МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ЗАХИСТ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ**

Студент групи СЗД-41 Зерницький Богдан Миколайович _____
(підпис)

Науковий керівник: д.т.н**.** Ахрамович Володимир Миколайович _____
(підпис)

Нормоконтроль _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Зерницькому Богдану Миколайовичу

1.Тема роботи: Захист корпоративної електронної пошти

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: методи захисту, можливі для реалізації захисту корпоративної електронної пошти.

4. Предметом дослідження: є технології захисту, які забезпечують безпеку в корпоративній електронній пошті, та можуть бути реалізовані в компаніях.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту в корпоративній електронній пошті.

6. Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз роботи корпоративної електронної пошти;
- аналіз та дослідження загроз в корпоративній електронній пошті;
- створення рекомендацій щодо застосування щодо захисту корпоративної електронної пошти.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Ахрамович В.М.

(підпис)

Завдання прийняв до виконання _____ Зерницький Б.М.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «____» _____2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	16.01.23	
2	Обґрунтування актуальності теми роботи	23.01.23	
3	Написання першого розділу роботи	13.02.23	
4	Написання другого розділу роботи	20.03.23	
5	Написання третього розділу роботи	02.05.23	
6	Написання висновків по роботі	08.05.23	
8	Підготовка демонстраційних матеріалів	18.05.23	
9	Підготовка доповіді	25.05.23	
10	Захист в ДЕК		

Студент: СЗД -41 Зерницький Б.М. _____
(підпис)

Науковий керівник: д.т.н. Ахрамович В.М. _____
(підпис)

Нормоконтроль: _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Текстова частина бакалаврської роботи містить 62 сторінки, 9 рисунків, 1 таблицю.

Актуальний захист корпоративної електронної пошти є надзвичайно важливим, оскільки від коректності та безпеки цієї пошти залежить діяльність багатьох компаній та організацій. Корпоративна електронна пошта часто містить конфіденційну та важливу інформацію, таку як деталі фінансових операцій, персональні дані клієнтів, інтелектуальну власність.

Об’єкт дослідження: методи захисту, можливі для реалізації захисту корпоративної електронної пошти.

Предмет дослідження є технології захисту, які забезпечують безпеку в корпоративній електронній пошті, та можуть бути реалізовані в компаніях.

Мета роботи: удосконалення та рекомендації щодо застосування методів захисту в корпоративній електронній пошті.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз роботи корпоративної електронної пошти;
- аналіз та дослідження загроз в корпоративній електронній пошті;
- створення рекомендацій щодо застосування щодо захисту корпоративної електронної пошти.

Новизна отриманих результатів полягає в наступному:

1. Розглянуті основні загрози які загрожують безпеці корпоративної електронної пошти.

2. Розроблено рекомендації щодо захисту корпоративної електронної пошти.

Галузь використання — інформаційна безпека.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА ЕЛЕКТРОННА ПОШТА, ЕЛЕКТРОННА ОШТА, СПАМ, БРУТФОРС, ПРОТОКОЛИ, МЕТОДИ ЗАХИСТУ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЧЕННЯ.

ABSTRACT

Text part of the bachelor thesis contains 62 pages, 9 figures, and 1 table.

The up-to-date protection of corporate email is extremely important, as the activities of many companies and organizations depend on the correctness and security of this email. Corporate email often contains confidential and important information, such as details of financial transactions, personal data of customers, intellectual property, and more.

Object of research: methods of protection that can be used to protect corporate e-mail.

The subject of the research: is security technologies that provide security in corporate email and can be implemented in companies.

The purpose of the work: to improve and recommend the use of security methods in corporate e-mail.

To achieve this goal, the following main tasks are performed:

- analysis of corporate e-mail;
- analysis and research of threats in corporate e-mail;
- development of recommendations for the use of corporate email security.

The novelty of the results obtained is as follows:

1. The main threats that threaten the security of corporate e-mail are considered.

2. Recommendations for the protection of corporate e-mail are developed.

The field of application is information security.

KEYWORDS: CORPORATE E-MAIL, E-MAIL, SPAM, BRUTE FORCE, PROTOCOLS, PROTECTION METHODS, MALWARE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

E-mail (Electronic Mail) – електронна пошта

IMAP (Internet Message Access Protocol) – протокол доступу до інтернет повідомлень

MS (Microsoft) – Майкрософт

MITM (Man in the Middle) – атака «Людина посередині»

MFA (Multi-Factor Authentication) – багатофакторна аутентифікація

POP3 (Post Office Protocol) – поштовий офісний протокол

SMS (Short Message Service) – коротке текстове повідомлення

SMTP (Simple Mail Transfer Protocol) – простий протокол пересилання пошти

SSL (Secure Sockets Layer) – протокол захищених сокетів

VBA (Visual Basic for Applications) – мова програмування Visual Basic

БД – База Даних

КЕП – Корпоративна Електронна Пошта

ПК – Персональний Ком’ютер

ШПЗ – Шкідливе Програмне Забезпечення

ВСТУП

Актуальність теми пояснюється тим, що на сьогоднішній ІТ-сектор розвивається надзвичайно швидко. Кожна компанія має власний сайт, електронну пошту та сторінку в соціальних мережах. Тому інформаційна безпека і захист інформації є дуже важливим.

Через розширення компаній шляхом використання глобальної мережі збільшується комунікація через Інтернет. Хоча спілкування в інтернеті ведеться багатьма способами і найпопулярнішими з них є соціальні мережі та месенджери, незважаючи на їх поширення, електронна пошта вже ще залишається популярним методом комунікації між людьми, а в діловому середовищі вона найпоширеніша. Також слід зауважити, що авторизація на більшості електронних ресурсів вимагає наявність електронної пошти. Тож її захист від несанкціонованого доступу є дуже важливим на сьогоднішній день.

Особливій увазі щодо захисту електронної адреси почали приділяти після повномасштабного вторгнення Російської Федерації на територію України. З 24 лютого 2022 року кількість кібератак на українські сервіси істотно зросла, в тому числі на скриньки корпоративних електронних адрес, як державних установ так і приватних підприємств. За даними корпорації Майкрософт – Україна на даний час, перебуває на другому місці в світі, по кількості кібератак, на її долю припадає близько 19% від всіх кібератак в світі. Гакерські атаки на КЕП призводять до витоку конфіденційної інформації, відкриття доступу до корпоративної мережі або пошкодження даних, що має як репутаційні так і фінансові наслідки для компаній. Тому забезпечення захисту корпоративної електронної пошти на даний момент є актуальним та важливим завданням.

Об’єктом дослідження: методи захисту, можливі для реалізації захисту корпоративної електронної пошти.

Предметом дослідження є технології захисту, які забезпечують безпеку в корпоративній електронній пошті, та можуть бути реалізовані в компаніях.

Мета роботи: дослідження загроз безпеки, які існують в корпоративній електронні пошті та розробка рекомендацій, щодо її захисту від спаму, шкідливого програмного забезпечення, брутфорсу.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз роботи корпоративної електронної пошти;
- аналіз та дослідження загроз в корпоративній електронній пошті;
- створення рекомендацій щодо застосування щодо захисту корпоративної електронної пошти.

Новизна отриманих результатів полягає в наступному:

1. Розглянуті основні загрози які загрожують безпеці корпоративної електронної пошти.

2. Розроблено рекомендації щодо захисту корпоративної електронної пошти.

Галузь застосування: Результатами та рекомендаціями, отримані в ході виконання даної роботи можна керуватися при захисті корпоративної електронної пошти.

РОЗДІЛ 1 КОПРОРАТИВНА ЕЛЕКТРОННА ПОШТА

1.1 Корпоративна електронна пошта

Електронна пошта, також відома як e-mail — це електронна система обміну повідомлень, що дозволяє користувачам обмінюватися текстовими повідомленнями, аудіо повідомленнями, файлами, зображеннями, відео та іншими матеріалами за допомогою мережі Інтернет [1].

Корпоративна електронна пошта – це електронна пошта, яка надається співробітникам компанії або організації з метою спілкування та обміну інформацією між співробітниками та зовнішніми контактами. Вона також може бути використана для відправлення та отримання електронних повідомлень, документів, фотографій, відео та іншого контенту, що стосується діяльності компанії чи організації.

Кожен користувач корпоративної електронної пошти має унікальну адресу пошти, яка складається імені користувача та доменного імені:

1) **Ім'я користувача** — це унікальний ідентифікатор, який вибирає користувач при створенні своєї електронної пошти. Воно зазвичай передує символу "@". Ім'я користувача може складатись з букв, цифр та деяких спеціальних символів, таких як крапка, підкреслення та деякі інші.

2) **Доменне ім'я** — це частина адреси електронної пошти після символу "@". Це ім'я вказує на домен, на якому розташована поштова скринька користувача. Доменне ім'я може містити букви, цифри та деякі спеціальні символи, такі як дефіс.

Отже, назва електронної пошти виглядатиме наступним чином:

"**ім'я_користувача@доменне_ім'я**"

Наприклад, якщо користувач має електронну пошту "**name@domen.ua**", то "name" - це ім'я користувача, а "domen.com" - це доменне ім'я [2].

Кількість доменів на одну адресу взагалі не обмежена. Права частина домену після крапки, називається доменом верхнього (першого) рівня. В даному випадку, домен з назвою .ua – це національний домен України в мережі. Для всіх країн світу,

також існують коди які обов’язково мають складатися з 2 літер латинського алфавіту, наприклад:

- .uk – Велика британія;
- .us – Сполучені Штати Америки;
- .fr – Франція;
- .de – Німеччина;
- .ca – Канада;
- .jp – Японія;
- .au – Австралія.

Однак, домен верхнього рівня не обов'язково має бути кодом країни. Також в світі використовують Загальні домени верхнього рівня, що використовуються певними організаціями, без прив’язання до конкретної країни, наприклад [3]:

- COM – бізнес та комерційні організації;
- EDU – заклади освіти;
- NET – відкритий структурований домен, призначений для розподіленої мережі комп'ютерів ;
- ORG – некомерційні організації;
- INT – міжнародний домен;
- GOV – державні структури.

Домени другого рівня призначені для ідентифікації окремих організацій, компаній або фізичних осіб в Інтернеті. Вони можуть використовуватися для створення унікальної адреси корпоративної електронної пошти. Наприклад, КЕП Державного університету телекомунікацій info@dut.edu.ua, містить домен другого рівня у вигляді напису dut, саме він використовується для ідентифікації якому саме начальному закладу належить дана пошта. Два інші домени в даній пошті .edu та .ua позначають, що пошта належить освітній організації, що знаходиться в державі Україна відповідно.

Всі поштові скриньки знаходяться на спеціальних серверах електронної пошти, в яких для кожної скриньки відведено спеціальне місце та забезпечується збереження

та обробка пошти. Користувачі можуть отримати доступ до своїх електронних скриньок використовуючи програми для електронної пошти, такі як Microsoft Outlook, Mozilla Thunderbird або Apple Mail. Вони підключаються до серверів електронної пошти за допомогою протоколу IMAP або POP3, щоб отримувати та відправляти повідомлення.

У деяких випадках користувачі можуть використовувати веб-інтерфейси, щоб отримати доступ до своїх електронних скриньок через веб-браузер. Це означає, що електронна пошта зберігається на серверах електронної пошти, і користувачі можуть отримувати до неї доступ з будь-якого пристрою з доступом до Інтернету.

На одному сервері не може бути дві електронні адреси з однаковими іменами користувачів, тому що вони використовуються для ідентифікації конкретного користувача в мережі Інтернет. Якщо два користувачі використовують однакову електронну адресу, то система не зможе їх розрізнити між собою. Крім того, електронні адреси використовуються для доставки повідомлень, тому якщо два користувачі мають однакову електронну адресу, то система не зможе визначити, кому з них потрібно доставити повідомлення.

Оскільки кількість можливих електронних адрес обмежена, відбувається конкуренція за їх використання, і тому кожен користувач повинен вибрати унікальну адресу, яку ніхто інший не використовує. Саме тому, провайдери електронної пошти перевіряють на унікальність електронні адреси при реєстрації нових користувачів, щоб забезпечити їх унікальність.

Користувачі можуть надсилати електронні повідомлення зі свого електронного поштового клієнта на адреси інших користувачів. Електронні повідомлення зберігаються на поштових серверах, де вони можуть бути збережені та переглянуті отримувачем у будь-який час. Крім того, багато електронних поштових служб дозволяють користувачам організовувати та керувати своїм електронним листуванням, створювати папки для зберігання повідомлень та фільтрувати та сортувати вхідні повідомлення за різними параметрами.

Електронна пошта є одним з найбільш поширених та ефективних засобів комунікації в сучасному світі. Вона використовується як для особистих, так і для професійних цілей, і дозволяє людям залишатися в зв'язку та обмінюватися інформацією з будь-якої точки світу, однак щоб користуватися всіма її можливостями, необхідно мати доступ до мережі Інтернет.

1.2 Принцип роботи КЕП

Процес роботи корпоративної електронної пошти складається з декількох етапів:

1) **Створення повідомлення**: користувачі можуть скласти повідомлення на своєму комп'ютері або іншому пристрої, використовуючи програму для електронної пошти або веб-інтерфейс. Повідомлення може включати текст, зображення, вкладення та інші файли.

2) **Відправлення повідомлення**: коли користувач натискає кнопку "Відправити", програма для електронної пошти або веб-інтерфейс відправляє повідомлення на сервер електронної пошти, який користується протоколами SMTP або ESMTP для доставки повідомлення.

3) **Передача повідомлення**: після того, як повідомлення надійшло на сервер електронної пошти, воно може бути передано через мережу Інтернет до сервера електронної пошти отримувача. Цей процес використовує протоколи, такі як SMTP або POP3, для передачі повідомлення.

4) **Доставка повідомлення**: коли повідомлення дістається до сервера електронної пошти отримувача, воно зберігається на сервері до того часу, коли отримувач візьме його зі своєї скриньки. Отримувач може отримати повідомлення за допомогою програми для електронної пошти або веб-інтерфейсу.

5) **Читання повідомлення**: коли отримувач відкриває повідомлення, він може прочитати його текст, переглянути зображення, відкрити вкладення та виконати інші дії з повідомленням.

