Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеню бакалавра

студента *Іванова Станіслава Сергійовича*

академічної групи *125-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1] _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи протидії фішингу в корпоративній пошті*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	доцент Пілова Д.П.	95	відмінно	

Рецензент				

Нормоконтролер	проф. Гусєв О.Ю.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та комунікацій
_____д.т.н., проф. Корнієнко В.І
«_____»_____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеню бакалавра

студенту ***Іванову С. С.*** **академічної групи** ***125-19-1***

(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1] _____

за освітньо-професійною програмою ***Кібербезпека***

_____

(офіційна назва)

на тему ***Методи протидії фішингу в корпоративній пошті***

_____,

затверджену наказом ректора НТУ «Дніпровська політехніка» від ***16.05.2023*** № ***350-с***

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Аналіз актуальності питання. Постановка задачі.	15.05.2023
Розділ 2	Аналіз існуючих методів протидії фішингу, розробка рекомендацій щодо їх впровадження.	30.05.2023
Розділ 3	Обчислення витрат на впровадження запропонованих рекомендацій, визначення їх економічної ефективності.	05.05.2023

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі 01.05.2023

Дата подання до екзаменаційної комісії 13.05.2023

Прийнято до виконання _____ ***Іванов С.С.***
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __с., __рис., __табл., __додатка, _джерел.

Об'єкт дослідження: корпоративні сервіси електронної пошти.

Мета роботи: підвищення ефективності протидії фішинговим атакам на корпоративні сервіси електронної пошти.

Предмет дослідження: методи протидії фішингу в корпоративній пошті.

Методи розробки: аналіз, опис, порівняння.

У першому розділі проведено аналіз актуальності питання, наведено теоретичні відомості про архітектури сервісів корпоративної пошти, фішингові атаки та їх наслідки. Виконана постановка задачі кваліфікаційної роботи та сформульовано висновки.

У спеціальній частині наведено загальні відомості щодо методів протидії фішингу, проаналізовано існуючі комплексні рішення протидії фішинговим атакам. Розроблено рекомендації щодо впровадження методів протидії фішингу в організації, залежно від обраної ними архітектури корпоративної пошти, та зроблено висновки щодо виконаної роботи.

В економічному розділі визначено економічну доцільність запропонованих рекомендацій щодо впровадження методів протидії фішингу. Проведено розрахунки капітальних (фіксованих) витрат, поточних (експлуатаційних витрат), загального збитку внаслідок успішної фішингової атаки та загального ефекту від впроваджених рекомендацій, сформульовано висновки на основі отриманих результатів.

Практичне завдання роботи полягає в розробці рекомендацій, щодо впровадження методів протидії фішингу в сервісах корпоративної пошти.

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ФІШИНГ, КОРПОРАТИВНА ПОШТА, ПРОТИДІЯ ФІШИНГУ.

ABSTRACT

Explanatory note: __pp., __pic., __tables, __app, __sources.

Object of research: corporate e-mail services.

Purpose: to increase the effectiveness of countering phishing attacks on corporate email services.

The subject of the study: methods of countering phishing in corporate email.

Research methods: analysis, description, comparison.

The first section analyzes the relevance of the issue, provides theoretical information about the architecture of corporate email services, phishing attacks and their consequences. The task of the qualification work is formulated and conclusions are drawn.

The special section provides general information on methods of counteracting phishing, analyzes existing comprehensive solutions to counteract phishing attacks. Recommendations for the implementation of phishing prevention methods in organizations, depending on their chosen corporate email architecture, are developed, and conclusions are drawn.

The economic section determines the economic feasibility of the proposed recommendations for the implementation of phishing countermeasures. The author calculates capital (fixed) costs, current (operating) costs, total damage due to a successful phishing attack, and the overall effect of the implemented recommendations, and formulates conclusions based on the results obtained.

The practical significance of the work is to develop recommendations for the implementation of phishing countermeasures in corporate email services.

INFORMATION SECURITY, CYBERSECURITY, PHISHING, CORPORATE MAIL, COUNTERING PHISHING.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

MFA – Multi-factor Authentication

АПЗ – антивірусне програмне забезпечення

БА – багатофакторна автентифікація

КМПФ – комплексні методи протидії фішингу

КП – корпоративна пошта

МПФ – методи протидії фішингу

ПЗ - Програмне забезпечення

ПК – персональний комп'ютер

СФС – система фільтрації спаму

ФА – фішингова атака

ШІ – Штучний інтелект

ІКС – інформаційно-комунікаційна система

ІС – інформаційна система

ЗМІСТ

С.

ВСТУП

Метою кваліфікаційної роботи є підвищення ефективості протидії фішинговим атакам на корпоративні сервіси електронної пошти.

Об'єктом дослідження було обрано корпоративні сервіси електронної пошти, як найпоширеніший спосіб комунікації в організаціях.

Предметом дослідження стали методи протидії фішингу, через їх важливість для забезпечення інформаційної безпеки організації від атак цього типу.

В зв'язку зі щорічним зростанням загальної кількості фішингових атак та значним збільшенням фінансової шкоди, яку вони завдають організаціям, впровадження методів протидії фішингу стає все більш необхідним.

Через перехід багатьох працівників на віддалений спосіб роботи, велика кількість організацій змушені були вирішувати проблему комунікації між співробітниками. Ключовим рішенням в цьому питанні стало створення та впровадження власних корпоративних сервісів електронної пошти, отже впевнено можна сказати, що за останні роки значно збільшилась кількість організацій, що обирають саме технології корпоративної пошти для побудови систем внутрішньої комунікації.

Враховуючи ці тенденції, зросла кількість методів і засобів протидії фішингу, ця індустрія активно розвивається, постійно впроваджуються нові стандарти та політики, отже впевнено можна стверджувати, що розробка рекомендацій щодо впровадження методів протидії фішингу в корпоративних сервісах електронної пошти стає все більш актуальним питанням.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз актуальності проблеми

Відповідно до дослідження Tessianза 2021 рік, при проведенні якого було проаналізовано близько 4 млрд. листів, в середньому один працівник отримує 14 фішингових листів на рік[3]. Найбільшою популярністю серед фішерів користуються сфери роздрібної торгівлі, виробництва, харчових продуктів та напоїв, дослідження і розвитку та технологій. Цікавим виявилось те, що зловмисники переважно зосереджуються не на великих компаніях, а на малих. Це пов'язують з тим, що малі компанії хоч і мають меншу цінність, проте стан захищеності їх систем на порядок нижчий ніж у великих корпорацій. Графік кількість листів з фішингом, що приходили за рік на одну корпоративну пошту відповідно до індустрії зображено на рис. 1.1.

Рисунок 1.1 - Середня кількість фішингових листів на пошту за рік в індустрії

Також важливим параметром є час, в який відправляються фішингові листи, відповідно до того ж дослідження найпопулярнішим часом серед зловмисників є проміжок з 14:00 до 18:00. Враховуючи це, можна прийти до висновку, що фішинг є найбільш ефективним саме в кінці робочого дня, коли працівники вже втомлені і їх увага розосереджена. Графік кількості отриманих фішингових листів за відповідну годину зображений на рис. 1.2.

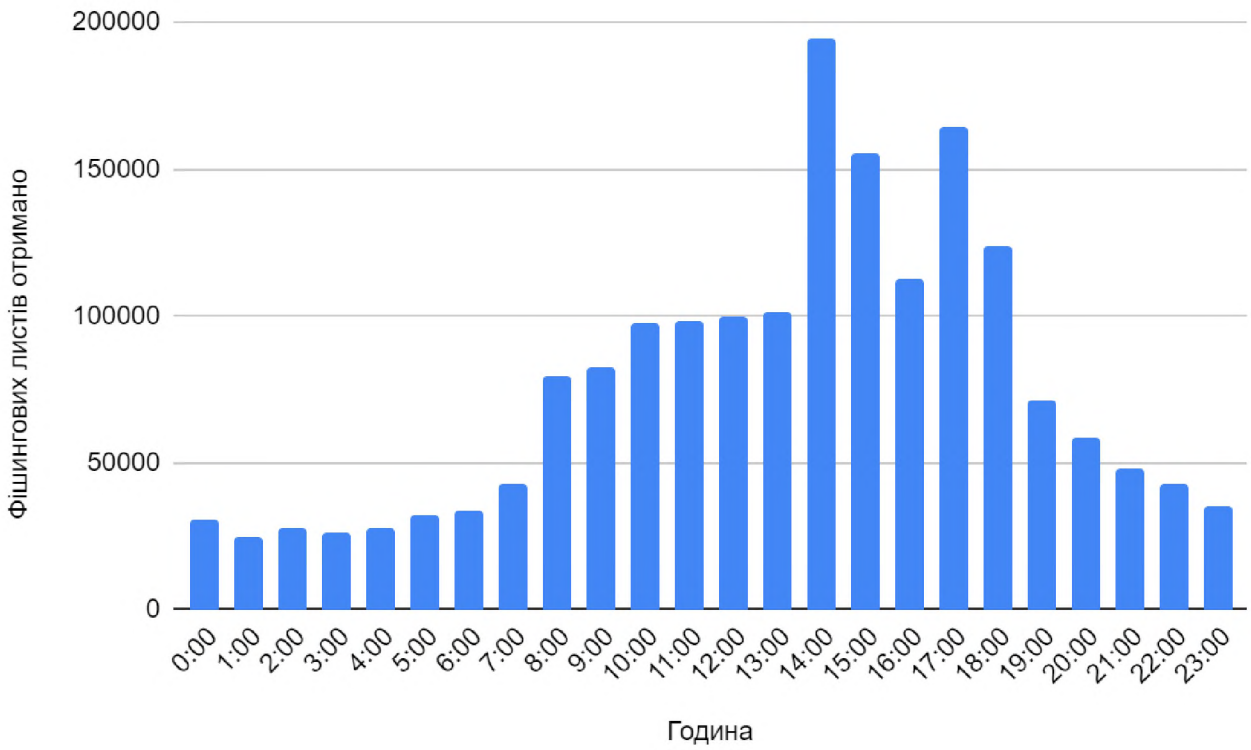

Рисунок 1.2 – Кількість отриманих фішингових листів за певну годину

Дослідження ESET у 2021 році виявило зріст кількості фішингових атак на пошту у період з травня по серпень на 7,3%, також цю тенденцію підтвердило дослідження IBM за 2021 рік, за його результатами загальна кількість фішингових атак зросла на 2% у період між 2019 і 2020 роками[4, 5]. Враховуючи ці дані можна стверджувати, що актуальність даної проблеми росте з кожним роком.

У звіті CISCO про тенденції загроз кібербезпеці за 2021 рік, наведена інформація, що у 86% організацій як мінімум одна особа перейшла за

фішинговим посиланням. Також у звіті компанії сказано, що 90% витоку даних в організація приходиться саме на фішингові атаки[6]. Також CISCO зазначили, що протягом року фішингові атаки відбуваються не рівномірно. Як правило, різкий зріст фішингових атак відбувається у грудні, перед новорічними святами, тоді кількість атак зросла на 52%, також незначний зріст відбувається в «Чорну п'ятницю». Таке збільшення атак можна пояснити тим, що відповідно до рис. 1.1, найбільша кількість листів надходила організаціям, що займаються роздрібною торгівлею. Саме в період знижок та свят ці компанії отримують найбільші прибутки, тому фішери, знаючи це, ретельно готуються до атак, та проводять їх у період, коли вони зможуть завдати найбільших збитків.

