераховані:

- види інформації,
- права людей на володіння інформацією,
- охорона права на інформацію,
- суб'єкти і об'єкти інформаційних відносин,
- основні принципи інформаційних відносин.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» заходи захисту критично важливої інформації в інформаційно-телекомунікаційних системах.

Постанова КМУ №611 від 09.08.1993 має в собі перелік та обґрунтування, яка інформація не може бути віднесена до комерційної таємниці.

У наш час законодавча база в цілому гарно підходить для теми дипломної роботи, і це дуже гарно, бо через це стає можливим більш комплексно, детально, та глобально регламентувати питання захисту критично важливої інформації при використанні такого ресурсу, як корпоративна електронна пошта.

Висновки за розділом 1

У першому розділі було розглянуто основні терміни і положення сфери які регламентують захист конфіденційної інформації, та інші види інформації, які можуть зустрічатися при роботі з корпоративною електронною поштою . Переважна кількість визначень, які стосуються авторського права є зазначеними у Статті 505 Цивільного Кодексу України «Поняття комерційної таємниці», та Закон України «Про інформацію».

У даному розділі було також визначено основні види використання корпоративної електронної пошти, її схема роботи та базові принципи захисту інформації, яка проходить через цей суб'єкт інформаційної системи.

У цьому розділі було встановлено основні учасники, при робот корпоративної пошти:

- Поштовий сервер
- Відправник повідомлення
- Отримувач повідомлення
- SMTP - шлюз

Проведений аналіз та порівняння дають можливість визначити наступні кроки проведення дослідження:

1. Визначити основні загрози для корпоративної пошти.
2. Знайти методи усунення цих загроз.
3. Розробити вимоги до систем безпеки електронної корпоративної пошти.

РОЗДІЛ 2
ОСНОВНІ ЗАГРОЗИ І МЕТОДИ ЇХ УСУНЕННЯ

2.1 Вимоги захисту від загроз для корпоративної пошти

Зростаючий обсяг конфіденційної комерційної інформації та інформації, що ідентифікує особистість, яка передається по електронній пошті, створює загрозу витоку актуальною як ніколи. Зловмисники постійно розробляють нові, все більш складні методи атак, такі як цілеспрямовані і змішані атаки. Метою цих атак є доставка шкідливого ПЗ, що проникає в центри обробки даних, де зберігаються цінні конфіденційні бізнес дані. Традиційні засоби захисту, включаючи між мережеві екрани і антивірусні рішення для кінцевих пристроїв, не в змозі відобразити такі атаки.

Для вирішення цих завдань сучасним організаціям необхідне рішення для захисту електронної пошти, яке забезпечить багаторівневу систему безпеки. На мій погляд ось такі вимоги, компанії повинні дотримуватися при покупці рішення для захисту електронної пошти, щоб захистити себе від спаму, вірусів, змішаних загроз і витоку даних, а також гнучкості рішень для захисту електронної пошти.

При виборі рішень для захисту електронної пошти організаціям рекомендується використовувати наступні критерії. Це допоможе їм придбати надійну багаторівневу систему безпеки, необхідну для захисту бізнесу від сучасних загроз вхідної та вихідної електронної пошти. Рішення для захисту електронної пошти повинна гарантувати такі можливості:

- аналіз великих масивів даних і глобальна колективний захист інформації:
- захист від спаму і вірусів;
- захист від загроз і засоби відновлення;
- засоби запобігання витоку даних і шифрування;

- гнучкі варіанти розгортання.

Вимога 1: аналіз великих масивів даних і глобальна колективна захист інформації

Зростання обсягів даних, що надходять в інтернет- та поштові шлюзи, привертає увагу хакерів. Щоб захистити замовників від постійно посилюється потоку відомого шкідливого ПЗ, традиційні постачальники систем безпеки створюють хмарні антивіруси, по суті, переміщаючи сигнатури в хмару, щоб забезпечити захист всієї клієнтської бази за допомогою колективного імунітету.

Однак саме по собі це рішення не захищає від сучасного шкідливого ПЗ, розрахованого на подолання традиційних систем з сигнатурним методом виявлення. Комплексного захисту можна домогтися тільки за рахунок безперервного аналізу, контролюючи поведінку файлу навіть після його потрапляння в вашу середу. Якщо місце розташування файлу змінюється, постійний моніторинг дозволяє виявити, стримати і усунути загрозу, відстеживши шлях зараженого файлу до його джерела.

Вимога 2: захист від спаму і вірусів

Розсилка спаму - складна проблема, яка вимагає комплексного і багаторівневого рішення. Сучасні методи атак націлені на подолання традиційних спам-фільтрів електронної пошти за рахунок розсилки «Спаму на снігоступах». Цей метод атаки полягає в розсилці спаму дрібними порціями з великої кількості серверів при частій зміні вмісту повідомлення, щоб обійти системи виявлення. Подібна тактика служить яскравим прикладом необхідності багаторівневої системи захисту електронної пошти, що містить кілька спільно працюють модулів, які виступають в якості «системи стримувань і противаги» один для одного, щоб не тільки підвищити ефективність захисту, але і скоротити кількість помилкових спрацьовувань.

Вимога 3: захист від загроз і засоби відновлення

Навіть при наявності багаторівневого підходу до забезпечення безпеки електронної пошти деякі витончені атаки здатні подолати ряд первинних

рівнів захисту. Для того щоб виявити шкідливі файли, які проникли в систему, і допомогти антивірусним програмам визначити масштаб атаки і оперативно стримати її і усунути загрозу, необхідні засоби безперервного аналізу і ретроспективного захисту.

Вимога 4: засоби запобігання витоку даних і шифрування

Сучасні рішення для забезпечення безпеки електронної пошти, що надають можливість виявлення, блокування та управління ризиками в вихідної електронної поштою, допомагають знизити ймовірність випадкової або навмисної витоку критично важливих даних з мережі. Такий захист можуть забезпечити рішення, які використовують засоби шифрування і запобігання витоку даних на основі політик і з урахуванням змісту (DLP). Захист від спаму і антивірусне сканування вихідного трафіку поряд з його обмеженням допомагає організаціям запобігати витоку даних, дотримуватися нормативно-правову відповідність і не допускати попадання комп'ютерів або адрес електронної пошти в чорні списки.

Вимога 5: гнучкі варіанти розгортання

Не існує двох організацій з однаково спроектованої мережею та інфраструктурою. Щоб відповідати вимогам інформаційної безпеки і експлуатації, постачальник системи захисту електронної пошти повинен запропонувати гнучкі варіанти розгортання, які дозволять вам управляти системою безпеки найбільш зручним способом - з розміщенням на своїй території, в хмарі або з використанням гібридних моделей.

2.2 Основні загрози, що походять від корпоративної пошти

Корпоративна пошта є одним з основних векторів атаки зловмисника. Тому надійний захист поштового трафіку – це не забаганка, а необхідність для існування і розвитку компанії, захисту її іміджу.