6) **Відповідь на повідомлення**: якщо отримувач хоче відповісти на повідомлення, він може скласти відповідне повідомлення, яке буде відправлене назад на сервер електронної пошти відправника за допомогою протоколів SMTP або ESMTP.

7) **Зберігання повідомлення**: після того, як повідомлення було відправлено і отримано, воно може бути збережено на сервері електронної пошти відправника або отримувача. Користувач може також зберігати повідомлення на своєму пристрої за допомогою програми для електронної пошти або іншої програми для роботи з електронною поштою [2].

Загалом, процес роботи корпоративної електронної пошти продемонстрований на рис. 1.1, він базується на передачі повідомлень через мережу Інтернет за допомогою протоколів, таких як SMTP, POP3 та IMAP, а також на зберіганні повідомлень на серверах електронної пошти. Користувачі можуть взаємодіяти зі своїми повідомленнями за допомогою програм для електронної пошти або веб-інтерфейсів, що дає можливість швидко і зручно комунікувати через мережу Інтернет.

Рис. 1.1 — Схема передачі повідомлення електронною поштою

1.3 Сховище повідомлень

Сховище повідомлень корпоративної електронної пошти є важливою складовою будь-якого провайдера електронної пошти та виконує роль централізованого зберігання всіх вхідних та вихідних повідомлень. Коли користувач

відправляє електронне повідомлення, воно надсилається на сервер провайдера електронної пошти, де зберігається до того часу, поки його не буде видалено користувачем, зі свого поштового ящика. Кожен провайдер електронної пошти (такий як Gmail, Zoho, Outlook тощо) має своє власне e-mail-сховище, куди зберігаються всі повідомлення користувачів.

E-mail-сховище має декілька важливих функцій, що забезпечують безпеку та зручність користування електронною поштою. Одна з основних функцій - це збереження повідомлень на сервері провайдера електронної пошти. Це забезпечує збереження ваших повідомлень у випадку втрати доступу до вашого комп'ютера чи пристрою.

Друга важлива функція - це керування повідомленнями. Завдяки email-сховищу, користувач може створювати папки та зберігати повідомлення в окремих категоріях. Це дозволяє організовувати свою електронну пошту, швидко знаходити повідомлення та зберігати їх у відповідних категоріях.

Третя функція - це фільтрація повідомлень. Користувач може налаштувати правила фільтрації, щоб зменшити кількість небажаних повідомлень в вашому основному поштовому ящику. Це дозволяє отримувати лише повідомлення, які цікавлять користувача.

Крім того, деякі провайдери електронної пошти надають можливість резервного копіювання повідомлень та налаштування автоматичного видалення старих повідомлень з вашого поштового ящика, що зменшує ризик переповнення поштової скриньки та зниження продуктивності роботи з електронною поштою.

Усі ці функції зробили email-сховище незамінною складовою для користувачів електронної пошти. Завдяки централізованому зберіганню, організації та фільтрації повідомлень, а також захисту від шкідливих вірусів та спаму, email-сховище забезпечує зручне та безпечне користування електронною поштою.

1.4 Основні протоколи електронної пошти

Протоколи електронної пошти – це набір правил та процедур, які дозволяють різним поштовим службам та клієнтам обмінюватися електронними повідомленнями. Вони регулюють процеси, пов'язані зі створенням, відправкою, прийманням та обробкою електронних повідомлень.

Існує декілька протоколів електронної пошти, які використовуються для різних цілей, таких як SMTP для відправки повідомлень електронною поштою, POP3 та IMAP для отримання повідомлень в електронній пошті, а також протоколи, які забезпечують захист від спаму та вірусів [4].

1.4.1 Протокол SMTP

SMTP – це стандартний протокол, який використовується для надсилання електронної пошти в мережі Інтернет. SMTP є одним із найстаріших протоколів і був спочатку опублікований в RFC 821 у 1982 році. З того часу було опубліковано безліч інших RFC, які розширюють та покращують протокол.

SMTP заснований на простій моделі "відправник-одержувач". Коли відправник хоче надіслати повідомлення електронної пошти, він встановлює з'єднання з SMTP-сервером, який відповідає за доставку пошти на домен одержувача. Він потім передає повідомлення на сервер SMTP, який потім доставляє його на сервер одержувача.

SMTP використовує TCP-порт 25 для надсилання повідомлень. Під час встановлення з'єднання SMTP сервер спілкуються між собою відповідно до протоколу та обмінюються інформацією про передачу повідомлень. Крім того, SMTP підтримує автентифікацію та шифрування, щоб захистити дані, що пересилаються.

SMTP надає кілька команд, які можуть бути використані для надсилання та доставки електронної пошти. Деякі з найбільш поширених команд SMTP включають:

- **HELO**: команда, що використовується для ініціалізації з'єднання SMTP;
- **MAIL FROM**: команда, яка вказує адресу відправника;

- **RCPT TO**: команда, яка вказує адресу одержувача;
- **DATA**: команда, що використовується передачі даних повідомлення;
- **QUIT**: команда, яка використовується для завершення з'єднання SMTP.

SMTP використовується в багатьох програмах, які вимагають надсилання електронної пошти, включаючи електронні поштові клієнти, веб-сервери та програми для автоматичного розсилання. Він також є частиною ширшої системи електронної пошти, яка включає інші протоколи, такі як POP3 і IMAP, які використовуються для отримання електронної пошти [5].

Однак протокол SMTP також має недоліки:

1. **Незахищеність:** Протокол SMTP не забезпечує захисту інформації, що передається між серверами електронної пошти. Це може призвести до того, що зловмисники можуть перехопити повідомлення та отримати конфіденційну інформацію.

2. **Спам:** Протокол SMTP не має ефективних механізмів для боротьби зі спамом. Це означає, що користувачі можуть отримувати велику кількість небажаних повідомлень, що може призвести до витрати часу та збільшення ризику пропустити важливу інформацію.

3. **Обмеження розміру повідомлень:** Протокол SMTP обмежує розмір повідомлень, що можуть бути відправлені, до 25 МБ. Це може бути недостатньо для відправлення великих файлів та додатків.

4. **Помилки доставки:** Протокол SMTP не забезпечує гарантій доставки повідомлень. Це означає, що повідомлення можуть бути не доставлені до отримувача, або можуть бути доставлені затримкою.

5. **Застарілість:** Протокол SMTP був розроблений у 1982 році та з того часу не був серйозно оновлюваний. Це може призвести до того, що протокол може стати менш ефективним та безпечним з плином часу.

Хоча SMTP має свої недоліки, він все ще є надійним та широко використовуваним протоколом електронної пошти. Тому для вирішення цих проблем були розроблені додаткові протоколи, такі як SMTPS (SMTP із SSL-шифруванням) та

STARTTLS (STARTTLS-шифрування SMTP). SMTPS використовує SSL-шифрування для захисту даних передачі, а STARTTLS забезпечує шифрування даних передачі за допомогою TLS (Transport Layer Security), коли з'єднання встановлюється між SMTP-серверами.

В цілому, SMTP є важливим протоколом, що використовується для надсилання електронної пошти в Інтернеті. Він був розроблений багато років тому, але до цього часу залишається незмінним у своїй основній функціональності. З тих пір були розроблені додаткові протоколи та методи, щоб забезпечити безпеку та захист від спаму, але SMTP продовжує бути основним способом надсилання електронної пошти.

1.4.2 Протокол POP3

POP3 – це протокол електронної пошти, що використовується для отримання повідомлень зі скриньки електронної пошти на локальний комп'ютер або мобільний пристрій. Цей протокол є одним з найбільш поширених та відомих протоколів для отримання електронної пошти.

Попередні версії протоколу POP були розроблені у 1984 році та використовувались для отримання повідомлень зі скриньки електронної пошти на локальний комп'ютер через дискову станцію. У 1988 році була випущена версія POP3, яка є найбільш популярною версією протоколу до цього часу.

Протокол POP3 працює на рівні прикладного програмного забезпечення та використовується для отримання повідомлень зі скриньки електронної пошти на локальний комп'ютер або мобільний пристрій. У порівнянні з протоколом SMTP, який використовується для відправки повідомлень, POP3 використовується для отримання повідомлень.

Основна функція протоколу POP3 полягає в тому, щоб дозволити користувачеві отримувати повідомлення зі своєї скриньки електронної пошти та зберігати їх на локальному пристрої для подальшого перегляду. Коли користувач запускає програму

електронної пошти на своєму пристрої, програма з'єднується з сервером електронної пошти за допомогою протоколу POP3 та отримує повідомлення зі скриньки.

Протокол POP3 працює на порту 110, але може використовувати також захищений порт 995 для забезпечення безпечної передачі даних. Дані, які передаються між сервером електронної пошти та клієнтом за допомогою протоколу POP3, передаються у вигляді текстових повідомлень з кодуванням ASCII або UTF-8. Крім отримання повідомлень, протокол POP3 також дозволяє користувачеві видаляти повідомлення, переміщати їх між папками та зберігати копії повідомлень на сервері [6].

Протокол POP3 має кілька недоліків, серед яких:

1. **Не підтримує синхронізацію повідомлень між різними пристроями.** Якщо користувач отримав повідомлення на одному пристрої, то воно не з'явиться на іншому пристрої, якщо користувач не виконає відповідні дії для синхронізації.

2. **Відсутність можливості перегляду повідомлень без їх завантаження на локальний пристрій.** Користувач повинен завантажити повідомлення зі скриньки на свій пристрій, щоб переглянути його, що може займати час та займати місце на диску.

3. **Відсутність можливості підключення до скриньки електронної пошти з декількох пристроїв одночасно.** Якщо користувач підключений до скриньки з одного пристрою, то він не може отримувати повідомлення на іншому пристрої.

4. **Відсутність можливості зберігання повідомлень на сервері після їх отримання на локальний пристрій.** Це означає, що користувач не може отримувати доступ до повідомлень з будь-якого пристрою після того, як він їх отримав на свій локальний пристрій.

5. **Відсутність захисту від спаму та вірусів.** Протокол POP3 не має вбудованих засобів захисту від спаму та вірусів, тому користувач повинен використовувати додаткове програмне забезпечення для захисту своєї електронної пошти.

6. **Обмежена функціональність.** Протокол POP3 не дозволяє виконувати багато дій, які є необхідними для сучасної електронної пошти, наприклад, пересилання повідомлень з однієї скриньки на іншу, автоматичне сортування повідомлень за папками, редагування повідомлень тощо.

7. **Проблеми зі сумісністю.** Протокол POP3 не завжди підтримується всіма поштовими серверами та поштовими програмами, що може створювати проблеми зі сумісністю та обмежувати можливості користувача.

Не зважаючи на недоліки, протокол POP3 залишається важливим компонентом інфраструктури електронної пошти, особливо для користувачів з низькою швидкістю Інтернету або обмеженим обсягом дискового простору на локальному пристрої. Для більш сучасної та функціональної електронної пошти використовуються більш сучасні протоколи, такі як IMAP та Exchange, які мають більше функцій та забезпечують кращу синхронізацію між різними пристроями та можливості захисту від спаму та вірусів.

1.4.3 Протокол IMAP

IMAP - це протокол електронної пошти, який забезпечує зручний та безпечний доступ до повідомлень на поштовому сервері. Протокол IMAP використовується для отримання та керування повідомленнями на сервері, а не для завантаження їх на комп'ютер користувача, як це відбувається за допомогою протоколу POP3. IMAP дозволяє користувачам працювати з повідомленнями на сервері з будь-якого пристрою з доступом до Інтернету.

Основною функцією протоколу IMAP є забезпечення безпечного та зручного доступу до повідомлень на поштовому сервері. Іншими словами, він дозволяє користувачам працювати з повідомленнями на сервері без потреби завантажувати їх на свій комп'ютер. Це забезпечує зручний та ефективний доступ до повідомлень з будь-якого місця та на будь-якому пристрої з доступом до Інтернету.

Основні переваги протоколу IMAP:

1. **Зберігання повідомлень на сервері**. Однією з найбільших переваг протоколу IMAP є зберігання повідомлень на поштовому сервері, що дозволяє користувачам з доступом до електронної пошти на кількох пристроях мати однаковий доступ до всієї своєї пошти та оновлювати її з будь-якого пристрою.

2. **Синхронізація.** Протокол IMAP дозволяє користувачам синхронізувати свою електронну пошту між різними пристроями, що дозволяє побачити всі зміни та відповіді на повідомлення, незалежно від того, на якому пристрої вони були зчитані.

3. **Керування повідомленнями на сервері**. Протокол IMAP дозволяє користувачам керувати повідомленнями безпосередньо на поштовому сервері, наприклад, видаляти або переміщати повідомлення між папками. Це дозволяє зберігати структуру папок та повідомлень на сервері, що спрощує організацію та пошук повідомлень.

4. **Більш безпечний доступ до пошти**. Протокол IMAP дозволяє користувачам безпечно отримувати доступ до своєї електронної пошти, забезпечуючи шифрування даних під час передачі.

Недоліки протоколу IMAP:

1. **Потреба в постійному підключенні до серверу**. Одним з недоліків протоколу IMAP є те, що для роботи з ним потрібне постійне підключення до поштового серверу. Це може бути проблемою у випадку відсутності доступу до Інтернету або невідповідної роботи поштового серверу.

2. **Велике споживання пропускної здатності Інтернету**. Щоб працювати з протоколом IMAP, необхідно виконувати багато запитів до сервера. Це може призвести до великого споживання пропускної здатності Інтернету, особливо в разі використання великої кількості повідомлень та великих вкладень.

3. **Небезпека вірусів та шкідливих програм**. Як і будь-який протокол, протокол IMAP не є повністю захищеним від вірусів та шкідливих програм. Якщо користувач отримує повідомлення з вірусом або шкідливою програмою, вони можуть поширитися на всі пристрої, на яких відкривається електронна пошта.

Протокол IMAP є потужним та корисним інструментом для роботи з електронною поштою, який забезпечує зручний та безпечний доступ до повідомлень на поштовому сервері. В порівнянні з іншими протоколами, він має декілька переваг, таких як керування повідомленнями на сервері та можливість працювати з повідомленнями на кількох пристроях одночасно.

У великих компаніях та організаціях, які використовують корпоративну електронну пошту, протокол IMAP часто використовують у поєднанні з іншими протоколами, такими як SMTP та POP3, для забезпечення ефективної та безпечної роботи з поштою.