За результатами дослідження Verizon 2021 Data Breach Investigations Report, 96% фішингових атак відбувались через пошту, 3% через підроблені веб-сайти, 1% через телефон[7].

Організовані групи кіберзлочинців обирали фішинг для нападу та подальшого розвитку своєї атаки в 65% відомих інцидентів, про це сказану у звіті Symantec Internet Security Threat Report 2019. В таблиці 2.2 вказані найпопулярніші тематичні лінії, які використали фішери під час для компрометації корпоративної пошти, відповідно до цього ж дослідження.

Таблиця 1.1 – Найпопулярніші тематичні лінії в фішингових листах для компрометації корпоративної пошти та частота їх використання

Тема листа	**Частота використання, %**
терміново	8
запит	5,8
важливо	5,4
оплата	5,2
увага	4,4
несплачений платіж	4,1
інформація	3,6
важливе оновлення	3,1
увага (скорочено)	2,3

Транзакція	2,3

Відповідно до рис. 1.2, при фішингових атаках з використанням шкідливого ПЗ в 2021 році, зловмисники найчастіше використовували файли наступних типів: скрипти, виконувані файли, архіви, файли програм Microsoft Office, та PDF файли.

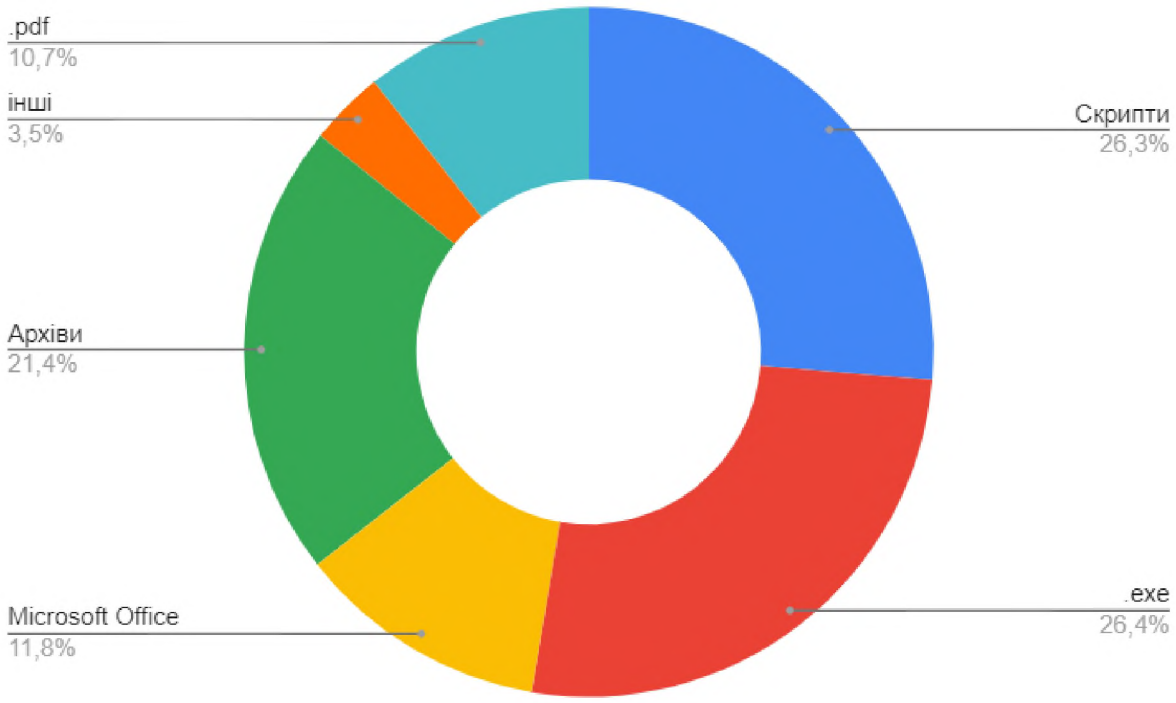

Рисунок 1.2 – Частота використання заражених файлів при фішингових атаках на корпоративну пошту

За результатами опитування лідерів організацій в питаннях інформаційної безпеки про вплив успішних фішингових атак, були отримані наступні дані:

- 60% організацій втратили дані
- У 52% організацій були викрадені облікові дані або зламані облікові записи
- 47% організацій були заражені програмами-вимагачами
- 29% організацій були заражені шкідливим ПЗ
- 18% організацій зазнали фінансових втрат

За даними IBM, загалом фішинг посідає друге місце серед найдорожчих причин витоку даних і коштує компаніям в середньому 4,65 мільйонів доларів

США. А фішингові атаки при яких зловмисники викрадають або підробляють легітимні корпоративні поштові скриньки - посідає перше місце, коштуючи компаніям в середньому 5,01 мільйони доларів США за один випадок.

За даними ФБР, в 2020 році організації зазнали збитків на суму 1,8 мільярди доларів США через фішингові атаки на корпоративні пошти. Також в звіті відмічається, що за 2020 рік значно зросла збитки в наслідок цих атак[8].

1.2 Аналіз технологій корпоративного сервісу електронної пошти.

Організація внутрішньої комунікації в сучасній компанії це надважлива задача. Правильно побудована модель комунікації між співробітниками в одній команді, між командами, на різних рівнях менеджменту значно прискорює бізнес-процеси, а також спрощує обмін повідомленнями між працівниками, ведення звітності, та проведення аудиту інформаційної безпеки. Корпоративна електронна пошта є базовою складовою будь-якої корпоративної мережі. Завдяки електронній пошті, яка функціонує лише в межах компанії, працівники можуть безпечно обмінюватись документами та важливою інформацією. Корпоративна пошта забезпечує конфіденційність даних, та їх безпеку, вона легко інтегрується з іншими інструментами комунікації. Все це робить її невід'ємною частиною сучасної організації і найпоширенішим способом їх внутрішньої комунікації.

Однією з ключових особливостей корпоративної пошти є використання власної доменної адреси. Корпоративні скриньки можуть бути створені з використанням домену, що належить конкретній організації, таким чином поштова адреса буде виглядати так: «name@company.com». Ця особливість сприяє прискоренню комунікацію між співробітниками компанії та зовнішніми контактами. А також дозволяє легко налаштувати фільтрацію повідомлень, якщо є необхідність переглядати або отримувати лише внутрішні листи.

Існує декілька способів організації власного поштового сервіса, доступні для організацій. Кожен з них має свої особливості, переваги, та, найголовніше, вартість та складність адміністрування.

Як правило, переважно розглядається три основних архітектури, а саме:

- поштовий сервіс з серверами розміщеними безпосередньо на підприємстві;
- оренда хмарних сервісів корпоративної пошти;
- використання домену на відомому поштовому сервісі.

Найпростішим шляхом організації корпоративної пошти буде вибір відомого поштового сервісу. Такими сервісами можуть стати пошти від Gmail, Yahoo!, Microsoft тощо. Проте це рішення підходить лише для невеликих організацій, єдина його перевага – простота. Корпоративні пошти, організовані в такий спосіб, сильно обмежені в налаштуваннях та не часто не дають змоги впровадити власні політики безпеки.

1.2.1 Особливості створення власного поштового сервісу з серверами розміщеними на підприємстві

Створення власного поштового сервісу з серверами розміщеними на підприємстві навпаки – найскладніший шлях організації корпоративної пошти. Типовий поштовий сервер складається з багатьох програмних компонентів, кожен з яких повинен бути налаштований, і налаштований так, щоб всі інші компоненти працювали правильно. Оскільки компонентів може бути дуже багато, налаштування поштового сервісу може викликати серйозні труднощі. Для організації базового поштового серверу необхідно три компонента:

- агент передачі пошти
- агент з доставки пошти
- сервер IMAP або POP3

Агент передачі пошти (Mail Transfer Agent) має два обов'язки: надсилання пошти на зовнішній поштовий сервер та отримання пошти від зовнішнього поштового сервісу . Прикладами таких агентів є Postfix, Exim, Sendmail.

Агент з доставки пошти, або локальний агент доставки, його задача полягає в отриманні пошти від MTA, та розміщення їх в поштовій скриньці відповідного користувача. Існують різні формати поштових скриньок, наприклад mbox і Maildir. Кожен агент підтримує повні формати поштових скриньок. Вибір формату поштової скриньки визначає спосіб зберігання повідомлень на поштовому сервері, що в свою чергу впливає на продуктивність доступу до поштової скриньки, використання ресурсів диска а також на сумісність імпорту та експорту повідомлень. До прикладів ПЗ, що забезпечує доставку пошти можна віднести Postfix і Dovecot.

IMAP або POP3 – це протоколи, які використовуються поштовими клієнтами – ПЗ яке використовується для читання електронної пошти та її отримання.

IMAP – складніший протокол, його особливістю є те, що він дозволяє декільком клієнтам підключатись до поштової скриньки одночасно. Повідомлення електронної пошти копіюються на клієнт, а оригінальне повідомлення залишається на поштовому сервері.

POP3 являється простішим протоколом, та на відміну від IMAP переміщує повідомлення електронної пошти на комп'ютер поштового клієнта, як правило цю ролі виконує локальний комп'ютер користувача.

Але базового функцій поштового сервісу замало, для отримання всіх переваг від використання власної корпоративної пошти, тому на додаток для них, потрібно ще встановити додаткові компоненти, такі як:

- фільтр спаму
- антивірус
- веб-пошта

Варто розуміти, що крім зазначених вище програмних компонентів, поштовому сервісу ще потрібне доменне ім'я, відповідні записи DNS і сертифікат SSL.

Основною задачею спам-фільтра є зменшення кількості небажаних повідомлень, які відображаються в поштовій скриньці користувача. Це

досягається шляхом застосування до всієї вхідної пошти певних правил та критеріїв, що враховують низку факторів, наприклад сервер що надіслав листа, чи текст повідомлення що міститься у листі. Якщо повідомлення не проходить фільтр, то воно або видаляється, або переміщається у спеціальну папку для подальшої перевірки чи на карантин, в залежності від налаштувань спам-фільтру. Неочевидною є можливість застосування спам-фільтру до вихідної пошти, проте це рішення може вберегти від небажаного спаму в разі отримання зловмисниками доступу до облікового запису електронної пошти. Одним з найпопулярніших є спам-фільтр з відкритим кодом під назвою SpamAssasin.

Антивіруси використовуються для виявлення вірусів, троянів та іншого шкідливого ПЗ у вхідній та вихідній пошті, популярним антивірусним механізмом з відкритим кодом є ClamAV.

Для спрощення роботи з поштовим сервером для користувачів використовують Веб-пошту. У контексті запуску поштового сервісу, веб-пошта – це поштовий клієнт, що надасть користувачу доступ до функцій поштового сервісу через веб-браузер. Компонент веб-пошти для якого потрібен веб-сервер, наприклад Nginx або Apache, може працювати на поштовому сервері. Популярними інструментами, для забезпечення функцій веб-пошти є Roundcube або Citadel.

