Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

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

спеціальність _____ 125 Кібербезпека
(код і назва спеціальності)

освітня програма _____ Кібербезпека
(назва освітньої програми)

на тему: «Засоби захисту інформації під час використання електронної пошти»

Виконавець: студент IV курсу, групи КБ-42

_____ **Ілля ГРИБАН**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності _____ 125 Кібербезпека
(код і назва спеціальності)

освітньої програми _____ Кібербезпека
(назва освітньої програми)

Студентові ___ **КБ-42** ___ **Грибану Іллі Олексійовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Засоби захисту інформації під час використання електронної пошти

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи та способи моделювання систем захисту електронної пошти, дослідження інфраструктури відкритих ключів, аналіз використання засобів захисту інформації

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно провести аналіз ефективних методів та систем які використовую для того, щоб захистити інформацію під час використання електронної пошти, провести порівняння та навести рекомендації для їх покращення

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Дослідження та аналіз ефективних методів захисту

інформації під час використання електронної пошти

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Ілля Грибан
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021-23.01.2022	*виконано*
2	Аналіз літератури	24.01.2022-13.02.2022	*виконано*
3	Збір відомостей щодо систем електронної пошти	24.02.2022-10.04.2022	*виконано*
4	Опис систем захисту електронної пошти	11.04.2022-24.04.2022	*виконано*
5	Дослідження властивостей засобів захисту електронної пошти	24.04.2022-16.04.2022	*виконано*
6	Проведення тестування технологій	17.04.2022-09.05.2022	*виконано*
7	Аналіз отриманих результатів дослідження	10.05.2022-03.06.2022	*виконано*
8	Оформлення пояснювальної записки	04.06.2022-06.06.2022	*виконано*
9	Підготовка до захисту дипломної роботи	07.06.2022-13.06.2022	*виконано*

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Ілля ГРИБАН
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Засоби захисту інформації під час використання електронної пошти» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 50 сторінок. Робота містить 6 рисунків, 5 таблиць. Список використаних джерел включає 40 джерел.

Мета роботи – розробка рекомендацій щодо захисту інформації під час використання електронної пошти.

Для досягнення зазначеної мети поставлено наступні завдання:

- Провести аналіз використання електронної пошти
- Провести аналіз вразливостей електронної пошти та додатків з якими вона взаємодіє
- Проаналізувати наявні технології захисту електронної пошти та рішення щодо їх використання
- Обґрунтування можливих методів та засобів захисту інформації електронної пошти
- Провести аналіз ефективних способів захисту інформації в сфері використання електронних скринь

Об'єкт дослідження – процес визначення ефективних засобів захисту інформації під час використання електронної пошти.

Предмет дослідження – методи, засоби і методики захисту інформації в системах електронної пошти

Розроблені рекомендації призначені для користувачів, що хочуть підвищити безпеку своїх даних при використанні електронної пошти

Ключові слова: електронна пошта, протоколи захисту інформації, моделювання засобів захисту, інфраструктура відкритих ключів, протоколи безпеки.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІВК	–	Інфраструктура відкритих ключів
MUA	–	Message User Agent
MTA	–	Message Transfer Agent
MDA	–	Mail delivery agent
MSA	–	Message Submission Agent
SMTP	–	Simple mail transfer protocol
POP3	–	Post Office Protocol 3
TCP	–	Transmission Control Protocol
IMAP	–	Internet Message Access Protocol
ПЗ	–	Програмне забезпечення
PGP	–	Pretty Good Privacy
S/MIME	–	Secure Multipurpose Internet Mail Extensions
PEP	–	Pretty Easy Privacy
PKI	–	Public Key Infrastructure
MIME	–	Multipurpose Internet Mail Extension
KCM	–	Key Continuity Management

ЗМІСТ

ВСТУП

Електронна пошта вже давно є важливою і дуже корисною технологією яка допомагає людям спілкуватися, надсилати документи 'та отримувати важливу інформацію онлайн за допомогою мережі Інтернет. Вона використовує протоколи комутації пакетів для надсилання повідомлень з будь-якої машини в мережі інтернет яка зв'язана в світі з будь-якою іншою машиною. Але електронна пошта вразлива для атак, оскільки фрагменти повідомлення або пакети роблять багато зупинок на різних серверах під час свого шляху. На кожній зупинці повідомлення міститься у «звичайному тексті», що означає, що його можна легко перехопити, переглянути та змінити, можливо без того, щоб відправник чи одержувач ніколи не дізналися. За останнє десятиліття кількість електронних повідомлень, що надсилаються через Інтернет, значно збільшився, тому безпека електронної пошти стає все більш важливою.

Ця дипломна робота є актуальною оскільки в ній розглядаються різні системи та комплекси - нові та застарілі які використовуються для того, щоб забезпечити безпеку користувача при використанні електронної пошти. Щорічно кількість людей та кількість електронних листів стрімко збільшується, а тому і необхідність в використанні більш захищених та ефективних методів захисту інформації під час використання електронної пошти. Враховуючи, що *метою роботи* є розробка рекомендацій щодо захисту інформації під час використання електронної пошти, то для її досягнення були визначені такі завдання:

- Провести аналіз використання електронної пошти
- Провести аналіз вразливостей електронної пошти та додатків з якими вона взаємодіє
- Проаналізувати наявні технології захисту електронної пошти та рішення щодо їх використання
- Обґрунтування можливих методів та засобів захисту інформації електронної пошти

- Провести аналіз ефективних способів захисту інформації в сфері використання електронних скринь

Об'єктом дослідження в даній роботі є процес визначення ефективних засобів захисту інформації під час використання електронної пошти.

Предметом дослідження методи, засоби і методики захисту інформації в системах електронної пошти

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1
БАЗОВІ ПОНЯТТЯ СИСТЕМ ЕЛЕКТРОННОЇ ПОШТИ

1.1 Історія виникнення систем безпеки

Сучасна безпека інформації майже така ж, як і в історії, за винятком контексту для його використання змінилася. Секретність все ще дуже важлива для військових операцій, але також і шифрування має багато застосувань у державному секторі, наприклад для захисту конфіденційності та конфіденційності. Сьогодні, мабуть, найпоширенішим з усіх механізмів аутентифікації є пароль. Сучасні користувачі комп’ютерів тепер повинні запам’ятовувати десятки паролів для того щоб отримати доступ до веб-сайтів, комп’ютерних систем, будівель та банківських рахунків. З такою великою кількість паролів, які потрібно запам'ятати, користувачі комп'ютерних систем стикаються з зростаючим тиском, щоб підтримувати їх практику безпеки. Хоча паролі набули широкого поширення, вони все ще мають багато недоліків, особливо те, що через природу людської пам’яті про них часто забувають. Таким чином, з’являються нові способи автентифікації без необхідності запам’ятовувати пароль. Один такий метод відомий як біометричний; аутентифікація шляхом розпізнавання людей. Технологічний прогрес останніх років дозволив комп’ютерам зберігати та розпізнавати відбитки пальців, перше цифрове використання якого було прийнято в 2013 році [1]. Крім відбитків пальців, можуть бути використані й інші біологічні ознаки для ідентифікації, як-от голоси, риси обличчя і, більш популярно, розпізнавання малюнків райдужної оболонки, який був вперше запатентований у 1989 році [2]. Проте біометричні технології дорогий і не зовсім точний, тому йому доведеться пройти довгий шлях до повної заміни паролі.

Американський дослідницький центр The Radicati Group Inc проводить щорічне дослідження яке показує кількість трафіку електронної пошти, на якому наглядно видно збільшення обсягу написаних електронних листів. Ці дослідження зображенні на рисунку 1.1 та таблиці 1.1 [3].

Таблиця 1.1

Щоденний трафік електронної пошти

Трафік електронної пошти	**2017**	**2018**	**2019**	**2020**	**2021**
Загальна кількість надісланих листів щоденно(мільярдів)	268	281.1	293.6	306.4	319.6
% Ріст		4.5%	4.4%	4.4%	4.3%

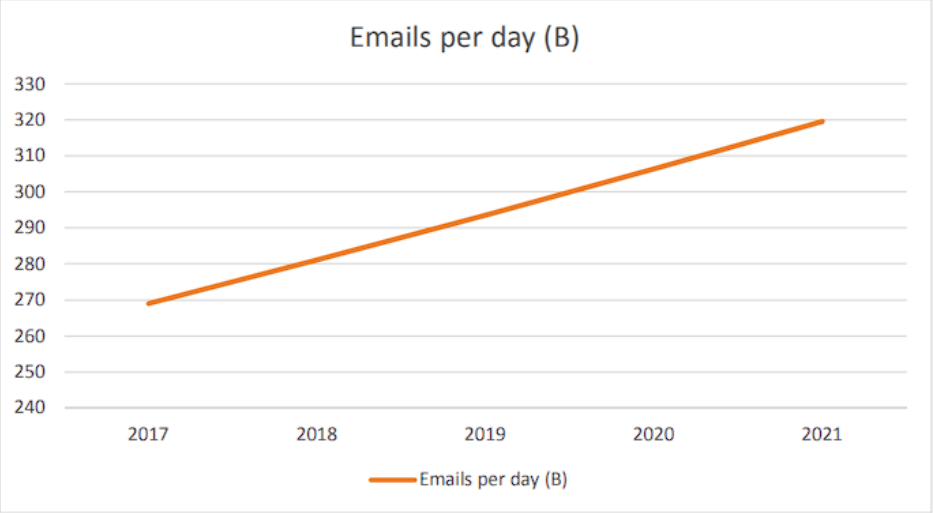

Рисунок 1.1 - Кількість відправлених електронних листів щодня

Оскільки електронна пошта та інтернет стають все більш і більш важливими каналами спілкування як для компаній, так і для окремих осіб різко зросло відчуття невідкладності для підвищення їх безпеки. Результати дослідження продемонстровано в наступній таблиці 1.2, та зображені на рисунку 1.2 [4].