Загалом, протокол IMAP є важливим елементом сучасної електронної пошти та дозволяє користувачам зручно та безпечно працювати з повідомленнями на поштовому сервері.

1.4.4 Протокол SSL

Протокол SSL є шифрувальним протоколом, який забезпечує безпеку передачі даних в Інтернеті. Цей протокол використовується в електронній пошті для захисту конфіденційної інформації, що передається між сервером і клієнтом.

SSL створений для того, щоб забезпечити безпеку передачі даних, шляхом шифрування інформації, що передається між двома кінцями зв'язку. Це означає, що будь-яка інформація, яка передається за допомогою SSL, є захищеною від прослуховування або зламу.

SSL використовує ключі для шифрування та дешифрування інформації, що передається між двома кінцями зв'язку. При цьому, клієнт та сервер обмінюються ключами перед початком передачі даних. Ключі застосовуються для створення шифрованого каналу, через який будь-які передані дані проходять.

SSL забезпечує автентифікацію сервера, використовуючи цифрові сертифікати, які видані відповідними центрами сертифікації. Клієнт може перевірити дійсність цифрового сертифікату, щоб переконатися, що він спілкується з правильним сервером. Якщо сертифікат не може бути підтверджений або якщо він містить помилки, клієнт може бути повідомлений про неправильність з'єднання, що може означати наявність потенційної MITM атаки.

Таким чином, SSL забезпечує безпеку під час передачі даних через Інтернет, захищаючи їх від перехоплення та незаконного доступу зловмисників. Важливою частиною безпеки є автентифікація сервера, яка дозволяє клієнту переконатися в тому, що він спілкується з правильним сервером, а не зі зловмисником, який намагається підробити з'єднання.

Хоча SSL є важливим засобом забезпечення безпеки при передачі даних в Інтернеті, він не є ідеальним і має свої недоліки:

1. **Відносна складність налаштування**: Налаштування SSL може бути складним і вимагати додаткового знання, що може становити проблему для менш досвідчених користувачів.

2. **Вартість**: Отримання сертифікату SSL може бути витратним, особливо для невеликих підприємств і малих бізнесів. Також, підтримка SSL може бути доцільною для великих підприємств, що мають багато веб-сайтів та сервісів.

3. **Відомі вразливості**: у SSL було виявлено кілька серйозних вразливостей, які можуть бути використані для зламування захисту. Наприклад, в 2014 році була виявлена вразливість Heartbleed, яка дозволяла гакерам отримувати конфіденційні дані з серверів.

4. **Швидкість**: використання SSL може знизити швидкість передачі даних через додаткову обробку, необхідну для шифрування та розшифрування інформації.

5. **Сертифікати**: для встановлення безпечного з'єднання SSL необхідно мати дійсний SSL-сертифікат. Однак, вірогідність того, що користувачі вважають сертифікати вірогідними, може бути обмеженою. Крім того, SSL-сертифікати можуть бути підроблені або отримані шляхом шахрайства.

6. **Вимоги до ресурсів**: для застосування SSL до потоків даних потрібні додаткові ресурси, такі як обчислювальна потужність та пам'ять. Це може знизити продуктивність, особливо для веб-сайтів з великою кількістю користувачів або великим обсягом даних.

Незважаючи на ці недоліки, SSL все ще залишається потужним засобом забезпечення безпеки при передачі даних в Інтернеті. Також варто зазначити, що SSL був розроблений давно і в наш час має свої обмеження.

1.5 Проксі-сервер

Проксі-сервер в КЕП — це проміжний сервер, що знаходиться між клієнтськими пристроями та серверами електронної пошти. Він може бути використаний для багатьох цілей, таких як підвищення безпеки, зменшення навантаження на сервери або забезпечення кращої продуктивності, однак найчастіше всього, він використовується для збільшення анонімності.

Схема роботи проксі-сервера, зображена на рисунку 1.2, спочатку користувач відправляє повідомлення, воно проходить через сервер-проксі, далі через мережу проходить безпосереднього на сервер корпоративної електронної пошти, після чого таким же самим шляхом, відповідь від сервера КЕП повертається на проксі-сервер, який передає її відправнику.

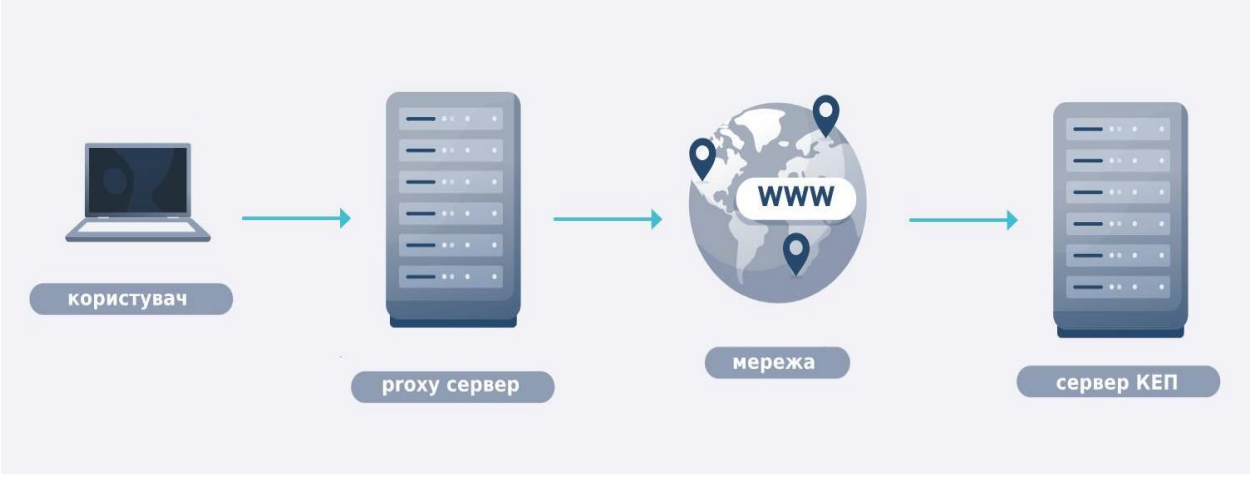

Рис. 1.2 — Схема роботи проксі сервера

Загалом, проксі-сервери поділяються на декілька видів:

1. **Прямий проксі-сервер:** він є найпоширенішим типом проксі — це посередник, який пересилає дані користувача від його імені. Даний проксі-сервер представляє

користувача у мережі. До того ж, він здатний забезпечити певний рівень захисту через те що, не надсилає трафік від користувача на сервер до тих пір, поки ці дані не перевіряться та не будуть визнані безпечними.

2. **Зворотний проксі-сервер** — сутність його роботи не сильно відрізняється від прямого прості-сервера, якщо прямий-проксі представляє користувача, то зворотний проксі використовується веб-сервером. Веб-сервери використовують зворотні проксі для гешування та отримання необхідних даних. Завдяки цим діям вони забезпечують безперебійність роботи для користувачів та зменшують навантаження на свої служби. Користувач не знає, що підключається до нього, але він може збирати необхідні дані з декількох серверів і потім передавати їх користувачу.

Для своєї роботи, проксі-сервери використовують певні протоколи — набори правил цифрової взаємодії, що визначають їхній спосіб налаштування, найчастіше використовуються такі протоколи:

1) **HTTP**: hypertext transfer protocol — використовується для гешування, тобто зберігання веб-сторінок та файлів для того, щоб пришвидшити доступ користувача до них на веб-сайтах, які відвідуються найчастіше. Загалом принцип роботи даного протоколу заключається в тому, що коли користувач виконує запит на доступ до веб-сторінки через проксі-сервер, протокол HTTP використовується для передачі запиту до сервера та повернення відповіді до клієнта через цей сервер. Проксі-сервер може бути налаштований для фільтрації даних, що передаються між клієнтом та сервером, щоб забезпечити безпеку даних. Наприклад, проксі-сервер може блокувати доступ до сайтів, які містять шкідливий контент, віруси або інші небезпечні джерела. Крім того, проксі-сервер може зберігати гешовану копію веб-сторінки, що дозволяє зменшити час завантаження сторінок при повторних запитах. Однак головний недолік даного протоколу заключається в тому, що він не шифрує дані які передає, тобто всю ту інформацію, яку він передає, зловмисники без особливих проблем здатні перехопити.

2) **HTTPS**: hypertext transfer protocol secure — в цілому, за принципом роботи даний протокол нічим не відрізняється від свого попередника, однак головна його

відмінність заключається в тому, що на відміну від HTTP він використовує шифрування SSL/TLS для захисту даних, що передаються між веб-сервером та користувачем. Тобто, даний протокол дозволяє забезпечити безпеку та конфіденційність даних, так як шифрування унеможливлює їх перехоплення та злам. Саме тому, протокол HTTPS також може бути використаний для передачі даних між клієнтом та проксі-сервером в корпоративній електронній пошті. Він здатний забезпечити більш високий рівень безпеки для передачі конфіденційної інформації, такої як логіни та паролі.

3) **SOCKS**: SOCKets Secure — зв’язується зі стороннім проксі-сервером і спрямовує трафік користувача через їх сервери на мережевому рівні, що нижче за HTTPS, задля обходу брандмауерів. SOCKS протокол забезпечує безпеку передачі даних між клієнтом та сервером, використовуючи шифрування трафіку, що проходить через проксі-сервер. Це дозволяє зменшити ризик перехоплення даних зловмисниками. Крім того, SOCKS протокол дозволяє користувачам з'єднуватися з будь-якими серверами, незалежно від їх протоколів, включаючи HTTP, HTTPS, FTP, SMTP та інші. Даний протокол може бути використаний для проксі-сервера в корпоративній електронній пошті, щоб забезпечити безпеку та конфіденційність даних, що передаються між клієнтом та сервером. SOCKS проксі дозволяє користувачам здійснювати з'єднання з будь-яким поштовим сервером, що забезпечує зручність та функціональність в роботі з електронною поштою [7].

У наш час є 2 найпопулярніші протоколи даного типу, а саме:

- SOCKS4 - цей протокол підтримує лише TCP з’єднання.
- SOCKS5 - цей протокол підтримує TCP, UDP, авторизацію по логіну і паролю та має можливість віддаленого DNS - запиту.

Окрім цього, необхідно зауважити, що протоколи типу SOCKS, не змінюють HTTP - заголовки, вони передають всю інформацію в чистому вигляді, лише через себе. З’єднання з веб-сайтом здійснюється під виглядом справжнього користувача однак, веб-сайт не зможе дізнатись справжньої IP-адреси користувача, пов’язано це з тим, що дані протоколи не передають жодної інформації про IP – адресу користувача.

Незважаючи на те, що проксі-сервери можуть забезпечити певний рівень безпеки та захисту, вони також мають свої недоліки:

- **Необхідність доступності сервера**: проксі-сервер є посередником між клієнтом та сервером, тому доступність проксі-сервера є ключовим чинником для успішної передачі даних.
- **Обмеження на доступ до деяких ресурсів**: адміністратори мережі можуть встановлювати обмеження на доступ до деяких веб-сайтів або ресурсів, що може обмежити користувачів у виконанні своїх завдань.
- **Можливість зламу**: проксі-сервер може стати об'єктом атак з боку зловмисників, що може призвести до скомпроментування даних на сервері.
- **Проблеми з прозорістю**: використання проксі-сервера може вплинути на прозорість передачі даних та може призвести до складнощів з моніторингом трафіку та виявлення проблем в мережі.

У підсумку, проксі-сервер може бути корисним інструментом для забезпечення безпеки та ефективності корпоративної електронної пошти. Він може фільтрувати небажані повідомлення, зменшувати навантаження на сервери та забезпечувати безпеку. Проте, необхідно налаштовувати його на оптимальні параметри, щоб забезпечити максимальну продуктивність та швидкістю.

Висновки до першого розділу

В даний час корпоративна електронна пошта є одним з найпоширеніших методів комунікації в різних компаніях. За допомогою неї користувач може швидко та зручно відправляти повідомлення своїм колегам та клієнтам. КЕП має унікальну поштову адресу, домен якої складається з назви компанії, якій вона належить, що додає електронній скринці іміджу в очах клієнтів. Вона має зрозумілий спосіб роботи та сховище повідомлень, де зберігаються всі листи, які були надіслані як з даної поштової скриньки, так і листи, які були надіслані на цю скриньку. Також КЕП

використовує різноманітні протоколи передачі повідомлень, що забезпечує її конфіденційність.

РОЗДІЛ 2 ЗАГРОЗИ БЕЗПЕЦІ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

2.1 Спам і його різновиди

Спам - це небажані повідомлення, які надсилаються користувачам без їхньої згоди та на їх електронну адресу. Спам може містити різноманітну рекламу, фішингові повідомлення, ланцюгові листи, віруси, а також інший шкідливий вміст. Однією з головних особливостей даного явища є те, що неможливо визначити, хто надіслав повідомлення, розсилання листів є масовим і це, в основному, небажана реклама комерційного чи агітаційного характеру. Такі листи часто містять шкідливе програмне забезпечення і мають шахрайський характер, вони можуть призвести як до моральних, так і до матеріальних збитків.

Англійське слово "Spam" виникло як назва консервованого м'ясного продукту, який був вироблений компанією Hormel Foods у 1937 році. Дана назва походить від скорочення слів "SPaced hAM" – що перекладається як пряне м'ясо. Продукт став дуже популярним під час Другої світової війни, коли армії союзників закуповували його як зручне та дешеве джерело білків для військових підрозділів. Після закінчення війни, "Spam" став доступним для широкої публіки та став популярним продуктом для людей з низьким рівнем доходів. Однак з часом, попит на цей товар зазнав спаду тому, щоб збільшити кількість продажів, була проведена перша активна рекламна компанія. Слово «спам» розповсюдилося ще більше, тепер воно було написане на вітринах магазинів, бортах трамваїв, автобусів, фасадах будинків, в газетах, по радіо безперестанку рекламувалися дані консерви.

