Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіті другий (магістерський)

Дослідження методів і засобів захисту електронної пошти

(тема)

Виконав:
студент 2 курсу, групи ІМІм-22-2
Шевчук В.В.
(прізвище, ініціали)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник: доц. Золотарьов В.А
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ ____ / Шевчук В.В. /
(підпис) (прізвище та ініціали)

Керівник _____ / Золотарьов В.А /
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Телекомунікації та радіотехніка

(код і повна назва)

Тип програми освітньо-наукова

Освітня програма Інформаційно-мережна інженерія

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
« 18 » березня 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Шевчуку Владиславу Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів і засобів захисту електронної пошти

затверджена наказом по університету від« 18» березня 2024 р. № 232 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 20 червня 2024 р.

3. Вхідні дані до роботи Дослідити вразливості персональної і корпоративної електронної пошти. З'ясувати інформаційні ризики застосування електронної пошти. Розглянути методи і засоби захисту персональної і корпоративної електронної пошти. Провести їх порівняльний аналіз методом аналізу ієрархії.

4. Перелік питань, що потрібно опрацювати у роботі Вступ

1. Загальні відомості про електронну пошту
2. Огляд основних загроз електронної пошти
3. Стандартні механізми захисту
4. Методи та засоби захисту електронної пошти
5. Порівняння методів захисту методом аналізу ієрархії

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій слайди презентації в форматі Power Point (мета та задачі роботи; загальні поняття електронної пошти; види основних загроз електронної пошти; стандартні механізми захисту; шифрування електронної пошти; аутентифікація та авторизація; технічні методи боротьби зі спамом; методи та засоби захисту електронної пошти; порівняння методів захисту методом аналізу ієрархії; ієрархія критеріїв вибору методів захисту; значення векторів глобальних пріорітетів; висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	18.03.2024	виконано
2	Підбір літератури за темою роботи	21.03.2024	виконано
3	Виконання розділу 1	24.03.2024	виконано
4	Виконання розділу 2	03.04.2024	виконано
5	Виконання розділу 3	16.04.2024	виконано
6	Виконання розділу 4	29.04.2024	виконано
7	Виконання розділу 5	15.05.2024	виконано
8	Оформлення презентаційного матеріалу,	27.05.2024	виконано
9	Подача диплома на перевірку та рецензування	14.06.2024	виконано

Дата видачі завдання 18 березня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Золотарьов В.А
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 64 с., 18 рис., 11 табл., 19 джерел, 2 додатка.

Об'єкт дослідження – методи та засоби захисту електронної пошти.

Мета роботи – дослідження та оцінка методів та засобів захисту електронної пошти, що забезпечують надійний захист від сучасних загроз, вибір найкращих із них за обраними показниками якості, методом аналізу ієрархій, а також дослідити існуючі проблеми захисту електронної пошти.

Кваліфікаційна робота присвячена дослідженню методів і засобів захисту електронної пошти. Розглядаються найпопулярніші загрози та атаки на електронну пошту, проаналізовано основні методи захисту, порівняні їх переваги та недоліки. Проведено порівняльну характеристику існуючих методів захисту запроваджених у поштових сервісах методом ієрархій, з метою виявлення найкращого з них.

ЕЛЕКТРОННА ПОШТА, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНІ РИЗИКИ, МЕТОДИ ЗАХИСТУ, ЗАСОБИ ЗАХИСТУ, S/MIME, PGP, TLS, ШИФРУВАННЯ.

THE ABSTRACT

Explanatory note: 64 p., 18 fig., 11 tab., 19 sources, 2 app.

The object of study is methods and means of protecting e-mail.

Purpose – to study and evaluate methods and means of protecting e-mail that provide reliable protection against modern threats, to select the best of them according to the selected quality indicators, the method of hierarchy analysis, and to study existing problems of e-mail protection.

The qualification work is devoted to the study of methods and means of protecting email. The most popular threats and attacks on email are considered, the main methods of protection are analyzed, their advantages and disadvantages are compared. A comparative characterization of the existing methods of protection implemented in email services using the hierarchy method is carried out in order to identify the best of them.

EMAIL, VULNERABILITIES, INFORMATION RISKS, PROTECTION METHODS, SECURITY TOOLS, S/MIME, PGP, TLS, ENCRYPTION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

3DES (Triple Data Encryption Standard) – блочний шифр зі симетричним ключем, який тричі застосовує алгоритм DES;

ABAC (Attribute-Based Access Control) – розмежування доступу на основі атрибутів доступу;

AES (Advanced Encryption System) – симетричний алгоритм шифрування;

DAC (Discretionary Access Control) – метод протидії фішингу;

DDoS (denial-of-service attack) – атака на відмову в обслуговуванні;

DES (Data Encryption Standard) – симетричний алгоритм шифрування;

DKIM (DomainKeys Identified Mail) – метод виявлення підробки листів електронної пошти;

DMARC (Domain-based Message Authentication, Reporting & Conformance) – механізми обміну інформацією між відправником та одержувачем про якість фільтрації спаму та фішингові атаки;

DNS (Domain Name System) – система доменних імен;

DNSBL (DNS-based Blackhole Lists) – чорні списки в реальному часі;

ECC (Elliptic-curve cryptography) – підхід до криптографії з відкритим ключем на основі алгебраїчної структури еліптичних кривих.

HSM (Hardware Security Modules) – Апаратний модуль безпеки;

HTTPS (HyperText Transfer Protocol Secure) – захищений протокол передачі гіпертексту;

IDS/IPS (Intrusion Detection and Prevention System) – це програмні або апаратні системи виявлення та запобігання вторгненням;

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

MITM (Man in the middle) – атака типу «людина посередині»;

MTA (Mail Transfer Agent) – агент пересилання повідомлень;

MX (mail exchanger) –тип DNS запису;

PGP (Pretty Good Privacy) – програма шифрування з публічним ключем;

POP3 (Post Office Protocol 3) – протокол поштового відділення

RBAC (Role-Based Access Control) – управління доступом на основі ролей;

RSA (Rivest–Shamir–Adleman) – криптографічний алгоритм із відкритим ключем;

S/MIME (Secure/Multipurpose Internet Mail Extensions) – стандарт для шифрування та підпису в електронній пошті за допомогою відкритого ключа.;

SMTP (Simple Mail Transfer Protocol) – простий протокол передачі пошти;

SPF (Sender Policy Framework) – інфраструктура політики відправника;

SSL (Secure Sockets Layer) – рівень захищених сокетів;

TSL (Transport Layer Security) – захист на транспортному рівні;

ПЗ – програмне забезпечення;

ЦС – центр сертифікації;

ШПЗ – шкідливе програмне забезпечення.

ВСТУП

У сучасному світі, де глобальна мережа Інтернет є повсюдно поширеною, особливо на підприємствах та в установах найвищого рівня, електронна пошта є одним з найважливіших засобів комунікації. Вона використовується як в особистих цілях, так і в бізнесі, урядових установах та інших організаціях, як спосіб швидкого обміну повідомленнями, документами, графічними, аудіо та відеоматеріалами. Незважаючи на численні переваги електронної пошти, вона є об’єктом численних загроз та атак. Захист електронної пошти від цих загроз є критично важливим завданням для забезпечення безпеки інформації та безперебійної роботи організацій.

Надійність захисту даних у системі електронної пошти безпосередньо впливає на загальний рівень інформаційної безпеки організації, а отже, і на ефективність діяльності, що підкреслює важливість створення надійного захисту для цього виду комунікацій. Основні проблеми, з якими стикаються користувачі електронної пошти, такі як спам, лавинне розсилання, фішинг, відмова у доступі та витік конфіденційної інформації, пов’язані з недостатнім рівнем захисту сучасних поштових систем.

Розробники систем захисту електронної пошти щорічно створюють нові методи та засоби, щоб вирішити проблеми захисту інформації, але з появою нових методів з’являються нові типи атак та вірусів, оскільки хакери, розробляють та розповсюджують віруси постійно, вигадують нові методи атаки, що вимагає безперервного розвитку та вдосконалення захисних заходів. Для забезпечення найвищого рівня захисту необхідно застосовувати комплексний та систематичний підхід, враховуючи всі загрози та ризики, пов'язані з безпекою електронної пошти [1].

Актуальність роботи обумовлена важливістю значення для підвищення рівня безпеки інформації, запобігання атакам та забезпечення надійної роботи організацій. Вивчення сучасних загроз та розробка ефективних методів захисту сприятиме зниженню ризиків, пов’язаних з електронною поштою, та підвищенню загального рівня кібербезпеки.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ЕЛЕКТРОННУ ПОШТУ

Електронна пошта – це засіб обміну повідомленнями з текстовим та графічним вмістом через інтернет, подібний до традиційної пошти, але у цифровій формі. Вона надає можливість автоматично відповідати на листи, надсилати їх кільком адресатам одночасно, а також перенаправляти їх на інші адреси.

Комунікація за допомогою електронної пошти відбувається в режимі реального часу, що дозволяє користувачам обмінюватися важливою інформацією незалежно від географічного розташування. Ця особливість робить електронну пошту привабливою для зловмисників, які, використовуючи різні види атак, такі як DDoS, фішинг, підміна доменів і т. д., намагаються отримати конфіденційну інформацію та здійснюють продаж її в dark net [2].

Електрону пошту можна поділити на індивідуальну та корпоративну.

− Індивідуальна електронна пошта призначена для особистого використання. Вона дозволяє користувачеві обмінюватися повідомленнями, включаючи текстовий та графічний вміст, з іншими користувачами через інтернет. Така пошта може бути використана для особистої комунікації, обміну файлами та збереження особистої інформації.

− Корпоративна електронна пошта, навпаки, призначена для використання в організаційному середовищі. Вона надає комунікаційні інструменти для співробітників та дозволяє їм обмінюватися інформацією щодо робочих завдань та проектів. Корпоративна пошта часто має розширені функції, такі як календар, спільний доступ до документів та можливості обміну інформацією в межах організації.

Для передачі пошти використовують наступні протоколи передачі:

− SMTP (Simple Mail Transfer Protocol) – найпростіший протокол передачі пошти. Це протокол зв'язку, який використовується для надсилання та отримання повідомлень електронної пошти через Інтернет. Поштові сервери та інші агенти пересилання повідомлень (MTA) використовують SMTP для надсилання, отримання та ретрансляції поштових повідомлень [3];

− POP3 (Post Office Protocol 3) – поштовий протокол, за допомогою якого завантажуються повідомлення на поштовий клієнт із віддаленого сервера. Таким

чином, щоб прочитати отримане повідомлення у поштовому клієнті, вам не потрібно підключатися до сервера [4];

− IMAP (Internet Message Access Protocol) – це двосторонній протокол доступу до електронної пошти, який копіює її з віддаленого сервера, зберігаючи при цьому оригінальну копію пошти на віддаленому сервері. Завдяки цьому протоколу можна не тільки отримувати повідомлення в клієнті, але й керувати повідомленнями на поштовому сервері [4];

Також існують більш захищені варіанти цих протоколі які використовують шифрування SSL або TSL, це IMAPS, POP3S та SMTPS.

Електронні повідомлення відправляються через поштові клієнти, які включають програми та веб-браузери. Цей процес аналогічний тому, як традиційні листи проходять кілька поштових відділень перед досягненням адресата. Принцип роботи пошти наведений на рисунку 1.1.