Таблиця 1.2

Зростання кількості користувачів електронної пошти в усьому світі

	2017	**2018**	**2019**	**2020**	**2021**
Користувачі електронної пошти з усього світу (як бізнес, так і персональні) (мільйони)	3718	3823	3930	4037	4147
% Ріст		3%	3%	3%	3%

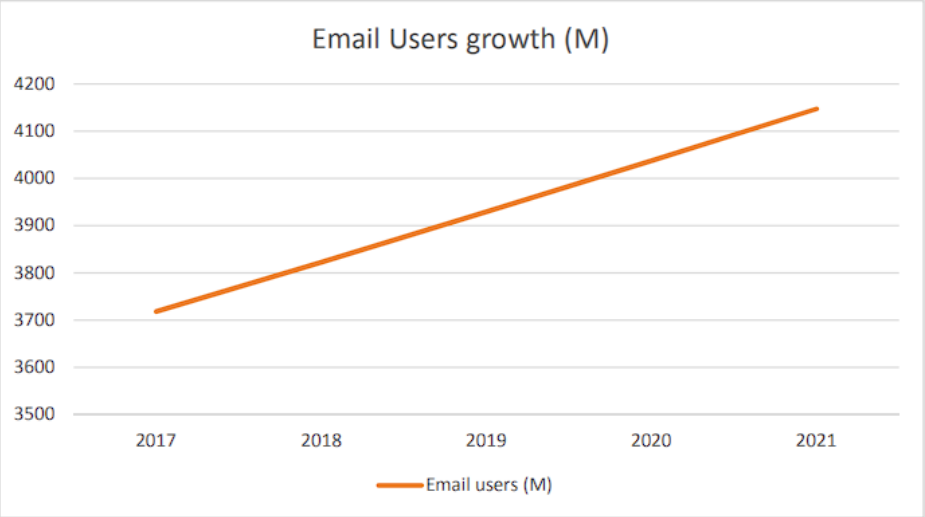

Рисунок 1.2 - щоденний зріст користувачів електронної пошти

Як я вже зазначив, шифрування інформації можливе вже давно, але в інтернеті запроваджено нові моделі загроз, головним чином через те, що інформація, що передається, зупинятиметься у багатьох небезпечних точках, перш ніж досягти місця призначення. Для боротьби з цими загрозами були розроблені системи, які вимагають єдиного ключа, який використовується відправником для шифрування та до одержувача для розшифровки повідомлень. Однак обмін секретним ключем може бути проблематичним, оскільки Інтернет не безпечний, а користуватися телефоном незручно. Єдиний спосіб надійно використовувати симетричний ключем до спілкування з ними в автономному режимі, наприклад, на зустрічі віч-на-віч, що, очевидно, не можливо, коли відправник і одержувач знаходяться далеко один від одного. Один ключ є секретним, і при цьому його не потрібно повідомляти, а інший є публічним і має бути оприлюдненим. Використання ключів взаємозамінне, тому повідомлення зашифрований одним ключем завжди можна розшифрувати за допомогою пари ключів і навпаки. Система відкритих ключів проклала шлях для інфраструктури відкритих ключів (ІВК), які забезпечують усі три вимоги до криптографії та інформаційної безпеки в загалом: конфіденційність, цілісність та доступність.

Рисунок 1.3 -Тріада інформаційної безпеки

1.2 Компоненти систем електронної пошти

Електронна пошта, або як її ще можна називати - e-mail, це технологія за допомогою якої можна надсилати електронні повідомлення або електронні листи іншим користувачам в мережі інтернет. Основний формат Інтернет-повідомлень, який використовується для електронної пошти, визначений RFC 5322, з кодуванням даних, що не є ASCII, і вкладень мультимедійного вмісту, визначених у RFC 2045 до RFC 2049, які спільно називаються багатоцільовими розширеннями Internet Mail або MIME. Розширення в міжнародній електронній пошті застосовуються лише до електронної пошти. RFC 5322 замінив попередній RFC 2822 у 2008 році, потім RFC 2822 у 2001 році замінив RFC 822 – стандарт для електронної пошти в Інтернеті протягом десятиліть. Опублікований у 1982 році, RFC 822 був заснований на більш ранньому RFC 733 для ARPANET [5]. Більшість сучасних графічних поштових клієнтів дозволяють використовувати звичайний текст або HTML для тіла повідомлення на вибір користувача. Повідомлення електронної пошти HTML часто містять автоматично створену копію простого тексту для сумісності. Переваги HTML включають можливість включати вбудовані посилання та зображення, виділяти попередні повідомлення в лапки, природне перенесення на будь-який дисплей, використовувати наголос, наприклад підкреслення та курсив, і змінювати стилі шрифту. Недоліки включають збільшений розмір електронної пошти, побоювання щодо конфіденційності, зловживання електронною поштою HTML як вектора фішингових атак і поширення шкідливого програмного забезпечення [6].

Компонентами електронної пошти є так звані сервери електронної пошти - це служби які використовуються для пересилання електронних повідомлень. Ці системи складаються з різних елементів які можна назвати компонентами. За їх допомогою користувачі пишуть і відправляють листи.

1. Поштовий агент користувача (MUA — Message User Agent).
2. Транспортний агент (MTA - Message Transfer Agent).
3. Агент доставки пошти. (MDA – Mail delivery agent).
4. Агент подачі повідомлень (MSA - Message Submission Agent).

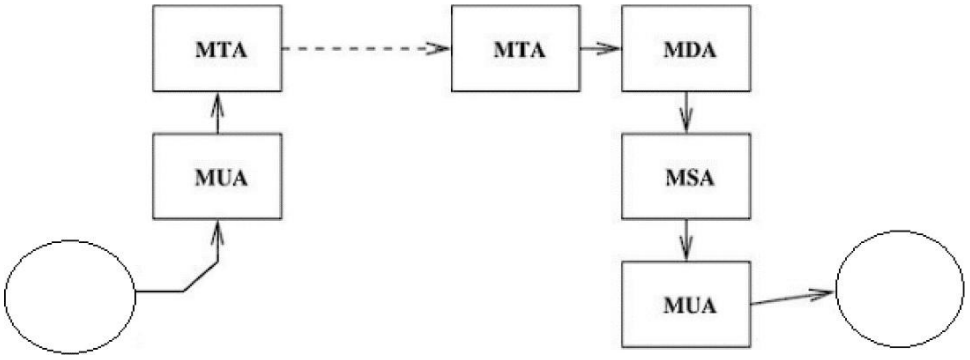

Рисунок 1.4 - приклад роботи компонентів систем електронної пошти

1.2.1 Поштовий агент користувача (MUA — Message User Agent).

Поштовий агент користувача (MUA — Message User Agent) - це програма за допомогою якої можна отримувати та надсилати електронні листи. При відправленні, пошта спочатку надходить до поштового серверу, після чого обробляється та пересилається до місця призначення. Одержувач отримує електронну пошту, використовуючи свою програму електронної пошти, щоб підключитися до поштового сервера, який запитує елементи з поштової скриньки.

Також ще існує веб-орієнтований поштовий агент, в якому програма електронної пошти напряму вбудована у сайт для загального використання. а сервері розміщено багато облікових записів поштових скриньок, до яких користувачі можуть отримати доступ, вказавши ім'я користувача та пароль. Після входу в поштову скриньку можна писати та надсилати електронні листи або збирати електронні листи. Кожен користувач має унікальну адресу електронної пошти, призначену веб-сайтом для його чи її ексклюзивного використання.

1.2.2 Поштовий транспортний агент (MTA - Mail transport agent).

Поштовий транспортний агент (MTA - Mail transport agent) - метою цього агенту є 2 :

1. По-перше, це прийняття пошти від користувача агенту, після чого пересилання його на інший транспортний агент.

2. По-друге, прийняття пошти від інших транспортних агентів.

Після отримання пошти від агенту він перевіряє правильність на адрес призначення, та доставку пошти за призначенням. Також поштовий транспортний агент перевіряє чи наданих лист був призначений для данного домену та чи є поштова скринька користувача на машині. Якщо після всіх перевірок все є правильно то він приймає це повідомлення(лист) та після чого доставляє його до агенту доставки пошти.

1.2.3 Агент подачі повідомлення (MSA – Message submission agent).

Агент подачі повідомлення (MSA – Message submission agent) - це програма(програмний агент) який отримує електронне повідомлення від поштового агенту користувача і водночас працює з поштовим транспортним агентом для доставки пошти. Цей агент використовують для того, щоб поділити 2 складові частини обробки поштових повідомлень:

1. Прийом повідомлень;

2. Доставку повідомлень.

Також при своїй роботі цей агент повинен перевірити, чи є імена вузлів повність визначеними, перевірити всі можливі помилки перед тим як надіслати листа до транспортного агенту, а також здійсниними автентифікацію клієнта. Ще одна перевага полягає в тому, що MSA і MTA можуть мати різні політики фільтрації спаму. Більшість MSA вимагає аутентифікації у формі імені користувача та пароля, наданих автором. Тому будь-які повідомлення , отримані таким MSA , можна простежити до автора який має прямі стосунки з MSA.

1.2.4 Агент доставки пошти (MDA – Mail delivery agent).

Агент доставки пошти (MDA – Mail delivery agent) - це програма яка отримує електронні повідомлення від MTA. Взагалі Існує багато різних способів зберігання пошти у поштових скриньках. Це може бути один файл користувача, в якому лежить вся його пошта. Це може бути директорія, в якій кожен лист представлений як окремий файл. Це може бути база даних. Транспортні агенти, після того як вони приймають лист для користувача, повинні якось помістити його в поштову скриньку. Тому було введено проміжний шар програмного забезпечення, що бере на себе обслуговування поштових скриньок. Одним із компонентів цього програмного забезпечення є Агенти доставки пошти. Транспортний агент передає листа агенту доставки, а вже Агент доставки сам вирішує, як і де зберегти лист користувача. Як агент доставки може виступати найпростіша програма, яка просто складає пошту в скриньку. Так і програми фільтри, які можуть щось зробити з поштою, перед тим як помістити її в поштову скриньку. Також потрібно відмітити правила відхилення повідомлення які залежать від того, якщо повідомлення є поданням або релеєм.