Розглянувши особливості організації власного поштового сервісу потрібно розглянути переваги які він надає.

Перша і найочевидніша перевага – можливість повного налаштування поштового сервісу корпоративної пошти майже на найнижчому рівні. Організація має змогу самостійно обирати набір технологій, їх налаштування в залежності від особливостей своєї діяльності. Є можливість обмежити надходження повідомлень, що відповідають певному шаблону, або навпаки, отримувати лише ті повідомлення, що відповідають потрібному шаблону.

Організація, що володіє власним поштовим сервером повністю несе відповідальність за збереження приватності та конфіденційності даних. Хоч це і звучить як певний недолік, проте лише організація, що володіє даними може

знати реальну їхню цінність, та вкладати в збереження інформації ту кількість часу і ресурсів, що відповідає їй. Збереження критичних даних безпосередньо на території організації значно зменшує ймовірність їх витоку.

Зберігання даних на території організації забезпечує більш жорсткий контроль над своїми даними. Якщо листи будуть зберігатись на орендованому поштовому сервісі, що знаходиться в США, то за законами США, власник серверу вимушений буде надати доступ до ваших листів за вимогами правоохоронних органів.

Відповідальність за обслуговування серверів буде лежати на плечах організації, яка є власником поштового серверу. Ніхто не застрахований від збою в роботі орендованого серверу, часто це може призвести до зупинки роботи організації, фінансових втрат внаслідок зупинки бізнес-процесів чи взагалі втрати даних. Фізичне володіння сервером дає змогу швидше відновити його роботу, або запустити резервний сервер в разі його наявності.

Організація несе відповідальність свого поштового сервісу. Якщо електронна пошта організації розміщена на тому ж сервері, що і організація яка відсилає спам або інші зловмисні листи, то є ймовірність потрапити до списку блокування в антиспам системах інших поштових сервісів. Шанс цього буде ще більшим, якщо постачальник послуг є не добросовісним і повільно реагує на скарги та повідомлення про порушення правил.

Проте далеко не кожна організація повинна керувати власним поштовим сервером. Складність налаштування вимагає наявності в організації людини, що буде слідкувати за роботою та надавати технічну підтримку серверу, впроваджувати на нього нові технології, встановлювати оновлення та проводити вчасну заміну обладнання. А переваги отримані внаслідок володіння власним сервером важливі далеко не кожному, саме тому розумніше буде скористатись наступним способом.

1.2.2 Аналіз Особливостей створення корпоративної пошти на хмарних сервісах

Найпоширеніший спосіб організації власної корпоративної пошти. Він підкупає своєю простотою та різноманітністю. Існує багато компаній, що надають послуги зі створення поштового сервісу та його адміністрування, організація отримує можливість використання власного домену незалежно від того, де було придбане її доменне ім'я.

Дані організації будуть зберігатись на серверах компанії, що надають послуги з оренди поштового серверу. Корпоративні листи можуть займати великий простір на диску, використовуючи хмарні технології, можна легко докупити додаткове місце для зберігання даних для кожної поштової адреси.

Швидка і ефективна технічна підтримка, яка переважно працює цілодобово, в разі виникнення проблем дозволяє організації залишити заявку на вирішення несправності в будь-який час. Популярні компанії, що надають послуги з оренди хмарних сервісів електронної пошти наймають найкращих технічних спеціалістів, та постійно працюють над їх навчанням, це майже на 100% гарантує швидке вирішення проблем, та збереження даних компаній.

Ціна таких послуг досить доступна, що дає змогу навіть організаціям з невеликим бюджетом користуватись першокласним сервісом корпоративної пошти, що є економічно ефективним рішенням.

Безпека корпоративної пошти, що знаходиться на орендованому сервері організована за загальноприйнятими стандартами, та з урахування тенденцій розвитку індустрії інформаційної безпеки. Це забезпечує нормальний рівень захисту для корпоративних даних організації.

Наявність багатьох хостинг-провайдерів електронної корпоративної пошти дозволяє організації обрати такий сервіс, що підходить саме до їх вимог.

Наприклад для компанії, що користується ПЗ від Microsoft Office ідеально підійде Microsoft 365. Він забезпечує всі необхідні функції для корпоративної пошти: надсилання та отримання електронних листів, можливість отримання власної доменної адреси, захист від спаму та запобігання втраті даних. Також

використання корпоративної пошти від Microsoft дає доступ до багатьох інших інструментів.

Якщо організація віддає перевагу зберіганню інформації в хмарі, то Google Workspace стане чудовим вибором. Додатково до сервісу корпоративної пошти, надається доступ до інструментів Google, включаючи Chat для миттєвого обміну повідомленнями, Meet для голосових чи відеоконференцій, та веб-додатки для редагування документів.

При наявності особливих вимог, та бажання персоналізованого налаштування кожної поштової скриньки можна обрати IceWarp. Цей сервіс дає змогу налаштувати виділення пам'яті для кожного працівника.

Для організації, що потребує особливої конфіденційності, то варто звернути увагу на корпоративну пошту від Fastmail.

1.2.3 Узагальнена оцінка використання власної корпоративної пошти

Використання власної доменної адреси організації забезпечує максимальний контроль над своєю поштою. Компанія може вільно вводити власні політики, правила, обмеження та умови щодо використання власної пошти, включаючи політику безпеки, розмір поштової скриньки тощо. Це дозволяє підтримувати власну стандартизацію та єдність у внутрішній комунікації. При використанні стандартизованого способу створення логіну користувача, кожен співробітник отримає персоналізовану адресу, а іншим співробітникам буде достатньо знати ім'я людини, якій вони хочуть надіслати листа. Наприклад пошта користувача Іванов Станіслав Сергійович, буде виглядати як «ivanov_s_s@company.com». Проте це несе й певні ризики, знаючи принципи за якими створюється логін користувача електронної пошти, зловмиснику буде простіше його підробити.

Використання власний домен в поштовій адресі підкреслює серйозність та професійність організації перед співробітниками, клієнтами та партнерами.

Безпека та захист конфіденційної інформації – одна з найголовніших особливостей корпоративної пошти. Наявність власної пошти дає змогу організації самостійно забезпечити конфіденційність і цілісність даних, а також захист від несанкціонованого доступу з використанням власних підходів та політик до забезпечення інформації.

Найпоширенішим методом захисту є шифрування повідомлень. Шляхом шифрування початковий текст повідомлення перетворюється на шифротекст, який зможе прочитати лише адресат повідомлення, який володіє відповідними ключами для розшифрування. Цей метод захисту забезпечує конфіденційність інформації під час її транзиту через мережу.

Наступні за поширенням методи захисту - 2FA (двофакторна автентифікація) та обмеження використання слабких паролів. 2FA значно підвищує рівень безпеки, тому що в разі її використання, користувачу крім паролю потрібно буде вводити одноразовий код отриманий, наприклад, через SMS. Таким чином забезпечується контроль доступу до поштових скриньок і зводиться до мінімум можливість несанкціонованого доступу в корпоративну мережу. Це є особливо важливим для корпорацій, з різними рівнями повноважень працівників та доступу до інформації.

Загальна безпека корпоративної пошти також залежить від власного захисту самого поштового сервера та інфраструктури. Тому організації використовують механізми захисту від проникнення, та системи моніторингу проникнень, для запобігання несанкціонованому доступу до інформації.

Отже забезпечення безпеки корпоративної пошти є важливим завданням для організацій, особливо для тих, що використовують в своїй роботі інформацію з обмеженим доступом. Саме механізми власної корпоративної пошти дозволяють організації контролювати всі механізми забезпечення безпеки інформації на найнижчому рівні.

1.3 Аналіз методів реалізації фішингових атаки на корпоративну пошту

Фішинг — це кіберзлочин, у якому особа або цільові особи зв'язуються електронною поштою, телефоном або текстовими повідомленнями з метою спонукати людей надати конфіденційні дані, як-от особисту інформацію, дані банківських і кредитних карток, а також паролі.[11]

Фішер – зловмисник, що користується інструментами фішингу, та спеціалізується на кіберзлочинах з їх використанням. Задача фішера полягає у введені жертви в оману з метою збору персональної інформації про неї, отриманням несанкціонованого доступу до інформації з обмеженим доступом чи порушення її цілісності.

Основна мета фішингу полягає в тому, щоб змусити жертву розкрити свої особисті дані. Існує декілька видів фішингу, основні з яких:

- Сайт-підробка;
- SMS фішинг;
- Вішинг (Vishing);
- Фішинг з використанням електронної пошти.

Другий за популярністю метод фішингу. Головною його особливістю є підроблений веб-сайт відомої компанії, що є головним інструментом шахрайства. Головною задачею зловмисників, що використовують цей метод фішингу є дуже детальне відтворення сайту відомих компаній, соціальних мереж, банків тощо. Використовуючи це метод, шахраї мають на меті досягнути максимальної віддачі, та отримати максимальну можливу кількість жертв для подальшого використання або продажу їх персональних даних. Наступним кроком є просування підробленого сайту та пошук потенційних жертв, для цього найчастіше використовують рекламні інструменти, та інструменти SEO оптимізації. SEO оптимізація – вдосконалення сайту, для його просування у видачі пошукових систем. Гарно оптимізований сайт завжди буде на перших місцях при пошуку, що сильно збільшує кількість потенційних жертв, які за власним бажанням відвідають сайт-підробку.

SMS фішинг, або Смішинг – метод фішингу основним інструментом якого є SMS повідомлення. Цей метод фішингу є одним з найпростіших з технічної

точки зору, тому що не потребує гарних технічних навичок, вміння розробки сайтів чи їх просування. В той же час зловмисник має вміти зацікавити жертву досить коротким повідомленням, викликати довіру та спровокувати до наступних дій. Основною задачею шахрая є проведення дуже ретельного аналізу потенційної жертви, скласти її психологічний портрет, та сформувати важелі психологічного впливу. Ціль повідомлення перевести жертву у додаток, або веб-сайт, що буде збирати її персональні дані. Найвідоміший хрестоматійний приклад використання цього методу фішингу, це розсилка повідомлень, про виграш цінного призу в лотереї, які були поширеними декілька років тому, при переході по посиланню з повідомлення, людину повідомляли про необхідність сплати комісії перед отриманням виграшу, або повністю ввести дані банківської картки, для отримання призу.

Вішинг (Vishing) або Voice Phishing – метод фішингу основним інструментом якого є телефонні дзвінки. Цей метод, як і SMS фішинг не потребує особливих технічних навичок, проте його не можна назвати простим. Найголовніша його складність полягає в необхідності володіння зловмисником навичок ораторської майстерності, здатності до швидкого аналізу певної жертви в режимі реального часу, вміння швидко знаходити слабкі місця, та важелі впливу на конкретну людину. Цей метод використовується як для збирання персональних даних звичайних людей, переважно це дані банківських карток, так і для проникнення в більш захищенні корпоративні мережі. Особливістю цього виду фішингу є час для прийняття рішення жертвою, який сильно обмежений, через те, що професійний зловмисник майстерно її опрацьовує і нав'язує потрібні жертві думки. Цей метод фішингу успішно застосовував на практиці і згодом детально описував колишній хакер, а нині консультант з інформаційної безпеки, та письменник Кевін Митник, в своїй книзі під назвою «Ghost in the Wires: My Adventures as the World's Most Wanted Hacker»[10].