Одною з основних загроз для електронної пошти є **фішингові атаки.** Фішингові атаки – це різновид інтернет-шахрайства який полягає у тому, що

зловмисник імітую що він надсилає листа з компанії або сайту яким може користуватися ціль. Наприклад, ви можете отримати електронний лист, схожий на лист з банку, або навіть від IT спеціалістів з вашої компанії, з проханням вислати логін та пароль.

Зазвичай фішингові атаки використовуються для:

- вимагання приватних даних, таких як паролі, логіни, CVV та номер картки;
- влучення зловмисного коду на підприємство за допомогою підставних вкладених файлів, або гіперпосилань.

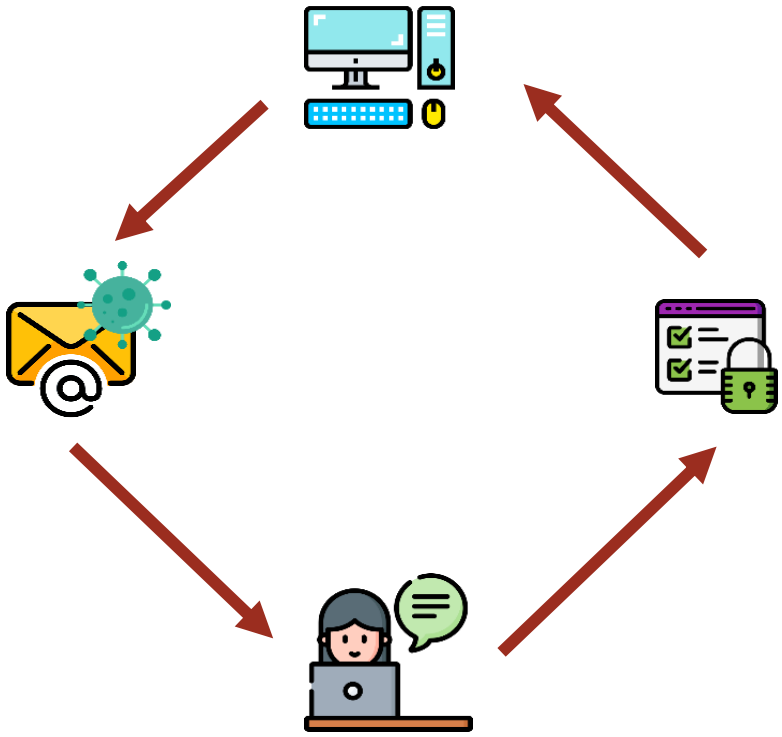

Рисунок 2.1 – Схема фішингової атаки

У наш час, також дуже популярним стало явище під назвою BYOD, тим паче під час всесвітнього локдауну. Цей принцип полягає у тому, що співробітники компаній можуть використовувати свої власні електроні пристрої при роботі. І справді, це звучить дуже практично і дає багато плюсів, але ці плюси відчувають користувачі, а ні як не співробітники СБ

компанії. Адже поки пристрої знаходяться на території підприємства і контролюються СБ – все в безпеці, але у той момент, коли люди починають використовувати свої пристрої за периметром компанії і, наприклад, підключаються до корпоративної робочої пошти через відкриту мережу Wi-fi – то з’являються великі ризики для всієї корпоративної мережі.

Не завжди цілю хакерської атаки є отримання яких ось даних чи фінансова вигода. Популярною атакою на корпоративну електрону пошту є (D)DoS -атака, або її ще називають «відмова в обслуговувані».

Існує два різновиди такої атаки:

- DoS (від англ. Denial of Service - відмова в обслуговуванні): кібератака, яка здійснюється зловмисником на самоті, тобто потужностями однієї машини, і спрямована на те, щоб довести один з мережевих ресурсів організації «до ручки» потоком запитів, що перевищують пропускну здатність системи.
- DDoS (від англ. Distributed Denial of Service) - це також ситуація, коли мережевий ресурс припиняє відповідати на запити користувача в результаті кібератаки. Він просто не встигає реагувати на всі одержувані пакети, серед яких велика частина не від справжніх користувачів, а від зловмисників. Різниця тільки в одному: напад здійснюється силами сотень вільних або невільних учасників.

Джерелом шкідливого трафіку може виступати група зловмисників (людей) або ботнет - мережа із заражених шкідливим кодом комп'ютерів / смартфонів / серверів (ботів). Такі пристрої, як зомбі, непомітно для їх власників, розсилають запити туди, куди їм накажуть організатори атаки. Другий варіант більш поширений і дешевий в реалізації, причому з кожним роком стає все доступнішим за ціною.

Мимовільними учасниками ботнету стають навіть домашні або офісні роутери, в яких не змінили заводський пароль. Все частіше «сміттєвий» трафік приходить з заражених смартфонів. А тепер уявіть світ, в якому

Інтернет речей переміг: поголовно підключені до мережі кавоварки, камери спостереження, смарт-телевізори та інші мешканці розумних будинків теж ризикують опинитися в ролі співучасників. За різними оцінками, число DDoS-атак у світі зростає на 20-30% щороку.