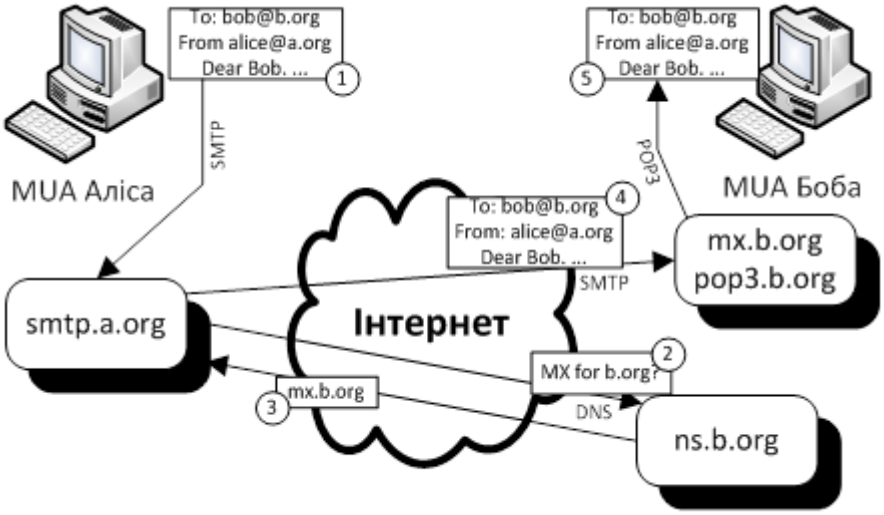

Рисунок 1.1 – Принцип роботи електронної пошти

При відправленні електронного повідомлення відбуваються кілька етапів:

− поштовий сервер відправника (MTA) ініціює з’єднання за допомогою протоколу передачі (SMTP);

− SMTP перевіряє дані поштового конверта, визначаючи адресу одержувача, та використовує DNS для перетворення доменного імені в IP-адресу;

− SMTP знаходить сервер обміну поштою (MX), пов'язаний із доменним ім'ям одержувача, і відправляє повідомлення на цей сервер;

− електронне повідомлення зберігається на поштовому сервері одержувача, до якого можна отримати доступ через протоколи поштового відділення (POP) або доступу до інтернет-повідомлень (IMAP). POP завантажує повідомлення на пристрій одержувача та видаляє його з сервера, тоді як IMAP дозволяє зберігати повідомлення на сервері, надаючи доступ до них з будь-якого підключеного пристрою [2].

Електронний лист складається з трьох основних компонентів: SMTP-конверт, заголовок та тіло.

− Конверт SMTP – складається з адреси електронної пошти обох учасників листування. Ці дані вказують поштовому серверу, куди відправити повідомлення, так само як поштовий оператор посилається на адресу на конверті, щоб доставити лист. У процесі доставки цей конверт відкидається та замінюється щоразу, коли лист передається на інший сервер.

− Заголовок містить важливу інформацію про відправника та одержувача, здебільшого заголовок збігається з інформацією, яка міститься в SMTP-конверті, а також містить низку необов'язкових полів, які дозволяють одержувачу відповісти, переслати, класифікувати, заархівувати або видалити повідомлення.

− Тіло містить інформацію, яку відправник хоче надіслати: текст, зображення, посилання, відео або інші вкладені файли, за умови, що їхній розмір не перевищує обмежень поштового клієнта.

Електронна пошта є основним методом атаки для кіберзлочинців, які можуть легко підробляти повідомлення, використовуючи ім’я або особистість жертви. Далі розглянуто основні загрози електронної пошти.

2 ОГЛЯД ОСНОВНИХ ЗАГРОЗ ЕЛЕКТРОННОЇ ПОШТИ

Атаки на електронну пошту залишаються одними з найпоширеніших методів кіберзлочинців для компрометації особистої та корпоративної інформації. У 2023 р. такими атаками стали: фішинг, спуфінг, атаки типу «людина посередині» (MITM), цільовий фішинг, програми-вимагачі, віруси/шкідливе програмне забезпечення, DDoS атаки та спам.

З розвитком технологій кіберзлочинці вдосконалюють свої методи. Порівняння вдалих атак у 2023 р. і 2020 р. наведено на рисунку 2.1 [5].

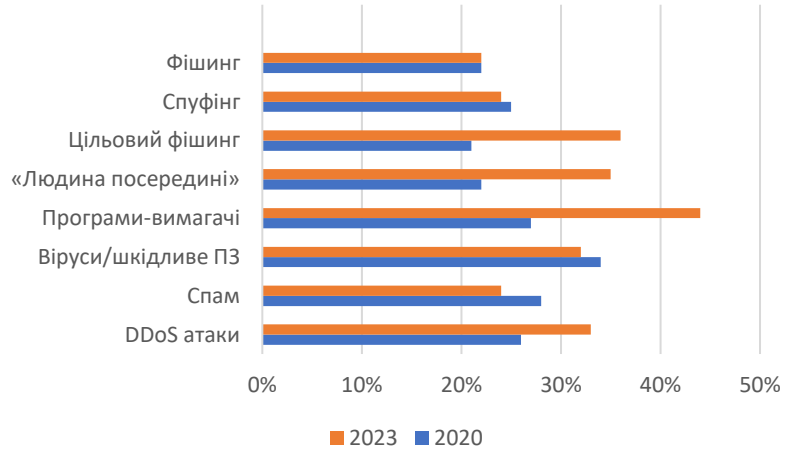

Рисунок 2.1 – Діаграма вдалих атак на електронну пошту

Далі детальніше розглянемо наведені атаки.

– Фішинг (Phishing) – це вид інтернет-шахрайства, який спрямований на порушення конфіденційності даних користувачів. Основним завданням фішингу є отримання логіна та пароля від певного сайту або ресурсу. За останні роки зафіксовано зниження частки масової розсилки фішингових листів. Це пов’язано з тим, що великі компанії приділяють все більше уваги захисту конфіденційних даних користувача. Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, E-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама [6].

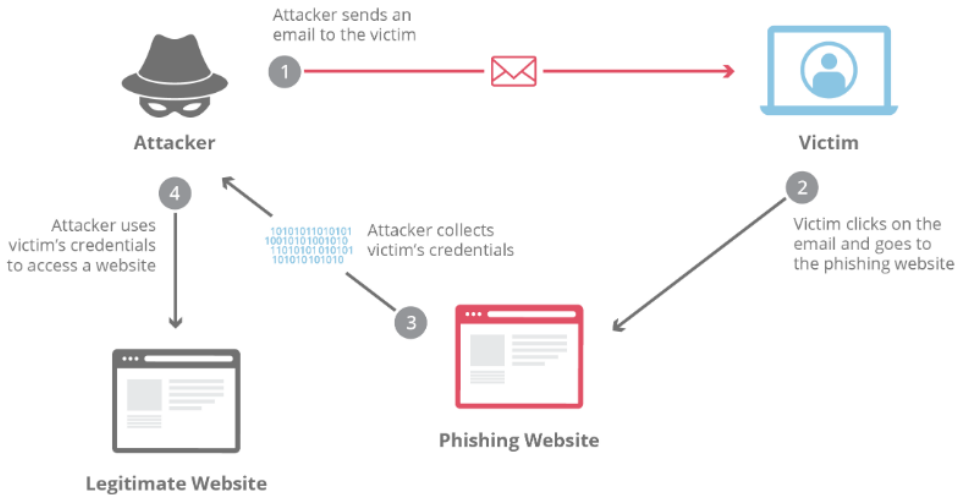

Рисунок 2.2 – Принцип дії фішингу

– Спуфінг (Spoofing) – це кібер-атака, в рамках якої шахрай видає себе за якесь надійне джерело, щоб отримати доступ до важливих даних або інформації. Така заміна може відбуватися через веб-сайти, електронну пошту, телефонні дзвінки, текстові повідомлення, IP-адреси та сервери. Як правило, основна мета спуфінгу – отримати доступ до особистої інформації, обійти контроль доступу до мережі або розповсюдити шкідливе програмне забезпечення через посилання на заражені веб-сторінки або заражені файли, вкладені в електронний лист/повідомлення.

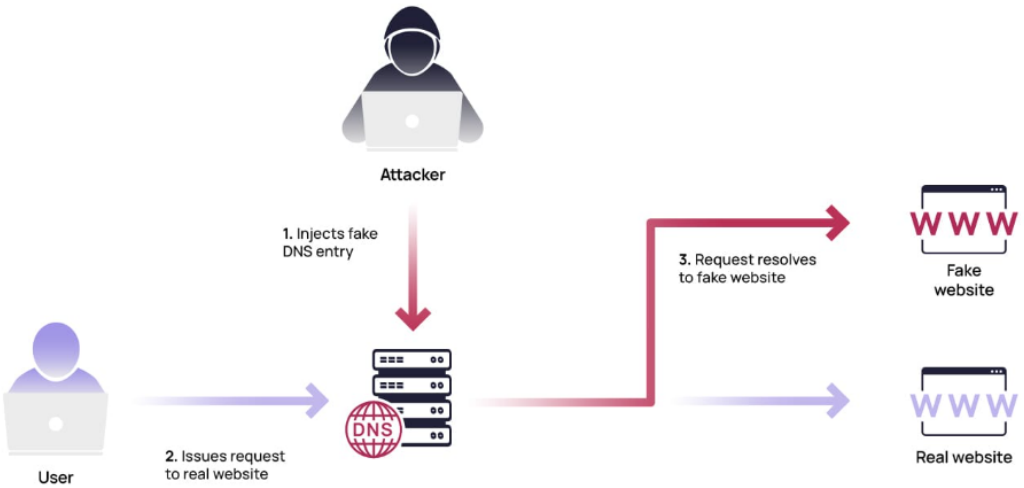

Рисунок 2.3 – Принцип дії спуфінгу

– Атаки типу «Людина посередині» (MITM) – полягає в тому, що зловмисник встигає перехопити або змінити комунікацію між двома сторонами, які спілкуються безпосередньо один з одним. Мета атаки – полягає у порушенні цілісності даних через викрадення особистої інформації, таку як облікові дані для входу в систему, дані рахунків і номери кредитних карток. Цілями зазвичай стають користувачі фінансових додатків, SaaS-бізнесу, сайтів електронної комерції та інших веб-сайтів, де потрібен вхід в систему [6].

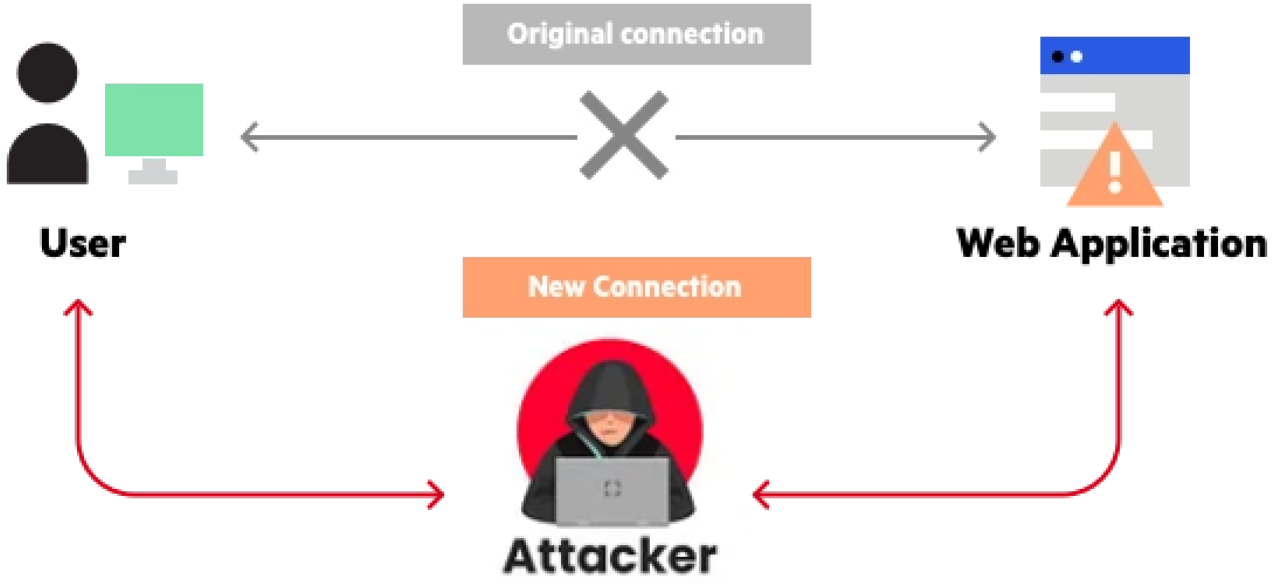

Рисунок 2.4 – Принцип дії атаки MITM

– Цільовий фішинг (Spear phishing) – вид фішингової атаки електронної пошти, спрямований на конкретну організацію чи особу з метою отримання несанкціонованого доступу до конфіденційної інформації. Подібно до електронних листів, які надсилаються під час звичайних фішингових атак, цільові фішингові повідомлення також надходять із надійного джерела. Зазвичай фішингові повідомлення надходять від великої та відомої компанії чи веб-сайту з широкою базою користувачів, наприклад Google або PayPal. Однак у випадку цільового фішингу джерелом електронного листа, швидше за все, є особа з компанії одержувача, як правило, хтось із владних повноважень або хтось, кого ціль знає особисто.