Фішинг з використанням пошти (Email Phishing) найпоширеніший вид фішингу, при якому зловмисники розсилають підроблені електронні листи, видаючи себе за представників відомих організацій або осіб. Листи можуть

містити привабливі повідомлення, заклики, в яких просять відкрити файли, відправити файли, перейти за посиланням на підроблений веб-сайт, де жертва повинна ввести свої особисті дані. На відміну від інших способів фішингу, цей спосіб в першу чергу орієнтується на організації. Дуже часто цей спосіб фішингу використовують в якості початкового етапу, для проникнення в мережу компанії, при проведенні комплексних атак. Враховуючи ці особливості, а також цільових жертв, можна прийти до висновку, що саме цей метод фішингу приносить найбільші збитки і робить це серйозною потенційною проблемою для всіх організацій. Цей метод фішингу дуже розвинений. У потенційного зловмисника є багато простору для творчості і створення унікального листа, а також досить чітке розуміння психологічного портрету жертви. До того ж легко створити класифікацію жертв, відповідно до займаних посад, а адресу електронної пошти часто можна легко знайти на сайті компанії. Тому сучасні організації повинні бути зацікавлені в забезпеченні безпеки своїх корпоративних мереж від цього виду фішингу як ніхто інший, і приділяти цій проблемі достатню кількість уваги.

1.3.1 Оцінка наслідків фішингу для організації

Загроза фішингу є дуже потужним викликом для співробітників організації, що забезпечують безпеку інформації. Це серйозна загроза безпеці корпоративних даних. Як правило, зловмисники використовують фішингові атаки для отримання несанкціонованого доступу до інформації з обмеженим доступом, такої як корпоративні дані, персональні дані працівників, паролі, фінансова інформація. Викрадення, пошкодження, або публікація цих даних може призвести до репутаційних та фінансових втрат. Та призвести до значних фінансових та правових наслідків.

Успішна фішингова атака може призвести до втрати конфіденційної інформації, яка є важливої для організації. Наприклад до внутрішньої пошти, інформації про клієнтів чи фінансової системи. Це може призвести до втрати

важливих договорів чи порушення законодавства. Все це приведе за собою серйозні фінансові збитки, втрати довіри клієнтів та судових позовів.

Фішингові атаки можуть призвести до порушення безпеки мережі та інфраструктури організації. Зловмисники можу використовувати фішинг для проникнення в мережу організації, розповсюдження шкідливого ПЗ, такого як віруси, трояни, шпигунське ПЗ. Це може призвести до порушення працездатності та збоїв інформаційних систем, втрати даних, компрометації мережевої інфраструктури, або втрати контролю над мережею. Порушення безпеки мережі може мати серйозні наслідки для організації, включаючи втрату продуктивності, недоступність послуг для користувачів, та затрати на відновлення ІС.

Також фішингові атаки можуть порушити відпрацьовані бізнес-процеси. Наприклад фішингова атака може скомпрометувати доступ до облікових записів співробітників, що призведе до втрати даних або порушення робочих процесів. Це може призвести до зниження продуктивності організації, та збільшення часу на відновлення працездатності ІС.

Одним з найсерйозніших наслідків фішингових атак можуть стати репутаційні втрати. У разі успішної атаки, яка призведе до втрати конфіденційних даних користувачів організація може втратити довіру клієнтів, користувачів чи загалом громадськості. Репутаційні втрати мають довготривалі наслідки, їх відновлення потребує багато часу та ресурсів.

1.3.2 Дослідження типових методів фішингових атак на корпоративну пошту

Для розуміння і розробки алгоритму протидії фішинговим атакам на корпоративну пошту, важливо проаналізувати існуючі методи цих атак, та поділити їх за спільними ознаками. З типових методів фішингу можна виділити наступні:

- Підробка керівника (CEO Fraud)
- Маніпуляція посиланнями (Link Manipulation)

- Підробка веб-сайту (Fake Website)
- Ін'єкція вмісту (Content Injection)
- Людина посередині (Man-In-The-Middle)
- Розповсюдження шкідливого ПЗ
- Недобросовісна реклама (Malvertising)

Підробка керівника. Для реалізації цього методу фішингу зловмисники використовують адресу електронної пошти, відому співробітникам як пошта їх керівника. Як правило електронний лист містить термінове прохання до жертви переслати або відкрити якісь файли, надати конфіденційну інформацію чи встановити якусь програму на свій ПК. Для створення такої пошти зловмисники використовують схожу доменну адресу, на доменну адресу компанії, на яку проводять атаку, найчастіше просто змінюють один символ, на схожу цифру, або іншу літеру. Якщо співробітник компанії не уважний, то атака з великою ймовірністю буде успішною, тому що досить часто працівники не можуть відмовити керівнику в проханні через страх втратити свою посаду або взагалі роботу.

Маніпуляція посиланнями (Link Manipulation) – форма фішингу, принцип роботи якої полягає в створенні такого зловмисного посилання, ніби воно відноситься до ресурсу організації жертви. Фішери часто використовують URL-адреси та субдомени з орфографічними помилками. Іноді зловмисники змінюють текст, який відображається для посилання, щоб він виглядав наче справжнє посилання, але насправді перенаправляв на підроблений веб-сайт. Хоч і більшість застосунків дозволяє попередній перегляд посилання при наведенні на них курсором, але потенційна жертва може не звернути на це увагу. Також при використанні смартфону далеко не завжди є можливість попереднього перегляду.

Підроблення веб-сайту (Fake Website) найчастіше використовується у парі з маніпуляцією посиланнями, проте він може бути і цілком самостійним. Шахрайський веб-сайт створюється таким чином, щоб він максимально детально повторював сторінку сайту певної організації. Брендинг, логотипи, вміст сторінки – все це повинно бути в точності таким, як на оригінальному сайті, за

умови повної відповідності оригінальному сайту, жертва навіть не здогадається, що варто перевірити його справжність. Найпопулярнішими цілями для відтворення є сторінки авторизації чи надсилання форми (наприклад дані банківської карти чи персональні дані). Зазвичай атаки з використанням цього методу фішингу супроводжуються листами з терміновим проханням чи вимогою перейти на сайт, текст листа часто намагається викликати тривогу у жертви, щоб приспати пильність.

Ін'єкція вмісту (Content Injection) – складний метод фішингу, для реалізація якого фішер шукає вразливості у надійному веб-сайті та завдяки ним замінює частину вмісту сторінки. Це робиться для того, щоб перевести користувача з довіреної сторінки на сторінку для вводу персональних даних. Наприклад фішер може знайти вразливість на веб-сайті, що публікує новини, та підробити статтю, ніби якась організація через фінансові труднощі оголосила про план по звільненню частини співробітників. Для перегляду списку співробітників, що потраплять під звільнення необхідно авторизуватись через корпоративний аккаунт цієї організації. Після чого листи з посиланням на цю статтю розсилаються на корпоративну пошту співробітникам організації, а вони в свою чергу відправляють дані облікових записів зловмиснику.

Людина посередині (Man-In-The-Middle) – поширена атака, що скоріше відноситься до активного прослуховування, та перехоплення повідомлень. Її ключовою особливістю є те, що зловмисник знаходиться між двома людьми, що спілкуються між собою і не підозрюють про наявність зловмисника. Проте у фішингових атаках також користуються цією особливістю. Зловмисник може почати звичайне листування з жертвами від імені один одного, просто копіюючи листи. Таким чином жертви навіть не підозрюватимуть, що їх листи буде переглядати третя особа, та обмінюватись інформацією з обмеженим доступом.

Розповсюдження шкідливого ПЗ з використанням корпоративної пошти – метод фішингу, при використанні якого зловмисник розсилає на корпоративну пошту листи, що містять документи чи фотографії з вбудованим в них шкідливим ПЗ. Для заохочення жертви до відкриття листа часто використовують

привабливі назви, наприклад: «Список працівників на підвищення», «Наказ про підвищення заробітної плати», «Умови отримання додаткової премії» та інші. Або ж навпаки, назви що викликають тривоги, чи термінові прохання перевірити чи відкривається файл.

Метод фішингу в використанням недобросовісної реклами полягає в тому, що фішер створює рекламні оголошення з привабливими картинками та текстами, та розповсюджує їх. Рекламні банери можуть розміщатись на різних веб-ресурсах чи присилатись прямо на пошту. Також зловмисник може створити власний сайт, розміщувати на ньому корисну інформацію та додатково вбудувати недобросовісну рекламу. Посилання на цей сайт розповсюджується серед працівників організації під прикриттям ознайомлення з інформацією, проте частина людей може зацікавитись недобросовісною рекламою та перейти по ній.

Варто розуміти, що дуже фішери не обмежуються лише одним методом фішингу. Найкращий результат дає саме їх комбінування та комплексне застосування, таким чином часто поєднують метод підробки веб-сайту з маніпуляцією посилання, додаткового до цього можуть скористатися підробкою керівника. Атаку з використанням методу «Людина посередині» об'єднати з розповсюдженням шкідливого ПЗ. Таким чином можна створити безліч подібних комбінацій в залежності від вмінь зловмисника, що сильно ускладнює процес виявлення фішингу в корпоративній пошті з боку звичайного працівника і автоматизованих систем з протидії фішингу.

1.4 Постановка задачі

Результати актуальних досліджень фішингу в корпоративній пошті показали, що кількість подібних інцидентів з роками лише збільшується, також збільшуються збитки компаній в результаті успішних атак. Також варто виділити що фішинг корпоративної пошти організацій посідає перше місце за:

- середньою сумою збитків на організацію в разі однієї успішної атаки;
- частотою проведення фішингових атак відносно інших видів атак;

- кількістю втрачених даних організаціями;
- серед типів атак, що використовують організовані злочинні групи для проникнення в систему організації.

У зв'язку з цим, розробка рекомендацій щодо застосування методів протидії фішингу в корпоративній пошті набуває особливої актуальності в наш час.

Отже для виконання кваліфікаційної роботи необхідно:

- проаналізувати існуючі методи та рішення для протидії фішингу в корпоративній пошті;
- визначити особливості організацій, та потрібний їм рівень захисту від фішингових атак;
- розробити рекомендації щодо застосування методів протидії фішингу, враховуючи особливі потреби різних організацій.