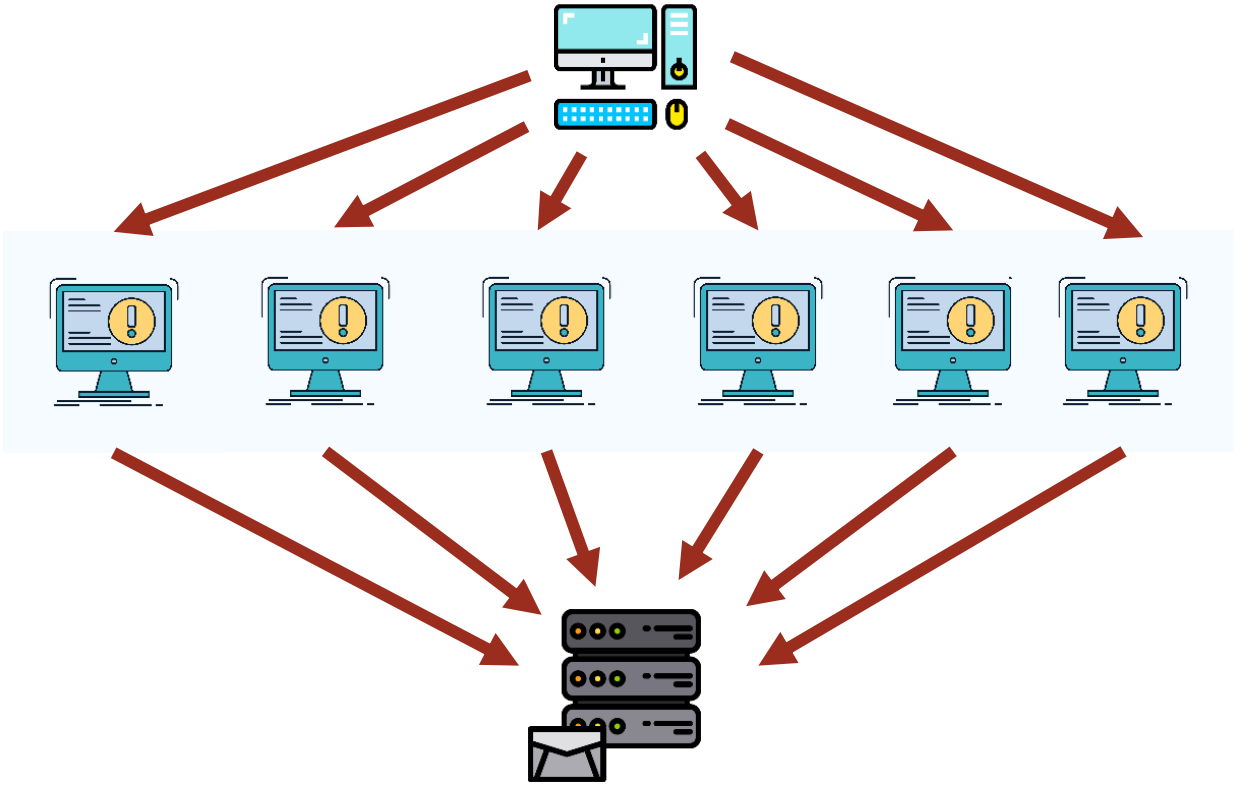

Рисунок 2.2 – Схема DDos атаки

2.3 Основні заходи захисту корпоративної пошти

Одним з головних аспектів який може нашкодити інформаційній безпеці підприємстава, є співробітники. Через свою халатність, або безграмотність у питаннях інформаційної безпеки, люди можуть навіть не підозрювати, що через те, що вони відкрили якусь ссилку яка їм прийшла на пошту, вони впустили небезпечний вірус у систему всього підприємства.

Тому в першу чергу треба забезпечити високий рівень інформаційної грамотності співробітників шляхом тестувань, лекцій і систематичних перевірок на знання в сфері інформаційної безпеки. Кожен співробітник який стикається з корпоративною поштою має знати такі правила:

1) Ніколи не запускати отримані по електронній пошті програми, навіть якщо лист прийшов від відомої особи.
2) Нікому не давати свій пароль, навіть добре знайомим колегам, співробітникам з IT-підрозділів і службі безпеки. Чи не ділитися даними про акаунт з іншими.
3) Відкриваючи отримані документи, не варто дозволяти використання макросів.
4) По можливості користуватися поштовими клієнтами останніх версій.
5) Використовувати тільки корпоративні поштові скриньки.
6) Не переглядати на роботі свою особисту пошту на безкоштовних поштових сервісах і не відвідувати сайти, не пов'язані з роботою.
7) Не довіряти навіть «відомим» адресами. Адреса відправника дуже легко підробити. Кіберзлочинці часто саме цим і користуються. Завжди варто перевіряти відправника, в разі підозр - краще зателефонувати йому, якщо використаний адреса Вашого знайомого або колеги. Не поспішайте відкривати вкладені файли і переходити за посиланнями, навіть якщо лист виглядає як повідомлення від відомої особи.
8) Якщо поштове повідомлення запитує ваш пароль, або вимагає пароль натомість на отримання будь-якої послуги, то не варто вводити його. Швидше за все, це витівки зловмисників.
9) Не встановлювати не дозволені до використання у вашій компанії програми і програми, не призначені для виконання посадових обов'язків.

Надійним захистом від спаму та (D)DoS атак є встановлення поштового фільтру, який буду перевіряти всі вхідні пакети до того, як вони поступлять до мережі.

Поштовий фільтр має два варіанти розміщення:

- Локально в самій компанії.
- Віддалено на сторонніх сервісах за схемою SaaS.

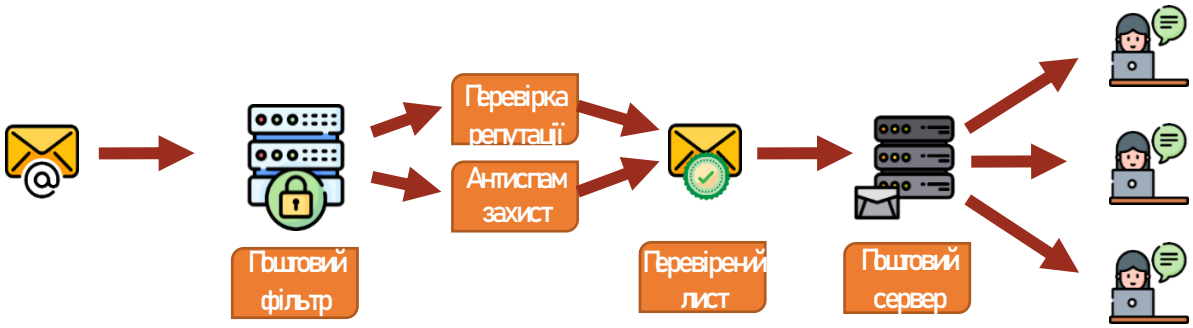

Рисунок 2.3 – Схема роботи поштового фільтру

Поштовий фільтр виступає в ролі шлюзу безпеки корпоративної електронної пошти, який виконує наступні функції:

Перевірка репутації відправника – за допомогою SBRS в реальному часі перевіряє репутацію відправника. Листи що не пройшли перевірки, або можливо прийшли від потенційно шкідливих відправників можуть бути заблоковані або піддані додатковій перевірці. За допомогою цієї функції відсівається більше 80% небажаних листів. Перевіряється тільки заголовок повідомлення, що знижує завантаженість на трафік.

Антиспам - використовує контекстний аналіз повідомлення, оцінюється вміст, порядок побудови, перевірку на наявність веб-посилань і їх самих у повідомленні (за допомогою SBRS). Після перевірки лист або відхилюється, або відсилається користувачеві з відповідною позначкою.

Outbreak фільтри - дозволяють захистити від атак нульового дня, завдяки тому, що є можливість аналізу більше 25% світового інтернет трафіку. Завдяки цьому аналізу з’являється можливість перевіряти аномалії поштового трафіку (наприклад, масова розсилка повідомлень з підозрілим

вмістом, вкладеннями, посиланнями) і автоматично створювати і розсилати на шлюзи правила, і пересилає аномалії в карантин.

Класична антивірусний захист - виробляє сигнатурної сканування вмісту повідомлень.

Захист від шкідливих програм (AMP) - проводить постійний статичний або динамічний аналіз файлів, що проходять і пройшли через систему сканування. Дозволяє відстежувати траєкторію поширення шкідливих файлів в мережі при роботі з іншими продуктами безпеки, наприклад з firewall.

Запобігання витоку даних (DLP) - виконується перевірка вмісту вихідної пошти на наявність конфіденційної користувальницької (паспортні дані, номер кредитної картки тощо) і / або корпоративної інформації (внутрішні документи). Шифрування - дозволяє здійснювати шифровану передачу повідомлень за допомогою технології SSL / TLS, між шлюзами безпеки електронної пошти, що унеможливлює прочитання повідомлення, навіть якщо воно було перехоплено по шляху до одержувача.