Наприклад, деякі сайти можуть налаштувати свої MTA для відхилення всіх команд для повідомлень, які не посилаються на локальних користувачів, і вони можуть налаштувати MSA так, щоб відхилити всі надіслані повідомлення які не надходять від авторизованих користувачів, а авторизація заснована на будь-яку аутентифіковану особу або кінцева точку, яка знаходиться в межах а захищеного середовища IP [7].

1.3 Сучасна архітектура (SMTP)

Simple mail transfer protocol (SMTP) - це простий протокол для передачі пошти, який є загаланьно прийнятим протоколом. SMTP вперше був описаний в RFC 821 (1982); останнє оновлення в RFC 5321 (2008) включає розширення, що масштабується, — ESMTP (Extended SMTP) [8]. В даний час під "протоколом SMTP", як правило, мають на увазі і його розширення. У загальноприйнятій реалізації він використовує DNS визначення правил пересилання пошти. Тобто основним його призначенням є доставка готових повідомлень(листів) та маршрутизація.

Різні домени мають власні незалежні поштові системи. Кожен домен електронної пошти може мати кілька користувачів. (Насправді, однак, організація або особа може мати кілька доменів, які обслуговуються (фізично) однією поштовою системою). Поведінка систем під час спілкування одна з одною суворо стандартизована з використанням протоколу SMTP (і відповідність цьому стандарту, а також універсальна підтримка DNS усіма учасниками є основним протоколом, який спілкується «всім усім» без попереднього). У певній системі електронної пошти (зазвичай в межах однієї організації) може бути багато серверів електронної пошти, які виконують пересилання електронної пошти та інші пов’язані з електронною поштою завдання: фільтрація спаму, антивірусне сканування вкладень, автоматичні відповіді, архівування вхідної/вихідної пошти, надання доступу користувачам через різні методів, від POP3 до ActiveSync.

Взаємодія між серверами в поштовій системі може відповідати загальним правилам (використання DNS і маршрутизації пошти через SMTP) і власним корпоративним правилам (за допомогою програмного забезпечення). Загалом взаємодія між поштовою системою та користувачем є нерегульованою та може бути довільною, хоча взаємодія між користувачем і поштовою системою має як відкриті, так і закриті (пов'язані з програмним забезпеченням певного виробника) протоколи.

1.4 Протокол POP3

Post Office Protocol 3 (POP3) - являється мережевим протоколом 3 версії який використовуюється для для того, щоб клієнт мав можливість отримувати електронного листа електронної пошти з серверу. У концепції зберігання пошти пошта на сервері тимчасово зберігається в обмеженій кількості (подібно до поштової скриньки для паперової пошти), і користувач періодично отримує доступ до поштової скриньки та «забирає» лист (тобто поштовий клієнт завантажує копію листа, адресованого йому і видаляє оригінал з поштової скриньки). Протокол POP3 працює на основі цієї концепції.

Підключення POP3 можна описати 4 кроками:

1. Клієнт підключається до сервера (стан авторизації);
2. Клієнт отримує електронну пошту (стан транзакції);
3. Сервер видаляє збережені повідомлення (стан обновлення);
4. Клієнт відключається від сервера [4].

Після встановлення з'єднання протокол POP3 проходить три стани поспіль:

- Авторизування клієнта через аутентифікатор.
- Клієнт отримує інформацію про стан поштової скриньки, отримує та видаляє електронні листи.

- Сервер оновлень видаляє вибрану електронну пошту та закриває з’єднання. Хоча POP3 підтримує можливість отримувати одну або кілька електронних листів і залишати їх на сервері, більшість програм електронної пошти просто завантажують усі листи та очищають поштову скриньку на сервері. Порівняння роботи протоколів наведено нижче (табл. 1.3).

Таблиця 1.3

Порівняння SMTP та POP3

	SMTP	**POP3**
Для чого розроблений	Спочатку SMTP був розроблений як відкритий відправник пошти, призначений для того, щоб дозволити кожному комп’ютеру в мережі надсилати електронну пошту через нього, а не лише відомим користувачам.	Оригінальний дизайн POP3 мав допомогти користувачам, яким було потрібно тимчасове підключення до Інтернету. З подальшим розвитком POP3 тепер підтримує кілька методів аутентифікації, щоб запобігти несанкціонованому доступу до електронної пошти.
Робота протоколів	SMTP вступає в силу, коли повідомлення надсилається на SMTP-сервер через поштовий проксі-сервер користувача.	Протокол POP3 допомагає надавати доступ до поштових скриньок на серверах через IP-мережу.
Призначення	SMTP був призначений для надсилання та пересилання електронної пошти з поштового проксі користувача на вказану адресу.	Протокол POP3 буб розроблений для того щоб допомогти отримувати та організувати повідомлення електронної пошти, які існують на сервері для того щоб вони були доступні за наданими адресами.

1.5 Маршрутизація пошти

Коли отримується електронний лист з поштового сервера, відбувається перевірка за заздалегідь заданими правила, які встановлюються відповідно до вмісту електронної пошти, домену адреси або просто імені користувача). Якщо схожості правила немає, то відбувається перевірка чи домен пошти знаходить на локальному сервері. Якщо домен не локальний - буде використовуватися програма маршрутизації пошти, якщо локальний - то повідомлення буде прийняте до обробки.

Маршрутизація використовує лише доменну частину адреси одержувача (тобто частину після знаку @). Пошук у всіх записах MX для домену одержувача. Вони перераховані в порядку спадання пріоритету. Якщо адреса поштового сервера збігається з одним із вузлів, зазначених у записі MX, усі записи з пріоритетом, нижчим за пріоритет вузла в записі MX (і власний запис MX вузла) відкидаються та доставляються до перших відповідних вузлів. в порядку спадання пріоритету). Це робиться, якщо поштовий сервер відправника є ретранслятором для поштового сервера одержувача. Якщо запис MX для домену не знайдено, він спробує доставити пошту на запис A, що відповідає домену. Якщо для цього поля немає запису, формується повідомлення про відмову о недоставці. Це повідомлення складається з пошти “ВІД”, відправник вихідного листа вказується в полі «Кому», а в полі “Від" - електронної пошти типу xxx@servername. Ім’я сервера – це ім’я хоста в Інтернеті, який генерує повідомлення. ПОШТА ВІД: <> дозволяє захистити ваш поштовий сервер від нескінченних повідомлень про помилки між серверами - якщо сервер виявить, що він не може доставити лист з порожньою зворотною адресою, він знищить його. Повідомлення про доставку також можуть створюватися через певний період часу. Це трапляється, коли виявлена проблема визначається як тимчасова, але черга повідомлень застаріла.

В тому випадку коли в мережі є різні DNS-сервери (наприклад, зовнішні – в Інтернеті, локальні – у своїх межах), «внутрішній» DNS-сервер, який є одержувачем найвищого пріоритету, може вказувати на сервер, недоступний в Інтернеті, де пошта надсилається з перенаправлення ретрансляції для одержувального вузла Інтернету. Цей розділ дозволяє маршрутизувати пошту між серверами без доступу до Інтернету за загальними правилами. Як тільки пошта досягає сервера призначення, він тимчасово або постійно зберігає отриману пошту. Існує дві різні моделі пошти: концепція поштових скриньок і поштових терміналів.

1.6 Релеї

DNS дозволяє призначити будь-який Інтернет-сайт як хост-сервер (запис MX), який не обов’язково є частиною доменної зони одержувача. Це можна використовувати для налаштування публікації (пересилання) пошти через сторонній сервер. Сторонній сервер (наприклад, більш надійний, ніж сервер користувача) отримує пошту для домену користувача та пересилає її на поштовий сервер користувача, коли виникає така можливість. Історично не було можливості контролювати, хто «пересилає» пошту (або не надає їй належної ваги), і сервер без такого контролю передає пошту в будь-який домен. Такі сервери відомі як відкриті реле (нові відкриті реле зараз в основному через неправильну конфігурацію).

Для їхніх користувачів сервер поштової системи є ретранслятором (користувач відправляє пошту не на сервер поштової системи одержувача, а на свій поштовий сервер, який пересилає лист). У багатьох мережах провайдерів можливість надсилання повідомлень за межі мережі через SMTP відключена (через троянські програми віруси використовують цю функцію). У цьому випадку провайдер надає власний SMTP-сервер, через який вся пошта відправляється за межі мережі. Відкриті реле — це реле, які не перевіряють, що користувач є «самим» (перевірка може базуватися або на мережевій адресі комп’ютера користувача, або на ідентифікації користувача за допомогою пароля/сертифікату). Його робота зображена нижче на рисунку 1.3.

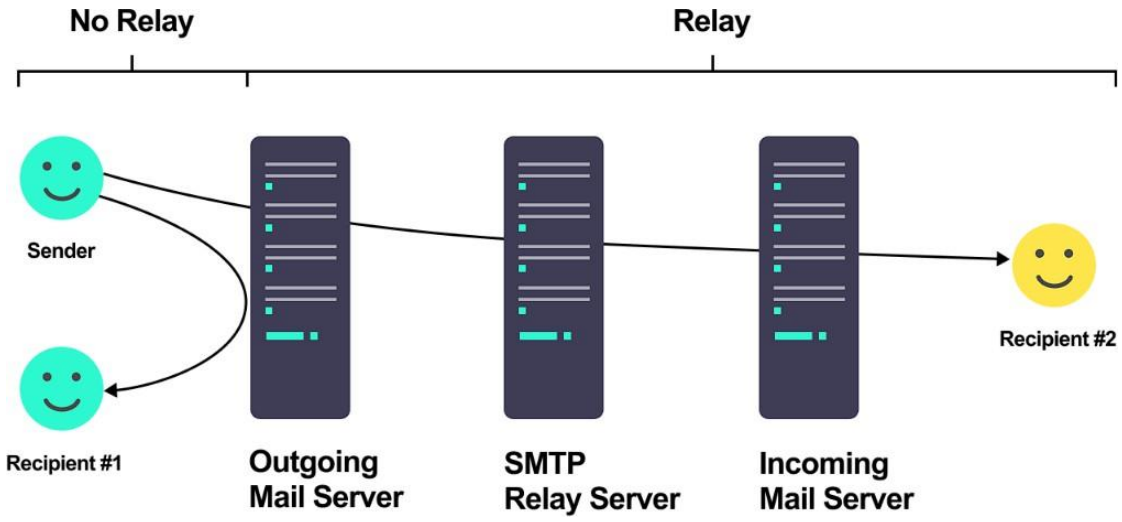

Рисунок 1.2 - SMTP Relay

1.7 Аналіз протоколу IMAP

IMAP (Internet Message Access Protocol) - інтернет-протокол який використовується для доступу до електронної пошти. Цей протокол діє по принципу, що всі транзакції пов'язані з поштою, зберігаються на серверах, тому коли користувач до поштової скриньки для перегляду кореспонденції (архівованої та нової) та написання вже нових повідомлень, а також написання відповідей на написані користувачу листів. Таке зберігання поштового листування вимагає значно більших можливостей від поштових серверів, тому було зроблено поділ між поштовими серверами, що надсилають пошту, і серверами зберігання листів.