1.5 Висновки

В результаті роботи над першим розділом було:

- проведено аналіз актуальності питання;
- визначено поняття корпоративної пошти, актуальність та переваги її використання, а також різні архітектури КП;
- визначення можливих наслідків фішингу корпоративної пошти для організацій;
- розглянуто існуючі методи фішингових атак на корпоративні пошти, їх особливості та сфери застосування;
- була виконана постановка задачі на спеціальну частину.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз методів протидії фішингу в корпоративній пошті

Враховуючи популярність фішингових атак та тенденції їх розвитку, ця проблема стає все більш серйозним викликом для фахівців з кібербезпеки. Тож не дивно що індустрія методів захисту від атак цього типу не стоїть на місці та постійно розвивається. Кожного року впроваджуються нові стандарти та політики захисту, розробляється ПЗ для протидії фішингу та програми по навчанню персоналу. Отже тепер потрібно більш детально розібрати існуючі методи протидії фішингу в корпоративній пошті.

2.1.1 Оцінка антивірусних засобів для протидії фішингу

Одним з ключових інструментів для захисту від кібератак в цілому і від фішингу зокрема є встановлення антивірусного ПЗ. Не дивлячись на те, що дане ПЗ є передостанньою лінією захисту, варто приділяти достатньо уваги для його вибору, встановлення та налаштування. Саме антивірус може вберегти від переходу на шкідливий сайт чи відкриття зараженого файлу в тому разі, якщо жертва повелась на фішинговий електронний лист. Варто зазначити, що для підтримки ефективності антивірусного ПЗ важливо регулярно слідкувати та встановлювати його оновлення. Також важливо пам’ятати, що жоден антивірус не дає 100% гарантій успішного захисту проти фішингових атак, тому не варто розглядати цей метод захисту як самостійний.

Популярним рішенням є антивірус з відкритим кодом ClamAV. Головна його мета – інтеграція із серверами електронної пошти для перевірки файлів прикріплених до повідомлень. Великою перевагою використання саме цього антивірусу є його постійні оновлення баз даних сигнатур, іноді оновлення відбуваються по декілька разів на день, це забезпечує гарний захист навіть від нових загроз. Завдяки чудовій оптимізації, даний антивірус дуже швидко

проводить сканування файлів та не навантажує сильно систему. Ще з переваг варто відзначити безкоштовність даного ПЗ, та простоту у встановленні, таким чином можна дуже легко значно підвищити безпеку власного поштового сервісу.

Антивірус від ESET також включає антифішингові рішення. Він включає наступні методи виявлення фішингових атак:

- власну антифішингову базу даних;
- інструменти порівняння URL-адрес веб-сайтів;
- аналіз поведінки фішингових сайтів.

Власна антифішингова база даних дає змогу оперативно протидіяти виникаючим загрозам. Відразу після виявлення нової загрози, вона додається до бази даних та попадає в список блокування антивірусом. Ключовим параметром ефективності цього методу виявлення фішингових атак є частота оновлення бази даних.

Інструменти порівняння URL-адрес веб-сайтів дає змогу виявляти вже відомі фішингові сайти та блокувати до них доступ. Аналіз поведінки фішингових сайтів дозволяє виявляти нові загрози на основі їх зловмисної поведінки. Це призводить до їх автоматичного блокування, та досить високої ефективності проти нових загроз, що працюють використовуючи стандартні шаблони поведінки.

Популярним серед організацій є антивірус BitDefender, за результатами тестування антифішингових функцій від компанії AV-Comparatives він отримав оцінку 96% ефективності[12]. Для протидії фішингу BitDefender використовує власний захищений браузер, створений для забезпечення конфіденційності і безпеки онлайн-банкінгів, електронних покупок та інших типів онлайн-транзакцій.

Найпопулярнішим антивірусом є Windows Defender, головна причина його успіху – використання в якості вбудованого антивірусу Windows. Особливістю цього антивіруса є широка можливість налаштувань, можна повністю створювати та налаштовувати власні політики захисту від фішингу. Можна налаштувати рівень перевірки від стандартного до найбільш агресивного.

2.1.2 Аналіз системи фільтрації спаму та фішингу

Враховуючи те, що більшість фішингових атак починаються саме з електронної пошти, не дивно що системи фільтрації спаму та фішингу відіграють важливу роль в протидії атакам цих типів. При правильному налаштуванні саме фільтр має відбивати найбільшу кількість атак, та не допускати їх до працівників.

Сучасні системи фільтрації пошти використовують багаторівневий підхід, що забезпечує гарну ефективність роботи та оптимізацію процесів. Якщо фішинговий лист зміг пройти попередній рівень фільтрації, то він потрапляє на більш суворий. Таким чином до поштової скриньки користувача потрапляє лише невелика частина з усіх листів. Схематично принцип роботи багаторівневої системи фільтрації спаму зображено на рис. 2.1.

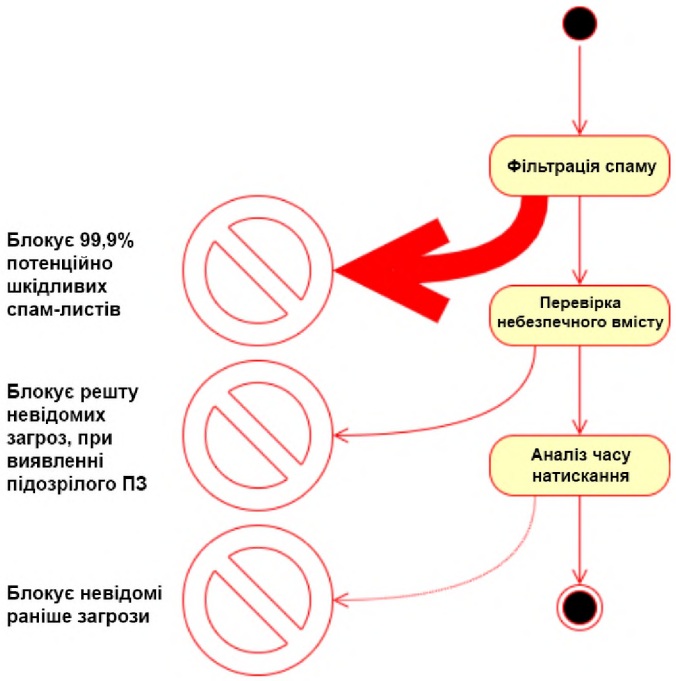

Рисунок 2.1 – Схема роботи багаторівневого спам-фільтру

Системи фільтрації зазвичай встановлюються на рівні поштового сервера або веб-додатку електронної пошти. Вони автоматично перевіряють листи на

наявність ознак спаму та фішингу і при необхідності блокують ці листи чи відправляють їх на карантин до спеціальних папок.

Системи фільтрації використовують різні методи та технології для виявлення спаму та фішингу. Це можуть бути спеціальні алгоритми, евристчні аналізатори, перевірка за чорним списком IP-адрес, аналіз ключових слів тощо.

До переваг використання систем фільтрації можна віднести:

- ефективне виявлення спаму та фішингових листів, що призводить до значного зниження кількості небажаних листів у поштовій скриньці користувачів;
- більшість таких систем працює в режимі реального часу, це означає що потенційно небезпечний лист не буде зберігатись в скриньці і очікувати моменту перевірки, при правильній роботі фільтру цей лист навіть не дійде до скриньки;
- широкі можливості для налаштувань дозволяють кожній організації налаштувати спам-фільтр відповідно до своїх вимог та особливостей.

Проте системи фільтрації мають і певні недоліки, які важливо враховувати при їх використанні. В першу чергу до цих недоліків відносяться:

- іноді системи фільтрації можуть помилково сприймати легітимні листи як спам або фішинг та блокувати їх, що, в свою чергу, може призвести до втрати важливої інформації або комунікаційних перешкод для користувачів;
- зловмисники постійно адаптуються до захисних методів та навчаються обходити системи фільтрації, через це вони не завжди можуть забезпечувати надійний рівень захисту.

Всі ці недоліки можна обійти, якщо вчасно оновлювати відповідне ПЗ для роботи системи фільтрації, та слідкувати за актуальністю встановлених налаштувань.

З існуючих фільтрів можна виділити наступні:

- SpamAssasin;

- Microsoft Exchange Online Protection;
- Google Mail Anti-Phishing

SpamAssasin – це платформа для захисту від спаму з відкритим кодом, яка надає системним адміністраторам фільтр для класифікації електронної пошти та блокування спаму (небажаної масової електронної пошти). Це ПЗ має багато плагінів для інтеграції широкого спектру розширених евристичних і статистичних тестів аналізу заголовків та основного тексту листів, включаючи аналіз тексту, та списки блокування DNS і бази даних спільної фільтрації.

Microsoft Exchange Online Protection – сервіс фільтрації спаму та фішингу, який надається Microsoft для користувачів їхнього сервісу корпоративної пошти. Він використовує багато методів для виявлення й блокування небажаних повідомлень.

Google Mail Anti-Phishing – фільтр що в своїй роботі використовує поштовий сервіс від Google. Особливістю цього фільтру є використання технологій ШІ та машинного навчання в своїй роботі.

2.1.3 Пропозиції щодо застосування стійкої до фішингу багатофакторної автентифікації

Використання стійкої до фішингу MFA – це один з видів багатофакторної автентифікації, його особливість полягає в тому, що він забезпечує захист від спроб злому процесу автентифікації з використанням методів фішингу. Стійкість до фішингу досягається тим, що кожна сторона не лише повинна надати підтвердження особи, але й тим, що вона має намір діяти цілеспрямовано. Паролі, коди активації через SMS, одноразові паролі не вважаються механізмами протидії фішингу. Це пов'язано з тим, що всі ці інструменти можуть додати роботи фішеру, проте їх все ще можуть викрасти під час атаки. Стійка до фішингу MFA заснована на криптографії та, вона виключає використання спільних кодів доступу і в результаті зменшує здатність зловмисників перехоплювати та відтворювати їх. Стратегія OMB M-22-09 Zero Trust від Білого

дому конкретно описує дві технології, стійкі до фішингу: стандарт FIDO2 WebAuthn і смарт-картки PIV[9].

Смарт-картки PIV використовують криптографію на основі інфраструктури відкритих ключів (Public Key Infrastructure). Ця ж технологія використовується для банківських карток, електронних паспортів і систем контролю доступу. Приклад вигляду смарт-картки PIV приведений на рис. 2.2.

Рисунок 2.2 – Зовнішній вигляд смарт-картки PIV

WebAuthn & FIDO забезпечує новітній захист від фішингу. Він є похідним від протоколу U2F (Universal 2nd Factor), що був розроблений компанією FIDO Alliance для підтримки онлайн-автентифікації без будь-яких спільних секретів. З

часом протокол U2F удосконалювали і в результатів він перетворився на FIDO2, глобальний стандарт автентифікації, який навіть включає безпарольний MFA. FIFO2 складається з двох галузевих стандартів, а саме WebAuthn та CTAP2, які працюють узгоджено. WebAuthn дозволяє онлайн сервісам використовувати автентифікацію FIDO через стандартний веб-API, а CTAP2 – це протокол прикладного рівня, який використовується для зв'язку між системою та зовнішнім автентифікатором. Схема роботи протоколу FIDO2 зображена на рис. 2.3.