Аби запобігти витік інформації при використанні моделі BYOD, фахівцям кібербезпеки треба підготувати систему до цього. Дуже гарним рішенням, буде використання віртуального приватного з'єднання, або просто VPN. Це дозволить співробітникам переглядати дані на мобільних пристроях, але не зберігати їх на них. Перевага цього методу полягає в тому, що в разі втрати або знищення пристрою дані компанії не постраждають.

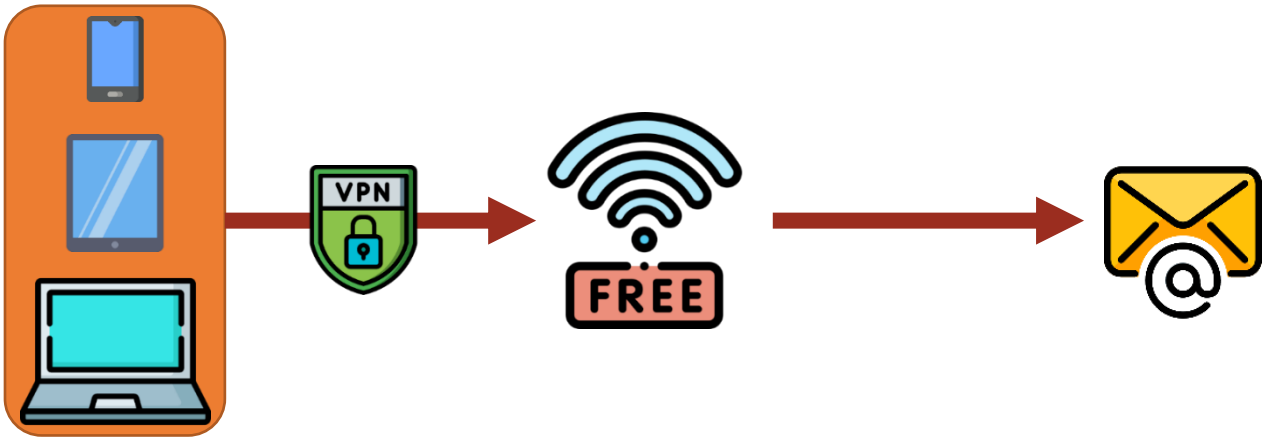

Рисунок 2.4 – Схема використання VPN при політиці BYOD

Інший варіант – використовувати зашифровані області зберігання даних на самому пристрої. Це відокремлює дані компанії від особистих даних і запобігає їх змішування. Якщо власні додатки компанії також експлуатуються в цій захищеній зоні зберігання, то це відомо як принцип «пісочниці». Знову ж таки, немає ніякого взаємодії між захищеною середовищем і за межами пісочниці. Якщо операційна система компанії і додатки компанії експлуатуються окремо від приватної зони, то ці рішення називаються «віртуалізацією». Це також дозволяє компанії впливати на актуальність операційної системи і забезпечувати її безпеку.

Висновки за розділом 2

У цьому розділі було детально вивчено усі види загроз, які можуть бути зв’язані з корпоративною електронною поштою. Ретельно дослідили кожну загрозу, та розробили рекомендації, які допоможуть запобігти втручання зловмисників до нашої системи.

Також ми розробили вимоги для компаній які використовують корпоративну пошту. Вони допоможуть обрати оптимальні рішення для будування інформаційної безпеки навколо нашого об’єкта дослідження. У цих вимогах ми прописали у якому векторі має бути спрямована СБ при налаштуванні корпоративної пошти на підприємствах.

Згідно до наведеної вище інформації можна стверджувати, що до найпопулярніших загроз відносяться:

- Політика BYOD.
- Фішингові атаки.
- (D)DOS атаки.
- Необізнаність співробітників компанії.

У даному розділі було проведено детальний аналіз цих загроз, аби зрозуміти, як краще за все запобігти витік чи втрату інформації при використанні корпоративної електронної пошти.

Проведений аналіз та порівняння дають можливість визначити наступні кроки проведення дослідження та реалізації програмного забезпечення:

1. Визначити програмний продукт, за допомогою якого можна буде реалізувати власний, конфігурований, поштовий сервер.
2. Розробити універсальні рекомендації для захисту корпоративної електронної пошти.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ ПОШТИ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ

3.1 Вибір програмних продуктів для створення поштової системи

Виконаємо налаштування поштового сервісу для системи CentOS 7, який буде придатний та оптимальний для роботи в локальній мережі.

Нам необхідно обрати ПЗ, що буде виступати в ролі транспортного агенту (MTA), агенту доставки (MDA) та користувацького агенту (MUA).

Поштовий клієнт взаємодіє з поштовим сервером, використовуючи протокол SMTP. На поштовому сервері одержувача повідомлення потрапляє в поштову скриньку, звідки за допомогою агенту доставки повідомлень (MDA) доставляється клієнту одержувача. Проте для MDA використовується не SMTP, а інший протокол — POP3 або IMAP — який також підтримується більшістю поштових серверів.

В якості транспортного агенту використовуємо Postfix, а в якості агенту доставки – Dovecot, який використовує протокол подання заявок Інтернет-повідомлень (IMAP) та протокол поштового відділення (POP3).

Також для забезпечення обміну налаштовуємо SASL, він відповідає за аутентифікацію між користувачем та сервером.

Для можливості керувати поштовими скриньками, віртуальними доменами та псевдонімами нам необхідно налаштувати веб-інтерфейс Postfixadmin.

І для отримання доступу до postfixadmin та легко управління віртуальними користувачами та доменами необхідно налаштувати LEMP: веб-сервер з Nginx та PHP. Та MySQL для зберігання всієї інформації.

Виходить, що ми встановили та налаштували Postfix за допомогою Dovecot, MySql, Nginx, Postfixadmin. І тепер можемо надсилати електронну пошту на наш сервер, але все робиться в командному рядку, й у віртуальних користувачів немає способу підключення для того, щоб надсилати пошту.

Отже нам необхідне програмне забезпечення, яке надасть інтерфейс для наших віртуальних користувачів для підключення, надсилання електронної пошти та керування їх поштовими скриньками. В якості такого ПЗ використовуємо RoundCube.

Також треба ПЗ, яке легко керує нашою базою даних для будь-яких маніпуляцій, тобто, в нашому випадку, PhpMyAdmin.