IMAP надає користувачам безліч варіантів використання поштових скриньок, розташованих на центральному сервері. Програми електронної пошти, для отримання доступу сховища, використовується заданий протокол , як якщо б воно було на комп’ютері одержувача. Електронною поштою можна керувати з комп’ютера користувача (клієнта) без постійного надсилання файлу, що містить весь вміст електронної пошти, із сервера і назад. IMAP призначений для заміни простішого протоколу POP3, який має такі переваги:

- Клієнти можуть створювати, видаляти та перейменовувати поштові скриньки на сервері, а також переміщувати електронну пошту з однієї поштової скриньки в іншу. Листи можна позначити як прочитані, важливі тощо.
- Клієнти можуть підтримувати постійне з'єднання з сервером а також сервер повідомляє клієнта про зміни в поштовій скриньці, включаючи нові листи. Забезпечує механізм розширення можливостей протоколу.
- Електронна пошта зберігається на сервері, а не на клієнті.
- Доступ до поштової скриньки можна отримати з різних клієнтів.
- Також підтримується багатоклієнтський доступ.
- Протокол містить механізми, які можуть сповіщати клієнтів про зміни, внесені іншими клієнта [9].

Для вирішення проблеми перегляду та маніпуляції властивостями поштового повідомлення безпосередньо на сервері, а також подолання низки інших функціональних обмежень було розроблено протокол IMAP4, його підтримка у більшості комерційних систем очікується у найближчому майбутньому. Слід зазначити, що як випадку використання класичного клієнта (команда mail), так випадку застосування POP3 або IMAP4 відправка підготовлених клієнтом повідомлень вимагає наявності сервера SMTP. Тобто можна зазначити що протокол IMAP набуває все більшої популярності в використанні через переваги над іншим протоколами а також підтримкою декількох девайсів [10].

1.7.1 Стандарт IMAP4

IMAP4 (Internet Message Access Protocol 4) - це остання випущена версія розширеного стандарту IMAP. Його перевагами та особливостями можна назвати:

- Створення ієрархії електронної скриньки;
- Часткове завантаження змісту електронної пошти;
- Зміна властивості електронної пошти (розміта, обмін повідомлень електронною поштою);
- Переглядання та перевірка оглавнення листа перед його завантаженням.

Висновки за розділом 1

Оскільки електронна пошта та інтернет стають все більш і більш важливими каналами спілкування як для компаній, так і для окремих осіб різко зросло відчуття невідкладності підвищення їх безпеки. Тому в першому розділі дипломної роботи були висвітлені та описані базові поняття та системи захисту безпеки електронної пошти.

Дослідження незалежної дослідницької групи The Radicati Group Inc вкотре підтверджує велике щорічне зростання кількості користувачів (в тому числі неосвічених в роботі систем для захисту від зловмисників та їх атак) а також кількісний ріст відправлених листів, що в свою чергу означає потребу в збільшеності можливостей та потужностей серверів на яких працюють системи електронної пошти, підвищення ефективності та розповсюдження вже робочих і зарекомендованих методів які напряму збільшують загальну захищеність кожної людини. Як вже було написано, існує багато дійсно ефективних методів які потрібно і далі розвивати, нові версії вже відомих засобів підвищують неможливість в тому, щоб без проблем обходити вже відомі і більш застарілі способи які потребують покращень.

У розділі розглянуті також були розглянуті такі теми:

- Поштовий агент користувача (MUA — Message User Agent).
- Транспортний агент (MTA - Message Transfer Agent).
- Агент доставки пошти. (MDA – Mail delivery agent).
- Агент подачі повідомлень (MSA - Message Submission Agent).
- (SMTP)
- POP3
- Маршрутизація пошти
- Релеї
- IMAP
- IMAP4

РОЗДІЛ 2
ВРАЗЛИВОСТІ ТА ПРОБЛЕМАТИКА СИСТЕМ ЕЛЕКТРОННОЇ ПОШТИ

2.1 Загрози поштової служби

Так як при використанні електронної пошти використовується приватна інформація або якість приватні данні, звичайно існує загроза перехоплення, крадіжки або просто знищення цінної інформації. Щоденно за допомогою різних атак або методик піддаються загрозі мільйони користувачів та приватних повідомлень або даних. Зловмисники створюють нові методи та способи для обхіду систем захисту і кількість цих атак різко зростає. Далі наведені деякі популярні види атак які безпосередньо спрямовані на використання проти систем електронної пошти:

- Спам
- Різні шкідливі ПЗ
- Фішинг атаки
- Back scatter

Напевно найбільш популярніших але найменш ефективнішим видом атаки є спам. Мета спаму може бути різним, наприклад зловмисник просто хоче знизити ефективність роботи певної організації або більш небезпечним бот-мережі, більш відомі як “зомбі”. Ці мережі надсилають великий обсяг спаму, при чому користувач про це не знає. Хакери контролюючи ці системи можуть відправлять велику обсяг інформації, при цьому робити це з не підозрілих аккаунтів.

Різні шкідливі програмні забезпечення можуть мати різну мету та в свою чергу різну ефективність. В основному зловмисники їх використовують для отримання нелегального доступу до машини звичайного користувача, яка в свою чергу використовую ресурси цієї машини для завдання шкоди власнику через видаляння, знищення, спотворення, крадіжкою або просто підміни важливої інформації.

Також одним із самих відомих типів атаки є фішинг в системах електронної пошти. Основою таких атак є розсилання зловмисником на пошту звичайних користувачів повідомлення, які є схожі на ті, які відправляються з довірених та перевірених джерел. Основна мета - заставити нічого не підозрюючого користувача перейти за спеціальним посилання яке є дуже схоже з оригіналом для того щоб отримати доступ до системи користувача або до його приватних даних та інформації. Дослідження групою спеціалістів Cleardin показало, що найбільш небезпечним типом атак для звичайного користувача є фішинг атака, оскільки потрапити в пастку шахрая дуже легко, щорічно мільйони користувачів страждають від втрати своєї приватної інформації [11]. Більше докладніше можна побачити в таблиці 2.1.

Таблиця 2.1

Статистика фішинг атак

	2017	**2018**	**2019**
Кількість людей на яких була спрямована фішинг атака (мільйони)	87.3	97.6	100+
Відсток людей який постраждав від фішинг атаки	24%	27%	23%

Back scatter - це термін, який характеризує листи, які відсилаються звичайному користувачу, як відповідь на його лист (насправді цей лист є фейковим, його вони ніколи не відсилали. Це відбувається коли спам містить фальшивий адрес, який буд відісланий зловмисником. Тоді таке повідомлення відхиляється одержувачем (точніше його сервером) і це призводить до тощо, що відповідь на цей лист відправляється на фальшивий адрес. Результатом такої атаки є появи великої кількості помилок на електронній пошті користувача.

2.2 Небезпека при використанні електронної пошти

Електронна пошта використовує протоколи комутації пакетів для надсилання повідомлень з будь-якої машини яка зв'язана з інтернетом в світі з будь-якою іншою. Електронна пошта вразлива для атак, оскільки фрагменти повідомлення або пакети роблять багато зупинок на різних серверах під час свого шляху. зупинці повідомлення міститься у «звичайному тексті», що означає, що його можна легко перехопити, переглянути та змінити, можливо без того, щоб відправник чи одержувач ніколи не дізналися. За останнє десятиліття кількість електронних повідомлень, що надсилаються через Інтернет, сильно збільшилася, тому безпека електронної пошти стає все більш важливою. Спільний з іншими формами щодо безпеки, безпека електронної пошти також обертається навколо чотирьох основних принципів; таємність, цілісність, аутентифікація та невідмовність. Якщо інформація, надіслана за допомогою електронної пошти, вважається таємною, то це повинні робити лише відправник і одержувач повинні вміти зрозуміти повідомлення. Секретною інформацією може бути будь-що, що вважатиметься відправлене відправником , наприклад, особисте спілкування з друзями та родиною, банк даних облікового запису або результати дослідження. Крім секретності, необхідно також захистити повідомлення електронної пошти від зміни під час передачі без того, щоб відправник або одержувач помітили. Замість запобігання таким змінам вмісту повідомлення, які можуть бути складними, технологія безпеки електронної пошти зазвичай попереджають відправника і одержувача про ці зміни. Перевірка змін повідомлення таким чином відоме як його цілісність і важливо в боротьбі з шахрайством, де деталі можна змінити, щоб підписатися на послуги під фальшивою особою. Ще один важливий аспектом безпеки електронної пошти є підтвердження особи відправника повідомлення, відомий як аутентифікація. Повідомлення електронної пошти мають заголовки повідомлень, які показують, звідки походить повідомлення, проте багато користувачів не усвідомлюють, що ці заголовки можуть бути підроблені, щоб справжній відправник повідомлення змінено.

Це може призвести до надмірної довіри до вмісту повідомлення, завдяки чому одержувач може передати конфіденційну інформацію, не знаючи про справжню особу відправника. Невідмовність дає однозначну відповідальність за надіслані та отримані повідомлення, що важливіше там, де повідомлення мають нести юридичну відповідальність. Інфраструктура відкритих ключів (ІВК) надає засоби для забезпечення виконання цих чотирьох факторів.