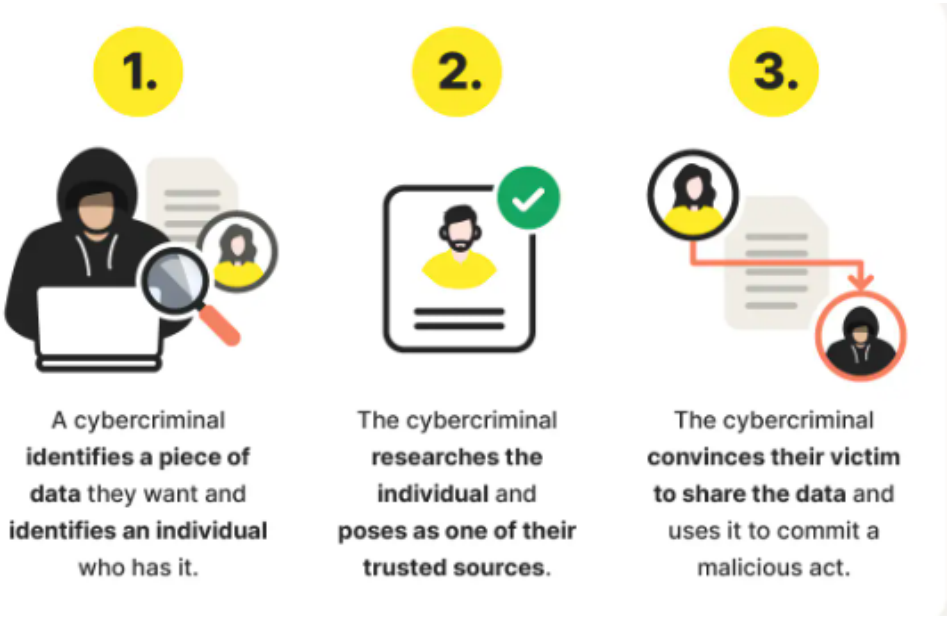

Рисунок 2.5 – Принцип дії цільового фішингу

– Програми-вимагачі (Ransomware) – це тип зловмисного програмного забезпечення спрямоване на порушення цілісності інформації, яке шифрує важливі дані організації, такі як файли, документи та зображення, а потім вимагають від компанії викуп за відновлення доступу до цих даних. Щоб досягти успіху, зловмисне ПЗ має отримати доступ до цільової системи, зашифрувати файли та вимагати від компанії викуп. Зазвичай потребують викуп у криптовалюті, щоб опублікувати зашифровані файли даних [6].

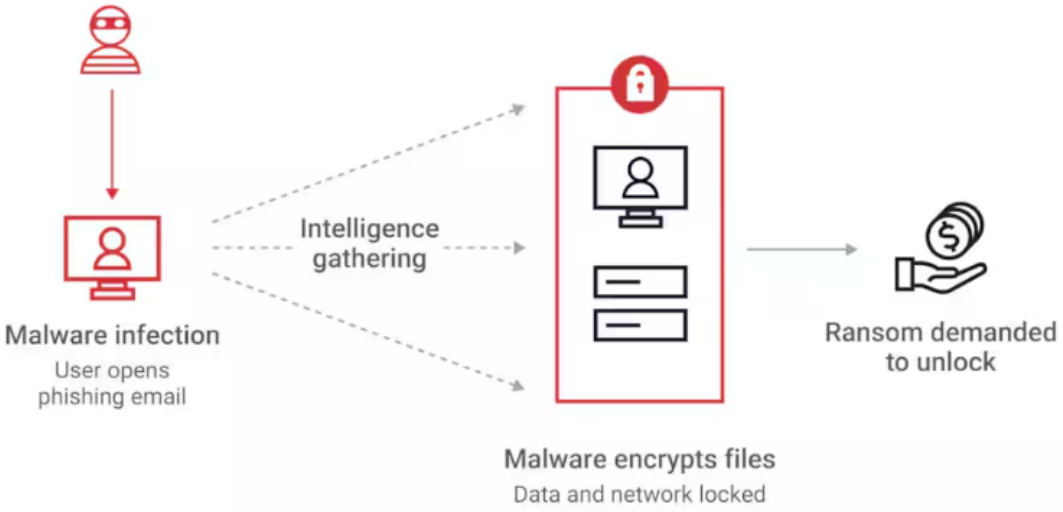

Рисунок 2.6 – Принцип дії програм-вимагачів

– Віруси/шкідливе програмне забезпечення (malware) – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем, частіше проявляється у вигляді коду, скрипту, активного контенту або іншого програмного забезпечення. Зловмисне програмне забезпечення залишається однією з найпоширеніших і найефективніших загроз IT-безпеці. Від вірусів і троянів до рекламного програмного забезпечення та програм-вимагачів, зловмисне програмне забезпечення дозволяє злочинцям викрадати гроші та дані, захоплювати комп’ютери, стежити за діяльністю комп’ютера та завдавати шкоди або порушувати бізнес-операції або для знищення інформації.

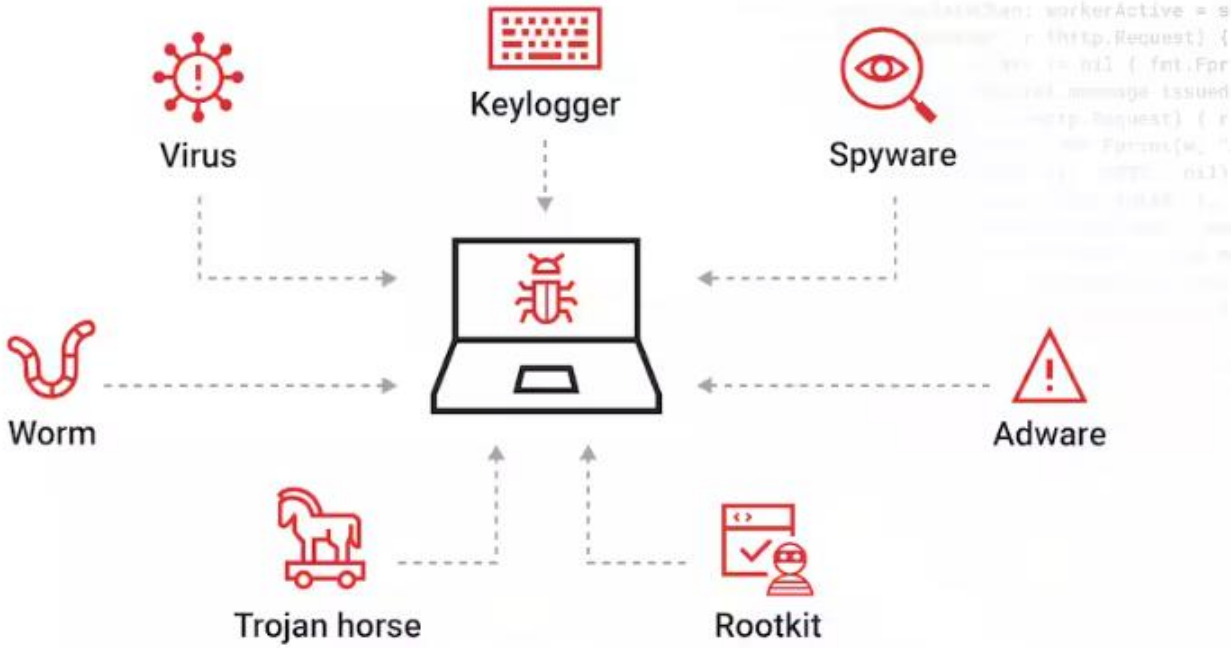

Рисунок 2.7 – Види шкідливого програмного забезпечення

– DDoS атаки (відмова в обслуговуванні) – це тип кібератак, спрямований на порушення доступності до інформації в якій зловмисник переповнює веб-сайт, сервер або мережевий ресурс шкідливим трафіком. Як наслідок, ресурс виходить з ладу або не може працювати, відмовляючи в обслуговуванні законним користувачам і перешкоджаючи законному трафіку прибути до місця призначення.

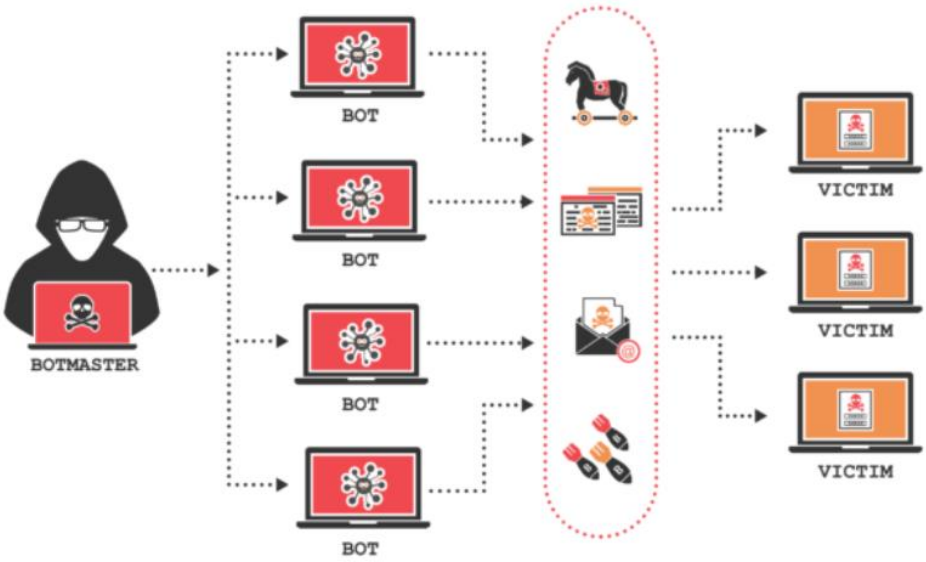

Рисунок 2.8 – Принцип дії DDoS атаки

– Спам (Spam) – це небажані повідомлення у будь-якій формі спрямовані на порушення конфіденційності інформації, які надсилаються у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів, надісланих на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа або навіть голосову пошту.

На даний час ці атаки являються найпоширенішими та з кожним роком стають більш досконалими та менш помітними. Для протидії з ними використовують різноманітні методи захисту електронної пошти.

3 СТАНДАРТНІ МЕХАНІЗМИ ЗАХИСТУ

Стандартні механізми захисту електронної пошти – це сукупність технологій, методів та політик, спрямованих на забезпечення конфіденційності, цілісності, доступності і автентичності електронних листів. Вони допомагають захистити користувачів і організації від різних типів загроз.

В результаті проведеного аналізу обрано існуючі механізми захисту, які найбільш ефективні при комплексному застосуванні. До таких механізмів відносять шифрування, аутентифікація та авторизація, а також використання технічних методів боротьби зі спамом.

3.1 Шифрування

Шифрування – процес перетворення даних в зашифрований формат так, що тільки авторизовані користувачі можуть отримати доступ до інформації. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. Серед шифрування виділяють три основних типи симетричне, асиметричне та гібридне шифрування.

3.1.1 Симетричне шифрування

Метод симетричного шифрування, використовує один криптографічний ключ для шифрування і дешифрування даних. Використання одного ключа для обох операцій робить процес простим. Існує велика кількість алгоритмів симетричного типу [7].

Найбільш поширені з них – AES, DES та 3DES.