Пізніше у 1990-х роках, коли електронна пошта стала все більш поширеною та користувачі почали отримувати все більше небажаних повідомлень, термін "Spam" почав вживатися для опису надмірної кількості небажаної електронної пошти. З того часу слово "спам" стало загальноприйнятим терміном для опису будь-якої небажаної та надмірної кількості повідомлень будь-якого типу. Спамерам вигідно розсилати такі

повідомлення тому, що необхідна для них інформація доходить до величезної кількості людей, без особливих старань. Але спам зустрічається не лише в електронній пошті, він трапляється у соціальних мережах, на форумах, у месенджерах, на дошках оголошень, мобільному телефоні, у коментарях у блогах тощо. Однак, тема даної роботи базується саме на захисті корпоративної електронної пошти, тому далі буде розглядатися спам саме в ній.

Існує кілька різновидів спаму в корпоративній електронній пошті, які, хоча можуть бути досить надокучливими, не приносять значної шкоди:

1. **Рекламні повідомлення:** Ці повідомлення містять рекламу товарів або послуг, що зазвичай не мають нічого спільного з роботою або бізнесом. Хоча вони й можуть бути надокучливими, але зазвичай не становлять загрози безпеці даних.

2. **Сповіщення від соціальних мереж:** Більшість соціальних мереж надсилають сповіщення на електронну пошту, коли відбуваються певні події, такі як коментарі, повідомлення або запрошення. Ці повідомлення також можуть бути надокучливими, але вони не становлять серйозної загрози безпеці даних.

3. **Розсилки новин:** Багато компаній надсилають щотижня або щомісяця новини своїм клієнтам.

4. **Сповіщення про важливі події:** Деякі повідомлення можуть містити інформацію про важливі події, такі як зміни в розкладі роботи, оголошення про нових співробітників або повідомлення про відкриття нового відділу.

У будь-якому випадку, важливо розпізнавати та уникати шкідливих повідомлень, що містять віруси або посилання та завжди слід бути обережним при відкритті незнайомих повідомлень або при переході за посиланнями, особливо якщо вони виглядають підозріло [8].

2.1.1 Фішингові атаки

Якщо звичайний спам приносить певний дискомфорт при роботі і не несе значної шкоди, то спам із застосуванням фішингових атак становить велику небезпеку і може нанести значних збитків як компанії , так і самому користувачу.

Фішинг - це вид кібератаки, при якому зловмисники надсилають електронні листи, щоб отримати доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, персональні дані та інші конфіденційні дані користувачів.

Ці електронні листи можуть виглядати так, що надійшли від довіреної особи або організації, наприклад, колег по роботі, банку чи веб-сайтів, на яких була використана електронна адреса для реєстрації раніше, але насправді це фальшиві повідомлення від зловмисників. У листах можуть міститися посилання на фальшиві веб-сайти, які нагадують оригінальні, і які використовуються для вводу користувача в оману та отримання доступу до його конфіденційної інформації.

Саме поняття фішингу в електронній пошті з'явився більше 20 років тому, і з тих пір зловмисники постійно вдосконалюють свої методи, щоб отримувати доступ до конфіденційної інформації користувачів. На жаль, це залишається популярним видом кібератак, оскільки багато користувачів все ще не усвідомлюють ризики та не беруть необхідних заходів для захисту своїх особистих даних [9].

Різновиди фішингових атак в електронній пошті:

- **Атаки із використанням фальшивого логотипу**: це один з найпоширеніших видів фішингу, при якому зловмисники намагаються надіслати листи, які видаватимуться за ті, що надійшли від надійного джерела, наприклад, від ваших колег, менеджерів компанії, партнерів або банку.
- **Атаки з використанням фішингових посилань**: зловмисники намагаються надіслати листи, в яких містяться посилання на фальшиві веб-сайти, які нагадують оригінальні, для введення в оману користувачів, щоб вони ввели свої конфіденційні дані, такі як логіни, паролі, номери кредитних карт та інше.
- **Атаки з використанням вкладених файлів**: найбільш небезпечний варіант фішингу, а саме зловмисники можуть надіслати вам листа, в якому міститься вірусний файл, який при відкритті може не просто завдати шкоди вашому комп'ютеру, а й

взяти під контроль всю систему компанії, яка під’єднана до цього ПК. Також зловмисники можуть використовувати шкідливий файл для отримання ваших конфіденційних даних.

- **Атаки з використанням соціальної інженерії**: зловмисники можуть використовувати методи соціальної інженерії, щоб змусити користувача розкрити свої конфіденційні дані, наприклад, відображаючи повідомлення, яке буде видаватися, ніби воно надходить від організації, яка має довіру користувача [10].

2.2 Шкідливі програми в корпоративній електронній пошті

Віруси та шкідливі програми в корпоративній електронній пошті можуть стати серйозними проблемами для компанії та користувача. Ці програми можуть пошкодити комп'ютерні системи, викрасти конфіденційну інформацію, використовувати ресурси комп'ютера для шахрайської діяльності або заморозити роботу всієї системи.

Комп'ютерний вірус – це програмний код, який може само копіюватися та вбудовуватися в інші файли та програми на комп'ютері, без згоди користувача. Вірус може мати різні наслідки, від дрібних незручностей, таких як зниження продуктивності комп'ютера, до серйозних наслідків, таких як втрата даних або доступу до комп'ютерної системи.

Віруси можуть поширюватися корпоративною електронною поштою в різних форматах, наприклад, через вкладення в електронних листах або через посилання на зловмисні веб-сайти в тексті листа, який був відправлений зловмисниками користувачам. Віруси у вкладеннях можуть приймати форму документів, архівів, виконуваних файлів, які надходять на електронну пошту з незнайомих або підозрілих джерел. При відкритті таких листів, на комп'ютері користувача можуть запускатися шкідливі програми, які починають працювати паралельно з іншими додатками і можуть нанести шкоду системі або викрадати конфіденційну інформацію.

Також віруси можуть поширюватися через посилання в електронному листі на зловмисні веб-сайти. Натиснувши на таке посилання, користувач може бути перенаправлений на інфікований веб-сайт, який завантажує на його комп'ютер шкідливі програми або віруси без згоди користувача [11].

2.2.1 Макровіруси

Макровіруси - це тип вірусів, який інфікує макроси, що зберігаються в зовнішніх файлах програмного забезпечення, таких як Microsoft Word, Excel, Acces, Power Point і т.д. При відкритті документа дані макроси виконуються внутрішніми інтерпретаторами цих програм. Вони широко поширилися завдяки величезним можливостям мови Visual Basic, яка використовується в найпопулярнішому офісному пакеті в Microsoft Office.

Вони можуть використовувати макроси для автоматичного виконання зловмисних дій на комп'ютері користувача, таких як розповсюдження вірусу через електронну пошту, шифрування файлів або крадіжка конфіденційної інформації.

Макровіруси були вперше виявлені в 1990-х роках, коли Microsoft Office став більш популярним і почав використовуватися у бізнесі та домашній сфері. На той час ці віруси були досить поширеними, оскільки більшість користувачів Office не були обізнані з можливими ризиками.

Дані типи вірусів можуть бути розповсюджені через електронну пошту, завантажені з інтернету або передані з одного комп'ютера на інший за допомогою знімних носіїв, таких як флешки або зовнішні жорсткі диски. Однак основний метод поширення макровірусів - через електронну пошту.

Макрос, написаний на мові VBA і інтегрований в документ Microsoft Word або Excel, має всі можливості, що і звичайна програма. Він може форматувати жорсткий диск або просто видалити будь-яку інформацію, вкрасти важливі файли або паролі відправивши їх електронною поштою. Найбільша небезпека вірусів цього класу заключається в тому, що вони здатні паралізувати роботу цілого офісу компанії.

Швидкість поширення макровірусів збільшується завдяки тому, що вони можуть використовувати адресну книгу користувача для автоматичного відправлення електронних листів зі зловмисними макросами всім контактам у списку. Як тільки один користувач стає жертвою макровірусу, його адресна книга стає наступною метою [12].

Також ці віруси небезпечні тим, що поширюються вони цілком в звичайному незашифрованому вигляді, це означає, що людина яка отримала такий вірус і має навички в роботі з мовою VBA, то вона без проблем зможе модифікувати вірус на свій лад та зробити його невидимим для антивірусів нового покоління. Тобто користувач використовуючи антивірус, модифікує макровірус до тих пір, поки антивірус не перестає його розпізнавати як вірус. Фактично, таким чином, з’являються нові модифікації вже відомих вірусів і для того, що антивірус його зміг розпізнати, він спочатку повинен потрапити в антивірусну лабораторію і лише після цього будуть додані функції детектування і знешкодження його нової модифікації. Так фахівцям Українського Антивірусного Центру відомо більше 100 модифікацій вірусу Macro.Word97.Thus, більше 200 модифікацій Macro.Word97.Marker і більше 50 модифікацій Macro.Word97.Ethan [13].

2.2.2 Інтернет Хробаки

Хробаки - це спеціальні програмні коди, які можуть розповсюджуватися шляхом копіювання самих себе з одного комп'ютера на інший, з використанням мережі Інтернет. Хробаки, що поширюються через корпоративну електронну пошту, стали одним з найпоширеніших видів атак на підприємства.

Хробаки зазвичай приходять у вигляді вкладень до листів електронної пошти, які, як правило, мають підозрілий вміст, наприклад, інструкції щодо відкриття документу або виконання макросів. Після відкриття вкладення, хробак може автоматично розповсюджуватися на інші комп'ютери в мережі, використовуючи адреси електронної пошти, знайдені в адресних книгах жертв [14].

Для кінцевих користувачів, поштові хробаки діляться на два основні класи:

- Хробаки, які запускаються без відома користувачів;
- Хробаки, які активізуються, лише втому випадку якщо користувач збереже приєднаний до листа файл і запустить його.

Поштові хробаки другого типу розраховані на те, що користувач, з певних причин, самостійно відкриє вкладення, яке було приєднано до листа. Щоб спонукати користувачів відкривати заражені файли, автори хробаків використовують різні психологічні прийоми. Найпоширеніший з них – видати заражений файл, за важливий документ, фотографію або корисний додаток, наприклад, хробак під назвою I-Worm.LovGate створює певні відповіді на листи, що знаходяться в поштовій базі; I-Worm.Ganda маскує себе під інформацію, про бойові дії в Іраку. Найчастіше хробаки використовують "подвійні розширення", у цьому випадку файл, що приєднаний до листа має ім'я типу: "Doc2.doc.pif", "gif.jpg.com". Цей принцип розрахований на те, що поштові клієнти не відображатимуть повне ім'я їх фалів через те, що їх назва занадто довга, і користувач не побачить подвійного розширення. Тобто в даному випадку зловмисники користуються тим, що користувач буде думати, що файл є звичайним документом або зображенням, але насправді він буде виконуваним файлом з розширенням: .exe, .com, .pif, .scr, .bat, .cmd і т.д. При відкритті такого файлу – хробак активізується.

Один з найвідоміших прикладів черв'яка, що поширювався через корпоративну електронну пошту є черв'як ILOVEYOU, який був виявлений в 2000 році. Черв'як ILOVEYOU поширився на мільйони комп'ютерів у всьому світі, завдавши збитків на суму більше 10 мільярдів доларів [15].

В будь-якому випадку, незалежно від наявності або відсутності шкідливого функціоналу, поштові черв'яки шкідливі вже тільки тому, що вони існують. Це пов'язано з тим, що розмножуючись вони перевантажують канали зв'язку і часто настільки, що повністю паралізують роботу користувача або цілої організації.

2.2.3 Троянські програми

Наступними за поширеністю є програми типу Trojan і Backdoor. Відмінність їх роботи полягає в тому, що троянська програма виконує активні дії під час роботи комп’ютера, наприклад, видаляє програми, змінює їх зміст, викрадає дані компанії через мережу, без відома користувача. В той час як Backdoor програми - відкривають віддалений доступ до ПК і очікують команди зловмисника. То для простоти розуміння, в даній роботі, такі типи програм будуть називатися троянськими.

Головна відмінність троянських програм від іншого ШПЗ в тому, що вони не мають можливості розмножуватися самостійно. Вони одноразово встановлюються на ПК і напротязі довгого часу виконують свої функції. При цьому, троянський кінь не може самостійно переміститися з одного комп'ютера в локальній мережі на інший.

Причина великої поширеності даного типу ШПЗ криється в тому, що вони дуже непомітні. Часто вони є супутниками мережевих або поштових черв'яків. Так, поштовий хробак I- Worm.LovGate при попаданні на комп'ютер встановлює в систему модуль типу backdoor, що відкриває для зловмисника доступ до комп'ютера, використовуючи мережеву TCP / IP і відправляє йому лист, в якому вказується ім'я користувача, ім'я ПК і мережеву адресу зараженого комп'ютера, тобто початкові дані, які будуть використані для подальших атак на користувача [14].

Всі троянські програми діляться на три основні класи:

- **Логічні бомби** – ШПЗ, яке використовує різні методи для видалення або модифікації інформації в певний час або з використанням певної умови, наприклад, настання певної дати або часу.
- **Шпигунські програми** – вони збирають інформацію про користувача, сортують її певним чином та відправляють зібрані дані за допомогою електронної пошти, хоча користувач і може помітити, що програма відправила лист зловмиснику, але через специфічну роботу електронної пошти, видалити такий лист неможливо.
- **Програми типу BackDoor** – дані програми створюються для організації віддаленого управління ПК жертви або отримання команд від зловмисника, наприклад,

використовуючи вже відому адресу корпоративної електронної пошти, зловмисник може відправляти інше ШПЗ, таким чином взаємодіючи з програмами даного типу.

Всі три типи програм є однаково небезпечними для користувачів та компанії. Кожен з них здатний або знищити дані, або вкрасти цінну інформацію, що здатне нанести матеріальної та репутаційної шкоди [16].

2.3 Брутфорс

Брутфорс (Brute force) – також відомий як метод «Грубої сили», є одним з популярних методів несанкціонованого доступу до КЕП, який полягає у принципі перебору паролів та логінів, до того часу, доки не буде знайдена правильна комбінація символів.

Метод злому брутфорс займає досить багато часу, але приносить багато користі зловмиснику, тому він залишається досить популярним методом злому у гакерів, а враховуючи те, що потужності сучасних ПК щороку лише збільшуються, то даний метод ставатиме лише популярнішим в майбутньому.