Інфраструктура відкритих ключей — це інфраструктура, яка дозволяє здійснювати аутентифікацію та шифрувати дані по інтернету. У ІВК кожному користувачеві призначається унікальний закритий ключ, який повинен залишатися для нього секретним, і є унікальним відкритий ключ, який слід розкрити та опублікувати. Відкриті і закриті ключі шифрують дані формат, який не можна читати, і функціонують таким чином, що порядок, у якому вони використовуються неважливо (відкритий ключ може розшифрувати те, що зашифровано приватним ключем, і навпаки). До забезпечуючи секретність, відправник повідомлення може зашифрувати його за допомогою відкритого ключа одержувача, який можна знайти в каталозі. Тоді одержувач і тільки одержувач можуть розшифрувати повідомлення у доступний для читання формат за допомогою власного приватного ключа.

Для забезпечення аутентифікації та цілісності повідомлень можна використовувати цифровий підпис. Цифровий підпис вимагає короткого дайджесту створюється повідомлення під назвою «хеш». Кожне повідомлення створює унікальний хеш, і це неможливо відновити хеш назад у вихідне повідомлення. Потім цей хеш підписується з відправниками закритий ключ (таким чином шифруючи його) і надіслати разом з оригінальним текстовим повідомленням. Це вкладення відоме як цифровий сертифікат. Одержувач може застосувати відкритий ключ відправника до хешу, щоб розшифрувати його, а потім створити власний хеш отриманого текстового повідомлення.

У межах PKI можна використовувати одну з кількох систем для обміну захищеними повідомленнями. Найбільш популярними є три розширена - (pEp), Pretty Good Privacy (PGP) і S/MIME. PGP — це ще одна схема шифрування повідомлень, випущена в 1991 році. PGP мав перевагу в тому, що був відкритий вихідний код і, отже, безкоштовний у використанні та розробці. Знову ж таки, PGP не набув широкого поширення або довготривале прийняття через відсутність взаємодії з популярними поштовими клієнтами. У 1997 PGP був випущена у вигляді нової комерційної версії, яка включала плагіни, які дозволяли його використовувати популярні поштові клієнти [12]. Формати повідомлень PGP були в кінцевому підсумку стандартизовані RFC 1991, 2015 і 2440; однак PGP так і не набрав популярності. Усі ці системи відповідають стандарту, відомому як «x.509». Цей стандарт описує ієрархічна структура PKI. У цій ієрархії цифрові сертифікати видаються Certificate Authority (CA), яка є глобальною довіреною установою, яка запевняє одержувачів електронної пошти, що ідентичність відправника дійсна.

Також можна відмітити, посилаючись на дослідження групи The Radicati Group, те що насправді тільки 12% відсотків людей не знають, що таке цифровий підпис та шифрування. В основному це були представники вікових груп які не були зацікавленні в тому, щоб захистити себе під час пересилання електронних листів. Але більшість з них всех ж таки говорили, що їм дуже зручно надсилати та отримувати електронні листи, що можливо свідчить про те, що представлення та поняття шифрування та цифрового підпису виходить за межі тощо, що більшість людей вважає звичайним використання електронної пошти. Ці результати можливі, на мою думку, що все ж таки більшість людей байдуже хто читає їх листи та їм просто не хочеться витрачати час на налаштування та використання шифрування.

По статистиці – ризик безпеки підвищується, чим частіше конфіденційну інформацію надсилають у незашифрованому вигляді, однак навіть один незашифрований електронний лист може стати найслабшою ланкою в ланцюжку протоколу безпеки користувача та розкривати цінну інформацію, яка може бути використана, наприклад, для крадіжки особистих даних.

2.3 Проблематика роботи з PKI

При використанні PKI виникає багато завдань, пов’язаних з керуванням ключами, які необхідно виконати час від часу, включаючи отримання цифрового сертифіката, поновлення сертифіката або його анулювання. Процес поновлення простроченого сертифіката в Thawte було задокументовано, щоб вивчити її складність. Thawte Consulting — це центр сертифікації (CA) для сертифікатів X.509. Thawte була заснована в 1995 році Марком Шаттлвортом в Південній Африці [13]. Створено обліковий запис користувача з Thawte і кожен етап, необхідний для поновлення сертифіката, проходив як пересічний користувач зробив би.

На кожному етапі процес ретельно розглядався з точки зору користувача усвідомлювати будь-які труднощі в міру їх виникнення у користувача. Коли термін дії сертифіката закінчується, ЦС надсилає електронною поштою попередження про це, після чого існує лише короткий період, протягом якого можна надсилати електронні листи за допомогою цифрового підпису, термін дії сертифіката якого закінчився, але одержувачу цих листів буде представлений страшний вигляд попередження про недійсний сертифікат. Після цього поштовий клієнт зазвичай видає попередження, якщо ви спробуєте надіслати підписане повідомлення з терміном дії сертифіката.

Відвідавши веб-сайт CA, власника сертифіката просять ввести свій пароль; це ще одна можливість для зручності використання недоліки паролів, щоб зірвати процедуру. Посилання для поновлення сертифікатів чітко не видно але вимагає деякого пошуку через навігацію веб-сайту що можете спричинити деякі незручності при використанні. Після цього поштовий клієнт зазвичай видає попередження, якщо ви спробуєте надіслати підписане повідомлення з терміном дії сертифіката.

Коли буде досягнуто правильну сторінку, яку було заздалегіть вибрано користувачем, йому пропонується вибрати один із двох форматів сертифікатів; «X.509» або «розробники безпеки додатків», що є потенційно незрозумілим вибором для користувачів [14].

Після вибору типу сертифікат, цього разу потрібно натиснути ще три кроки, перш ніж буде запропоновано інший вибір між усіма адресами електронної пошти, які належать до сертифіката. Необхідно вибрати лише одну з цих адрес електронної пошти та включити в сертифікат, хоча веб-сторінка дозволена кілька адресами, які потрібно вибрати. Це створює певну плутанину для користувача щодо адреси слід вибрати і чи можна буде підписувати електронні листи, надіслані з адрес які не були відібрані. Далі потрібно прийняти інше рішення; чи приймати значення за замовчуванням розширення сертифікатів або налаштувати їх. Після цього список з 11 різних «CSP» на вибір представлено без пояснення, що таке CSP. Після вибору параметра за замовчуванням відкривається діалог box попереджає, що лише надійним веб-сайтам слід дозволити запитувати сертифікат із так чи ні вибір продовжити. Після вибору «так», користувач повідомляє, що сертифікат не буде містити їх ім'я, якщо вони не приєдналися до «павутини довіри Thawte», але далі не було інформацію про це. Після цього було представлено екран стану сертифіката, який показував стан щойно оновлений сертифікат як «оглядає». Цей статус змінився з на вісім хвилин «готовий». Власнику сертифіката було надіслано електронний лист із підтвердженням запиту на новий сертифікат. Це повідомлення також містило інформацію про два способи відображення імені власника в сертифікат. Перший – отримати валідацію сертифікованого бухгалтера, практикуючого адвоката, або менеджер банку. Другою була раніше згадана «павутина довіри». Мережа довіри вимагає відвідування двох окремих «нотаріусів» з документами, що підтверджують особу, щоб вони могли підтвердити свою особу, багато з яких стягують плату за цю послугу. Для користувачів, які випадково живуть десь далеко, шанси бути поруч з нотаріусом зменшуються. Після підтвердження нотаріусом сертифікат буде містити повне ім'я власника. Однак якщо вони вирішили не мати свого посвідчення особи перевірено, користувачі все ще можуть підписувати електронні листи електронною поштою, за винятком того, що сертифікат лише підтвердить , а це можна отримувати тільки на пошту за адресою відправника, а не підтверджувати особу. Це може бути у випадку, коли багато звичайних користувачів електронної пошти не зможуть перевірити сертифікат на кожному отриманому електронному листі і візьме

піктограму цифрового підпису, щоб негайно висловити довіру. Це може дати небезпечну помилку почуття авторитету, якщо передбачається, що цифрові підписи однозначно підтверджують ідентичність відправника, що не обов'язково відповідає дійсності. Це пізнавальне покрокове керівництво продемонструвало складність одного завдання, з яким, ймовірно, зіткнеться власник цифрового сертифіката.

Уся процедура оновлення сертифіката вимагала більше 30 кроків, які включали шість пунктів, у яких можна було змінити налаштування, одну точку, де потрібно було вибрати пароль, чотири пункти, де потрібно було ввести пароль. Сертифікат відкритого ключа може бути відкликаний центром сертифікації. Кожен раз, коли сертифікат зустрічається, його потрібно перевіряти, щоб переконатися, що він не був відкликаний (і, отже, недійсний). Цей процес забирає додатковий час і може стати дуже складним, якщо список відкликання дуже великий і часто оновлюється. Однак, якщо статус відкликання не перевірено, є ймовірність того, що підпису можна помилково довіряти. Як видно, це може виявитися надзвичайно складним і тривалим процесом, особливо для користувачів, які не володіють IT.

Гарфінкель провів дослідження зручності використання Key Continuity Management (KCM) - програмне забезпечення, розроблене для мінімізації складності пошуку та аутентифікації відкритих ключів кореспондентів, а також створення власних пар ключів. Хоча KCM покращує керування ключами, він також відкриває три нові моделі атак, до яких, як показує дослідження Гарфінкеля, користувачі все ще сприйнятливі, зокрема соціальні інженерна атака [15]. Крім того, KCM в першу чергу не допомагає отримати цифровий ідентифікатор.

2.4 Протокол PGP

PGP – Pretty Good Privacy **(**протокол Дуже гарною конфіденційністю) - це протокол який був розроблений Філом Цимерманном у 1991 році з вихідним кодов у вільному доступі за допомогою FTP-сервера [16]**.** При його розробці основною метою було створення протоколу який би міг забезпечити цілісність та секреність електронної пошти.

Перші досліждення систем захисту електронної пошти на базі PGP показували, що використання цього протоколу не є безпечним. Але вже пізніше було доведено, що ці дослідження були проведені не в правильному середовищі для демонстрації ефективності PGP. Усіма наступними дослідженнями було доведено велику ефективність захисту цього протоколу [17].