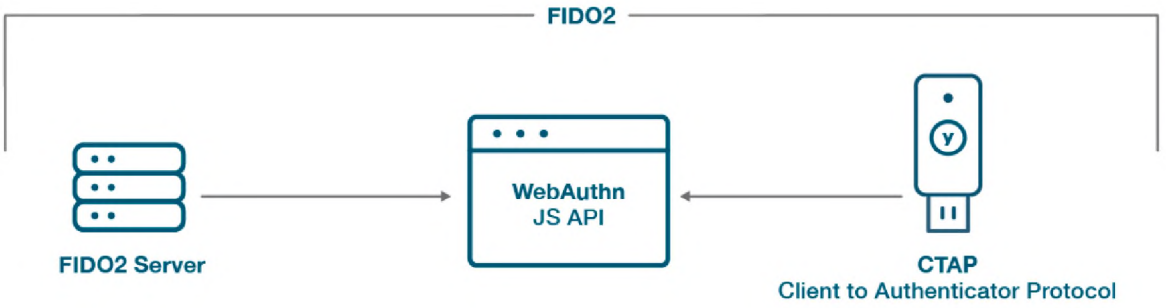

Рисунок 2.3 – Схема роботи протоколу FIDO2

Автентифікація, звітування та відповідність повідомлень на основі домену (DMARC) – протокол автентифікації електронної пошти, призначений для захисту організацій від фішингових атак і спуфінгу електронної пошти. Він дозволяє власнику домену публікувати політику в DNS-записах свого домену, вказуючи які поштові сервери мають право надсилати електронні листи від імені домену, а також дії, які приймають поштові сервери, якщо повідомлення не проходить оцінку DMARC. DMARC використовує два інші протоколи автетифкації електронної пошти, а саме SPF (Sender Policy Framework) та DKIM (DomainKeys Identified Mail). В разі, якщо повідомлення не проходить перевірку протоколом, то його можна розглядати як спам та відхилити, або перемістити на карантин. Для застосування цього протоколу, власник домену повинен створити запис DMARC у своєму DNS, який містить інформацію про політику електронної пошти власника домену та інструкції щодо надсилання звітів DMARC.

2.1.4 Аналіз програм з підвищення обізнаності працівників

З попереднього розділу зрозуміло, що фундаментальною особливістю фішингу є соціальна інженерія. Тобто головною вразливістю для атак цього типу є саме людина. Нажаль неможливо запрограмувати людину на виявлення фішингових листів, через це організації повинні проводити постійні навчання своїх працівників, для підвищення їх обізнаності в цій сфері і усвідомлення правильного алгоритму дій в разі виявлення підозрілого листа. Базова інформація про фішинг, якою повинні володіти працівники включає:

- загальні знаки фішингового листа. Наприклад теми що найчастіше використовуються, термінове прохання, підозрілі адреси відправників і запити надання інформації з обмеженим доступом;
- безпечні методи взаємодії з фішинговим листом. Важливо навчити працівників не натискати на посилання та вкладення, перевіряти справжність електронних листів, перш ніж виконувати якісь дії;
- повідомлення про підозрілі листи. Організація має заохочувати своїх працівників виявляти фішингові листи, та повідомляти про них відділ, що займається питаннями інформаційної безпеки.

Для підвищення ефективності навчання і закріплення отриманих навичок, варто регулярно проводити імітацію фішингових атак, та вимірювання рівня їх успішності. Ці тести можна проводити різними способами, зокрема надсиланням імітаційних фішингових листів на корпоративну пошту працівникам, та відслідковувати хто з них став жертвою. Висновки зроблені в результаті цих досліджень можуть бути використані для покращення роботи організації щодо виявлення фішингу:

- виявивши найбільш вразливих до фішингу працівників, компанія може переглянути свої підходи до навчання або ж провести додаткове навчання найвразливіших людей;
- отримані результати дозволяють оцінити ефективність впроваджених засобів безпеки, методів захисту від фішингу та технологій фільтрації від спаму;
- проводження регулярної імітації фішингових атак дозволить тримати працівників в тонусі, мотивувати їх частіше звертати увагу на підозрілі листи та відмічати їх, як потенційно небезпечні.

Для підготовки працівників можна обрати вже готові програми від передових компаній в сфері захисту інформації. Деякі з них пропонують просто базову теоретичну підготовку, якісь надають доступ до тренажерів, а якісь надають повноцінні інструменти для перевірки ефективності навчання. З найвідоміших програм підготовки працівників для протидії фішингу варто виділити наступні:

- ESET Cybersecurity Awareness Training;
- Hook Security PsySec Security Awareness Training;
- Phished;
- SafeTitan;
- Ironscales;
- Infosec IQ;

ESET Cybersecurity Awareness Training – програма з навчання працівників, що розроблена одним з найбільших постачальником послуг в сфері кібербезпеки. До неї входить як теоретична підготовка, так і повноцінні інструменти для практичної підготовки і перевірки результатів навчання, шляхом проведення симуляції фішингових атак, шаблони яких є в бібліотеці, або створені з нуля. Інструменти ESET мають широкий вибір налаштувань, можна групувати окремих користувачів, та цілі відділи для роботи з ними. Ця програма ідеально підходить для швидкого, але інформативного навчання.

Навчальна програма від Hook PsySec також має комплесний підхід і охоплює не лише фішинг, а й інші теми інформаційної безпеки, які повинні розуміти працівники. Навчальний контент поділяється на дві програми, початковий рівень, та заглиблений, відрізняються вони періодичністю проведення занять. Навчання початкового рівня проводяться щорічно, а заглибленого – раз на місяць. Підготовка від Hook включає тестування співробітників за допомогою симуляції фішингу, якщо співробітники реагують неправильно, то їм пояснюється яку саме помилку вони допустили.

Phished – це повноцінний навчальний заклад з питань безпеки, він навчає користувачів точно ідентифікувати потенційно загрозливі листи та повідомляти про них. Його підхід будується на чотирьох ключових принципах: підвищення обізнаності, моделювання фішингових атак, активне звітування та розвідка загроз. Метою використання цих принципів є перетворення людей на «живий брандмауер», який здатний вистояти проти атак соціальною інженерією. Для кожного учня автоматично створюються персоналізовані фішингові листи, щоб перевірити реакцію на загрози і пояснити правильний порядок дій в разі, якщо працівник потрапив на підроблений сайт. В поштовий клієнт інтегрується червона кнопка, для повідомлення про фішинг.

SafeTitan – навчальна платформа, що спеціалізується на знаннях з інформаційної безпеки, розроблена для того, щоб допомогти організаціям надати своїм працівникам ефективне навчання з кібербезпеки. Інструменти SafeTitan дозволяють ефективно виміряти ефективність навчання. Вони включають теоретичну підготовку і симуляцію фішингових атак, які можуть налаштовувати адміністратори. Проходження кожного курсу займає 8-10 хвилин. SafeTitan проводить втручання в режимі реального часу, та попереджає користувачів про ризиковану поведінку. На основі отриманої інформації, працівникам компанії рекомендуються навчальні матеріали, адаптовані до конкретно їхніх дій. SafeTitan легко інтегрувати в організацію завдяки інтеграції з Microsoft 365, Google Workspace та іншими компаніями, що надають послуги з оренди сервісів корпоративної пошти.

Ironscales – нова компанія, що займається безпекою електронної пошти. В свої програмах навчання вони активно використовують технології штучного інтелекту і машинне навчання для протидії фішинговим атакам. Їхні рішення включають інтегровану систему симуляції фішингових атак та тренінги з питань безпеки, щоб навчити працівників виявляти то відмічати потенційно шкідливі листи. Їх підхід дозволяє легко надсилати відеоролики з певними темами саме тим людям, які їх потребують.

Infosec IQ – постачальник інформації про інформаційну безпеку. Вони забезпечують професійне навчання та сертифікацію працівників. Програма навчання розрахована на 12 місяців. За допомогою технологій Infosec IQ організації можуть створювали власні фішингові кампанії або обрати їх з великої бібліотеки шаблонів, щоб зробити працівників більш стійкими до найсерйозніших загроз. Програма від цієї компанії постійно покращується та адаптується до нових загроз.

2.1.5 Оцінка методів з використанням штучного інтелекту

Останнім часом системи ШІ зробили відчутний технологічний стрибок, тож не дивно, що організації почали їх використовувати для виявлення фішингових атак і протидії їм. Цей спосіб працює на основі алгоритму та зосереджується на розумінні, а також на розпізнаванні шаблонів із величезних куп даних для створення системи, що може виявляти незвичайно поведінку та аномалії. З часом модель штучного інтелекту розвивається, починає розуміти особливості кожної організації, та виробляє особливий підхід до фільтрації листів, на основі даних отриманих під час аналізу моделей нормальної поведінки. Функції штучного інтелекту дозволяють ідентифікувати фішингові листи, спам, поширення шкідливого ПЗ, а також витік корпоративних даних.

Для розуміння принципу роботи систем ШІ для протидії фішингу, потрібно розібрати якими саме способами він виявляє фішингові листи.

Успішна система на штучному інтелекті та машинному навчанні – система що повністю перевіряє лист на аномалії та попереджувальні сигнали про фішинг, починаючи від метаданих, до вмісту повідомлення. Це включає сповіщення на основі поведінки електронної пошти та може виявити підробленого відправника, або перевірка мети повідомлення, то сповіщення користувача в разі використання підозрілих термінових тем. Зазвичай при читанні фішингового листа виникає нав'язане відчуття терміновості, якщо в тексті містяться слова, що вимагають швидкої дії, то система система зробить попередження про небезпеку. Проте особливою рисою ШІ є те, що вони більш детально аналізують листа, наприклад якщо в тексті буде йти мова про термінову знижку, то система перемістить це до папки спами, а якщо прохання терміново скинути гроші, то лист буде помічений як фішинговий.

ШІ має змогу аналізувати контекст повідомлень, що робить його найбільш ефективним автоматизованим методом протидії фішингу. Завдяки цьому лист аналізується повністю, а не просто порівнюється з наявними шаблонами. Цей інструмент буде аналізувати чи була попередня історія листування користувачів, зв'язок між темою листа та його вмістом і даними, що просять надати в листі.

Вміння аналізувати манеру спілкування користувачів дає змогу системі ШІ з великою ймовірністю встановити особу відправника. В разі якщо зловмисники отримали доступ до облікового запису одного зі співробітників та пишуть листи від його імені, штучний інтелект може помітити зміну стилю спілкування та попередити про це службу безпеки організації.

Одним з відомих інструментів для протидії фішинговим атакам на базі ШІ є ПЗ Egress Defend. Воно поєднує інтелектуальні технології для захисту організації від складних фішингових атак і попереджає та залучає користувачів за допомогою контекстних кольорових попереджувальних банерів. Це ПЗ використовує технології машинного навчання, соціальний граф і методи обробки природної мови, спільна робота яких дозволяє виявляти складні загрози, що оминули існуючі попередні методи захисту.

2.2 Аналіз комплексних рішень для протидії фішингу в корпоративній пошті

Враховуючи актуальність розробки антифішингового ПЗ, не дивно що в індустрії з'явились передові компанії які надають послуги зі встановлення повноцінного комплексу програм та впровадження політик, що підвищують стійкість організації до фішингових атак.