Даний спосіб підбору паролів хороший тим, що пароль можна зламати, але це може зайняти досить тривалий час, від декількох секунд, до років. Тому даний спосіб злому паролів не завжди є доцільним, якщо власник КЕП, яку хочуть зламати, поставився до захисту пошти ретельніше і не використав паролі типу «12345», «qwerty» або «password», а використав великі, малі символи, а також до всього цього додав цифри та дозволені спеціальні символи. Однак на спеціальних форумах та ресурсах можна знайти словники з паролями, які містять мільйони паролів справжніх користувачів, та шаблонів для паролів.

Найчастіше метод брутфорсу використовують для отримання несанкціонованого доступу до електронної пошти. При його отриманні, у гакера буде повний контроль над всією інформацією, що знаходиться на електронній пошті. На даний момент, сотні гакерів кожного дня зламують тисячі електронних адрес, в пошуках різноманітної інформації. Листи, що містяться на електронній пошті гакери най-

частіше використовують для злому інших сервісів, до яких ця пошта прив'язана. Найпоширеніші випадки злому електронної пошти, це спосіб отримати доступ до сторонніх ресурсів, наприклад:

- Соціальних мереж: Facebook, Instagram, YouTube і т.д.
- Ігрових платформ: Steam, GoG, Epic Store, Playstation Network і т.д.
- Онлайн гаманців: PayPal, Payeer, Global24 і т.д.

Однак у випадку корпоративної електронної пошти, зловмисники намагатимуться в вкрасти корпоративні документи компанії, які надсилалися або були отримані в цій пошті, потім гакери намагатимуться шантажувати компанію зливами цієї інформації їх конкурентам, що нанесе непоправну шкоду. Також зловмисники можуть використати цю пошту для надсилання ШПЗ іншим користувачам, які вважають цю пошту надійною, що паралізує роботу компанії [17].

Види брутфорсу:

1. **Брутфорс за допомогою словників паролів:** сутність цього методу заключається в тому, що для нього необхідний лише логін електронної пошти, до якого буде підбиратися пароль та словник паролів, який ймовірно цей пароль містить. Даний тип брутфорсу вимагає пристойну кількість часу, тому що в найбільших словниках міститься декілька мільярдів типів паролів. Списки паролів можуть містити різні слова та комбінації слів, такі як прості слова, числа, дати народження та інші персональні дані. Існує багато різних словників паролів, які можна знайти в мережі або створити самостійно.

2. **Метод прямого брутфорсу** - метод для якого потрібна база даних, що містить в собі адреси електронних скриньок у вигляді mail;pass, user;pass, number;pass. Загроза цього методу заключається в тому, що для отримання такої бази даних не потрібно мати професійні навички або витрачати багато часу. Щоденно гакери з усього світу викладають у мережу або продають на спеціалізованих форумах тисячі таких баз, серед якої може бути й пошта вашої компанії. Прямий брутфорс є найбільш простим і прямолінійним видом атаки. За допомогою програмного забезпечення, яке автоматично перебирає всі можливі комбінації символів, зловмисники можуть зламати пароль

дуже швидко. Чим складніше пароль, тим більше часу зловмисникам потрібно для його зламання.

3. **Брутфорс повного перебору паролю** – даний метод направлений на конкретну електронну пошту. Він схожий на брутфорс за допомогою словників паролів, однак тут використовується підбір по одному символу, тобто мільйони комбінацій, з цим методом практично не використовують. Цей метод можна використовувати для злому паролів будь-якої складності, оскільки він здатний перебрати всі можливі комбінації символів пароля. Однак, його успішність залежить від кількості можливих комбінацій, які можуть складатися з символів пароля. В Таблиці 2.1 наведено кількість комбінацій для паролів та час на їх перебір, в залежності від їх довжини, за умови, що швидкість перебору складає 100000 паролів в секунду.

Таблиця 2.1

Таблиця комбінацій для паролів

Кількість знаків	Кількість комбінацій	Стійкість	Час перебору
1	36	5 біт	менше 1 секунди
2	1296	10 біт	менше 1 секунди
3	46656	15 біт	менше 1 секунди
4	1679616	21 біт	17 секунд
5	60466176	26 біт	10 хвилин
6	2 176 782 336	31 біт	6 годин
7	78 364 164 096	36 біт	9 днів
8	$2{,}821\ 109\ 9 \times 10^{12}$	41 біт	11 місяців
9	$1{,}015\ 599\ 5 \times 10^{14}$	46 біт	32 роки
10	$3{,}656\ 158\ 4 \times 10^{15}$	52 біти	1 162 роки
11	$1{,}316\ 217\ 0 \times 10^{17}$	58 біт	41 823 роки
12	$4{,}738\ 381\ 3 \times 10^{18}$	62 біти	1 505 615 роки

Таким чином, брутфорс повного перебору паролю може бути дуже ефективним, якщо пароль складається з невеликої кількості символів. Однак, для паролів, які складаються з більшої кількості символів, такий метод може займати значно більше часу.

2.3.1 Програмні засоби для брутфорсу

Програмні засоби для брутфорсу - це ШПЗ, які автоматизує процес перебору можливих комбінацій паролів, логінів або інших ідентифікаторів доступу для несанкціонованого доступу для електронної пошти. Такі програми можуть бути використані для зловживання та порушення безпеки системи. Принцип її роботи заключається в тому, що програма зв'язується сервером електронної пошти за допомогою проксі-сервера який вказується в даній програмі. Далі поштовий сервер надсилає відповідь з результатом авторизації, тобто чи підійшов пароль до тієї пошти, яка була взята з бази даних. Найбільша загроза від таких програм заключається в тому, що для користування ними, не потрібно знати мов програмування, тому що дане програмне забезпечення можна знайти у вільному доступі.

Ці програми створені з хорошим інтерфейсом, який буде зрозумілий більшості користувачів. Також вони мають багатий функціонал, такий як:

1. Використання різних видів проксі серверів (HTTPS, SOCKS4, SOCKS4a, SOCKS5).

2. Використання різних видів баз даних які місять назви електронних адрес та паролі (mail;pass, number;pass, user;pass).

3. Наявність пошуку на пошті електронних листів від конкретного відправника, тобто можна вказати поштову адресу відправника і програмне забезпечення знайде всі листи, які були ним прийняті або відправлені. Це частіше всього використовують, для пошуку листів від онлайн банків, крипто-гаманців та конкретних фірм, які займаються фінансами або інших сторонніх ресурсів, до яких потрібно отримати несанкціонований доступ.

4. Налаштування підключення до електронної пошти, тобто вибір між протоколами POP3 і IMAP.

5. Збереження результатів до окремих текстових файлів.

Дане програмне забезпечення є легкодоступним і його знаходження в мережі не складе великих проблем. Деякі програмні засоби створені для брутфорсу можуть бути умовно легальними, наприклад, якщо необхідно протестувати власну корпоративну електронну пошту на можливий предмет злому з боку зловмисників, для подальшого

підвищення її захисту від несанкціонованого доступу. Однак в статті 361, пункту 1, Кримінального кодексу України зазначено: «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.» [18]. Тому можна зробити висновок, що використання даного програмного забезпечення заборонене на території України.

2.3.2 Бази даних для брутфорсу

База даних для брутфорсу - це база даних, що містить список користувачів та їх паролів. Такі бази даних використовуються зловмисниками для несанкціонованого доступу до корпоративної електронної пошти, задля крадіжки конфіденційної інформації та інших зловмисних дій.

Бази даних для брутфорсу бувають 3 типів:

1. **Mail;pass** – така база даних представлена у вигляді адреси електронної пошти та паролю: login@mail.com;password. Даний вид авторизації користувачів, використовує більшість веб-сайтів, бо він дуже простий в розумінні та найкраще запам’ятовується.

2. **Number;pass** – даний вид бази даних являє собою номер телефону та пароль: phone_number;password. Цей вид авторизації на даний час розповсюджений не так сильно як mail;pass, через те, що для реєстрації свого облікового запису необхідно мати персональний номер мобільного телефону.

3. **User;pass** – ця база даних представлена у вигляді логіну та паролю: user;password. Таку авторизацію, найчастіше використовують веб-сайти, які не потребують електронної пошти для авторизації, тому дізнатись справжню електронну пошту власника такого облікового запису, використовуючи даний спосіб авторизації, зловмисник не може.

На жаль, в наш час, у відкритому доступі дуже багато таких баз даних. Пов’язано це передусім з розвитком комп’ютерних технологій, що спрощує гакерам

їх злочинну діяльність. Однак, перед тим, як такі бази даних потраплять до відкритого доступу, вони проходять декілька етапів.

На першому етапі, коли гакери намагаються отримати доступ до БД сайту, вони можуть дістати всю інформацію у вигляді HTML коду, таблиць SQL, текстових файлів і так далі. Всі файли такого типу, називаються дампами. **Дамп** - це копія даних з одного джерела, збережена у вигляді файлу, який може бути використаний для відновлення цих даних в майбутньому. У контексті баз даних, дамп зазвичай створюється з метою зберігання резервних копій баз даних, щоб мати можливість відновити дані в разі їх втрати, пошкодження або інших проблем. Він може бути виконаний вручну за допомогою спеціальних програм, або автоматично настроюватися на сервері баз даних за розкладом. Однак слід відмітити, що більшість веб-сайтів використовують методи шифрування паролів, а порою і всієї конфіденційної інформації користувачів. Через це, навіть якщо гакер і отримав доступ до бази даних сайту, він однаково не зможе використовувати цю інформацію, без знання спеціального ключа, за допомогою якого було зашифровано ці паролі та логіни. Однак, задачею розшифрування такої інформації займаються люди іншої спеціалізації – криптоаналітики.

На другому етапі, криптоаналітики використовують свої методи, задля розшифровування бази даних для отримання повного обсягу необхідної інформації. На даному етапі, вони також використовують метод брутфорсу, через те, що для розшифрування документу необхідно підібрати спеціальний ключ. На щастя, такий спосіб злому використовує мільйони комбінацій, тому розшифрування документу займає величезну кількість часу. Щоб розшифрувати такі фали, криптоаналітику необхідно мати сервери з величезною кількістю процесорів та відеокарт, однак через ситуацію на ринку відеокарт, на даний момент, такий метод вимагає великої кількості коштів та ресурсів. Однак, на чорному ринку, за розшифрований дамп, замовники готові платити тисячі доларів, якщо конкуруюча компанія понесе через це великі збитки.

На третьому етапі, після розшифровки криптоаналітиком бази даних, він пересилає її замовнику, в ролі якого, як правило, виступає гакер. В свою чергу гакер вирішує, що далі робити з цією базою даних. Однак слід зауважити, все що має на меті

гакер це вигода і несанкціоновані дії щодо користувачів сайту, з якого було отримано базу даних. Зловмисник може продати базу на чорному ринку, або використати дані в своїх цілях. На цьому моменті, коли гакер використав розшифровану базу даних у власних інтересах, він може передати її до мережі, у відкритий доступ, де всі охочі можуть нею скористатися, саме через це, даний етап несе велику небезпеку, тому що потрапивши у руки іншого зловмисника, він може використати цю базу даних у зовсім інших цілях, що нанесе ще більше збитків.

Висновки до другого розділу

Хоча корпоративна електронна пошта є популярним методом обміну повідомленнями, однак в процесі її використання існують серйозні загрози безпеці, які можуть бути потенційно небезпечними як для користувачів так і для компаній.

Велика кількість спаму може «завалити» поштові скриньки співробітників і заважати нормальній роботі. Флуд-атаки, коли на адресу електронної пошти надходять величезні обсяги повідомлень, також можуть перевантажити систему та призвести до затримок в роботі КЕП.

Зловмисники використовують методи фішингу для викрадення особистої інформації, облікових даних або навіть фінансових ресурсів. Вони можуть надсилати підроблені електронні листи, що схожі на офіційні повідомлення, або використовувати маніпулятивні техніки для отримання доступу до важливої інформації.

Корпоративна електронна пошта може бути використана для розсилки шкідливих програм, таких як віруси, троянські програми або шпигунське ПЗ. Ці програми можуть пошкодити систему, викрасти інформацію або встановити незаконний доступ для зловмисників.

Використання слабких або легко відгадуваних паролів може зробити облікові записи корпоративної електронної пошти вразливими до зламу. Також, недостатня практика регулярної зміни паролів або використання одного пароля для різних сервісів може збільшити ризик несанкціонованого доступу.

Недостатня свідомість та недостатні знання про безпеку електронної пошти серед співробітників можуть призвести до небезпеки. Необережні дії, такі як відкриття підозрілих посилань або відповіді на фішингові листи, можуть призвести до компрометації системи та витоку конфіденційної інформації.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

3.1 Захист КЕП від методу атаки брутфорс

Як зазначено в другому розділі, метод атаки брутфорсом є досить поширеним явищем в мережевому середовищі, більшість поштових сервісів ніяк не захищені від даного типу атак, тому єдиний спосіб захисту від них, це дотримуватися рекомендацій, які повинні забезпечити захист корпоративної електронної пошти. На жаль, з розвитком в галузі комп'ютерних технологій, неможливо забезпечити стовідсотковий захист облікових записів від злому збоку зловмисників, однак якщо дотримуватися всіх рекомендацій щодо захисту КЕП, то це зменшить вірогідність злому до мінімуму.

Хоча певні ресурси на які забезпечують функціонування корпоративної електронної пошти, не піддаються брутфорсу програмним методом, наприклад, Gmail, Hotmail та Zoho, вони відслідковують всі запити, що надсилає програмне забезпечення для брутфорсу та блокують доступ до пошти, однак це не гарантує повну безпеку, тому користувачам необхідно власноруч налаштовувати КЕП від несанкціонованого доступу.

3.1.1 Створення надійного паролю

Користувач може захистити свою пошту від методу брутфорсу – самостійно. Виходячи з другого розділу, можна зрозуміти, шанс того, що гакери отримають базу даних для брутфорсу є дуже малим. Через це, гакери не завжди намагаються отримати доступ до цієї бази даних. Тому, користувачу необхідно використовувати різні паролі для КЕП та інших сторонніх ресурсів, це різко зменшить шанс того, що зловмисник зможе отримати доступ до пошти. Однак, необхідно звернути увагу на те, що всі паролі, не мають бути схожими один на одного, а мати кардинальні відмінності, така

необхідність зумовлена тим, щоб у разі отримання гакером одного з паролів користувача, він не міг шаблонним методом отримати пароль для корпоративної електронної пошти.