– AES (advanced encryption system) – є одним з найбільш поширених алгоритмів шифрування. Відноситься до сімейства блокових шифрів з різною довжиною ключів і різними розмірами блоків. AES працює методами підстановки і перестановки. Спочатку незашифровані дані перетворюються в блоки, а потім шифрування застосовується з використанням ключа. Процес шифрування складається з різних процесів, таких як зсуви рядків, змішування стовпців і додавання ключів. Залежно від довжини ключа виконується 10, 12 або 14 таких трансформацій (раундів).

– DES (data encryption standard) – вид симетричних блокових шифрів який перетворює 64-бітні блоки даних відкритого тексту в зашифрований текст шляхом поділу на два окремих 32-бітних блока, застосовуючи процес шифрування до кожного окремо. Включає в себе 16 циклів різних процесів – таких як розширення, перестановка, заміна або інші операції – через які будуть проходити дані в зашифрованому вигляді. В кінцевому підсумку 64-бітові блоки зашифрованого тексту створюються в якості вихідних даних.

– 3DES (triple data encryption standard) –симетричний блоковий шифр, який був розроблений для посилення безпеки стандартного DES. У 3DES дані шифруються тричі за допомогою трьох різних ключів DES, що значно підвищує стійкість до атак [7].

Симетричне шифрування має помітні переваги, насамперед своєю простотою. Використання одного ключа для шифрування і розшифрування спрощує процес. До додаткових переваг належать:

– швидкість: алгоритми симетричного шифрування працюють значно швидше, ніж їхні асиметричні аналоги.

– обчислювальна потужність: обчислювальні ресурси, необхідні для симетричного шифрування, порівняно нижчі.

– мінімальний вплив на швидкість Інтернету: симетричне шифрування не чинить істотного впливу на швидкість передачі даних через Інтернет.

3.1.2 Асиметричне шифрування

Метод асиметричного шифрування застосовує складніший підхід ніж симетричне шифрування, а саме кілька математично взаємопов’язаних ключів. Цей тип шифрування також відомий як криптографія з відкритим ключем та включає в себе «відкритий ключ» і «закритий ключ».

До переваг цього типу шифрування відносять підвищену безпеку через використання двох ключів. Крім того, асиметричне шифрування дає змогу встановлювати зашифровані з’єднання без необхідності автономного обміну ключами, що спрощує процес. Найпоширенішим асиметричним алгоритмом виділяють алгоритм RSA [8].

RSA (Rivest–Shamir–Adleman) – асиметричний криптографічний алгоритм, який широко використовується для безпечної передачі даних. Алгоритм RSA базується на обчислювальній складності, факторизації великих чисел і включає

використання двох ключів: публічного та приватного. Публічний ключ використовується для шифрування, а приватний – для розшифрування.

Безпека RSA базується на складності факторизації великого числа n, яке є добутком двох великих простих чисел. Сучасні криптографічні додатки використовують ключі розміром щонайменше 2048 біт для забезпечення високого рівня безпеки.

RSA широко використовується для захисту даних, цифрових підписів і обміну ключами в таких протоколах, як SSL/TLS, PGP та інші.

Хоча асиметричні алгоритми шифрування, як RSA і ECC, забезпечують надійний захист і автентифікацію, вони мають свої обмеження. Симетричне шифрування, вирізняється високою швидкістю та ефективністю, але не має можливості перевірки автентичності. Для розв’язку цих проблем створили синергію систем шифрування, звідки виникла концепція гібридного шифрування, що використовує переваги симетричного та асиметричного шифрування.

3.1.3 Гібридне шифрування

Гібридне шифрування – це комбінація методів симетричного та асиметричного шифрування. Воно широко використовується в сертифікатах SSL/TLS, який встановлює безпечне з’єднання між серверами та клієнтами.

Гібридне шифрування реалізує практичне рішення, яке вирішує недоліки окремих методів шифрування. Використовуючи симетричне шифрування для передачі даних, забезпечується швидка та ефективна комунікація. А використання асиметричного шифрування забезпечує необхідну перевірку особистості, гарантуючи безпечну взаємодію між сторонами [7].

– Переваги гібридного шифрування включають:

– симетричне шифрування, завдяки своїй здатності швидко шифрувати великі обсяги даних, прискорює процеси шифрування і дешифрування, забезпечуючи швидке передавання даних;

– асиметричне шифрування гарантує, що доступ до зашифрованих даних отримає передбачуваний одержувач, перевіряючи особистість обох сторін, які беруть участь у комунікації;

– гібридне шифрування забезпечує баланс, даючи змогу безпечно й ефективно обмінюватися даними в різних сценаріях.

3.2 Аутентифікація та авторизація

3.2.1 Аутентифікація електронної пошти

Автентифікація електронної пошти – це набір методів, спрямованих на надання інформації про походження повідомлень електронної пошти шляхом перевірки права власності на домен будь-яких агентів передачі повідомлень (MTA), які брали участь у передачі та, можливо, зміні повідомлення.

Оскільки SMTP не має функції аутентифікації, було розроблено багато пропозицій автентифікації електронної пошти, але лише нещодавно отримали широке поширення три – SPF, DKIM і DMARC. Результати такої перевірки можуть бути використані в автоматизованому фільтруванні електронної пошти або можуть допомогти одержувачам під час вибору відповідної дії [9-10].

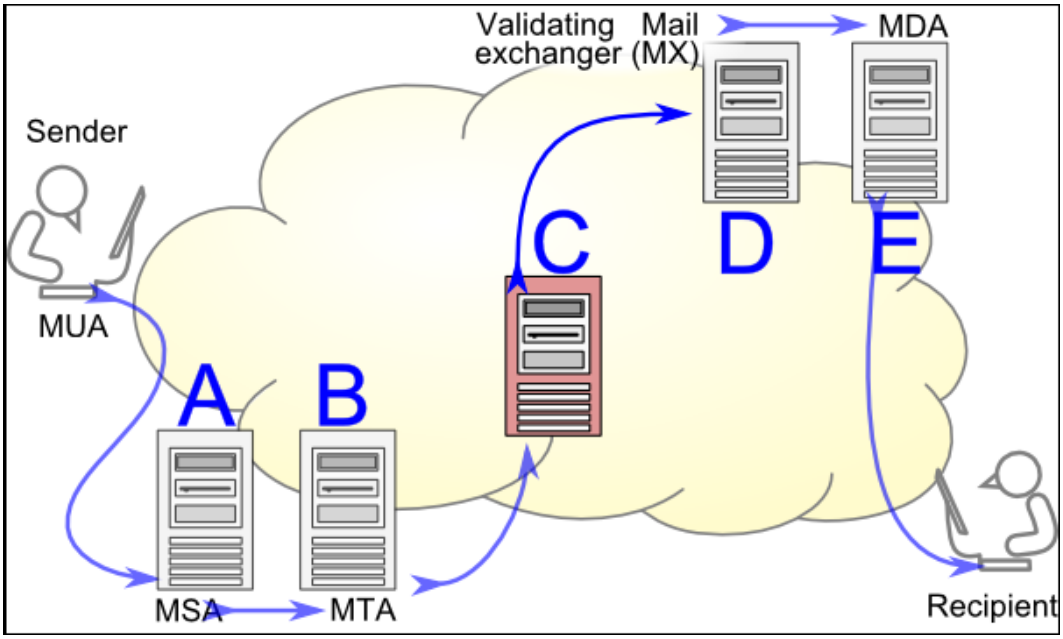

Рисунок 3.1 – Автентифікація електронної пошти

– SPF (Sender Policy Framework) – це протокол автентифікації електронної пошти, який дозволяє лише авторизованим відправникам надсилати імейли від імені офіційного домену компанії. Імейли, надіслані неавторизованими або нелегітимними відправниками, зазнають м’якої або жорсткої відмови SPF, залежно від налаштування SPF. Також дозволяє власникам доменів створювати список, з яких IP-адрес дозволено надсилати електронні листи з конвертами, використовуючи DNS-записи в домені. Це допомагає серверам одержувачів фільтрувати фальшиві та справжні листи. Сервери одержувачів можуть також

відкидати несанкціоновані та ненадійні листи ще до отримання тіла повідомлення. Принципи роботи SPF подібні до принципів роботи списків чорних дір на основі DNS або DNSBL.

– DKIM (DomainKeys Identified Mail) – це протокол аутентифікації електронної пошти, що дозволяє організаціям підписувати електронні листи цифровим підписом, які отримувачі можуть перевірити для підтвердження їх автентичності. Це допомагає захистити електронні листи від підробки та забезпечує їх цілісність. Процес підписання DKIM визначає, які поля включити до підпису DKIM-запису. Ці поля включають адресу «від», тіло, тему та інші. Ці поля повинні залишатися незмінними під час пересилання, інакше автентифікація DKIM не пройде.

– DMARC (Domain-based Message Authentication, Reporting & Conformance) – це протокол автентифікації, політики та звітності електронної пошти. Базується на протоколах SPF і DKIM, додаючи посилання на доменне ім'я автора «From», опубліковані політики для обробки одержувачами помилок автентифікації та звітність від одержувачів до відправників, для покращення та контролю захисту домену від шахрайської електронної пошти.

3.2.2 Авторизація електронної пошти

Авторизація електронної пошти – визначає, до яких ресурсів і функцій електронної пошти користувач має доступ після успішної аутентифікації. Авторизація контролює, що користувач може робити в межах поштової системи.

Визначають кілька моделей авторизації.

– DAC (Discretionary Access Control) – це тип контролю доступу, який надає або обмежує доступ до об’єкта за допомогою політики доступу, визначеної групою власників об'єкта. Механізм управління DAC визначається ідентифікацією користувача за допомогою наданих облікових даних під час автентифікації, таких як ім’я користувача та пароль.

– RBAC (Role-Based Access Control) – це підхід до обмеження доступу до системи авторизованими користувачами, до реалізації обов’язкового контролю доступу (MAC) або дискреційного контролю доступу (DAC). Контроль доступу на основі ролей визначений навколо ролей і привілеїв. Компоненти RBAC, такі як роль-дозволи, користувач-роль і відносини між ролями, спрощують виконання призначень користувачами.

– ABAC (Attribute-Based Access Control) – це модель авторизації, яка оцінює атрибути, а не ролі для визначення доступу. Мета ABAC – захистити такі об’єкти, як дані, мережеві пристрої та IT-ресурси від несанкціонованих користувачів та дій не визначених політикою безпеки організації.

3.3 Технічні методи боротьби зі спамом

В результаті проведеного аналізу існуючих методів технічного захисту, обрано набір методів, найбільш ефективно фільтруючих спам при їх комплексному застосуванні. Існують два основні технічні методи захисту від спаму: фільтрація надходження спаму на стороні сервера та на стороні клієнта.

3.3.1 Фільтрація на стороні сервера

Фільтрацію на стороні сервера в свою чергу поділяють на чорні списки, сірі списки та перевірку адреси відправника [11-12]:

– чорні списки, вони ж DNSBL (DNS-based Blackhole Lists). Це один з найстаріших методів боротьби зі спамом. Принцип його роботи полягає у занесення до чорних списків IP-адресів комп’ютерів, з яких ведеться розсилання спаму;

– сірі списки – принцип дії яких базується на тактиці розсилки спаму, який як правило, розсилається в дуже короткий час. Робота сірого списку полягає в навмисній затримці листів на деякий час. При цьому адреса і час пересилки заноситься в базу даних сірого списку. Якщо віддалений комп’ютер є справжнім поштовим сервером, то він повинен зберегти лист в черзі і повторювати пересилання протягом п’яти днів;

– перевірка адреси відправника – допомагає забезпечити автентичність листів і захиститися від спуфінгу та фішингу. За замовчуванням поштові сервери визначають лише IP-адресу сервера, на якому нібито розташований електронний ящик відправника. Повна перевірка адреси відправника полягає в тому, що поштовий сервер користувача встановлює з’єднання з віддаленим поштовим сервером і починає діалог.

3.3.2 Фільтрація на стороні клієнта

Фільтрацію на стороні клієнта в свою чергу поділяють на фільтр Баєса та контентну фільтрацію:

– фільтр Баєса – метод фільтрації спама, в основі якого лежить застосування теореми Баєса. При навчанні фільтра, для кожного зустрінутого в повідомленнях слова розраховується і зберігається його «вага» – оцінка ймовірності того, що лист з цим словом– спам. У найпростішому випадку в якості оцінки використовується частота: «появ в спамі/появ всього». Фільтри Баєса не потребують постійних налаштувань, достатньо лише попередньо обучити фільтр.