Головною перевагою комплексного антифішингового ПЗ є простота в його установці та налаштуванні. Як правило ці рішення включають повний пакет необхідних програм та політик, після установки і впровадження яких, організація значно підвищить свій рівень захисту. При виборі комплексного рішення, організація зберігає велику кількість часу, яку б могла витратити на пошук потрібного інструменту для одного рівня захисту. Наприклад потрібно було б знайти спам-фільтр, антивірус для перевірки файлів, антивірус для перевірки посилань та інструмент, що дозволить налаштувати правила фільтрації листів, а після вибору ще потрібно налаштувати їх так, щоб вони правильно працювали один з одним.

Саме тому передове комплексне рішення повинно містити в собі всі компоненти, що перераховані в минулому розділі, або більшу частину з них. Для забезпечення найкращого результату, варто розглядати компанії, які додатково до технічних рішень надають програми з навчання працівників для протидії фішинговим атакам.

З популярних комплексних антифішингових рішень можна виділити наступні:

- антифішинговий сервіс від Area 1 Horizon;
- Avanan Cloud Email Security;
- Cofense;
- GreatHorn;
- IRONSCALES.

В кожного з них є свої особливості, недоліки та переваги над іншими, тож важливо розібрати їх більш детально.

Антифішинговий сервіс від Area 1 Horizon. У компанії є унікальна платформа, яка працює через API, а також оснащена аналітикой та рекомендаціями. До ключових функцій цього рішення відноситься:

- захист електронної пошти через георозподілену службу агента передачі пошти;
- автоматична інтеграція з серверами Windows, BIND і DNS;
- гнучкі з'єднувачі пристроїв для брандмауерів, веб-проксі або DNS-шлюзів;
- Постійне навчання та підрахунок балів за понад 100 моделями аналітики;
- Запатентовані алгоритми ідентифікації кампанії та кореляції атак;
- Захист мобільних користувачів і користувачів у роумінгу.

Особливістю цього по є модель оплати. Компанія стягує плату лише за загрози та атаки, які виявляє програмне забезпечення, що дозволяє прямо пов'язати інвестиції організації в кібербезпеку з можливими фінансовими втратами внаслідок успішного інциденту.

Avanan — це рішення безпеки електронної пошти, яке захищає від фішингових атак будь-який клієнт електронної пошти/службу обміну миттєвими повідомленнями, включаючи Microsoft 365, Microsoft Teams, Slack тощо. Це корисно для виявлення кампаній соціальної інженерії, які можуть запускатися через канали співпраці, у додаток до традиційної електронної пошти. До функціоналу ПЗ від Avanan можна віднести:

- можливість інтеграції хмарної програми для інструментів співпраці, електронної пошти, обміну повідомленнями та файлами;
- основна модель аналізу, навчена на передових шаблонах загроз;
- система ШІ для виявлення зв'язків між співробітниками, звичками електронної пошти та спілкуванням;

- Єдиний інтерфейс керування загрозами з універсальним контролем політики;
- Підключення до програм SaaS на основі маркерів OAuth із шифруванням TLS;
- Команда експертів для оперативного реагування на інцидент.

Головною особливістю цього рішення є те, що він не змінює записи обмінника поштою під час позначення чи блокування фішингових листів, це не дає змоги зовмисникам дізнатись про використання антифішингового ПЗ в організації.

Confense – комплексний інструмент для протидії фішингу. Додатково до набору ПЗ, вони також організовують навчання працівників для розпізнавання і розуміння алгоритму дій в разі фішингової атаки. До основних функцій цього рішення відносяться:

- база даних актуальних загроз, що містить понад 25 мільйонів глобальних звітів;
- інтеграція з безпекою кінцевих точок, брандмауерами нового покоління, системами SIEM та SOAR;
- служба карантину електронної пошти для автоматичного виявлення та ізоляції загроз;
- система симуляції фішингових загроз для навчання персоналу та підтримки їх в тонусі;
- автоматичний аналіз фішингової електронної пошти та система протидії спаму;
- Інтерфейс для співробітників, який допомагає розпізнавати фішингові атаки.

Рішення від компанії Confense ідеально підходить для великих організацій з різних галузей, для яких важливо підтримувати високий рівень навченості працівників, та мати високоякісну автоматичну систему захисту від фішингових атак.

Хмарна служба захисту під назвою GreatHorn створена для захисту від фішингових атак на каналах Office 365 та G Suit. В першу чергу вона розрахована на протидію напрямленому фішингу в сервісах корпоративної пошти, а також поширенню шкідливого ПЗ або програм-вимагачів. Рішення від GreatHorn працює з використання ШІ та машинного навчання. До його функціоналу відноситься:

- виявлення загроз за замовчуванням та автоматичний карантин;
- можливість пошуку і виправлення інцидентів у режимі реального часу;
- RESTful API для інтеграції з наявними рішеннями безпеки;
- Керована безпека електронної пошти та спеціальні політики, налаштовані експертами;
- Поінформованість кінцевих користувачів через банери, реальні попередження, порушення політики тощо;
- Можливість попереднього перегляду підозрілих посилань.

Цей комплекс ПЗ виділяється серед інших використання штучного інтелекту, що забезпечує його надійною та точною розвідкою про загрози. Він ідеально підходить для малого та середнього бізнесу, яким потрібна гнучка система безпеки корпоративної пошти.

Компанія IRONSCALES надає повноцінну платформу безпеки корпоративної пошти, яка працює на основі штучного інтелекту. Вона може допомогти організації виявляти, прогнозувати та протидіяти фішинговим атакам. До основних функцій комплексного рішення від IRONSCALES належить:

- симуляція загрози для аналізу фішингових атак і навчання користувачів;
- захист корпоративної пошти на рівні кожної поштової скриньки та рівноцінний пошук загроз;
- Захист від вкладених файлів зловмисного програмного забезпечення та підозрілих URL-адрес;
- Реагування на інциденти на основі ШІ;
- Віртуальний аналітик і помічник SOC під назвою Themis;
- Пошук як внутрішніх загроз, так і зовнішніх.

Крім технічних рішень, IRONSCALES надає ще послуги з навчання працівників протидії фішингу. Їх рішення охоплюють весь спектр заходів із запобігання фішингу, та якісно протидіють таким типам атак, як підміна керівника, компрометація корпоративної пошти ти видавання себе за бренд, які є найпоширенішими в галузі.

2.3 Класифікація організацій що потребують захисту від фішингу

На основі проведеного аналізу технологій корпоративної пошти, варто виділити три основні типи організацій, відповідно до обраної ними архітектури корпоративної пошти. Такі організації можна поділити на:

- ті що володіють власним сервісом корпоративної пошти з серверами розміщеними на території підприємства – перший тип;
- ті що використовують сервіс корпоративної пошти взятий в оренду – другий тип;
- ті що використовують поштові скриньки відомих поштових сервісів – третій тип.

Враховуючи особливості кожної архітектури варто розуміти потреби організації, що її використовує. Таким чином, для організації першого типу характерними відмінностями будуть:

- потреба в особливому рівні інформаційної безпеки;
- потреба у внутрішньому контролі та контролі доступу;
- наявність власних стандартів та політик безпеки;
- великий обсяг інформації з обмеженим доступом, що циркулює в корпоративній мережі;
- бажання бути незалежними від сторонніх постачальників.

До організацій першого типу можна віднести:

- Банки та інші фінансові структури (інвестиційні фонди, пенсійні фонди, кредитні організації). Вони мають високі вимоги до безпеки та конфіденційності, власний сервер дає змогу повністю контролювати комунікацію в межах внутрішньої мережі.
- Державні організації. Вони часто працюють з інформацією з обмеженим доступом і піддаються великій кількості кібератак. Власний поштовий сервер дає змогу постійно забезпечувати безпеку та контроль над засобами комунікації.
- Великі корпорації. Корпорації часто мають великий штаб працівників та часто володіють значним обсягом інформації, що робить нерентабельною оренду готових поштових серверів.
- Юридичні фірми. Часто вони працюють з конфіденційною інформацією клієнтів, витік цих даних може серйозно вплинути на репутацію організації та призвести до тяжких юридичних наслідків.
- Організації обмежені законом. Для організацій що працюють в сфері охорони здоров'я, телекомунікацій та інших критичних галузях, уряди країн часто встановлюють особливі вимоги щодо збереження та передачі даних.

Серед всіх, найбільша кількість саме організацій другого типу, вони віддають перевагу швидким, але ефективним рішенням за відносно невелику вартість. Для організацій цього типу характерними особливостями будуть:

- потреба в достатньому рівні інформаційної безпеки, без особливих вимог;
- відсутність великого бюджету на забезпечення інформаційної безпеки;
- потреба в наявності зручного методу комунікації між співробітниками;
- відсутність або недостатня кількість кваліфікованих спеціалістів з адміністрування серверів та забезпечення інформаційної безпеки.

Якщо розглядати конкретніше, то до них можна віднести:

- Малі та середні підприємства. Як правило у них сильно обмежений бюджет та технічні ресурси, а оренда сервісу корпоративної пошти

дозволяє зосередитись на основній діяльності, без потреби створення повноцінного IT-відділу.

- Компанії з декількома офісами. Для цих компаній володіння власним сервером може бути надто дорогим, проте вони потребують внутрішньої комунікації.
- Новостворені IT-компанії або стартапи. Як вже згадувалось вище, наявність власної корпоративної пошти позитивно впливає на репутацію компанії, та викликає більше довіри, тому це допоможе ефективніше залучати інвестиції.

Найбільш вразливими до фішингових атак є компанії третього типу, через досить умовне відношення їх способу комунікації до корпоративної пошти. Для компаній цього типу є характерними наступні особливості:

- повна відсутність IT-ресурсів у організації;
- відсутня потреба у постійній діловій комунікації між співробітниками;
- локальність бізнесу;
- мала кількість працівників;
- малі обсяги інформації з обмеженим доступом в організації.

Як правило ці організації схожі тим, що не розглядають свою діяльність як щось глобальне, працівники дуже рідко користуються поштою в своїй роботі, вони віддають перевагу спілкуванню в робочих чатах. До організацій цього типу можна віднести:

- Невеликі офлайн бізнеси. Найчастіше в таких бізнесах пошта використовується лише як інструмент для реєстрації на курсах підвищення кваліфікації, в соціальних мережах тощо.
- Організації без IT-відділу з малою кількістю працівників. В таких організаціях відсутній сенс постійного спілкування через корпоративну пошту, найчастіше всі питання вирішуються по телефону, а пошта використовується лише для передачі невеликої кількості внутрішньої документації.

- Невеликі державні установи, працівники яких не мають достатньої кваліфікації в сфері інформаційної безпеки.

2.4 Розробка рекомендацій щодо впровадження методів протидії фішингу

При розробці рекомендацій щодо впровадження методів протидії фішингу, важливо врахувати особливі потреби організацій, що відносяться до одного з трьох класів. Для організації першого класу важливим є високий рівень захисту, та гнучкі налаштування систем протидії фішингу. Для організації другого класу підхід повинен бути якомога простішим, проте забезпечувати надійний рівень захисту. Організації третього класу потребують значної інформаційної підготовки працівників та найпростіших рішень.