Для того, щоб створити надійний пароль, що забезпечить його надійність від злому гакерами – необхідно дотримуватися наступних рекомендацій:

1. **Уникати від використання особистої інформації**. Особиста інформація включає в себе ім’я, дату народження, домашню адресу, номер телефону та іншу інформацію, що може знаходитися у вільному доступі. Хоча паролі створені таким методом легше запам’ятовуються, однак це спростить гакеру його роботу;

2. **Використовувати довгий пароль.** Чим пароль довший, тим більша ентропія, таким чином, його буде набагато важче зламати. Для кращого захисту – треба використовувати не менше 15 символів.

3. **Використовувати різні символи**. Для покращення якості паролю, окрім звичайних літер, необхідно використовувати великі літери, цифри та спеціальні символи типу !, @, #, $, % і т. д.

4. **Не використовувати словникові слова.** Дуже часто гакери використовують метод перебору за словником і якщо такі слова будуть використані в паролі, то це збільшить шанс на його злом.

5. **Необхідно уникати простих фразеологізмів**. Фрази по типу «mypassword» або «ilovecats», легко зламуються.

6. **Не використовувати паролі від вже зламаних облікових записів.** Гакери використовують різні бази даних які містять паролі, від зламаних облікових записів . Якщо ваш пароль скомпрометовано (дізнайтеся про це за допомогою нашого інструменту), хакери зможуть легко його вгадати.

7. **Використовувати генератор паролів.** Генератор паролів — це певний інструмент, що допомагає користувачам створити пароль, на злом якого знадобиться дуже багато часу.

На останньому пункті, необхідно зупинитися детальніше. Хоча пароль можна розробити власними силами, але також це можна зробити за допомогою генератора

паролів, що забезпечить його надійність, складність та унікальність. Однак, недолік даного методу полягає в тому, що пароль згенерований такою програмою звичайному користувачеві майже неможливо запам’ятати, що вносить певні незручності в його подальшому вводі, однак його перевага заключається у відсутності такого пароля в словниках паролів, тобто він буде унікальним. Також, згенерований таким чином пароль, дуже складно підібрати методом повного перебору символів.

Використовуючи веб-сайт www.eset.com, який надає можливість згенерувати унікальний пароль, можна перевірити надійність таких паролів, наприклад, на рисунку 3.1 зображено згенерований пароль «wdzA0mqOs» за допомогою Генератора паролів. Для зручності, на сайті вже вказано надійність даного паролю.

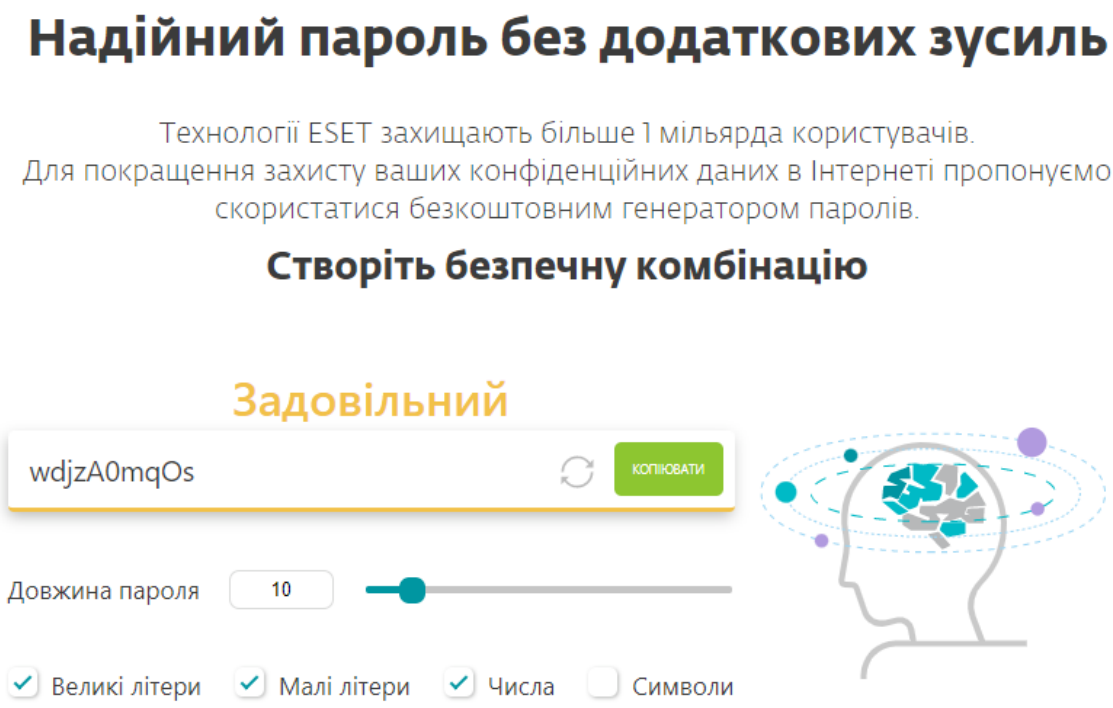

Рис. 3.1 — Генератор паролів

Однак для кращої перевірки надійності даного паролю, буде використано веб-сайт https://uk.vpnmentor.com/tools/passwordmeter . Як зображено на рис. 3.2, на злом

даного паролю, гакеру знадобиться приблизно 31 рік, хоч це і виглядає дуже переконливо, однак найкращу безпеку здатен забезпечити пароль в якого 15 і більше символів.

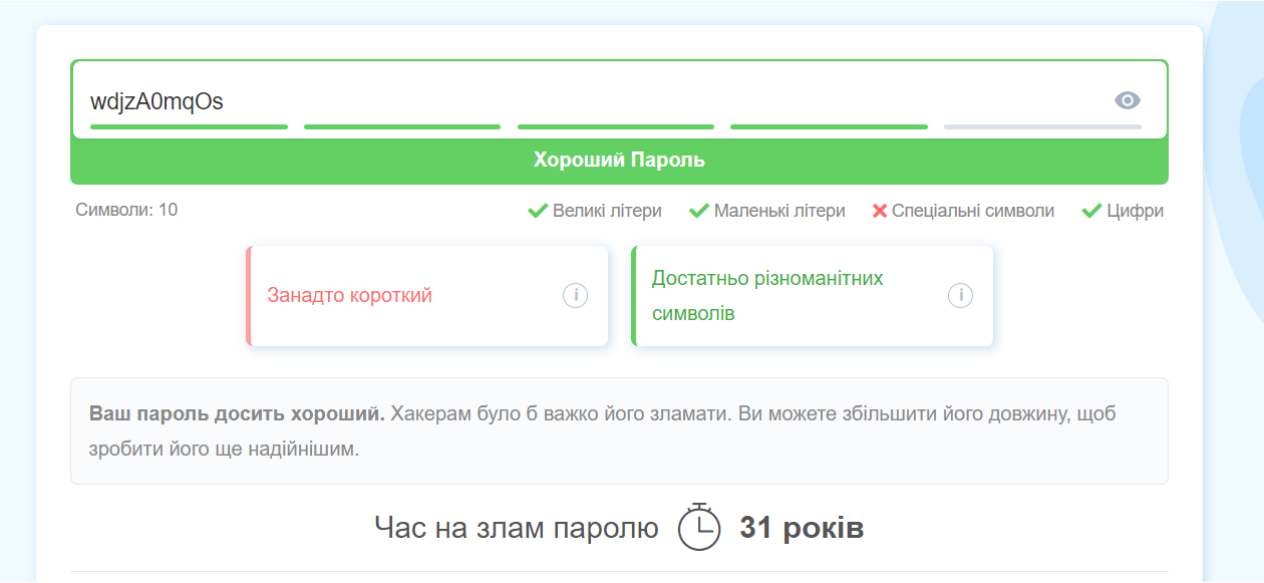

Рис. 3.2 — Перевірка надійності паролю

Як можна побачити на рис. 3.3, на пароль «WPs=YE=59Npo5DY» який включає в собі 15 символів, що був згенерований генератором паролів, гакеру знадобиться «століття» на його прямий злом.

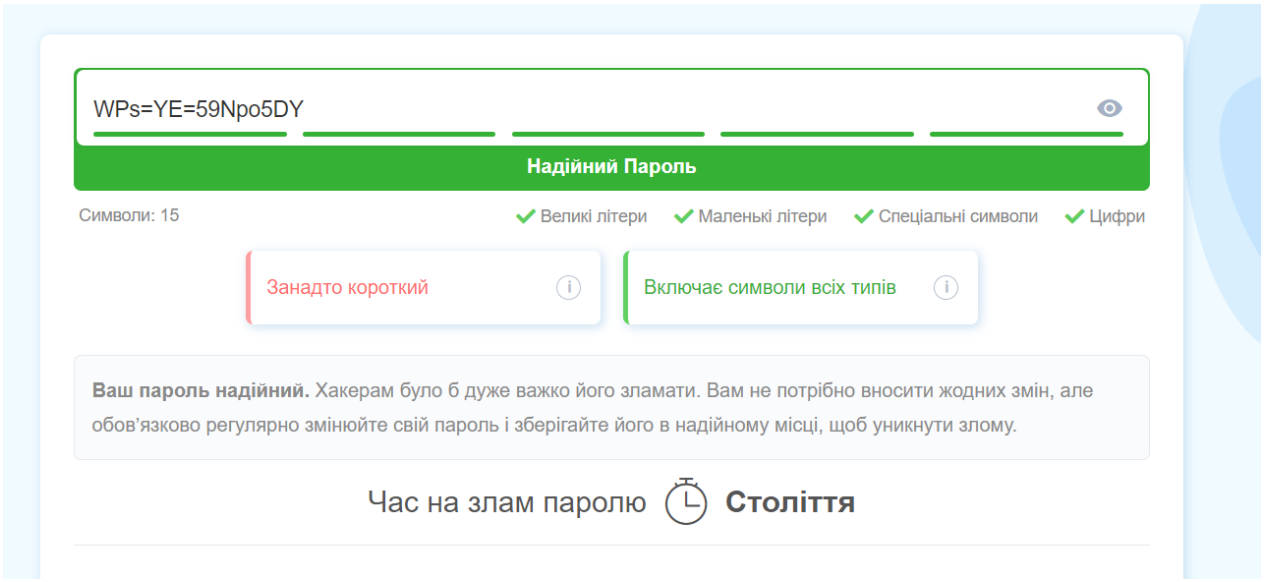

Рис. 3.3 — Перевірка надійності паролю з 15 символами

Тому, для захисту корпоративної електронної пошти рекомендується використовувати паролі, що згенеровані за допомогою генератора паролів, та містять 15 та більше символів.

3.1.2 Двофакторна аутентифікація

Використання надійного паролю дозволяє забезпечити надійний захист від методу брутфорс-атак. Однак, надійність захисту можна подвоїти – використовуючи двофакторну аутентифікацію. Двофакторна автентифікація – це використання одразу двох різних способів підтвердження. Вона дає можливість значно посилити рівень захисту корпоративної електронної пошти та убезпечити персональні дані від гакерів. Метод її роботи заключається в тому, що навіть якщо пароль до пошти було скомпрометовано, то для подальшого входу в обліковий запис знадобиться додаткове підтвердження. Тому для захисту КЕП – необхідно обов'язково використовувати двофакторну аутентифікацію, що забезпечить надійний захист від несанкціонованого доступу.

Zoho corporation, на якій знаходиться корпоративна електронна пошта, має декілька методів MFA:

1. **MFA на основі SMS** – для початку, необхідно зареєструвати SIM-карту на платформі Zoho. Після чого, при вході в КЕП, необхідно буде ввести не лише електронну пошту та пароль до неї, але й ввести спеціальний одноразовий код, який був надісланий на мобільний телефон, який було зареєстровано. Однак недоліком даного методу є те, що його можна обійти, якщо зловмисник вкраде SIM-карту користувача або якщо користувач отримує SMS на пристрій, який заражений шкідливим програмним забезпеченням.

2. **MFA на основі одноразового паролю –** принцип роботи такий самий, як і в MFA на основі SMS, однак одноразовий код прийде в спеціальний додаток OneAut, який необхідно буде ввести при аутентифікації до корпоративної електронної пошти. Даний метод є одним з найкращих, через те, що для того, щоб вкрасти такий код – зловмиснику необхідно вкрасти ваш телефон, що є дуже малоймовірним.

3. **MFA за допомогою ключового слова –** даний метод аутентифікації заключається в тому, що при в ході в обліковий запис окрім звичайного паролю необхідно

ввести спеціальне ключове слово. Ненадійність даного методу в тому, що зловмисники можуть з легкістю скомпрометувати таке слово, тому не рекомендується застосовувати даний мето двофакторової аутентифікації.

4. **MFA на основі ключа безпеки –** один з методів двофакторової автентифікації. Ключ безпеки - це фізичний пристрій, який зазвичай підключається до порту USB комп'ютера. При вході в систему, користувач вводить свій логін та пароль, а потім підключає Ключ безпеки до комп'ютера. Даний ключ генерує одноразовий код, який користувач повинен ввести для підтвердження своєї ідентичності. Його перевага заключається в тому, що його майже неможливо підробити і без даного ключа зловмисник не зможе увійти до корпоративної електронної пошти.

3.1.3 Додавання дозволених IP-адрес для входу

IP-адреса може використовуватися для обмеження доступу до певних ресурсів в інтернеті. Наприклад, компанія може обмежити доступ до своєї мережі тільки для працівників, які працюють в офісі, і встановити фільтри, які блокують доступ з інших місць.

Одним з методів захисту ресурсів від несанкціонованого доступу в корпоративну електронну пошту є налаштування списку дозволених IP-адрес. Це означає, що тільки користувачі з дозволеними IP-адресами можуть отримати доступ до ресурсу. Це може допомогти запобігти атакам ззовні, а також зменшити ризик порушення безпеки, якщо у користувача було викрадено логін пошти та пароль. Однак, варто зазначити, що цей метод не є повністю безпечним, оскільки IP-адреса може бути підроблена. Крім того, якщо користувачі динамічної IP-адреси, то їхній IP-адрес може змінюватися з часом, що може створювати проблеми з доступом до ресурсу.

У будь-якому випадку, список дозволених IP-адрес може бути корисним інструментом для забезпечення безпеки ресурсу. Важливо також періодично переглядати і оновлювати список дозволених IP-адрес, щоб виключити доступ з небезпечних мереж

або заблокувати доступ користувачів, які більше не повинні мати доступ до ресурсу. Дані дії дозволять збільшити безпеку корпоративної електронної пошти.