Працює PGP просто: є 2 ключі, один з них відкритий - для шифрування та блокування повідомлення, а другий ключ - приватний, для розшифрування та розблокування повідомлення. Відсилаючи відкритий ключ відправнику, для того щоб вони могли зашифрувати повідомлення, потрібно використати приватний для його розшифрування.

Із відомих і поширених мінусів потрібно виділити важкість в адмініструванні, а також проблеми з сумісністю, оскільки відправник та отримувач повинні мати сумісні версії PGP. Наприклад, якщо ви шифруєте електронний лист за допомогою PGP з одним із методів шифрування, одержувач має іншу версію PGP, яка не може прочитати дані то повідомлення не можливо буде відправити.

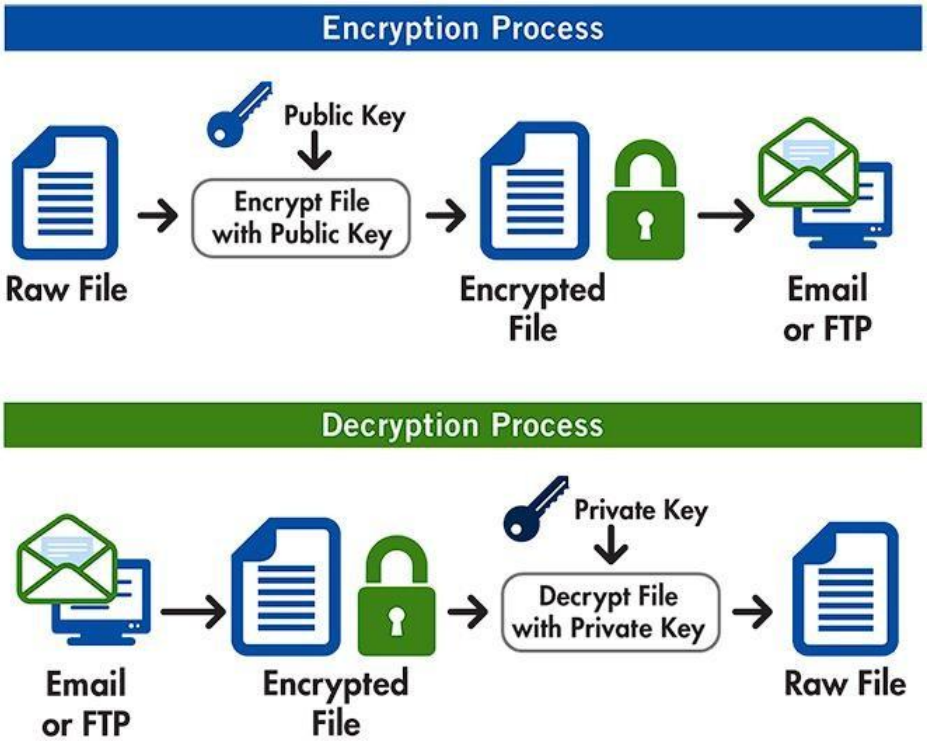

Рисунок 2.1 - процес шифрування та розшифрування.

2.5 Протокол S/MIME

S/MIME - Secure/Multipurpose Internet Mail Extension (Безпечне/багатоцільове розширення пошти) - протокол який є розширення більш застарілого багатоцільового розширення пошти. За допомогою MIME, данні які не передаються ASCII, надсилати електронною поштою. MIME переформотує задані дані на стороні відправника і поставляє їх клієнту MTA. Тобто MIME перетворює дані, які не передаються в ASCII, до даних в них, та навпаки. S/MIME додає деякі нові типи заголовків вмісту, щоб увімкнути служби безпеки в MIME.

Так як S/MIME використовує асиметричну інфраструктуру відкритих ключів (PKI), він використовує два математично пов’язані ключі для забезпечення безпеки електронної пошти. Коли електронний лист підписується, призначений одержувач повинен підтрвердити, що повідомлення дійсно було надіслано вами та не було підробленим чи зміненим. Коли електронний лист надсилається з вашого комп’ютера на пристрій одержувача, шифрування даних гарантує, що вміст повідомлення не може бути прочитаний будь-яким зловмисником, який проходить через мережу.

Основними перевагами сертифікату S/MIME можна відмітити те, що він надає дві ключові функції безпеки електронної пошти - шифрування та цифровий підпис. Шифрування забезпечує конфіденційність даних, а цифрові підписи - цілісність та невідмовність повідомлень.

2.6 Протокол pEp

Pretty Easy Privacy (pEp) - це система яка було створення для шифрування інформації, яка автоматично керує ключами шифрування через систему бібліотек. Його застосовуються для того, щоб простим способом переводити інформацію на наскрізне шифрування (зі стандартного) в основному використовуючи систему електронної пошти.

Тобто це набір рішень в відкритому доступі, які кожен можете додати до своїх інструментів. Працює на присторях з системами Android, IOS, Linux та Windows/ За допомогою створених інструментів він шифрує інформацію там, де вони були створені - починаючи з електронної пошти, SMS та закінчуючи різними додатками на кшталт Facebook, Telegram тощо. pEp є новим рішенням але стрімко набуває все більшої популярності завдяки своїй ефективності, простоті в роботі та доступності.

Потрібно відмітити, стало відомо, що на початку свого існування, засновники компанії, що створили pEp, були знайденні в тому, що платили за підроблені статті та огляди свого продукту. Це певним шляхом сильно вплинуло на репутацію системи [18].

Висновки за розділом 2

Можна підсумувати, що рівень безпеки електронної пошти не є таким настільки високим, як очікувалося. Однією з причин цього можна назвати погане використання безпеки програмного забезпечення.

Користувачі, а в деяких випадках і розробники вважають, що складність у використанні – це частина безпеки. Це означає, що хоча теоретично дуже високий рівень безпеки існує але на практиці це рідко зустрічається, оскільки користувачі воліють обходити системи. Сучасні методи показують, що паролі залишаються широко використовуваним механізмом безпеки але існує проблема зручності використання, які ще потрібно повністю вирішити.

Прозорість – це техніка, яка збільшила зручність використання програмного забезпечення, але досі неясно, наскільки прозорість є правильним рішенням, коли мова заходить про програмне забезпечення безпеки.

Можна сказати PKI є добре розробленою та технічно обґрунтованою схемою захисту електронні комунікації, однак залишається багато бар'єрів для його прийняття, таких як плутанина через численні стандарти, юридичні проблеми та труднощі з отриманням цифрового підпису.

Це надзвичайно складна система, в якій одна зміна матиме багато проблем, тому необхідно більше досліджень, щоб знайти спосіб нарешті використати його можливості для мас. PKI може захистити таємницю інформації під час транспортування та зберігання, якщо її достатньо використовувати належну роботу його користувачів. Аутентифікація, яку він пропонує, також може допомогти значно зменшити кількість соціальних, мережевих, інженерних атак, такі як фішинг, спам, крадіжка ідентифікації, шахрайство без карток і небажані електронні листи.

РОЗДІЛ 3
АНАЛІЗ ТА ПОРІВНЯННЯ ВІДОМИХ ПРОТОКОЛІВ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ПОШТИ

3.1 Технології наскрізного шифрування

Стандартизовані технології криптографічного захисту обміну електронною поштою доступний протягом десятиліть. Проте більшість користувачів покладається на незашифроване та неавтентифіковане повідомлення електронної пошти, часто без усвідомлення що існують механізми, які б пом’якшили наслідки безпеки з цим. Вже вище описані дві основні технології наскрізного шифрування (end-to-end encryption) існують протягом десятиліть, а саме Pretty Good Privacy (PGP) та Secure Multipurpose Internet Mail Extensions (S/MIME) . Нещодавно з’явилася ініціатива під назвою Pretty Easy Privacy (pEp). На жаль, ці технології ще майже не впроваджуються. Відповідно до незалежного дослідження більше 95% загального трафіку електронної пошти обмінюються без наскрізного обміну [19]. Оскільки програмне забезпечення безпеки часто базується на складних алгоритмах і концепціях, воно рідко викликає інтерес звичайному користувачеві.

Розуміння користувачами можливих загроз, ризиків та користі практики безпеки часто відсутні. У багатьох випадках це нерозуміння використовувалося для того, щоб звинувачувати користувача в безпеці невдачі.

Отже можна підсумувати, що один із основних методів підвищення загальної безпеки при використанні електронної пошти є підвищення базових знань користувача в цій сфері. Створення середовища, в якому використовується ітеративна розробка є важливим етапом для розроблення нових методів, щоб постійної переоцінювати цілі зручності використання для користувачів протягом усього процесу. Безпека повинна бути інтегрована в програмне забезпечення з самого початку, інакше це буде неефективно.

3.2 Тестування технологій з різними плагінами

Продовжуючи говорити про ці протоколи, я аналізував найбліш поширенні та відомі поштові агенти користувача (MUA), що нативно або за допомогою додаткових плагінів підтримують один з трьох технологій - PGP, PEP або S/MIME. Оцінивши зручність використання функцій шифрування в кожній з цих поштових програм, щоб отримати особисте враження та також передбачати проблеми, з якими можуть зіткнутися інші користувачі криптографічно захищаючи свої електронні листи. Тому я перевірив інтеграцію PGP, PEP та S/MIME у найбільш часто використовуваних сьогодні поштових програмах (MUA), які підтримуються наскрізне шифрування, та поставив наступні цілі:

1. Потрібно визначити, які з заданих технологій шифрування підтримують яку версію MUA;

2. Передбачити проблеми, з якими користувачі можна зіткнутися, намагаючись використовувати ці три технології в контексті конкретного MUA.

3. Для того щоб не було ніяких незручностей в подальшому дослідженні (наприклад проблеми з припиненням розробки, несумісність версій операційної системи, плагінів, тощо)

В наступній таблиці були написани поштові агенти користувача, які розглядалися в аналізі. В цій таблиці також зображено плагін, необхідний для додавання функцій PGP, pEp, S/MIME до MUA, якщо він не підтримується нативно розробником.