3.2 Програмна реалізація поштової системи

3.2.1 Встановлення PostfixAdmin

Почнемо з установки і налаштування панелі управління поштовим сервером postfix - postfixadmin. Без нього починати щось робити незручно, так як управляти користувачами, ящиками, аліасами буде нічим. За своєю суттю postfixadmin - набір php скриптів для управління записами в mysql базі даних, яку використовує сервер postfix під час своєї роботи. Відповідно, для роботи postfixadmin нам потрібен web сервер.

```
# yum install httpd php phpmyadmin mariadb mariadb-server php-imap
```

Рисунок 3.1 – Встановлення панелі управління поштового серверу

Цих пакетів з усіма залежностями буде досить для встановлення всіх необхідних компонентів веб сервера. Не випадково тут ставиться phpmyadmin, з ним зручно працювати з базою. У цьому випадку всі

користувачі будуть зберігатися в mysql, і в нас буде можливість туди зазирнути.

Запускаємо httpd і mariadb і додаємо їх в автозавантаження. Задаємо

```
# systemctl start httpd

# systemctl enable httpd

# systemctl start mariadb

# systemctl enable mariadb

# /usr/bin/mysql_secure_installation
```

пароль root для mysql.

Рисунок 3.2 – Встановлення пакетів для функціонування системи

Перевіряємо роботу web сервера. Заходимо на ip адресу сервера - http://188.35.19.125/, а також перевіряємо роботу phpmyadmin - http://188.35.19.125/phpmyadmin/. За замовчуванням в phpmyadmin доступ закритий. Після виконання цих дій ми можемо бачити це:

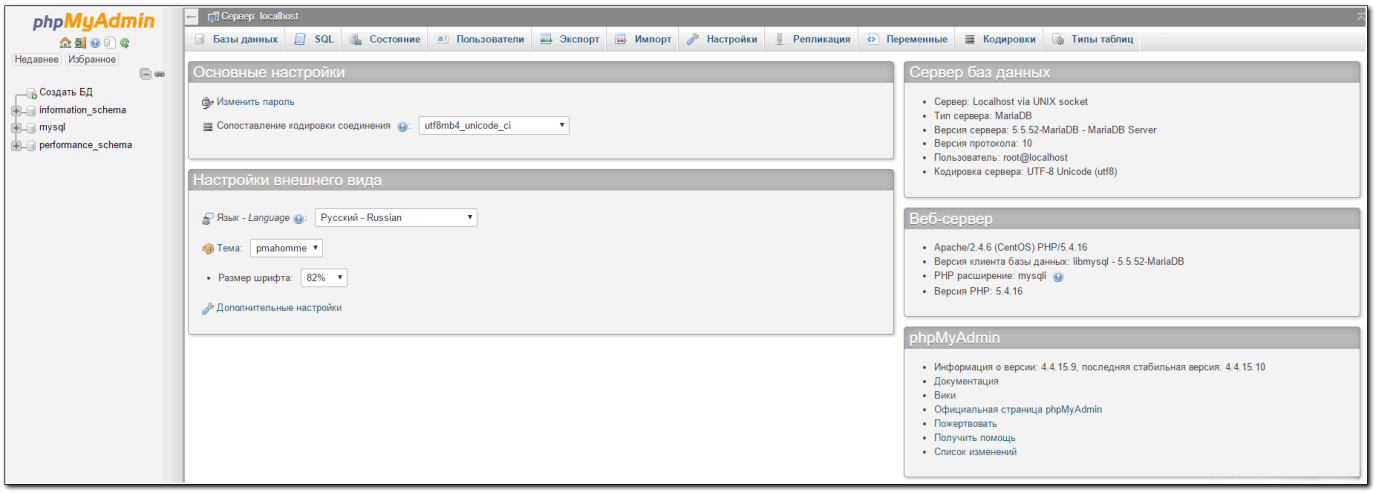

Рисунок 3.3 – Головний інтерфейс панелі phpmyadmin

Відразу створимо тут користувача postfix і однойменну базу даних. Запам'ятайте облікові дані, вони нам далі знадобляться.

Веб сервер готовий, продовжуємо настройку поштового сервера. Викачуємо останню версію postfixadmin.

```
# cd /usr/src

# wget https://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-
3.0.2/postfixadmin-3.0.2.tar.gz
```

Рисунок 3.4 – Викачуємо останню версію postfixadmin

```
# tar -xvzf postfixadmin-*

# mv /usr/src/postfixadmin-3.0.2 /var/www/html/postfixadmin
```

Рисунок 3.5 – Розпаковуємо архів і копіюємо в директорію веб сервера

```
# chown -R apache. /var/www/html/postfixadmin/
```

Рисунок 3.6 – Призначаємо власником користувача веб сервера

```
# mcedit /var/www/html/postfixadmin/config.inc.php

$CONF['configured'] = true;

$CONF['default_language'] = 'ru';

$CONF['database_type'] = 'mysqli';

$CONF['database_host'] = 'localhost';

$CONF['database_user'] = 'postfix';

$CONF['database_password'] = '12345678';

$CONF['database_name'] = 'postfix';

$CONF['admin_email'] = 'root@zeroxzed.ru';

$CONF['encrypt'] = 'md5crypt';
$CONF['default_aliases'] = array (
  'abuse'      => 'root',
  'hostmaster' => 'root',
  'postmaster' => 'root',
  'webmaster'  => 'root'
);
$CONF['domain_path'] = 'YES';
$CONF['domain_in_mailbox'] = 'YES';
```

Рисунок 3.7 – Редагуємо конфігураційний файл postfixadmin, та налаштовуємо параметри

Звертаю увагу на виділений параметр “md5crypt”. Він вказує на те, в якому вигляді зберігати паролі користувачів в базі даних. Звичайно, зберігати звичайним текстом без шифрування це поганий тон і може бути небезпечно. Тому ми вказуемо зберігання в зашифрованому вигляді.

Починаємо установку postfixadmin. Насамперед йде перевірка всіх необхідних для установки і роботи компонентів. Після цих дій ми маємо таку картину.

Вказуємо пароль установки і продовжуйте. Та отримуємо рядок з хешем цього пароля.

```
Everything seems fine... attempting to create/update database structure

Database is up to date

If you want to use the password you entered as setup password, edit config.inc.php or config.local.php and set
$CONF['setup_password'] = '67e46bdcc7aeb431f7af9a2d02f83352:30672e5a9deacaf505d32807b967caf9fd0c32ef';
```

Рисунок 3.8 – Отримання хешу зашифрованого паролю

```
# mcedit /var/www/html/postfixadmin/config.inc.php

$CONF['setup_password'] = '67e46bdcc7aeb431f7af9a6d02f43352:30672e5a9deacaf505d328
07b967caf9fd0c32ef';
```

Рисунок 3.9 – Додаємо отриману рядок в файл конфігурації postfixadmin

Використовуючи цей пароль, ми можемо створити обліковий запис адміністратора панелі управління. Робимо це, з огляду на, що пароль повинен містити не менше двох цифр. Після цього бачимо повідомлення про успішне додавання адміністратора.

Переходимо за посиланню і авторізуемся за допомогою облікового запису адміністратора, яку тільки що зробили. І бачимо основну сторінку інтерфейсу postfixadmin.