3.2 Захист КЕП від спаму

В наш час спамери збирають далі про електронні адреси з різних джерел, наприклад, форуми, соціальні мережі або з сайту компанії, де електронні адреси можуть знаходитися у відкритому доступі. Навіть якщо корпоративна електронна пошта не була передана третім особам, то вона все рівно може потрапити до бази спаму, наприклад, через взлом електронної пошти, на яку відправлялися листи з захищеної КЕП.

Якщо корпоративна електронна пошта потрапляє до бази спаму, то на цю пошту буде приходити багато листів від невідомих користувачів і позбутися від них є складною задачею. Однак, в такому випадку, головне дотримуватися наступних рекомендацій:

1) Якщо на пошту прийшов несанкціонований лист, то не потрібно його відразу відкривати, для початку треба перевірити чи є відправник цього листа в спам листах, наприклад, на сайті check.spamhaus.org зібрана велика база даних, в якій міститься багато доменів спамерів.

2) Якщо підозрілий лист прийшов від знайомої особи чи компанії, але сумніви відносно його “чистоти” все ж таки з'явилися, то рекомендовано зв’язатися з відправником за допомогою інших каналів зв’язку та уточнити чи справді цей лист був відправлений ним чи нею.

3) Якщо лист було відкрито, то в жодному разі не потрібно на нього відповідати. Якщо відповісти на цей лист, то спамери будуть розуміти, що дана КЕП існує і її власник досі активний. В таких листах часто використовуються певні маніпуляції, наприклад, можна відключити спам, натиснувши на певну кнопку, однак це пастка.

4) Не переходити по посиланню, що прикріплено в листі, якщо перейти по даному посиланні, то в користувача можуть бути вкрадені конфіденційні дані.

5) Якщо до листа прикріплений будь-який файл, в жодному разі не потрібно його завантажувати, бо це призведе до потрапляння в систему шкідливого програмного забезпечення, що виведе з ладу не тільки пошту, а й всю мережу.

При створенні корпоративної електронної пошти рекомендовано придумувати складну електронну адресу. Необхідно відштовхуватися, при виборі назви пошти, не від її милозвучності, простоти для запам'ятовування чи зручності при написанні, а навпаки, необхідно робити її якомога довшою. Це пов'язано з тим, що найчастіше всього обирають адреси для надсилання спаму, відштовхуючись від її престижної назви. Наприклад, шанс того, що корпоративна електронна пошта, що має назву адреси типу holowa@firmy.com , буде отримувати більше спаму ніж інші.

Зараз спамери використовують більш складних методів отримання електронних адрес. Вони застосовують спеціальні додатки під назвою - "словники", що генерують велику кількість символів, з яких складається електронна пошта. Однак це не єдиний спосіб, також спамери використовують спеціальні програми, що здатні завантажити електронні адреси із серверів. Однак існують методи захисту, від того, якщо КЕП потрапила до такої спам-бази:

1) **Чорні списки** - це записи електронних адрес або доменів, що раніше використовувалися для надсилання спаму. Коли фільтр буде створений і відправник листа присутній у чорному списку, то ця адреса буде вважатися небажаною і автоматично потраплятиме в спам. Наприклад, до чорного списку можуть потрапити ті електронні адреси які в минулому були помічені в шахрайстві. Основною проблемою чорного списку є те, що необхідно підтримувати його зміст в актуальному та достовірному стані.

2) **Білі списки** – є протилежними поняттю "чорний список". Вони складаються із списку електронних адрес та доменів, які є довіреними для користувача. Такі листи вважаються "білими" і можуть бути прочитані користувачем. Такий список можна налаштувати вручну і він буде мати набір довірених адрес та доменів, які можуть пройти через фільтри спаму та доставлятись до поштової скриньки. Білий список

дозволяє забезпечити надійний прийом листів від партнерів, клієнтів та інших довірених джерел.

Основний недолік білих списків полягає на припущенні того, що надійні електронні адреси не надсилатимуть небажану пошту. Однак, така теорія може виявитися невірною. Велика кількість спамерів використовує комп'ютери, які були уражені вірусами та троянами для розсилання розсилки спаму на всі контакти адресної книги, таким чином, можна отримати спам-повідомлення від надійного відправника, якщо його комп'ютер був заражений шкідливим програмним забезпеченням. Наприклад, корпоративна електронна пошта Zoho має налаштування чорного та білого списків, що зображено на рисунку 3.4, до яких можна додавати небажані електронні адреси, які автоматично потраплятимуть в спам, або довірені, що відправлятимуться у вхідні повідомлення.

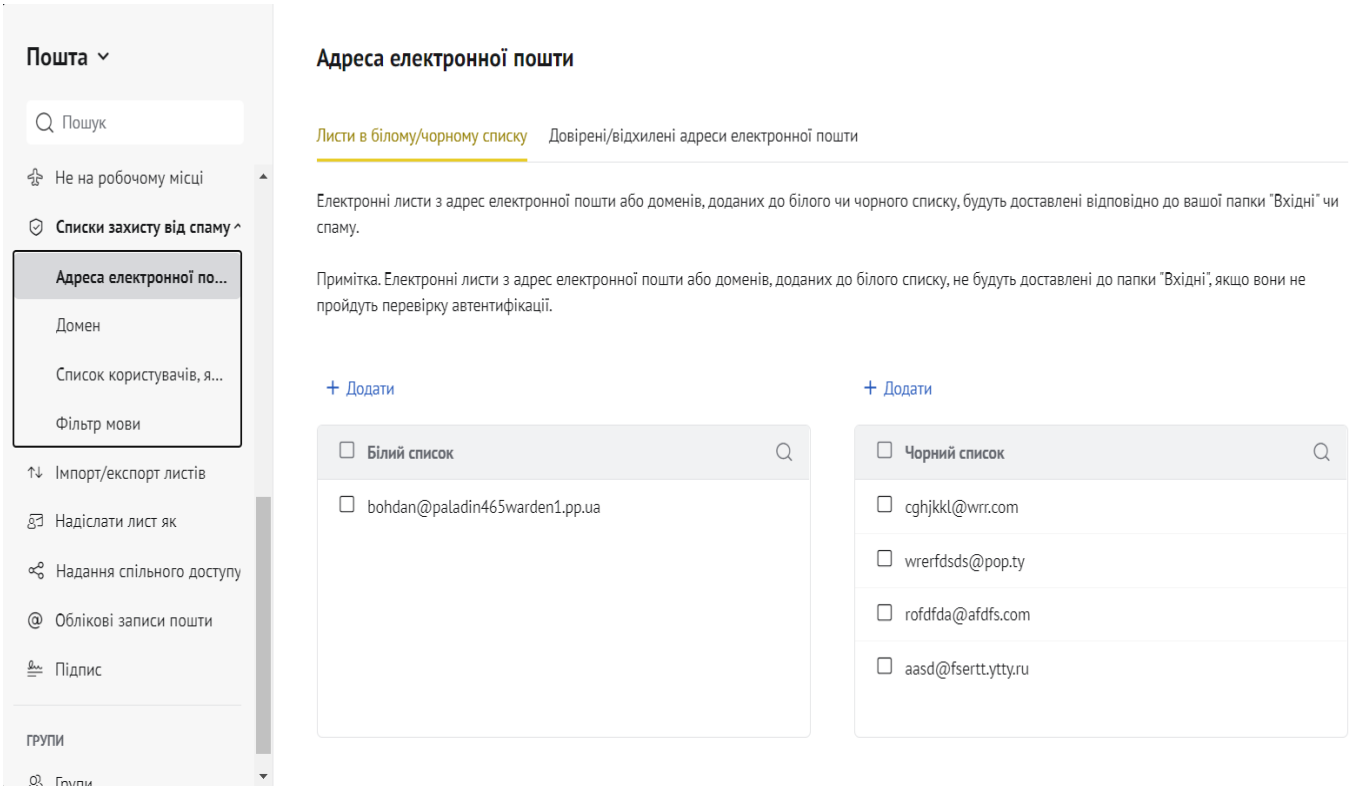

Рис. 3.4 — Білий та чорний списки в Zoho

3) **Сірий список** - це технологія фільтрації електронної пошти, яка дозволяє відсіяти небажані повідомлення від невідомих відправників. Коли повідомлення надходить на поштовий сервер отримувача, сервер може тимчасово відхилити його та

змусити відправника повторно надіслати повідомлення пізніше. Якщо повідомлення відправлене від легітимного відправника, то він спробує надіслати його ще раз через деякий час, тоді як надіслання спаму або фішингових повідомлень зазвичай не повторюються. Таким чином, сірий список допомагає знизити кількість небажаних повідомлень в корпоративній електронній пошті, але може затримувати доставку деяких легітимних повідомлень. Даний інструмент є більш надійним ніж чорні та білі списки, тому власникам корпоративної електронної пошти рекомендується його використовувати для захисту від спаму.

4) **Використання спам-фільтрів.** Спам-фільтри - це програми або сервіси, які автоматично відфільтровують небажані електронні листи з корпоративної електронної пошти. Вони працюють на основі різних алгоритмів і методів, щоб відрізняти електронні листи, які були надіслані спамерами від листів, що надіслали працівники компанії.

Основні методи спам-фільтрації включають:

- **Фільтрація на основі правил** - використовується набір правил, які відфільтровують спам на основі певних ключових слів або фраз, які зазвичай містяться в спам-листах.
- **Фільтрація на основі байесовських методів** - використовується статистичний аналіз для визначення того, чи є певний лист спамом, використовуючи модель ймовірності. Він використовується для визначення ймовірності того, що деяке повідомлення є спамом або не спамом. Алгоритм працює на основі попередньої навчальної вибірки спам та не спам повідомлень, з якої вивчається, які слова, фрази, символи, теми повідомлень та інші характеристики найчастіше використовуються в спамі та які - у легітимній електронній пошті.
- **Фільтрація на основі машинного навчання** - використовується навчання машини на великій кількості прикладів спаму та нелегітимних листів для визначення ймовірності того, що певний лист є спамом.

- **Фільтрація на основі списків блокування** - використовується список заблокованих IP-адрес, доменів та електронних адрес, які відомо пов'язані зі спамом або шахрайством.
- **Фільтрація на основі поведінки користувачів** - використовується аналіз поведінки користувачів для виявлення незвичайної або небезпечної активності, яка може вказувати на спам або шахрайство.
- **Фільтр мови** - це інструмент, який дозволяє фільтрувати та блокувати небажану мову, якою надсилаються листи на електронну пошту. В Zoho користувач може самостійно налаштувати даний фільтр. Наприклад, якщо листування з працівниками відбувається виключно українською мовою, то буде розумним заборонити листи, які будуть надходити всіма іншими мовами, що дозволить вберегти КЕП від великої кількості спаму з інших країн. Такий фільтр застосовується в системі КЕП Zoho, він зображений на рис. 3.5.

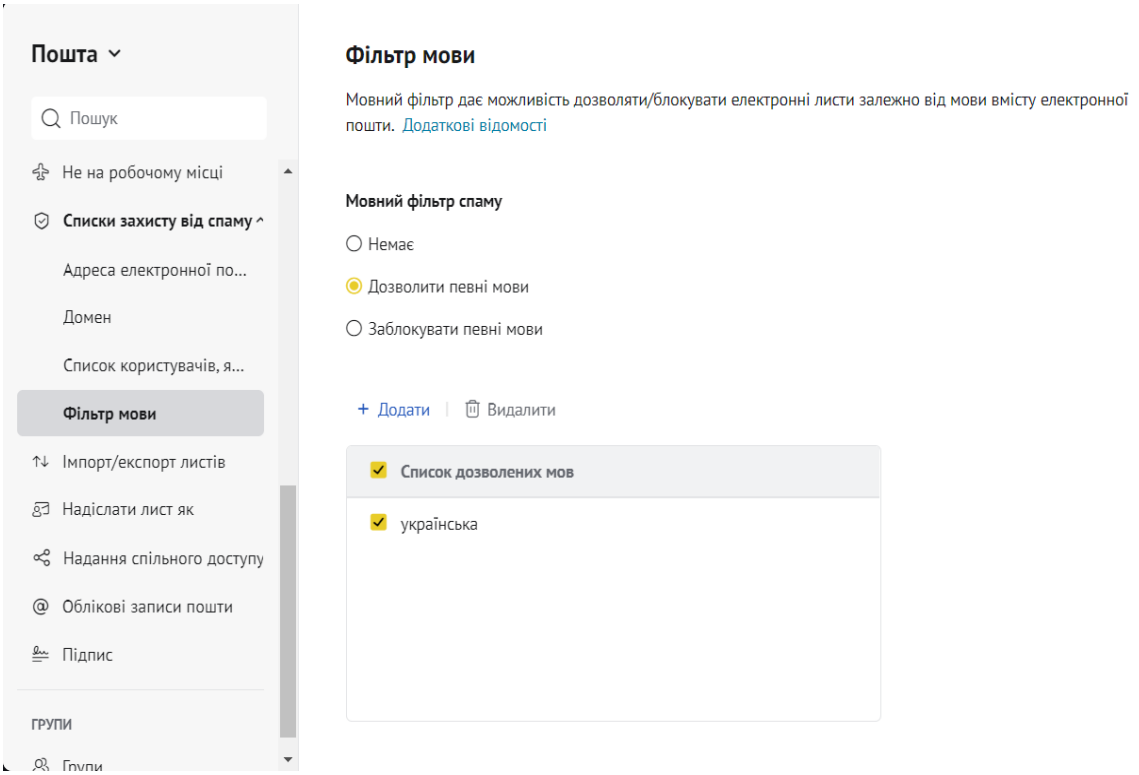

Рис. 3.5 — Фільтр мови в Zoho

5) **DKIM** (DomainKeys Identified Mail) - це технологія, яка допомагає перевіряти, що електронні листи були надіслані відповідно з домену, який заявлено в полі "відправник" електронного листа.

Для цього при відправленні листа в заголовок додається цифровий підпис, який засвідчує автентичність домену відправника. При отриманні листа, поштовий сервер отримувача перевіряє цей підпис за допомогою публічного ключа, який зберігається у DNS записах домену відправника. Якщо підпис справжній і збігається з публічним ключем, то лист буде відправлено адресату, однак в іншому випадку, він може бути помічений як недостовірний і потрапити в спам.