Тому що, навіть якщо технологію можна використовувати, її впровадження в систему електронної пошти може зробити це важко використовуючи і навпаки. Тому краще протестувати дві різні реалізації шифрування електронної пошти, щоб мати пряме порівняння зручності та комфорту їх використання. Зокрема, при тестуванні двох різних технологій, протестувавши реалізацію pEp і PGP або реалізацію S/MIME, щоб побачити, чи справді pEp відповідає своїй меті спрощення процесу шифрування пошти та.

Таблиця 3.1

Поширенні MUA та їх підримка PGP, pEp, S/MIME

Технологія	**MUA**	**Плагін**
PGP	Outlook desktop Thunderbird Maildrop	Gpg4o Enigmail Maildrop and Cryptoplugin
pEp	Windows 10 mail app Apple IOS Andoird	Не підтримується IPhone mail app Maildrop and Cryptoplugin
S/MIME	Outlook desktop iOS 12 Android	Нативна підримка IPhone mail app Maildrop and Cryptoplugin

Одразу помітив що зручність використання технології шифрування значною мірою залежить від її реалізації в поштовій програмі, що призводить до того, що одна і та ж технологія може бути трудомісткою для використання в одному MUA, але зручним в іншому MUA.

3.3 Аналіз роботи PGP та його недоліки

Використовуючи PGP, можна сказати, що він гарантує приватність, конфіденційність, автентичність та цілісність, на додаток до того факту, що не було жодних витрат за його використання. Але були деякі проблемами, бо процес порівняння відбитків пальців було складним і трудомістким (було спричинено загрузкою серверів і кількістю етапів для повного проведення). Є доцільним запропонування підтримки PGP на всіх можливих платформах і спростити порівняння відбитків пальців.

Також при роботі з PGP я зіткнувся з декількома незручностями в залежності від використаного MUA:

- Outlook 2016: процес отримування ключа одержувача був складним, оскільки конфігурація Gpg4o за замовчуванням полягає в підключенні до сервера ключів за допомогою незвичайного порту, що іноді призводить до порожньої відповіді або відхилення з'єднання. Не було можливості знайти та завантажити відкритий ключ одержувача на цьому сервері ключів. Насправді, для звичайного користувачів непросто виявити цю проблему але всього потрібно перейти до відповідних налаштувань Outlook, щоб змінити номер порту на той, який зазвичай використовується в поєднанні з цим сервером ключів. Більше того, під час створення нової безпечної електронної пошти та функції шифрування та/або підпису, графічний інтерфейс користувача спотворився. Кнопки, написи та текстові поля були вирівняні та перекривалися, що робило користувальницький інтерфейс майже непридатним для використання.
- Thunderbird: вимагав не тільки встановлення плагіна Enigmail, а й додаткові параметри конфігурації, які звичайному користувачу нелегко знайти. Потрібно активувати опцію «Примусово використовувати PGP» у налаштуваннях конфіденційності Thunderbird після встановлення плагіна. Крім того, повинна була бути опція «Активувати PGP». застосовується для кожного облікового запису електронної пошти в налаштуваннях облікового запису. Нарешті, крок «Отримати ключ одержувача» був визначений як складний, оскільки Enigmail шукав відсутні відкриті ключі одержувача лише на одному сервері одночасно. Це можна було вирішити користувачем змінивши сервер ключів, на якому Enigmail шукає відсутні ключі, що вимагає терпіння та бажання змінювати налаштування сервера ключів, доки не вдасться отримати відкритий ключ одержувача з одного із серверів, на якому одержувач опублікує свій ключ.
- Maildroid: взагалі не пропонував жодних функцій для створення пари ключів PGP безпосередньо на мобільному пристрої. Було кілька способів передати згенеровану пару ключів (наприклад, самостійно надіслати її електронною поштою, завантажити в хмару, обмін USB), але це вимагало багатьох взаємодію тому його використання значно знизив загальний досвід роботи.

Підсумовуючи, можна сказати, що PGP вимагає багато кроків налаштування для успішного використання, що особливо характерно при імпорті відкритих ключів одержувача.

Після роботи з PGP можна зробити висновок, що найскладнішим MUA для використання PGP був Thunderbird через труднощі, з якими користувачі можуть стикатися, крім того, що кнопки для виконання кроків налаштування є глибоко приховані в меню налаштувань.

На відміну від цього, FlowCrypt був найпростішим інструментом у використанні PGP з, оскільки він генерує пару ключів для нового користувача лише за кілька кліків і пошуків для ключа одержувача автоматично майже на всіх часто використовуваних серверах ключів. Тим самим FlowCrypt вирішує майже всі проблеми з зручністю використання.

На жаль, він має два недоліки: FlowCrypt завантажує лише згенеровану пару ключів на своєму власному сервері ключів, який невідомий більшості інших реалізацій PGP, таким чином імпорт відкритих ключів користувачів FlowCrypt ускладнюється для інших користувачів. По-друге, поки що FlowCrypt підтримує лише веб-пошту Gmail.

Вирішення наступним проблем може підвищити ефективність роботи даного протоколу при будь якому плагіни:

- Перевести всі версії PGP на один при роботі з плагінами, оскільки це може призвести до складнощів при адмініструванні;
- Часте виникнення проблеми з відновлення, оскільки потрібно використовувати спеціальну програму для отримання паролів. Наприклад користувач має доступ до комп’ютера що фізично відновити пароль. Але при використанні PGP не має такої можливості. Методи шифрування дуже надійні, тому вони не повертають забуті паролі, що призводить до втрати повідомлень або файлів.

3.4 Аналіз роботи pEp та його недоліки

pEp вимагав лише кількох кроків для його налаштування та використання порівняно з PGP та S/MIME. Завдяки автоматизованому управлінню ключами, нетехнічні формулювання у його користувача інтерфейси та абстракція функцій безпеки, pEp не показав проблем в зручності використання, які заважають користувачам використовувати його. Порівняння слів довіри через так зване рукостискання pEp, щоб встановити довіру до ключа одержувача, є зручним і досить легким методом. pEp виявився найпростішою технологією у використанні.

Якщо порівнювати з PGP та S/MIME можна сказати, що pEp має найбільшу зручність в своєму використання та ефективність в захисті інформації під час використання електронної пошти. Але на жаль при використанні pEp є проблеми з сумісність, оскільки цей протокол не є сумісним з усіма основними платформами.

3.5 Аналіз роботи S/MIME та його недоліки

- Outlook 2016/2013: опцію конфігурації, щоб можна було імпортувати власні цифрові сертифікати, було нелегко знайти, і потрібно було витратити багато часу в налаштуваннях для імпорту свого сертифіката. Крім того, зіткнувся з дивною помилкою. Можна шифрувати свої вихідні електронні листи лише під час відповіді на вже отриману зашифровану електронну пошту, але не можна зашифрувати новий лист, навіть якщо вони вже отримали сертифікат одержувача.
- iOS 12: використовуючи систему на базі iOS я розпаковував архів, який містить сертифікат, отриманий електронною поштою від центру сертифікації, який видав. Крім того, перед імпортом сертифіката їм потрібно було активувати S/MIME вручну в налаштуваннях iPhone. Однак відповідний параметр налаштування був досить прихований у меню налаштувань телефону.

- Android: за допомогою іншої платформи (ПК) я розпакував отриманий файл сертифіката. Потім перенесіть сертифікат назад на мобільний пристрій після його розпакував. Це була така ж проблема, як і для iOS. Можна було передати його, лише надіславши електронний лист із сертифікатом (файл .pfx) після змін параметрів налаштувань в телефоні (так як і на IPhone).

Підводячи підсумок, завдяки тому, як працює S/MIME, його можуть легко використовувати початкові користувачі, оскільки користувачам не потрібно генерувати жодних ключів. Вони отримують як публічний, так і приватний цифровий сертифікат, і їм залишається лише імпортувати його в MUA. Щойно користувач отримує підписаний електронний лист, публічний сертифікат відправника автоматично інтегрується в MUA. Таким чином, користувачам не потрібно виконувати будь-які додаткові завдання, крім налаштування S/MIME в потрібному MUA. Однак можна зробити висновок, що дуже важко використовувати S/MIME в Outlook, оскільки варіанти імпорту цифрового сертифіката важко знайти, і користувач може надіслати зашифроване повідомлення електронної пошти лише як відповідь на електронний лист, який уже захищений через S/ MIME . Крім того, на iOS дуже важко активувати S/MIME на пристрої, оскільки цей параметр нелегко знайти.

Висновки за розділом 3

В цьому розділі були проаналізовані та порівняні найбільш відомі протоколи при використанні різних операційних систем, пристроїв та плагінів, які використовуються в поштових агентах користувача (MUA) за допомогою нативної підтримки або плагінів в відкритому доступі.

Оцінив зручність використання функцій шифрування в кожній з цих поштових програм, щоб отримати особисте враження та також передбачати проблеми, з якими можуть зіткнутися інші користувачі криптографічно захищаючи свої електронні листи.

Після проведеного дослідження та порівнянь можна с певністю сказати, що нажаль використання наскрізного шифрування (end-to-end encryption) є не дуже популярним методом, який обґрунтовано малою кількістю нативної підтримки від розробників, що спричиняє появі різних плагінів від третьої сторони, що в свою чергу дається взнаки при роботі з програмним забезпеченням - низька швидкість роботи, кількість багів та проблеми з роботою інтерфейсу та його затримками в швидкості.

При все цілій підтримці зі сторони розробника, з постійними обновленнями та при переході на нові версії плагінів, та операційних систем, можливо значно підвищити працездатність перевірених агентів, що призведе до все більш поширеного використання цих програмних забезпечень і тому підніме загальну безпеку користувачів які використовують електронну пошту.

Підсумувавши можна впевнено сказати що pEp є найбільш перспективним протокол, завдяки своїй новизні, активній підтримці зі сторони розробника який постійно випускає нові оновлення.