– Контентна фільтрація – полягає у перевірці повідомлення на наявність притаманних спаму слів, фрагментів тексту, картинок. В результаті аналізу можна підрахувати «спамерську вагу» повідомлення.

3.3.3 Додаткові методи захисту

Контроль масовості – це додатковий метод який базується на виявленні в поштовому потоці масових повідомлень, які є абсолютно однаковими або відрізняються несуттєво. Щоб створити ефективний «масовий» аналізатор необхідні великі обсяги поштових повідомлень. Саме тому, даний метод пропонують великі виробники, що володіють величезними потоками пошти, яку можна надати аналізу.

Використання стандартних механізмів захисту електронної пошти є критично важливим для забезпечення безпеки та конфіденційності комунікацій. Кожен з цих механізмів має свої переваги та недоліки, і жоден з них не є абсолютно ефективним сам по собі. Тому найкращі результати досягаються при інтегрованому підході, який включає кілька рівнів захисту. Це допомагає забезпечити комплексний захист від широкого спектра загроз, підвищуючи загальну безпеку інформаційної інфраструктури організації.

4 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ

Захист електронної пошти стає першочерговим завданням для забезпечення безпеки конфіденційної інформації та запобігання фінансовим і репутаційним втратам. Відповідно, необхідний комплексний підхід, що включає використання різних методів та технологій захисту електронної пошти. Ці методи можна класифікувати на апаратні, програмні та криптографічні.

4.1 Апаратні методи захисту

Апаратні методи захисту електронної пошти використовують спеціалізовані пристрої для забезпечення безпеки комунікацій та зберігання даних. Ці методи включають модулі безпеки апаратного забезпечення (HSM), брандмауерів та системи виявлення та запобігання вторгнень (IDS/IPS) які можуть забезпечувати захист від шкідливого ПЗ, спаму та інших загроз.

4.1.1 Апаратні модулі безпеки (HSM)

Апаратний модуль безпеки (HSM) – це спеціалізовані апаратні пристрої, призначені для захисту та управління криптографічними ключами. HSM додає додатковий рівень безпеки до мережі та призначений для забезпечення спеціальної криптографічної функціональності. Даний метод найкраще захищає від спуфінгу та атак типу «людина посередині» [13].

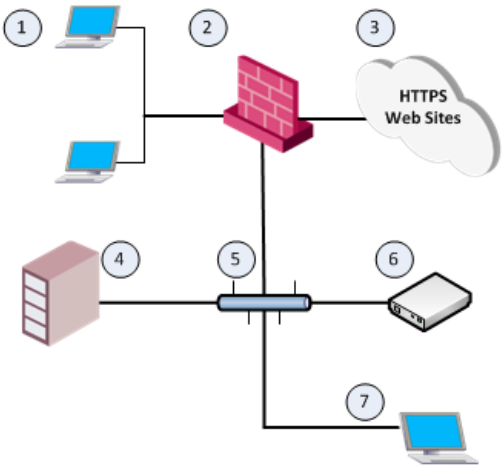

Рисунок 4.1 – Приклад застосування HSM

Приклад мережі з використанням HSM (рис. 4.1) може складатись з:

1. Внутрішні комп'ютери, які підключаються до веб-сайтів HTTPS через шлюз безпеки.

2. Шлюз безпеки з увімкненою функцією перевірки HTTPS.

3. HTTPS-сайти в Інтернеті.

4. Сервер управління безпекою, який керує шлюзом.

5. Мережа, що з'єднує.

6. Сервер HSM, який зберігає та обслуговує SSL-ключі та сертифікати для шлюзу HSM.

7. Робоча станція клієнта HSM, яка використовується для створення сертифіката центру сертифікації (ЦС) на сервері HSM.

До переваг HSM можна віднести наступне [13]:

– забезпечують надійний захист криптографічних ключів від несанкціонованого доступу і фізичних атак;

– криптографічні операції знаходяться в захищеному середовищі, що знижує ризик витоку ключів;

– зниження навантаження на основні процесори завдяки використанню HSM для криптографічних завдань;

– апаратура менш вразлива до деяких видів атак, таких як програмні експлойти.

До недоліків HSM можна віднести:

– висока вартість;

– налаштування та інтеграція можуть вимагати висококваліфікованого персоналу;

– займають фізичний простір і потребують належних умов для встановлення та функціонування;

– заміна або модернізація може бути складною та потребувати значних витрат.

HSM є ефективним засобом для захисту криптографічних ключів і виконання криптографічних операцій, таких як шифрування та цифрові підписи, які можуть значно підвищити рівень безпеки електронної пошти. Однак HSM не є універсальним засобом захисту від усіх типів атак.

4.1.2 Апаратні брандмауери

Апаратні брандмауери – це спеціалізовані пристрої, що використовуються для контролю та фільтрації мережевого трафіку на рівні мережевого обладнання. Вони працюють на фізичному рівні мережі що дозволяє здійснювати перевірку вхідного і вихідного мережевого трафіку, а також забезпечувати контроль доступу та інші політики безпеки.

Апаратний брандмауер, який підключений до мережної інфраструктури та аналізує пакети даних, щоб переконатися, що вони відповідають встановленим політикам безпеки. Коли дані намагаються увійти або вийти з мережі, брандмауер перевіряє джерело, місце призначення та іншу інформацію в заголовку кожного пакета на відповідність набору правил. Якщо пакет не відповідає цим правилам, брандмауер не пропускає його. Даний метод добре захищає від спуфінгу, MITM, Ransomware та частково від інших загроз [13].

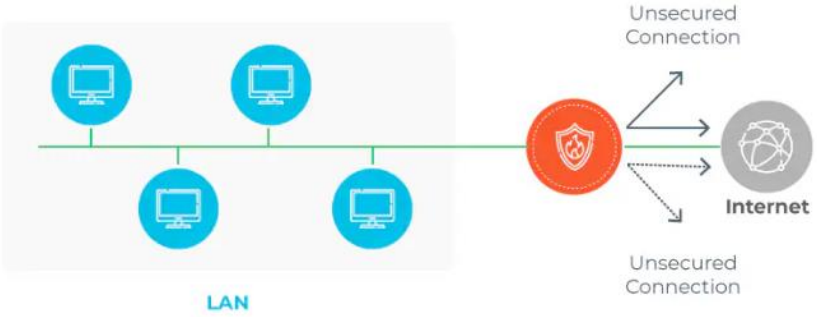

Рисунок 4.2 – Принцип дії апаратних брандмауерів

Переваги апаратних брандмауерів:

– мають велику швидкість обробки пакетів та можуть ефективно працювати з великим обсягом мережного трафіку;

– забезпечують ефективний захист від різних типів атак;

– працюють на фізичному рівні мережі

Недоліки:

– висока вартість

– налаштування брандмауерів може бути складним завданням.

У цілому, апаратні брандмауери є важливим елементом інфраструктури мережної безпеки, який дозволяє організаціям забезпечувати захист від різних видів атак та забезпечувати безпеку мережного зв’язку.

4.1.3 IDS/IPS

IDS/IPS (Intrusion Detection and Prevention System) – це апаратні системи виявлення та запобігання вторгненням, що забезпечують мережну безпеку. IDS – це пасивна система виявлення, яка у режимі реального часу аналізує весь трафік і за необхідності повідомляє про можливі загрози. Вона ніяк не модифікує мережеві пакети даних і не впливає на роботу мережевої інфраструктури, в той час як IPS здатна запобігти доставці пакетів подібно до того, як це робить брандмауер [14].

Виділяють три типи IDS за механізмом аналізу:

1. Сигнатурні IDS. Система виявлення вторгнень, що сильно нагадує звичний антивірус – вона також аналізує трафік та зіставляє отримані пакети з базою даних сигнатур.

2. IDS, засновані на аномаліях. У цьому випадку використовується технологія машинного навчання – система аналізуватиме роботу мережі та порівнюватиме її з аналогічним періодом у минулому.

3. IDS на правилах. Адміністратор може вручну прописати складні правила IDS, які дозволять виявляти загрози за непрямими чи прямими ознаками.

Переваги IDS:

– здатні виявляти різні види атак, включаючи вторгнення, шкідливі програми та інші загрози мережі;

– IPS може надавати активний захист, автоматично блокуючи або міткуючи трафік, що вважається підозрілим або шкідливим;

– дозволяє моніторити мережний трафік і виявляти аномальну активність.

Недоліки IDS:

– IDS/IPS можуть спричиняти ложнопозитивні спрацювання, що може спричинити перевантаження адміністративних ресурсів;

– деякі атаки можуть обходить захист IDS/IPS за допомогою шифрування трафіку або використання обхідних технік.

Апаратні методи захисту електронної пошти забезпечують надійний захист від різноманітних загроз завдяки використанню спеціалізованих пристроїв, таких як апаратні шлюзи безпеки, HSM, брандмауери та IDS/IPS. Ці методи допомагають знизити ризики перехоплення, модифікації та підробки електронних листів, забезпечуючи високий рівень конфіденційності, цілісності та доступності комунікацій [14].

4.2 Програмні методи захисту

Програмні методи захисту електронної пошти використовують спеціалізовані програми і служби для забезпечення безпеки електронної кореспонденції. Ці методи включають антивірусні програми та програмні фаєрволи.

4.2.1 Антивірусні програми

Антивірусні програми сканують – це спеціалізоване програмне забезпечення, яке перевіряє вхідні та вихідні повідомлення електронної пошти на наявність шкідливих програм, вірусів, троянських коней та іншого небажаного або небезпечного контенту.

До функцій антивірусних програм відносять:

– перевірка вкладень листів на наявність вірусів, троянів та іншого шкідливого ПЗ.

– постійне оновлення сигнатур вірусів для виявлення нових загроз.

– автоматичне видалення або ізоляція виявлених загроз.

– перевірка посилань у листах на предмет фішингу та інших небезпечних ресурсів.

Переваги антивірусних програм:

– автоматично сканують та фільтрують електронні листи, що знижує навантаження на користувачів;

– постійно оновлюються для захисту від нових та існуючих загроз.

– захищають як вхідні, так і вихідні листи, забезпечуючи комплексний підхід до безпеки електронної пошти.

Недоліки антивірусних програм:

– можуть генерувати фальшиві позитивні результати, що призводить до помилкової ізоляції безпечних листів.

– захист залежить від регулярності оновлень баз даних вірусів.

– можуть не виявляти нові, невідомі загрози або загрози, які обходять традиційні методи виявлення.

Антивірусні програми електронної пошти є важливою складовою системи безпеки, але для максимальної ефективності вони повинні використовуватись разом з іншими засобами захисту.

4.2.2 Програмний брандмауер

Програмний брандмауер – це брандмауер у формі програмного забезпечення, а не фізичного пристрою, який можна розгорнути на серверах або віртуальних машинах для захисту хмарних середовищ.

Програмні брандмауери призначені для захисту даних, робочих навантажень і додатків у середовищах, де розгортання фізичних брандмауерів ускладнене або неможливе: Програмно-визначені мережі (SDN), гіпервізори, публічні хмарні середовища, віртуалізовані центри обробки даних, філіали, контейнерні середовища, гібридні та мультихмарні середовища.

Програмні брандмауери використовують ті ж технології, що й апаратні (також відомі як брандмауери наступного покоління або NGFW). Програмні брандмауери пропонують кілька варіантів розгортання, щоб відповідати потребам гібридних/мультихмарних середовищ і сучасних хмарних додатків. Вони можуть бути розгорнуті в будь-якій віртуалізованій мережі або хмарному середовищі [15].