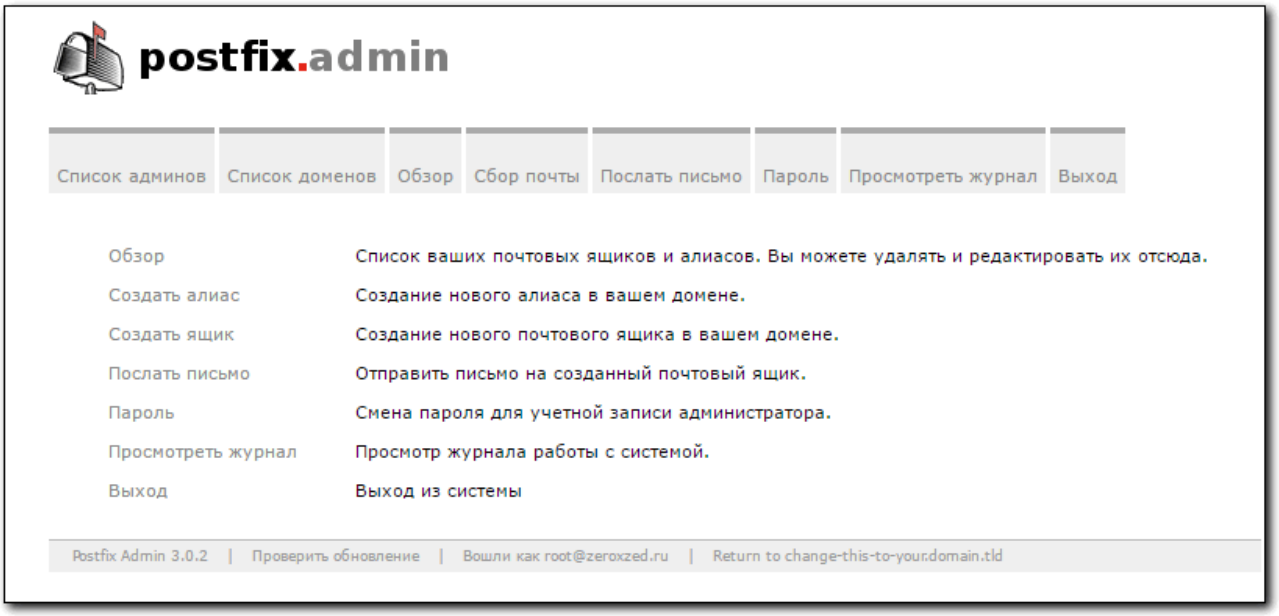

Рисунок 3.10 – Основна сторінка інтерфейсу postfixadmin

Після цього створюємо свій домен - zeroxzed.ru . При створенні домену були додані стандартні аліаси, одержувача для яких ми вказали ще в конфігу - ящик root@zeroxzed.ru. Створення таких алиасів вимога стандартів, але по факту, крім спаму, ви швидше за все нічого не будете отримувати за цими адресами.

Далі створимо поштову скриньку адміністратора - root@zeroxzed.ru. Для цього йдемо в розділ Огляд → Створити ящик і заповнюємо поля.

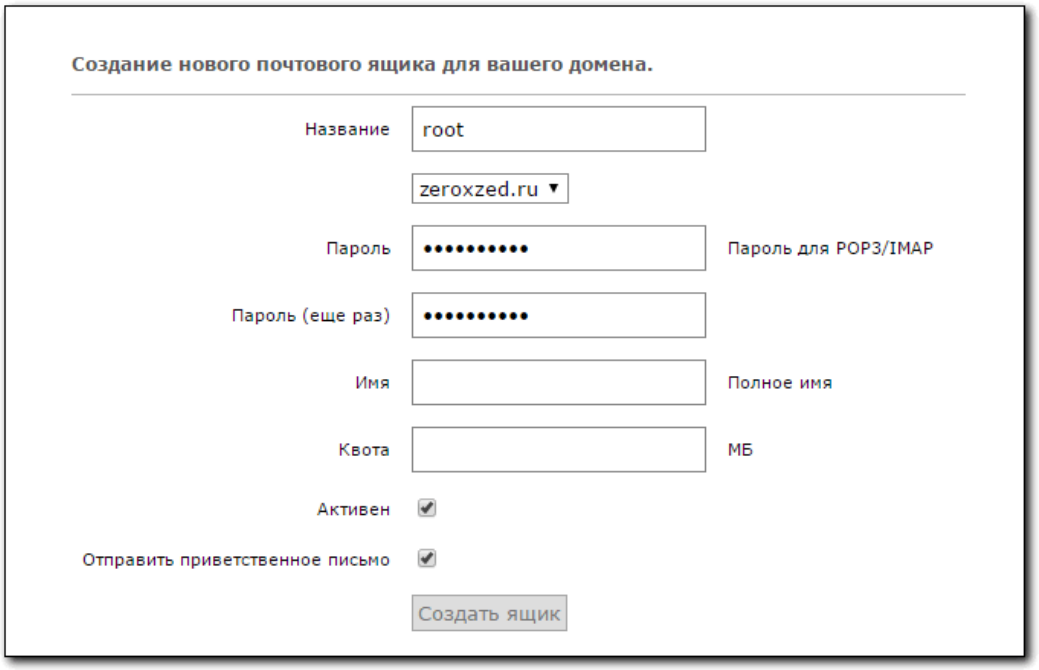

Рисунок 3.11 – Створення нової поштової скриньки

Безпосередньо ящик на диску створено не буде, так як у нас ще не налаштована поштова система, але запис в базі даних з'явиться. Це можна перевірити через phpmyadmin.

На цьому встановлення і налаштування postfixadmin завершуємо. Інтерфейс для управління поштовим сервером ми підготували. Тепер можна зайнятися безпосередньо налаштуванням postfix.

3.2.2 Налаштування Postfix

Головним механізмом нашого поштового сервера на linux - postfix. У дистрибутиві centos він вже встановлений, можна відразу переходити до налаштування.

```
# mcedit /etc/postfix/main.cf

# mkdir /etc/postfix/mysql && cd /etc/postfix/mysql

# mcedit relay_domains.cf

hosts = localhost

user = postfix

password = 12345678

dbname = postfix

query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '1'

# mcedit  virtual_alias_domain_maps.cf

hosts = localhost

user = postfix

password = 12345678

dbname = postfix

query = SELECT goto FROM alias,alias_domain WHERE alias_domain.alias_domain = '%d' and
alias.address = CONCAT('%u', '@', alias_domain.target_domain) AND alias.active = 1

# mcedit virtual_alias_maps.cf

hosts = localhost

user = postfix

password = 12345678

dbname = postfix

query = SELECT goto FROM alias WHERE address='%s' AND active = '1'

# mcedit virtual_mailbox_domains.cf

hosts = localhost

user = postfix

password = 12345678

dbname = postfix
```