ВИСНОВКИ

Згідно поставленої меті, був проведений аналіз використання електронної пошти, а саме в роботі було розглянуто технологію електронної пошти, основні системи та засоби безпеки які використовуються для захисту інформації під час використання електронної пошти. Проаналізовано та дослідженні найбільш розповсюдженні протоколи які використовуються для захисту інформації. Ці методи захисту і далі потрібно розвивати, створювати нові версії вже відомих засобів які підвищують загальну безпека електронних систем в мережі інтернет.

Проаналізовано дослідження таких видань як The Radicati Group, Inc та Cleardin на предмет щорічного підвищення популярності використання електронної пошти та кількість відісланих листів використовуючи системи електронної пошти. А також загальну кількість атак зловмисників які спрямовані на спричинення всяких різних атаки на кшталт фішинг, або спам атак. Також потрібно виділити що через незнання звичайної люди навіть самі звичайні атаки є досі дуже небезпечними, тому потрібно і далі освітлювати ці проблему яка дійсно є масштабною.

Ще вважливо відмітити небезпеку та проблематики з якими ми досі маємо справу. Проводячи аналіз вразливостей потрібно відміти рівень загрози користувачів які використовують електронну пошту. Бо насправді рівень безпеки електронної пошти не є таким настільки високим, як очікувалося. Однією з причин цього можна назвати погане використання безпеки програмного забезпечення. Користувачі, а в деяких випадках і розробники вважають, що складність у використанні – це частина безпеки. Це означає, що хоча теоретично дуже високий рівень безпеки існує але на практиці це рідко зустрічається, оскільки користувачі воліють обходити системи. Сучасні методи показують, що паролі залишаються широко використовуваним механізмом безпеки але існує проблема зручності використання, які ще потрібно повністю вирішити.

Підсумовуючи тему вразливостей електронної пошти та систем з якими вона взаємодія на прикладі PKI, можна сказати що хоча вона є добре розробленою та технічно обґрунтованою схемою захисту електронні комунікації, однак залишається багато бар'єрів для його прийняття, таких як плутанина через численні стандарти, юридичні проблеми та труднощі з отриманням цифрового підпису. Це надзвичайно складна система, в якій одна зміна матиме багато розгалужень, тому необхідно більше досліджень, щоб знайти спосіб нарешті використати його можливості для мас.

Проведено аналіз вже відомих, наявних а також нових технології, які використовуються для підвищення захисту користувача. Проведено дослідження протоколів та систем в яких вони використовуються, а саме MUA. Було виявлено, що не всі рішення є сприятливими для повноцінного використання і потребують змін або покращень - особливо плагіни, які не мають нативної підтримки від розробника.

Було обґрунтовано, чому можливі методи які використовуються під час роботи з електронною поштою є ефективними та навпаки - неефективними на основі таких протоколів як PGP, pEp, S/MIME використовуючи систему поштового агенту користувача MUA.

Також був проведений аналіз ефективних способів захисту інформації в сфері використання електронних скринь, Вони протестовані, порівнянні та проаналізовані згідно результатів основні протоколи для використання технології наскрізного шифрування (end-to-end encryption) які використовуються для захисту інформації під час використання електронної пошти та відправлення електронних листів, виявленні переваги та недоліки кожного, були написані висновки які вказують на проблематику в повсякденному використанні звичайному користувачу та поради щодо збільшення ефективності цій методів.

Таким чином, поставлені в роботі завдання виконані, а мета досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Effectiveness of Iphone’s Touch ID KSA Case Study [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/276302696_Effectiveness_of_Iphone's_Touch_ID_KSA_Case_Study

2. Recognition of Human Iris Patterns for Biometric Identification [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/228594200_Recognition_of_Human_Iris_Patterns_for_Biometric_Identification

3. The Radicati Group, Inc. A Technology market research firm [Електронний ресурс]. – Режим доступу: https://www.radicati.com/?page_id=54

4. Email Statistics Report, 2017-2021 [Електронний ресурс]. – Режим доступу: https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf

5. IETF Trust and the persons identified as the document authors [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc6409

6. Post Office Protocol - Version 3 [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc1939#page-5

7. An update to the email standards By Ken Simpson | 2, October 2008 [Електронний ресурс]. – Режим доступу: https://blog.mailchannels.com/2008/10/an-update-to-the-email-standards

8. Email policies that prevent viruses [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20070609214431/http://advosys.ca/papers/mail-policies.html

9. A comparative evaluation of imperative and functional implementations of the imap protocol [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/221211372_A_comparative_evaluation_of_imperative_and_functional_implementations_of_the_imap_protocol

10. Receiving Email with Internet Message Access Protocol (IMAP4) [Електронний ресурс]. – Режим доступу: https://www.2brightsparks.com/resources/articles/internet-message-access-protocol.pdf

11. Cleardin analysis of phising attack Statistics [Електронний ресурс]. – Режим доступу: https://www.clearedin.com/blog/phishing-attack-statistics#:~:text=An%20analysis%20of%20more%20than,over%2060%20million%20commercial%20users.

12. Daunting challenge of secure mail | The New Yorker | 2019/02/13 [Електронний ресурс]. – Режим доступу: https://www.newyorker.com/tech/annals-of-technology/%20the-daunting-challenge-of-securee-mail;%20last%20accessed%20on%202019/02/13.

13. Philip Zimmermann biography [Електронний ресурс]. – Режим доступу: https://philzimmermann.com/EN/background/index.html

14. Alma Whitten and J.D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Eighth USENIX Security Symposium (USENIX Security 1999), pages 14–28, Washington, D.C., 1999. USENIX Association.

15. p≡p Documentation [Електронний ресурс]. – Режим доступу: https://www.pep.security/docs/

16. A Security App's Fake Reviews Give Us a Window Into 'App Store Optimization' [Електронний ресурс]. – Режим доступу: https://www.vice.com/en/article/n7vxgd/a-security-apps-fake-reviews-give-us-a-window-into-app-store-optimization

17. Open PGP (wiki page) [Електронний ресурс]. – Режим доступу: https://wiki.p2pfoundation.net/Open_PGP

18. Thawte (wiki page) [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Thawte

19. Thawte Certificates guides page [Електронний ресурс]. – Режим доступу: https://www.digicert.com/campaigns/tls-ssl-certificate-renewals-thawte?s_kwcid=AL!15928!3!584726838952!e!!g!!thawte&mkwid=s_pcrid_584726838952_pdv_c_pmt_e_pkw_thawte_slid__product__pgrid_137705388670_ptaid_kwd

20. Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. [Електронний ресурс]. – Режим доступу: http://groups.csail.mit.edu/ana/Publications/PubPDFs/Simson.Garfinkel.thesis.2005.pdf

21. SMTP (wiki page) [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

22. Tom Van Vleck. The History of Electronic Mail. [Електронний ресурс]. – Режим доступу: https://www.multicians.org/thvv/mail-history.html

23. 2021 Email Usage Statistics [Електронний ресурс]. – Режим доступу: https://www.thexyz.com/blog/2021-email-usage-statistics/

24. Catarina, Jessica; Feitel, Jesse (2019). "Inadvertent Contract Formation via Email under New York Law: An Update". Syracuse Law Review.

25. "Mail Objects". Simple Mail Transfer Protocol. IETF. sec. 2.3.1. doi:10.17487/RFC5321. RFC 5321.

26. John Rhoton, Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP, Elsevier, ISBN 1-55558-212-5.

27. J. Klensin (October 2008), "Mail Objects", Simple Mail Transfer Protocol, sec. 2.3.1., doi:10.17487/RFC5321, RFC 5321.

28. John Rhoton, X.400 and SMTP: Battle of the E-mail Protocols, Elsevier, ISBN 1-55558-165-X.

29. Software That Tracks E-Mail Is Raising Privacy Concerns [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/2000/11/22/business/software-that-tracks-e-mail-is-raising-privacy-concerns.html

30. Віттен, А. та Тайгар, Дж. Д., «Чому Джонні не може зашифрувати: оцінка зручності використання PGP 5.0», представлений на Матеріалах 8-го симпозіуму з безпеки USENIX, Вашингтон, округ Колумбія, 1999 р.

31. Weirich, D. and Sasse, M.A., «Досить гарне переконання: перший крок до ефективної безпеки паролів для реального світу», представлена на New Security Paradigms Workshop, Cloudcroft, NM, США, 2001 p. 137-143

32. "Laying Out All The Evidence: Shiva Ayyadurai Did Not Invent Email". Techdirt. Retrieved September 5, 2020. [Електронний ресурс]. – Режим доступу:

https://www.techdirt.com/2019/05/22/laying-out-all-evidence-shiva-ayyadurai-did-not-invent-email/

33. Email Is Top Activity On Smartphones, Ahead Of Web Browsing & Facebook [Study] [Електронний ресурс]. – Режим доступу: https://martech.org/smartphone-activities-study-email-web-facebook/

34. Spam and phishing in Q1 2016 [Електронний ресурс]. – Режим доступу: https://securelist.com/spam-and-phishing-in-q1-2016/74682/

35. Martin, Brett A. S.; Van Durme, Joel; Raulas, Mika; Merisavo, Marko (2003). "E-mail Marketing: Exploratory Insights from Finland" [Електронний ресурс]. – Режим доступу:https://www.basmartin.com/wp-content/uploads/2010/08/Martin-et-al-2003.pdf

36. D. Crocker (July 2009), "Message Data", Internet Mail Architecture, sec. 4.1., doi:*10.17487/RFC5598*, RFC 5598, A message comprises a transit-handling envelope and the message content. The envelope contains information used by the MHS. The content is divided into a structured header and the body.

37. "Email is dying among mobile's youngest users [Електронний ресурс]. – Режим доступу: https://techcrunch.com/2016/03/24/email-is-dying-among-mobiles-youngest-users/

38. Rich Kawanagh. The top ten email spam list of 2005. ITVibe news, 2006, January 02, ITvibe.com Archived 2008-07-20 at the Wayback Machine

39. Ed Gerck, Overview of Certification Systems: x.509, CA, PGP and SKIP, in The Black Hat Briefings '99,

40. Mark Gasson, Martin Meints, Kevin Warwick (2005), D3.2: A study on PKI and biometrics, FIDIS deliverable (3)2, July 2005