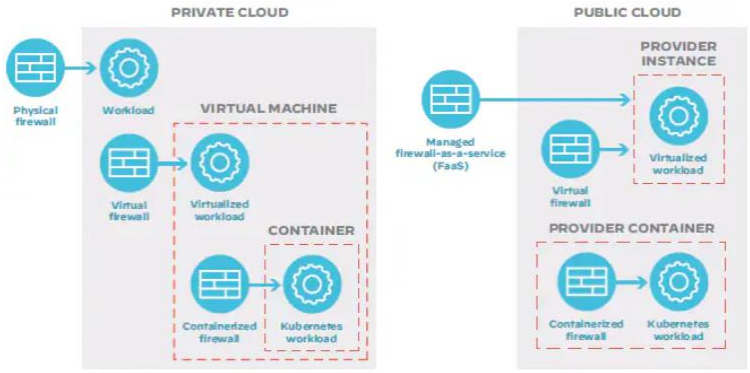

Рисунок 4.3 – Програмні брандмауери в гібридному/мультихмарному захисті

Переваги програмних брандмауерів:

– дешевші ніж апаратні брандмауери;

– ідеально підходить для особистого або домашнього використання;

– легко налаштовувати та переналаштовувати.

Недоліки програмних брандмауерів:

– забирає системні ресурси;

– іноді буває важко повністю видалити або деінсталювати брандмауер;

– не підходить там, де час відгуку є критично важливим.

4.3 Криптографічні методи захисту

Криптографічні методи забезпечують надійний захист електронної пошти, гарантуючи конфіденційність, цілісність і автентичність повідомлень. Використання криптографії допомагає запобігти перехопленню, модифікації та підробці електронних листів. Виділяють наступні основні криптографічні методи захисту електронної пошти.

4.3.1 S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) – це стандарт, який додає додатковий рівень безпеки і шифрує дані, що передаються електронною поштою. S/MIME використовує криптографію для цифрового підпису та шифрування електронної пошти, щоб запобігти несанкціонованому доступу до даних в електронному листі [16, 18].

S/MIME має дві функції безпеки:

– шифрування електронної пошти - шифрує вміст електронної пошти, що надсилається між двома користувачами з підтримкою S/MIME, щоб зробити його нечитабельним для будь-кого, окрім адресата;

– цифровий підпис – накладає цифровий підпис на електронні листи, що надсилаються між двома користувачами з підтримкою S/MIME, щоб усунути будь-який ризик підміни.

Процес починається з того, що відправник і одержувач володіють відкритими ключами один одного. Етапи шифрування електронної пошти виглядають наступним чином:

– Процес шифрування

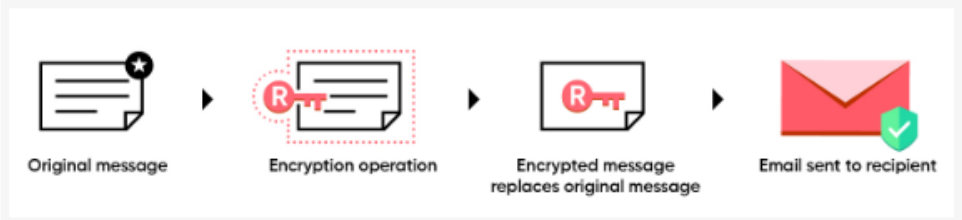

Рисунок 4.4 – Процес шифрування S/MIME

1. Як тільки відправник натискає кнопку «Надіслати», початкове незашифроване повідомлення перехоплюється.

2. Відкритий ключ одержувача використовується для шифрування оригінального повідомлення. В кінці процесу створюється зашифрована версія оригінального повідомлення.

3. Зашифроване повідомлення замінює оригінальне повідомлення.

4. Електронний лист надсилається одержувачу.

– Процес розшифрування

1. Одержувач отримує електронний лист.

2. Зашифроване повідомлення витягується.

3. Закритий ключ одержувача використовується для розшифрування зашифрованого повідомлення.

4. Оригінальне повідомлення отримується і відображається одержувачу.

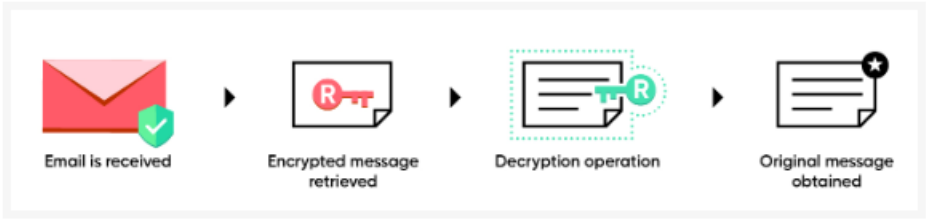

Рисунок 4.5 – Процес розшифрування

S/MIME підписує електронні листи цифровим підписом, щоб підтвердити особу відправника. Цифровий підпис надає наступні переваги:

– перевірка відправника – Цифрові підписи є унікальними для кожного користувача. Таким чином, це дозволяє одержувачу перевірити, чи дійсно електронний лист надіслала та людина, від якої він надійшов. Це усуває ризик підробки адреси електронної пошти [16, 18];

– неприйняття відмови – унікальність цифрового підпису гарантує, що автор електронного листа не зможе заперечити своє право власності на нього. Звинувачення в підробці можуть бути легко спростовані;

Процес починається з того, що відправник і одержувач володіють відкритими ключами один одного.

Цифровий підпис електронного листа працює наступним чином:

– Процес цифрового підпису

1. Як тільки відправник натискає кнопку «Відправити», оригінальне повідомлення перехоплюється.

2. Обчислюється хеш повідомлення.

3. Закритий ключ відправника використовується для шифрування хеш-значення.

4. Зашифроване хеш-значення додається до листа.

5. Імейл відправляється одержувачу.

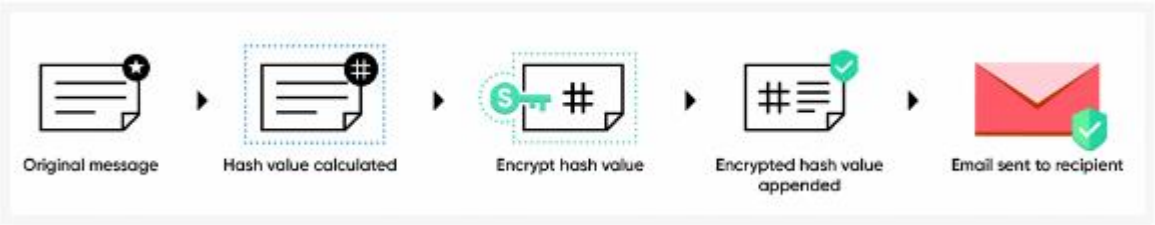

Рисунок 4.6 – Процес цифрового підпису

– Процес перевірки підпису

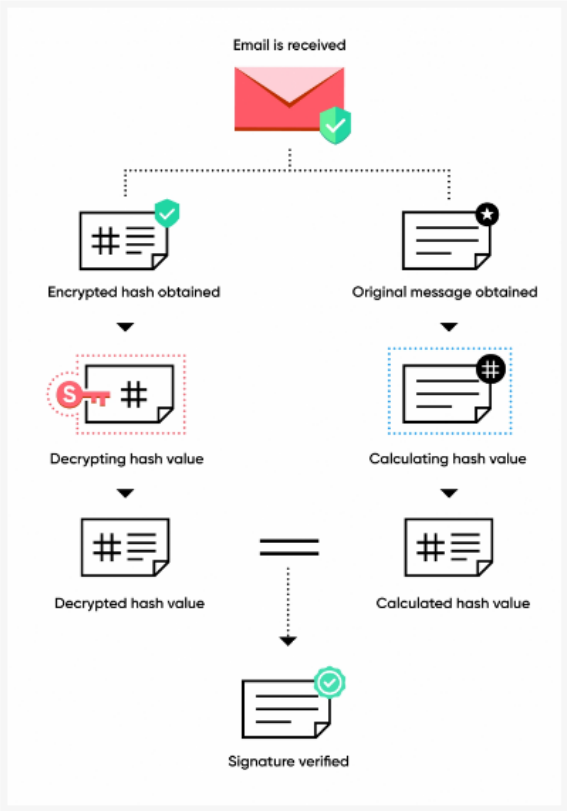

Рисунок 4.7 – Процес перевірки підпису

1. Як тільки відправник натискає кнопку «Відправити», оригінальне повідомлення перехоплюється.

2. Обчислюється хеш повідомлення.

3. Закритий ключ відправника використовується для шифрування хеш-значення.

4. Зашифроване хеш-значення додається до листа.

5. Імейл відправляється одержувачу.

Переваги використання S/MIME:

– доступний для різних сучасних поштових агентах, таких як Netscape, MS Outlook та інші.

– використовується в комерційних або промислових умовах.

– забезпечує достовірність та безпеку повідомлення.

– цифровий підпис захищає електронну пошту від підміни.

Недоліки використання S/MIME:

– не всі користувачі можуть скористатися перевагами S/MIME через примусову необхідність сертифікатів, оскільки деякі користувачі просто бажають шифруватися.

– не всі поштові клієнти підтримують підписи S/MIME.

4.3.2 PGP

PGP (Pretty Good Privacy) – це програма безпеки, яка використовується для дешифрування та шифрування електронної пошти та автентифікації електронних повідомлень за допомогою цифрових підписів та шифрування файлів. PGP підвищує безпеку електронної пошти, шифруючи дані, та робити цей метод спілкування більш приватним.

PGP є однин з перших криптографічних програм з відкритим ключем, який загальнодоступний та безкоштовний. Спочатку використовувався щоб окремі користувачі спілкувались на комп’ютерних серверах систем дошок оголошень. Пізніше було стандартизовано і підтримано іншими програмами, такими як електронна пошта. [16, 17, 18].

PGP використовує цифровий підпис (поєднання хешування і шифрування відкритим ключем) для забезпечення цілісності, автентичності та неможливості відмови. PGP використовує комбінацію шифрування з секретним ключем і шифрування з відкритим ключем для забезпечення конфіденційності. Таким

чином, можна сказати, що цифровий підпис використовує одну хеш-функцію, один секретний ключ і дві пари приватних і публічних ключів.

Переваги використання PGP:

– підробка неможлива, оскільки особистість відправника перевіряється за допомогою механізму довіри;

– кожен може легко завантажити його, оскільки він знаходиться у відкритому доступі в Інтернет;.

– зашифровані дані, тому вони не можуть бути змінені під час передачі;

– немає проблем із сумісністю.

Недоліки використання PGP:

– відкриті та закриті ключі необхідно ретельно зберігати, щоб їх можна було відновити в разі втрати;

– PGP використовує складну структуру для шифрування;

– відправник і одержувач використовують одну і ту ж версію PGP.

PGP працює завдяки поєднанню криптографії, стиснення даних і методів хешування. Він схожий на інші популярні методи шифрування, такі як Kerberos, який автентифікує користувачів мережі, рівень захищених сокетів (SSL), який захищає веб-сайти, і протокол захищеної передачі файлів (SFTP), який захищає дані в русі.

PGP використовує систему відкритих ключів, в якій кожен користувач має унікальний ключ шифрування, відомий публічно, і приватний ключ, який знає тільки він. Повідомлення шифрується, коли користувач надсилає його комусь за допомогою свого відкритого ключа, а потім розшифровується, коли одержувач відкриває його за допомогою свого закритого ключа. Він поєднує в собі криптографію з відкритим і закритим ключами, а також використання симетричних і асиметричних технологій для шифрування даних під час їхньої передачі мережею.

PGP складається з трьох етапів:

1. PGP генерує величезний, одноразовий відкритий алгоритм шифрування, який неможливо вгадати, і який стає випадковим сеансовим ключем;

2. Потім сеансовий ключ шифрується за допомогою відкритого ключа одержувача, який захищає повідомлення під час передачі. Одержувач ділиться цим ключем з усіма, від кого він хоче отримувати повідомлення;

3. Відправник повідомлення надсилає свій сеансовий ключ, після чого одержувач може розшифрувати повідомлення за допомогою свого приватного ключа.

Шифрування цілих повідомлень займає багато часу, але PGP шифрує їх за допомогою швидшого алгоритму. PGP стискає відкриті текстові дані, що економить місце на диску і час передачі, а також посилює криптографічну безпеку. Відкритий ключ використовується для шифрування коротшої версії, якою було зашифровано повне повідомлення. Обидва ключі надсилаються одержувачу, який використовує свій приватний ключ для розблокування коротшого ключа, а потім розшифровує повне повідомлення [18].