Використання DKIM допомагає захистити пошту від фішингу та інших видів шахрайства, пов'язаних зі зловживанням відправницьких адрес.

3.3 Захист КЕП від шкідливого програмного забезпечення

З розділу 2 можна зрозуміти, що віруси несуть найбільшу небезпеку для компанії, оскільки можуть повністю паралізувати її роботу. Саме тому, використання антивірусного захисту в корпоративній електронній пошті є дуже важливим. Антивірусний захист допомагає виявляти та блокувати шкідливі програми, які будуть прикріплені в електронних листах.

Антивірусний захист також допомагає попередити передачу шкідливих програм через електронну пошту до інших користувачів, що може значно зменшити ризик поширення вірусів і шкідливих програм в мережі організації. Окрім того, використання антивірусного захисту може допомогти виявити та запобігти атакам зловмисників на корпоративну мережу. Зловмисники можуть використовувати електронну пошту як вектор атаки, щоб проникнути в систему та виконати шкідливі дії.

Одним з методів захисту від шкідливого програмного забезпечення для корпоративної електронної пошти – є використання антивірусного програмного забезпечення ESET Internet Security. Даний антивірус виявляє та блокує віруси та інші

шкідливі програми, що можуть поширюватися через електронну пошту, за допомогою листів.

На рисунку 3.6 зображено налаштування «Захисту поштового клієнта» антивірусу ESET Internet Security, які користувач може використовувати для захисту корпоративної електронної пошти для захисту від шкідливого програмного забезпечення. Користувач може відфільтрувати захист на свій лад, наприклад, які саме листи додатку необхідно сканувати для виявлення ШПЗ.

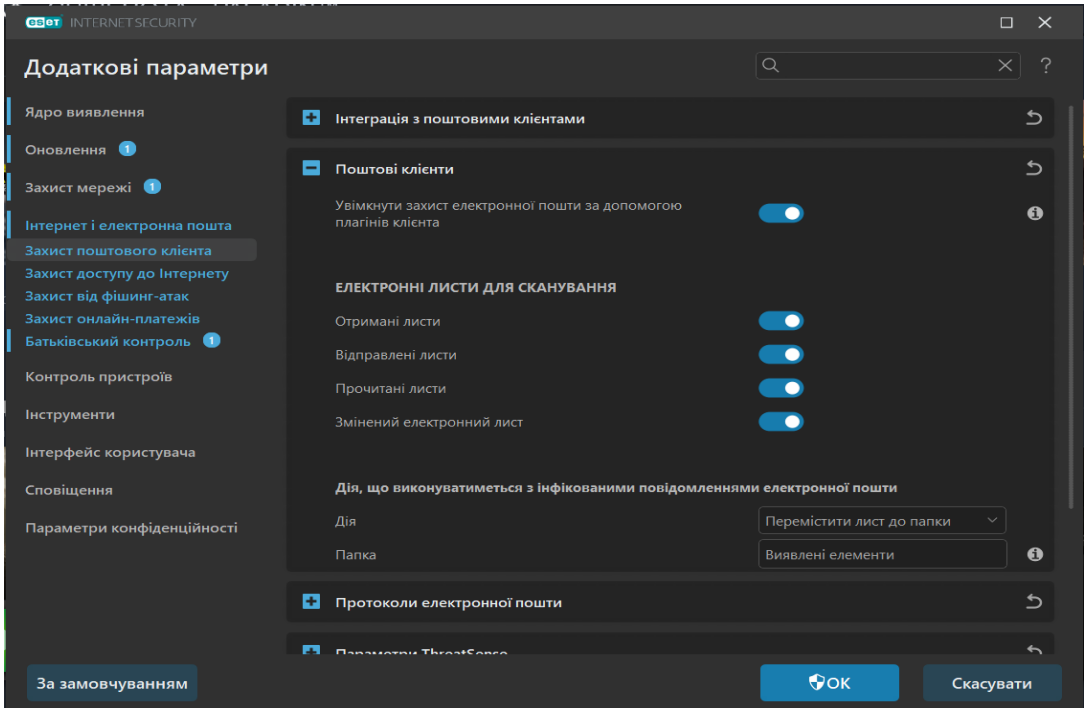

Рис. 3.6 — Налаштування «Захисту поштового клієнта»

Також даний антивірус дозволяє захисти користувачів не лише від ШПЗ, а й від фішингових посилань, що прикріплюються до вхідних листів, ESET має базу даних, в якій містяться багато посилань, що дозволяє уникнути листів з фішингом. На рисунку 3.7

Рис. 3.7 — Налаштування Eset захисту від фішинг-атак Eset

Загалом, для ефективного захисту корпоративної електронної пошти від вірусів рекомендується використовувати комплексний підхід, що включає в себе встановлення та налаштування антивірусного програмного забезпечення на всіх комп'ютерах і серверах, використання спам-фільтрів, обмеження можливості виконання програм та скриптів в електронних листах, а також проведення регулярних навчань та інструктажів співробітників з питань кібербезпеки та протидії соціальному інжинірингу. Доцільно також розглядати можливість використання спеціалізованих апаратних засобів, таких як файрволи та системи виявлення вторгнень, для додаткового захисту мережі інформаційної безпеки компанії.

3.4 Захист електронних листів в КЕП

Хоча при відправці повідомлення в електронній пошті лист шифрується власними протоколами, однак з розвитком технологій, зловмисники можуть його перехопити в процесі доставки та розшифрувати. Тому для підвищення захисту, рекомендується власноруч зашифровувати повідомлення, які відправляються в КЕП.

Щоб зашифрувати повідомлення в корпоративній електронній пошті, можна використовувати протокол S/MIME. Цей протокол дозволяє зашифрувати та підписати електронну пошту з використанням цифрових сертифікатів. Це забезпечує високий рівень безпеки та захисту конфіденційної інформації.

Для того, щоб зашифрувати повідомлення в корпоративній електронній пошті за допомогою протоколу S/MIME, необхідно мати встановлений цифровий сертифікат. Цифрові сертифікати можуть бути видані різними організаціями, такими як компанії, установи або державні органи. Зазвичай, для отримання цифрового сертифікату потрібно пройти процедуру перевірки особи, що гарантує, що тільки власник сертифікату зможе використовувати його для шифрування та підпису електронних повідомлень.

Після того, як цифровий сертифікат отриманий та встановлений на комп'ютері, можна використовувати S/MIME для шифрування та підпису електронних повідомлень. Для зашифрування повідомлення необхідно обрати опцію "шифрувати" та вибрати цифровий сертифікат відправника. Таким чином, тільки отримувач, який також має свій власний цифровий сертифікат, зможе розшифрувати повідомлення та прочитати його

3.5 Захист КЕП на законодавчому рівні

В Україні захист корпоративної електронної пошти регулюється Конституцією України, Законом України "Про захист персональних даних", Законом України "Про електронні документи та електронний документообіг", Законом України "Про інформацію", а також іншими нормативними актами.

Наприклад, Закон України "Про захист персональних даних" встановлює правила збору, обробки та зберігання персональних даних, включаючи електронну пошту. Закон України "Про електронні документи та електронний документообіг" встановлює вимоги до електронної пошти як засобу електронного документообігу.

Компанії, що працюють в Україні, повинні дотримуватися всіх законодавчих вимог щодо захисту корпоративної електронної пошти та персональних даних. Також компаніям рекомендовано розробити певні документи, які можуть включати політики безпеки, процедури, правила та рекомендації:

- Політика безпеки повинна визначати загальні принципи та мету захисту електронної пошти, а також визначати відповідальності та обов'язки всіх працівників, які мають доступ до корпоративної електронної пошти.
- Процедури повинні описувати практичні кроки, які потрібно вживати для захисту електронної пошти. Наприклад, процедури можуть включати інструкції щодо реєстрації нових користувачів електронної пошти, налаштування фільтрів спаму та вірусів, зміни паролів та ін.

- Правила повинні детально описувати те, що дозволено та не дозволено робити з корпоративною електронною поштою, включаючи обмеження щодо відправлення конфіденційної інформації та прикріплення файлів.
- Рекомендації можуть включати поради та практичні поради щодо захисту електронної пошти, такі як частота зміни паролів та перевірка електронної пошти на наявність спаму та вірусів.

Важливо ці документи регулярно оновлювати, щоб вони відображали останні тенденції та загрози в галузі захисту електронної пошти.

Висновки до третього розділу

Досліджуючи основні загрози, які існують в корпоративній електронній пошті, було розроблено рекомендації, дотримуючись яких окремі користувачі та компанії зможуть забезпечити захист власних КЕП, які вони використовують у власних цілях.

Рекомендації були розроблені на основі існуючих загроз, які були описані в другому розділі даної бакалаврської роботи. Вони засновані на створенні надійного паролю, використання якого здатне підвищити захист КЕП від атаки методом брутфорс, для збільшення надійності від взлому, користувачам рекомендується використовувати багатофакторну аутентифікацію, що зменшить ефективність даного методу атаки до мінімуму. Також, користувачі можуть додавати діапазон IP-адрес, з яких буде дозволено здійснювати вхід, що посилить захист від атаки брутфорс.

Для захисту від спаму, користувачам рекомендовано використовувати різні спам фільтри, що забезпечить певний рівень чистоти на робочому місці, хоча з розвитком IT-сектору в світі, гакери знаходять способи обійти такий метод захисту, то користувачі повинні ретельно перевіряти листи, отримані від незнайомих електронних адрес та не відкривати такі листи.

Для захисту від ШПЗ, рекомендовано використовувати спеціальні утиліти - антивіруси, які здатні виявляти потенційно небезпечні файли та забезпечувати захист ПК користувача. Також такі програми здатні фільтрувати самостійно електронні листи, що підвищить безпеку КЕП.

Щоб захистити повідомлення та файли, які надсилаються електронною поштою, рекомендується власноруч зашифровувати їх за допомогою спеціальних цифрових сертифікатів.

Окрім цього, компанії повинні дотримуватися всіх законодавчих вимог України, щодо захисту корпоративної електронної пошти та персональних даних. Рекомендується створити власну політику безпеки, яка буде включати дані рекомендації та проводити тренінги власного персоналу, який користується КЕП компанії.

ВИСНОВОК

Корпоративна електронна пошта є важливим інструментом комунікації для багатьох організацій. Вона відрізняється від звичайної електронної пошти своїми особливостями і функціоналом, що спрямовані на задоволення потреб і вимог бізнесу. Свідоме використання корпоративної електронної пошти сприяє покращенню продуктивності та співпраці всередині організації. Вона дозволяє легко обмінюватися інформацією, планувати зустрічі, вирішувати завдання і підтримувати зв'язок між співробітниками.

Проте, захист корпоративної електронної пошти має вирішальне значення. Існують різні загрози, які можуть призвести до витоку конфіденційної інформації, кібератак або інших негативних наслідків для компанії.

У бакалаврській атестаційній роботі були розглянуті та вирішені такі задачі:

1) У першому розділі було розглянуто принципи роботи корпоративної електронної пошти, яким чином здійснюється її функціонування та які проколи найчастіше використовуються для передачі та захисту електронних листів.

2) В другому розділі було досліджено основні загрози які здатні зашкодити роботі КЕП та несуть велику загрозу компаніям.

3) По закінченню дослідження, в третьому розділі, було розроблено рекомендації, які знадні забезпечити комплексний та ефективний захист користувачам при роботі з корпоративною електронною поштою.

Загалом, при дотриманні всіх рекомендацій, які були описані в третьому розділі, користувачі та компанії зможуть істотно підвищити захист своїх корпоративних електронних скриньок від різних атак та витоку конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кудрявцева С. П. Міжнародна інформація: навчальний посібник / С. П. Кудрявцева, В. В. Колос. – К.: Видавничий дім «Слово», 2005. – 400 с.

2. Сучасна інформатика [Електронний ресурс] – Режим доступу: World Wide Web. – URL: http://alextexnok.blogspot.com/p/blog-page_55.html

3. Що таке домен [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://hostiq.ua/ukr/info/what-is-domain/

4. Горбатий І.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / І.В. Горбатий, А.П Бондарєв. — Львів: Львівська політехніка, 2016. — 336 с.

5. Furnell L. E-mail Security. A Pocket Guide. / L. Furnell, P. Dowland. – UK: IT Governance Publishing, 2010. – P. 100

6. Choosing a POP3 Email App: All You Need to Know About Email Protocols [Електронний ресурс] – Режим доступу: https://www.getmailbird.com/pop3-email-account/

7. Проксі-сервер: що це таке і чи потрібен він вам? [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://surfshark.com/uk/blog/proxy-server

8. What is spam? [Електронний ресурс] – Режим доступу: World Wide Web. – URL:https://www.malwarebytes.com/spam

9. Що таке фішинг, та як від нього захиститися? [Електронний ресурс] / І. Молодження / 2019. – Режим доступу: World Wide Web. – URL: https://loando.ua/statis/shho-take-fishing-ta-yak-vid-nogo-zahistitisya

10. Різни види фішингових атак [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing

11. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/

12. Що таке макровіруси [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://best-free-soft.at.ua/publ/bezpeka_pk_shho_take_makrovirusi/shho_take_makrovirusi/16-1-0-63

13. Macro.Word 97.Thus.DA - новий і дуже небезпечний макровірус [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://unasoft.com.ua/ukr/news.php?id=9&sites=Ukraine

14. Коваленко М. М. Комп'ютерні віруси і захист інформації / М. М. Коваленко. - К.: Наук.думка, 1999. - 262 с.

15. ILOVEYOU – вірус всепоглинаючої любові [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://publish.com.ua/it-ta-web/i-love-you-virus-vsepoglinayuchoji-lyubovi.html

16. Троянські програми [Електронний ресурс] – Режим доступу: World Wide Web. – URL: http://pro-computer.pp.ua/4147-scho-take-troyani-scho-voni-roblyat-yak-vd-nih-zahistitisya-vse-pro-kompyuter.html

17. Brute Force Attack [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.imperva.com/learn/application-security/brute-force-attack/

18. Розділ XVI Кримінального Кодексу України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" [Електронний ресурс] / Стаття 361 в редакції Закону № 2289-IV від 19.11.2012 - Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/2289-15#Text