Рисунок 3.12 – Створюємо наступний конфіг та папку для файлів з конфігурацією підключення до mysql і самі файли підключення

```
query = SELECT domain FROM domain WHERE domain='%s' AND backupmx = '0' AND active = '1'

# mcedit virtual_mailbox_maps.cf

hosts = localhost

user = postfix

password = 12345678db

name = postfix

query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
```

```
submission inet n - n - - smtpd

 -o syslog_name=postfix/submission

 -o smtpd_tls_wrappermode=no

 -o smtpd_tls_security_level=encrypt

 -o smtpd_sasl_auth_enable=yes

 -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject

 -o smtpd_relay_restrictions=permit_mynetworks,permit_sasl_authenticated,defer_unauth_destination

 -o milter_macro_daemon_name=ORIGINATING
```

Рисунок 3.13 – Редагування файлу /etc/postfix/master.cf

Треба додати рядки, що стосуються налаштування Submission для того, щоб поштовий сервер працював на 587 порту. Смартфони дуже часто при налаштуванні використовують цей порт за замовчуванням, десь навіть без можливості змінити цю настройку. Наводимо секцію, що відповідає за цю роботу до наступного вигляду.

В цей же файл додаємо ще одне налаштування, яка буде вказувати postfix, що доставкою пошти у нас буде займатися dovecot, який ми налаштуємо слідом. Додаємо в master.cf в самий кінець.

```
dovecot unix - n n - - pipe

 flags=DRhu user=vmail:vmail argv=/usr/libexec/dovecot/deliver -f ${sender} -d ${recipient}

# mkdir /etc/postfix/certs

# openssl req -new -x509 -days 3650 -nodes -out /etc/postfix/certs/cert.pem -keyout
/etc/postfix/certs/key.pem
```

Рисунок 3.14 – Згенеруємо самоподпісанного SSL сертифікати для нашого поштового сервера. Створюємо директорію і самі сертифікати

Створимо файли для інформації про ящики, куди буде збиратися вся вхідна та вихідна електронна пошта.

Тепер створюємо дві поштові скриньки all_in@zeroxzed.ru і all_out@zeroxzed.ru через postfixadmin.

При використані протоколу POP3 це дозволяло організувати бекап всього листування, бо в цьому протоколі не зберігаються листи, як в IMAP. Ці ящики дуже швидко заповнюються і займають величезний обсяг, тому їх обов'язково треба чистити. Це можна організувати за допомогою простих скриптів, які регулярно зберігаюсь всю пошту в архіви і іменують їх за датою. Якщо треба знайти якийсь лист, то просто розпаковуємо потрібний архів.

У випадку з imap роль бекапа відпадає, так як вся пошта зберігається на сервері. Але ці ящики все одно бувають корисні, коли користувач, наприклад, видалив якийсь важливий лист і потім робить вигляд, що його й не було. Якщо цей лист прийшло тільки сьогодні і ще не встигло полетіти в бекап, то крім запису в логах про цей лист, ви не побачите вмісту. А з такими ящиками все відразу буде зрозуміло, і питання відпадуть. Останнє застосування - служба безпеки. Якщо у вас є хтось, кому належить читати всю переписку, то реалізувати цей функціонал можна таким простим чином.

Всі основні налаштування для postfix зроблені. Тепер треба налаштовувати dovecot - IMAP сервер нашої поштової системи.

3.2.3 Налаштування Dovecot

Займемося налаштуванням dovecot - сервер доставки пошти користувачеві по протоколам pop3 і IMAP. Я не бачу причин використовувати pop3. Він незручний в порівнянні з IMAP, тому ми будемо працювати лише з протоколом IMAP.

Встановлюємо необхідні для dovecot пакети та створюємо конфігураційні файли для доступу до mysql базі.

```
# yum install dovecot dovecot-mysql dovecot-pigeonhole

# mcedit /etc/dovecot/dovecot-mysql.conf

driver = mysql

default_pass_scheme = CRYPT

connect = host=127.0.0.1 dbname=postfix user=postfix password=12345678

user_query = SELECT '/mnt/mail/%d/%u' as home, 'maildir:/mnt/mail/%d/%u' as mail, 1000 AS uid, 1000
AS gid, concat('*:bytes=', quota) AS quota_rule FROM mailbox WHERE username = '%u' AND active = '1'

password_query = SELECT username as user, password, '/mnt/mail/%d/%u' as userdb_home,
'maildir:/mnt/mail/%d/%u' as userdb_mail, 1000 as userdb_uid, 1000 as userdb_gid,
concat('*:bytes=', quota) AS userdb_quota_rule FROM mailbox WHERE username = '%u' AND active = '1'
```

Рисунок 3.15 – Створення директорію і файлів для логів

```
# systemctl restart postfix

# systemctl start dovecot

# systemctl enable dovecot
```

Рисунок 3.16 – Створення директорію і файлів для логів

```
# mkdir /var/log/dovecot

# cd /var/log/dovecot && touch main.log info.log debug.log lda-errors.log lda-deliver.log lmtp.log

# chown -R vmail:dovecot /var/log/dovecot
```

Рисунок 3.17 – Створення директорію і файлів для логів

На цьому основна настройка поштового сервера на базі postfix і dovecot завершена. Можна перезапускати служби і перевіряти роботу системи.

3.2.4 Перевірка роботи поштового сервера

Самий надійний спосіб перевірити роботу поштового сервера - відправити на нього лист. Я відправлю зі своєї поштової адреси maksim.zharonkin@gmail.com на адресу root@zeroxzed.ru. Ось що буде прописано в логах, це означає що поштовий сервер нормально працює.

```
# cat /var/log/maillog

May 20 23:31:45 mail postfix/smtpd[28075]: connect from mail-yw0-f172.google.com[209.85.161.172]

May 20 23:31:46 mail postfix/smtpd[28075]: Anonymous TLS connection established from mail-yw0-
f172.google.com[209.85.161.172]: TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)

May 20 23:31:47 mail postfix/smtpd[28075]: D4263420BB7B: client=mail-yw0-
f172.google.com[209.85.161.172]

May 20 23:31:47 mail postfix/cleanup[28086]: D4263420BB7B: message-
id=<CAHWPLcOeqf6uNHRg34+wuppDUGPDLY=fp8s-E=o9fmxYMS48cQ@mail.gmail.com>

May 20 23:31:47 mail postfix/qmgr[28042]: D4263420BB7B: from=<maksim.zharonkin@gmail.com>,
size=2533, nrcpt=2 (queue active)

May 20 23:31:47 mail postfix/pipe[28089]: D4263420BB7B: to=<all_in@zeroxzed.ru>, relay=dovecot,
delay=0.39, delays=0.33/0.02/0/0.05, dsn=2.0.0, status=sent (delivered via dovecot service)

May 20 23:31:47 mail postfix/pipe[28090]: D4263420BB7B: to=<root@zeroxzed.ru>, relay=dovecot,
delay=0.4, delays=0.33/0.03/0/0.04, dsn=2.0.0, status=sent (delivered via dovecot service)

May 20 23:31:47 mail postfix/qmgr[28042]: D4263420BB7B: removed

May 20 23:31:47 mail postfix/smtpd[28075]: disconnect from mail-yw0-f172.google.com[209.85.161.172]
```

Рисунок 3.18 – Логи для перевірки відправленого листа

Лист було доставлено в зазначену скриню і в загальну скриню для збору всієї вхідної пошти. В директорії / mnt / mail була створена директорія з ім'ям домена zeroxzed.ru, а в ній створені 3 папки з іменами ящиків:

- all_in@zeroxzed.ru
- all_out@zeroxzed.ru
- root@zeroxzed.ru

Директорії з поштовими скриньками створюються в момент отримання першого листа в ящик. Непрочитане лист поміщається в директорію /new в поштовій скриньці. Після прочитання переноситься в /cur.