4.3.3 TLS

TLS (Transport Layer Security) – це широко розповсюджений протокол безпеки, розроблений для забезпечення конфіденційності та безпеки даних під час комунікацій через Інтернет. Основна сфера застосування TLS - шифрування зв'язку між веб-програмами та серверами, наприклад, веб-браузерами, які завантажують веб-сайт. TLS також може використовуватися для шифрування інших комунікацій, таких як електронна пошта, обмін повідомленнями та голосовий зв'язок через IP (VoIP) [19].

Шифрування TLS допомогає захистити веб-додатки від витоку даних та інших атак. Сьогодні HTTPS, захищений TLS, є стандартною практикою для веб-сайтів. Браузер Google Chrome поступово почав блокувати сайти, що не підтримують HTTPS, і інші браузери наслідували його приклад. Звичайні користувачі Інтернету з більшою обережністю ставляться до веб-сайтів, які не мають іконки замка HTTPS.

Щоб веб-сайт або додаток міг використовувати TLS, він повинен мати сертифікат TLS, встановлений на сервері походження (сертифікат також відомий як «SSL-сертифікат» через плутанину в назвах, описану вище). Сертифікат TLS видається центром сертифікації особі або компанії, яка володіє доменом. Сертифікат містить важливу інформацію про те, хто є власником домену, а також відкритий ключ сервера, обидва з яких важливі для перевірки автентичності сервера.

Криптографічні методи є основою для забезпечення надійного захисту електронної пошти. Використання TLS, PGP та S/MIME дозволяє забезпечити конфіденційність, цілісність і автентичність електронних листів. Інтеграція цих

методів у систему електронної пошти допомагає запобігти численним загрозам і зберегти безпеку важливих даних [19].

Переваги використання TLS:

– забезпечує шифрування даних, що передаються між клієнтом і сервером, захищаючи їх від несанкціонованого доступу;

– використання сертифікатів дозволяє автентифікувати сервер та клієнта, знижуючи ризик фішингових атак;

– захищає від атак типу «людина посередині» (MITM), ускладнюючи можливість перехоплення та модифікації даних.

Недоліки використання TLS:

– шифрування та дешифрування даних вимагає додаткових обчислювальних ресурсів, що може вплинути на продуктивність системи;

– Неправильна конфігурація TLS може призвести до зниження рівня безпеки або взагалі до відсутності захисту;

– Використання сертифікатів від довірених сертифікаційних центрів може бути дорогим, особливо для малих підприємств;

TLS є потужним інструментом для забезпечення безпеки мережевих з'єднань, захисту даних від прослуховування та модифікації, а також автентифікації сторін. Однак, як і будь-який інший засіб безпеки, він має свої недоліки, які слід враховувати під час його впровадження та експлуатації.

Отже криптографічні методи застосовуються для забезпечення надійного захисту електронної пошти. Використання TLS, PGP та S/MIME дозволяє забезпечити конфіденційність, цілісність і автентичність електронних листів. Інтеграція цих методів у систему електронної пошти допомагає запобігти численним загрозам і зберегти безпеку важливих даних.

5 ПОРІВНЯННЯ МЕТОДІВ ЗАХИСТУ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЇ

Для вибору єдиного найкращого методу захисту електронної пошти застосуємо метод аналізу ієрархій з урахуванням сукупності показників якості.

В якості об’єктів дослідження були обрані розглянуті методи захисту: HSM, апаратні брандмауери, IDS/IPS, антивірусні програми, програмні брандмауери, S/MIME, PGP, TLS.

В якості показників якості були обрані різні типи атак, від яких захищають ці методи, такі як фішинг, спуфінг, MITM, програми-вимагачі, ШПЗ, DDoS атаки та спам.

У таблиці 5.1 наведено порівняння методів захисту електронної пошти в розрізі перешкоді певних видів атак.

Таблиця 5.1 – Відомості про порівняння методів захисту електронної пошти

Методи захисту	Показники якості методів захисту						
	Фішинг	Спуфінг	MITM	Вимагачі	ШПЗ	DDoS атаки	Спам
HSM	Ні	Так	Так	Так	Так	Ні	Ні
Апаратні брандмауери	Ні	Частково	Частково	Частково	Частково	Так	Ні
IDS/IPS	Частково	Частково	Частково	Частково	Частково	Частково	Частково
Антивірусні програми	Частково	Ні	Ні	Так	Так	Ні	Частково
Програмний брандмауер	Частково	Частково	Ні	Частково	Частково	Частково	Частково
S/MIME	Так	Так	Так	Ні	Так	Ні	Так
PGP	Так	Так	Так	Ні	Ні	Ні	Ні
TLS	Частково	Так	Так	Так	Так	Частково	Ні

В результаті аналізу критеріїв було розроблено ієрархічне представлення задачі вибору найкращого методу захисту електронної пошти (рис. 5.1). На першому рівні знаходиться мета вибору найкращого методу захисту, на другому рівні – загрози для методів захисту, а на третьому рівні – вибрані методи захисту електронної пошти.

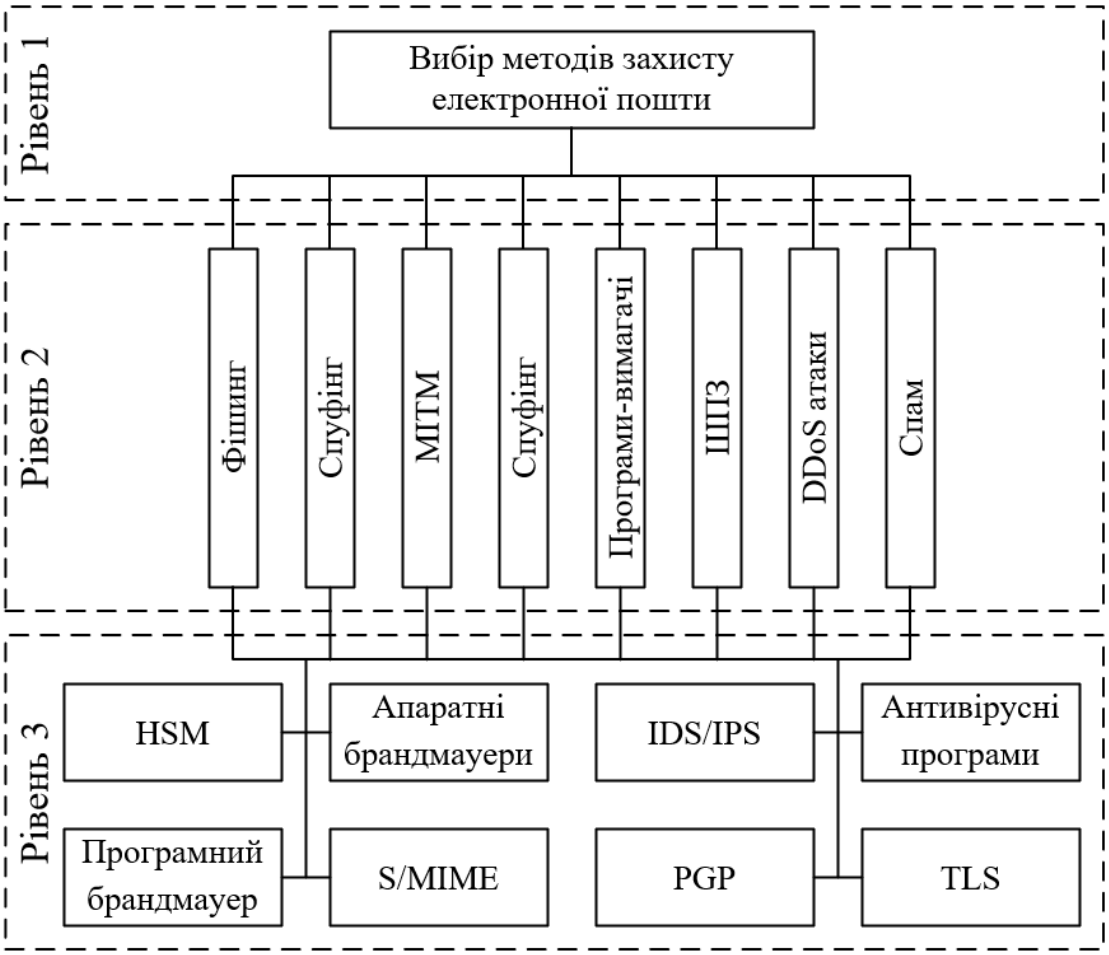

Рисунок 5.1 – Ієрархія критеріїв вибору

Для оцінки важливості критеріїв при побудові матриць парних порівнянь використовується таблиця важливості, яка базується на суб’єктивних судженнях експертів. Ці судження чисельно визначаються за шкалою відносної важливості елементів, що представлена в таблиці 5.2.

Таблиця 5.2 – Значення відносної важливості елементів порівняння

Відносна важливість	Визначення
1	Рівнозначна важливість елементів
3	Невелика перевага одного елемента над іншим
5	Помітна перевага одного елемента над іншим
7	Відчутна перевага одного елемента над іншим
9	Дуже велика перевага одного елемента над іншим
2,4,6,8	Проміжні оцінки між двома судженнями

Для розрахунку компонентів головного власного вектора матриці парних порівнянь показників якості обчислюється за формулою (5.1).

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}},\ j = \overline{1,n}, \tag{5.1}$$

де a_{ij} – оцінки парних порівнянь елементів вибору,

n – число показників якості.

Розрахуємо суму власного вектора за формулою (5.2).

$$S = \sum_{j=1}^{n} V_j, \tag{5.2}$$

Через компоненти головного власного вектора обчислюються відповідні компоненти вектора пріоритетів кожного з показників якості як нормовані значення за формулою (5.3).

$$P_j = \frac{V_j}{S},\ \ldots j = \overline{1,n}, \tag{5.3}$$

З використанням отриманих даних обчислюються значення компонентів вектора глобальних пріоритетів згідно формули (5.4).

$$C_i = \sum_{j=1}^{n} P_j Q_{ij},\ \ldots i = \overline{1,N}, \tag{5.4}$$

де N - число варіантів систем, що порівнюються.

Відповідно до методу аналізу ієрархій для сукупності показників якості (другий рівень ієрархії) була побудована матриця парних порівнянь (табл. 5.3). Для заповнення цієї таблиці було проведено попарне порівняння важливості захисту від атак для розглянутих методів. Діагональ цієї матриці заповнена значеннями «1», а елементи матриці під діагоналлю заповнені протилежними значеннями. А також розрахований власний вектор за формулою 5.1 та вектор пріоритетів за формулою 5.3.

Таблиця 5.3 – Матриця парних порівнянь показників якості та обчислення оцінки компонентів вектора пріоритетів

Критерії оцінки	Фішинг	Спуфінг	MITM	Вимагачі	ШПЗ	DDoS атаки	Спам	Власний вектор V_i	Вектор пріоритетів P_i
Фішинг	1	2	1/6	1/7	1/4	1/2	4	0.586	0.056
Спуфінг	1/2	1	1/7	1/8	1/5	1/4	2	0.367	0.035
MITM	6	7	1	1/2	2	4	8	2.798	0.265
Вимагачі	7	8	2	1	3	5	9	3.954	0.374
ШПЗ	4	5	1/2	1/3	1	2	5	1.65	0.156
DDoS атаки	2	4	1/4	1/5	1/2	1	3	0.93	0.088
Спам	1/4	1/2	1/8	1/9	1/5	1/3	1	0.274	0.026

Виконано парні порівняння варіантів на 3 рівні ієрархії. А саме порівняння методів захисту до обраних атак: фішинг, спуфінг, MITM, програми-вимагачі, ШПЗ, DDoS атаки та спам. А також отримано відповідні матриці парних порівнянь. В результаті обробки отриманих матриць обчислені згідно (5.1) та (5.3) власні вектори та вектори пріоритетів, які наведені у таблицях 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 та 5.10.

Таблиця 5.4 – Матриця парних порівнянь методів захисту відносно загрози фішингу

Фішинг	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1	1/3	1/3	1/3	1/5	1/5	1/3	0.386	0.039
Апаратні брандмауери	1	1	1/3	1/3	1/3	1/5	1/5	1/3	0.386	0.039
IDS/IPS	3	3	1	1	1	1/3	1/3	1	1	0.1
Антивіруси	3	3	1	1	1	1/3	1/3	1	1	0.1
Програмний брандмауер	3	3	1	1	1	1/3	1/3	1	1	0.1
S/MIME	5	5	3	3	3	1	1	3	2.59	0.26
PGP	5	5	3	3	3	1	1	3	2.59	0.26
TLS	3	3	1	1	1	1/3	1/3	1	1	0.1

Таблиця 5.5 – Матриця парних порівнянь методів захисту відносно загрози спуфінгу

Спуфінг	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1/3	1/3	1/5	1/3	1	1	1	0.542	0.064
Апаратні брандмауери	3	1	1	1/3	1	3	3	3	1.51	0.18
IDS/IPS	3	1	1	1/3	1	3	3	3	1.51	0.18
Антивіруси	5	3	3	1	1/3	1/5	1/5	1/5	0.767	0.091
Програмний брандмауер	3	1	1	3	1	1/3	1/3	1/3	0.872	0.104
S/MIME	1	1/3	1/3	5	3	1	1	1	1.066	0.127
PGP	1	1/3	1/3	5	3	1	1	1	1.066	0.127
TLS	1	1/3	1/3	5	3	1	1	1	1.066	0.127

Таблиця 5.6 – Матриця парних порівнянь методів захисту відносно загрози MITM

MITM	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1/3	1/3	1/5	1/5	1	1	1	0.508	0.054
Апаратні брандмауери	3	1	1	3	3	1/3	1/3	1/3	1	0.106
IDS/IPS	3	1	1	3	3	1/3	1/3	1/3	1	0.106
Антивіруси	5	1/3	1/3	1	1	1/5	1/5	1/5	0.508	0.054
Програмний брандмауер	5	1/3	1/3	1	1	1/5	1/5	1/5	0.508	0.054
S/MIME	1	3	3	5	5	1	1	1	1.968	0.209
PGP	1	3	3	5	5	1	1	1	1.968	0.209
TLS	1	3	3	5	5	1	1	1	1.968	0.209

Таблиця 5.7 – Матриця парних порівнянь методів захисту відносно загрози програм-вимагачів

Програм-вимагачів	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052
Апаратні брандмауери	3	1	1	3	1	1/3	1/3	3	1.147	0.136
IDS/IPS	3	1	1	3	1	1/3	1/3	3	1.147	0.136
Антивіруси	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052

Продовження таблиці 5.7

Програмний брандмауер	3	1	1	3	1	1/3	1/3	3	1.147	0.136
S/MIME	5	3	3	5	3	1	1	1/5	1.846	0.218
PGP	5	3	3	5	3	1	1	1/5	1.846	0.218
TLS	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052

Таблиця 5.8 – Матриця парних порівнянь методів захисту відносно загрози ШПЗ

ШПЗ	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052
Апаратні брандмауери	3	1	1	3	1	1/3	1/3	3	1.147	0.136
IDS/IPS	3	1	1	3	1	1/3	1/3	3	1.147	0.136
Антивіруси	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052
Програмний брандмауер	3	1	1	3	1	1/3	1/3	3	1.147	0.136
S/MIME	5	3	3	5	3	1	1	1/5	1.846	0.218
PGP	5	3	3	5	3	1	1	1/5	1.846	0.218
TLS	1	1/3	1/3	1	1/3	1/5	1/5	1	0.443	0.052

Таблиця 5.9 – Матриця парних порівнянь методів захисту відносно загрози DDoS атак

DDoS атаки	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1/5	1/3	1	1/3	1	1	1/3	0.542	0.054
Апаратні брандмауери	5	1	3	5	3	5	5	3	3.376	0.335
IDS/IPS	3	1/3	1	3	1	3	3	1	1.51	0.15
Антивіруси	1	1/5	1/3	1	1/3	1	1	1/3	0.542	0.054
Програмний брандмауер	3	1/3	1	3	1	3	3	1	1.51	0.15
S/MIME	1	1/5	1/3	1	1/3	1	1	1/3	0.542	0.054
PGP	1	1/5	1/3	1	1/3	1	1	1/3	0.542	0.054
TLS	3	1/3	1	3	1	3	3	1	1.51	0.15

Таблиця 5.10 – Матриця парних порівнянь методів захисту відносно загрози спаму

Спаму	HSM	Апаратні брандмауери	IDS/IPS	Анти-віруси	Програмний брандмауер	S/MIME	PGP	TLS	Власний вектор V_i	Вектор пріоритетів P_i
HSM	1	1	1/3	1/3	1/3	1/5	1	1	0.542	0.054
Апаратні брандмауери	1	1	1/3	1/3	1/3	1/5	1	1	0.542	0.054
IDS/IPS	3	3	1	1	1	1/3	3	3	1.51	0.15
Антивіруси	3	3	1	1	1	1/3	3	3	1.51	0.15
Програмний брандмауер	3	3	1	1	1	1/3	3	3	1.51	0.15
S/MIME	5	5	3	3	3	1	5	5	3.376	0.335
PGP	1	1	1/3	1/3	1/3	1/5	1	1	0.542	0.054
TLS	1	1	1/3	1/3	1/3	1/5	1	1	0.542	0.054

У таблиці 5.10 зведені отримані оцінки компонентів вектора пріоритетів показників якості, а також векторів пріоритетів методів захисту, по відношенню до фішингу, спуфінгу, MITM, програм-вимагачів, ШПЗ, DDoS атак та спаму. З використанням цих векторів пріоритетів обчислено значення компонентів глобального вектора пріоритетів згідно з формулою (5.4), які наведено в останньому стовпці таблиці 5.11.

Таблиця 5.11 – Результати обчислення значень компонентів глобального вектора пріоритетів

№	Методи захисту	Q_{ij}							C_i
		k_1	k_2	k_3	k_4	k_5	k_6	k_7	
1	HSM	0.039	0.064	0.054	0.052	0.052	0.054	0.054	0.053
2	Апаратні брандмауери	0.039	0.18	0.106	0.136	0.136	0.335	0.054	0.139
3	IDS/IPS	0.1	0.18	0.106	0.136	0.136	0.15	0.15	0.129
4	Антивірусні програми	0.1	0.091	0.054	0.052	0.052	0.054	0.15	0.059
5	Програмний брандмауер	0.1	0.104	0.054	0.136	0.136	0.15	0.15	0.112
6	S/MIME	0.26	0.127	0.209	0.218	0.218	0.054	0.335	0.203
7	PGP	0.26	0.127	0.209	0.218	0.218	0.054	0.054	0.196
8	TLS	0.1	0.127	0.209	0.052	0.052	0.15	0.054	0.108
P_j		0.056	0.035	0.265	0.374	0.156	0.088	0.026	

За максимальним значенням компонента вектора глобальних пріоритетів вибираємо найкращий метод захисту електронної пошти з урахуванням введених показників якості. Таким методом виявився криптографічний стандарт S/MIME, який забезпечую захист від самих небезпечних атак.

ВИСНОВКИ

В ході опрацювання технічного завдання до кваліфікаційної роботи, були виконані наступні етапи:

– розглянуті загальні відомості електронної пошти, а саме принцип дії, типи пошти та протоколи за якими вона працює;

– виконано огляд основних атак на електронну пошту, їх опис, принцип дії та на що спрямовані ці атаки;

– виконано систематизацію стандартних методів електронної пошти, включаючи детальний розгляд видів шифрування електронної пошти, та методи аутентифікації та авторизації користувачів;

– розглянуто методи та засоби захисту електронної пошти, а саме апаратні, програмні та криптографічні методи захисту електронної пошти;

– дослідження та порівняння методів захисту методом аналізу ієрархії.

За результатами дослідження методом аналізу ієрархії було з’ясовано, що кращім методом захисту електронної пошти є криптографічний стандарт S/MIME, який захищає від найвразливіших та небезпечних кібератак на електронну пошту, таких як фішинг, спуфінг атаки типу «людина в середені», від шкідливого програмного забезпечення, а також у боротьбі зі спамом. S/MIME використовує криптографію для цифрового підпису та шифрування електронної пошти, щоб запобігти несанкціонованому доступу до даних в електронному листі. Може використовувати як симетричні та і асиметричні протоколи та алгоритми шифрування, такі як RSA, ECC, 3DES та AES.

Підводячи підсумки S/MIME є потужним інструментом для забезпечення безпеки електронної пошти, пропонуючи надійні методи для шифрування повідомлень та автентифікації відправників.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Терейковський І. А. Методологія класифікації листів електронної пошти з використанням нейронних мереж / І. А. Терейковський // Захист інформації. - 2013. - т. 15, № 2. - С. 115-122. - Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2013_15_2_6.

2. Електронна пошта: історія виникнення та практичне майбутнє [Електронний ресурс] // Gigacloud. – 2023. – Режим доступу до ресурсу: https://gigacloud.ua/blog/navchannja/chi-e-majbutne-v-elektronnoi-poshti.

3. Simple Mail Transfer Protocol [Електронний ресурс] // Sendpulse. – 2023. – Режим доступу до ресурсу: https://sendpulse.ua/ru/support/glossary/smtp-protocol.https://aws.amazon.com/ru/what-is/smtp/

4. Гаврилюк В.І. Протоколи POP, IMAP, SMTP: основні принципи та застосування // Young Scientist. - 2020. - т. 19. - С. 119-121. - Режим доступу: https://libeldoc.bsuir.by/bitstream/123456789/38974/1/Gavrilyuk_Protokoly.pdf.

5. 2023 email security trends [Електронний ресурс] // Barracuda. – 2023. – Режим доступу до ресурсу: https://www.barracuda.com/reports/email-security-trends-report-2023.

6. Безпека електронної пошти [Електронний ресурс] // Eop-ai. – 2023. – Режим доступу до ресурсу: https://top-ai.com.ua/resursy/slovnyk-z-kiberbezpeky/bezpeka-elektronnoyi-poshty.

7. Шифрування: типи і алгоритми. [Електронний ресурс] – Режим доступу до ресурсу:https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

8. Асиметричне шифрування [Електронний ресурс] – Режим доступу до ресурсу: https://hostkoss.com/b/uk/encryption-types-algorithms/.

9. Як покращити доставлюваність за допомогою email-автентифікації [Електронний ресурс] – Режим доступу до ресурсу: https://stripo.email/ua/blog/how-to-improve-deliverability-with-email-authentication/.

10. Porter, C. Email security with Cisco IronPort. Cisco Press. – Indianapolis, 2012. – P. 576.

11. Schryen Guido. Anti-Spam Measures: Analysis and Design. – Aachen : Springer, 2007.–P. 61–70.

12. Tan Ying. Anti-Spam Techniques Based on Artificial Immune System. – Boca Raton : CRC Press, 2016. –P. 5–7.

13. William Stallings. Network Security Essentials: Applications and Standards. 6th edition, 2016. – 464p.

14. Fausto Marcantoni, IDS/IPS: Intrusion Detection/Prevention System // Università degli Studi di Camerino. – 2012. 65c. - Режим доступу: https://computerscience.unicam.it/marcantoni/tesi/IDS-IPS%20Intrusion%20Detection-Prevention%20System.pdf.

15. What is a Software Firewall [Електронний ресурс] – Режим доступу до ресурсу: https://www.paloaltonetworks.com/cyberpedia/what-is-a-software-firewall.

16. Secure/ Multipurpose Internet Mail Extensions (S/MIME) [Електронний ресурс] – Режим доступу до ресурсу: https://www.zoho.com/mail/help/s-mime.html.

17. PGP [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/computer-network-pgp.

18. Difference between PGP and S/MIME [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/pgp-vs-smime.

19. What is Transport Layer Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/#:~:text=Transport%20Layer%20Security%2C%20or%20TLS,web%20browsers%20loading%20a%20website.