3.3 Рекомендації з захисту корпоративної пошти

Після виконаної роботи треба підвести підсумки у формі рекомендацій що-до захисту корпоративної пошти на підприємствах. Стало зрозуміло, що при побудові власної корпоративної пошти компаніям треба наперед розуміти, з якими загрозами вони зіштовхнуться, а саме:

- Фішингові атаки.
- (D)DOS атаки.
- Політика BYOD.
- Інсайдери.
- Халатність та необізнаність співробітників.

При захисті від цих загроз співробітникам СБ треба використовувати такі методи, як:

1. Встановити власний поштовий сервер.
2. Правильно налаштувати FireWall.
3. Встановити поштовий фільтр.
4. Встановити систему запобігання витоку інформації DLP.
5. Використовувати VPN при віддаленому доступу до систем компанії.
6. Проводити інструктажі з співробітниками, використовуючи розроблені в цій дипломній роботі правила для персоналу.

Такий підхід допоможе компаніям любих розмірів запобігти витік інформації при використанні корпоративної електронної пошти. Ці рекомендації є універсальними, і підходять для любої мережі.

Висновки за розділом 3

У цьому розділі було ретельно розібрано які програмні продукти потрібні, аби розгорнути свій власний поштовий сервер, та крок-за-кроком була виконана інсталяція та налаштування усіх необхідних елементів, для повноцінного функціонування поштового сервісу.

В процесі налаштування та інсталяції було досліджено як саме працює електрона пошта, та детально вивчили протоколи прикладного рівня стеку TCP/IP та інформаційних технологій, що дозволяють створити сервіс електронної пошти.

Після цього мною були надані рекомендації, що до використання електронної пошти на підприємствах та повний розбір загроз і їх усунення.

Виконано практичну реалізацію власного поштового серверу на операційній системі CentOS 7, з використанням DNS-серверу для коректної навігації системи, Dovecote – сервіс доставки пошти користувачам за протоколами POP3/IMAP, postfix – наш поштовий сервер, та використання MySQL-бази даних для зберігання потрібної при роботі пошти інформації.

ВИСНОВКИ

У дипломній роботі було розв’язано актуальне завдання щодо побудови безпечної корпоративної пошти, та були розроблені актуальні рекомендації захисту інформації для підприємств різних масштабів. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено аналітичний огляд методів захисту від загроз різних типів, які можуть приміняться до корпоративних поштових сервісів . Також був виконаний ретельний аналіз загроз, їх небезпечність, методи їх застосування та цілі які вони можуть переслідувати.
2. Окрім цього були розроблені вимоги щодо побудови надійного захисту для сервісу корпоративної електронної пошти, які мають дотримуватися спеціалісти СБ за для впевненості у виборі механізмів захисту.
3. Було проаналізовано базові принципи роботи електронної пошти, схеми роботи листування на кожному її етапі, детально вивчені протоколи які використовуються при цьому інформаційному процесі, що дало нам можливість більш ретельно підійти до питань захисту корпоративної пошти в цілому.
4. Виконано практичну реалізацію власного поштового серверу на операційній системі CentOS 7, з використанням DNS-серверу для коректної навігації системи, Dovecote – сервіс доставки пошти користувачам за протоколами POP3/IMAP, postfix – наш поштовий сервер, та використання MySQL-бази даних для зберігання потрібної при роботі пошти інформації.

Підсумком цієї роботи стало створення комплексної рекомендації для компаній, які використовують у себе корпоративну електронну пошту, та були перераховані загрози при її використанні, а саме:

- Фішингові атаки.
- (D)DOS атаки.
- Політика BYOD.
- Інсайдери.
- Халатність та необізнаність співробітників.

Та методи та заходи захисту від цих загроза, а саме:

1. Встановити власний поштовий сервер.
2. Правильно налаштувати FireWall.
3. Встановити поштовий фільтр.
4. Встановити систему запобігання витоку інформації DLP.
5. Використовувати VPN при віддаленому доступу до систем компанії.
6. Проводити інструктажі з співробітниками, використовуючи розроблені в цій дипломній роботі правила для персоналу.

Також будо ретельно досліджено питання зв’язане з нормативно-правовою базою, яка регламентує захист інформації в полі корпоративної електронної пошти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. [Електронний ресурс]. – Режим доступу: https://faq.in.ua/articles/administruvannya/927-zakhist-elektronnoi-poshti/
2. [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/the-small-business-guide-to-secure-email
3. [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/blog/company/axxtel/349156.php
4. [Електронний ресурс]. – Режим доступу: https://www.policombank.com/data/anti_fishing.pdf
5. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/cybersafe/blog/212391/
6. [Електронний ресурс]. – Режим доступу: https://efsol.ru/articles/ddos-attacks.html
7. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/m/ru_ua/events/2017/cisco-connect/pdfs/email_Security_Best_Practice_RU.pdf
8. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/494788/
9. [Електронний ресурс]. – Режим доступу: https://ru.ccm.net/contents/160-kak-rabotaet-elektronnaya-pochta-mta-mda-mua
10. [Електронний ресурс]. – Режим доступу: https://kodeksy.com.ua/tsivil_nij_kodeks_ukraini/statja-505.htm
11. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
12. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

13. [Електронний ресурс]. – Режим доступу: https://eset.ua/ua/blog/view/60/opasnost-udalennogo-rezhima-raboty-kak-zashchitit-korporativnuyu-set

14. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/global/ru_ua/assets/securityforum/presentations/07_email_security.pdf

15. [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/threats/information-security-threats

16. [Електронний ресурс]. – Режим доступу: https://te-st.ru/2016/04/12/ddos-attack-what-to-do-2/

17. [Електронний ресурс]. – Режим доступу: https://www.tendence.ru/articles/zaschita-korporativnoi-pochty

18. [Електронний ресурс]. – Режим доступу: https://am-bits.com/2019/04/22/cisco-email-security-appliance-esa-5/

19. [Електронний ресурс]. – Режим доступу: https://ti.smart-soft.ru/support/documentation/doc30/online/smtp.htm#

20. Кроуз Д., Росс К. Компьютерные сети: нисходящий подход //— 2016. — С. 152-167.