2.4.1 Рекомендації для організацій першого типу

Зважаючи на особливості компаній першого класу, для створення високого рівня захисту від фішингових атак необхідно зібрати комплект ПЗ, що забезпечує високий рівень захисту на кожному етапі. Враховуючи серйозні вимоги до інформаційної безпеки варто віддавати перевагу перевіреним інструментам, або інструментам з відкритим кодом, а за можливості і потреби можна замовити розробку такого ПЗ «під ключ». До початку впровадження методів протидії фішингу, компанії необхідно ретельно підійти до розробки власної політики безпеки інформації та впровадження її в організації.

Першим важливим кроком буде встановлення системи фільтрації повідомлень від спаму та фішингу. Для правильної та коректної роботи фільтру потрібно врахувати параметри фільтрації, які відповідають вимогам конкретної організації. Для фільтрації повідомлень можна обрати описаний в кваліфікаційній роботі спам-фільтр з відкритим кодом SpamAssasin.

Другим кроком стане налаштування спам-фільтру відповідно до визначених організацією параметрів фільтрації. В разі вибору фільтру

SpamAssasin можна скористатись налаштуваннями евристичного та статистичного аналізу, та списків блокування за IP-адресою. Важливо не забувати, що фільтри можуть застарівати, тож варто регулярно аналізувати їх ефективність та іноді редагувати правила фільтрації.

Третій крок найважливіший – навчання працівників. Саме вони стануть наступною лінією захисту від фішингових атак. Найефективнішим шляхом навчання працівників буде вибір доступної програми з підготовки працівників до протидії фішингу від передових компаній. Ці програми відрізняються тривалістю навчання, кількістю та детальністю інформації, наявністю практичної підготовки, та інструментів для симуляції фішингових атак з метою перевірки ефективності навчання. З оглянутих у кваліфікаційній роботі, можна відмітити програми підготовки від: Phished, InfoSec IQ та ESET Cybersecurity Awareness Training. Але потрібно зауважити, що підходити до вибору програми підготовки з розумінням потреб конкретної організації.

Четвертий кроком повинна стати установка стійкої до фішингу багатофакторної автентифікації. Це захистить ІС організації в разі отримання зловмисниками доступу до облікових даних працівників. В кваліфікаційній роботі було описано реалізацію популярного методу багатофакторної автентифікації з використанням стандарту FIDO2 та смарт-картки PIV.

П’ятим кроком буде установка системи моніторингу та аналізу підозрілої активності. Найефективнішими рішеннями в цій сфері є системи, що побудовані з використанням технологій ШІ та машинного навчання. В кваліфікаційній роботі було описано ПЗ від Egress Defend.

В кінці важливо додатково зауважити про необхідність регулярних і своєчасних оновлень всього наявного антифішингового ПЗ через регулярно появу нових способів фішингових атак. Також варто пам’ятати, що жоден метод протидії фішингу окремо, так і їх комбінація не дає стовідсоткового захисту від фішингових атак, тому потрібно завжди слідкувати за тенденціями і новинами в індустрії, а також регулярно використовувати резервне копіювання даних для легкого і майже безболісного їх відновлення в разі втрати.

2.4.2 Рекомендації для організацій другого типу

Враховуючи особливі вимоги організацій другого типу, необхідно знайти такі методи протидії фішингу, які можна буде впровадити досить легко в існуючу інфраструктуру організації, при тому воно повинно підтримувати інтеграцію з сервісом, що надає послуги з оренди КП. Перед впровадженням методів протидії фішингу, важливим є створення та впровадження власної політики безпеки.

Найоптимальнішим рішенням в цьому разі буде вибір комплексної системи протидії фішингу. Переважно всі вони включають в себе основні методи протидії фішинговим атакам, що легко інтегруються в систему організації та злагоджено працюють між собою, вибудовуючи надійні лінії захисту.

Частина комплексних рішень з протидії фішингу включають в себе різнорівневе навчання працівників, та інтегровані системи перевірки якості отриманих навичок. Проте в цьому разі важливо підібрати рішення, що відповідає вимогам до навичок працівників, та враховуючи можливість адміністрування цих програм з навчання. Можливо в деяких випадках більш ефективним або доцільним буде обрати комплексну систему протидії фішингу окремо від програми навчання.

При виборі комплексного рішення, потрібно спиратись на можливість IT-відділу організації проводити ефективне його адміністрування, налаштування та оновлення. Якщо у організації є проблеми на цьому рівні, то варто звернути увагу на рішення, що включають в себе постійну технічну підтримку та адміністрування систем захисту. З розглянутих комплексних систем протидії фішингу, варто відмітити наступні:

- Антифішинговий сервіс від Area 1 Horizon – через його систему оплати, при використанні цього рішення організація буде платити лише за виявлені загрози;
- Avanan Cloud Email Security – через його непомітність для фішерів, та підтримку великої кількості поштових сервісів;

- IRONSCALES – через активне використання технологій штучного інтелекту та машинного навчання, а також наявність високоякісної програми підготовки працівників.

Ретельний аналіз вимог до комплексних рішень з протидії фішингу, а також розуміння можливостей організації може дозволити серйозно зекономити час та бюджет організації на значному підвищенні рівня власного захисту від фішингових атак.

2.4.3 Рекомендації для організацій третього типу

Характерною особливістю цих організацій є переважно дуже низька обізнаність працівників про фішингові загрози. До цього також додається нерегулярне використання поштових сервісів для внутрішнього спілкування, проте це тільки підвищує ймовірність успішної фішингової атаки. Проте ці організацій скоріше стають жертвами масового фішингу, ніж напрямленого, тож варто проектувати захист орієнтуючись на стандартні методи атак, без використання складних підходів. Перед початком впровадження методів протидії фішингу потрібно розробити політики безпеки інформації у організації щонайменше базового рівня.

Єдиним можливим першим кроком для підвищення рівня захисту від фішингу в такій організації є саме навчання працівників. Важливо обрати програму з навчання таким чином, що підвищити рівень знань співробітників до достатнього рівня. Найбільш ефективною буде програма з включеною практичною підготовкою та тестуванням шляхом симуляції фішингових атак. Варто наголосити про можливі ризики в разі успішної фішингової атаки як для організації, так і для її працівників.

За можливості варто розглянути варіанти встановлення антивірусного ПЗ з функціями протидії фішингу на ПК працівників, це може врятувати від вже відомих та поширених методів фішингових атак, та значно підвищить рівень захисту як організації, так і її працівників. При виборі антивірусного ПЗ варто спиратись на особливості організації, наприклад якщо потрібно регулярно проводити платежі, то можна скористатись рішенням від BitDefender, а для простого підвищення ймовірності виявлення фішингу можна обрати антивірус від ESET.

В табл. 2.1 наведено узагальнені рекомендації щодо впровадження методів протидії фішингу для компаній трьох типів.

Таблиця 2.1 – Рекомендовані методи протидії фішингу для компаній різних типів

		Рекомендовані методи протидії фішингу					
		Антивірусне ПЗ	Спам-фільтр	Навчання працівників	Стійка до фішингу БА	Моніторинг підозрілої активності	КСПФ
Тип компанії	Перший	Так	Так	Так	Так	Так	
	Другий			За необхідності			Так
	Третій	Так		Так			

2.5 Висновки

В результаті роботи над спеціальним розділом було:

- проаналізовано методи протидії фішингу в КП;
- проаналізовано комплексні рішення для протидії фішингу в КП;
- зроблено класифікацію організацій на основі їх вимог до інформаційної безпеки та архітектурі їх корпоративної пошти;

- розроблено рекомендації щодо впровадження методів протидії фішингу для кожного з трьох типів організацій;

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є визначення економічної доцільності впровадження методів протидії фішингу в інформаційні системи цільових організацій відповідно до запропонованих рекомендацій, для чого треба здійснити наступні розрахунки: фіксованих (капітальних) витрат, річних експлуатаційних витрат на утримання системи протидії фішингу, річного економічного ефекту від впровадження запропонованих рекомендацій.

3.1 Розрахунок фіксованих (капітальних) витрат на впровадження запропонованих методів протидії фішингу

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Для ефективного впровадження запропонованих методів протидії фішингу, варто уважно підійти до розробки політики безпеки організації. Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої організації, починаючи зі складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}} \qquad (3.1.)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{\text{в}}$ – тривалість розробки концепції безпеки у організації;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків;

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки.

Відповідно до формули 3.1, трудомісткість розробки політики безпеки буде дорівнювати:

$$t = 4 + 16 + 4 + 6 + 4 + 16 + 8 = 58 \text{ год.}$$

3.1.2 Розрахунок витрат на створення політик безпеки

Витрати на розробку політики безпеки $К_{рп}$ включають в себе витрати на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч} \quad (3.2)$$

Станом на 2023 рік, середня заробітна плата спеціаліста з інформаційної безпеки становить 180 грн на годину з урахуванням основної і додаткової заробітної плати, а також відрахування на соціальні потреби. Витрати на заробітну плату розраховуються за формулою:

$$З_{зп} = t * 180 \quad (3.3)$$

Отже в результаті заробітна плата за розробку політик безпеки інформації буде дорівнювати:

$$З_{зп} = 58 * 180 = 10440 \text{ грн.}$$

Вартість машинного часу для розробки політики безпеки інформації вираховується за формулою:

$$З_{мч} = t * С_{мч} \quad (3.4)$$

Де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість задіяних робочих станцій при написанні політики;

$С_е$ – тариф на електричну енергію, грн/кВт*година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р = 1920$)

Вартість 1 години машинного часу ПК буде дорівнювати:

$$С_{мч} = 0{,}5 \cdot 1 \cdot 6 + \frac{4780 \cdot 0{,}3}{1920} + \frac{1312 \cdot 0{,}1}{1920} = 3{,}82 \text{ грн}$$

Тоді вартість витрат машинного часу буде:

$$З_{мч} = 104 * 3{,}82 = 397{,}28 \text{ грн.}$$

Отже, згідно формулі 3.2, витрати на розробку політики безпеки будуть складати:

$$К_{рп} = 10440 + 397{,}28 = 10837{,}28 \text{ грн}$$

Враховуючи відмінності запропонованих рекомендацій для кожного з типів організацій, важливо врахувати їх при розрахунках капітальних витрат. Для розрахунку вартості впровадження методів протидії фішингу в організацію першого типу, кількість працівників була прийнята за 100. В таблиці 3.1 вказані рекомендовані методи протидії фішингу та вартість їх впровадження для обраної організації.

Таблиця 3.1 – Вартість методів протидії фішингу для організації першого типу

Методи протидії фішингу	**фіксована вартість, грн**	**щорічні витрати, грн**
Спам-фільтр SpamAssasin	0	0
ESET Cybersecurity Awareness Training	0	60000
Fido2 суміжні пристрої	110000	0
Egres Defend	0	348000

Капітальні витрати на впровадження запропонованих методів розраховуються за формулою:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн.;

$К_{зпз}$ – вартість закупівель ліцензійного ПЗ, тис. грн.;

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн.;;

$К_{аз}$ – вартість закупівлі апаратного забезпечення, тис. грн.;;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.;

Враховуючи відсутність залучення зовнішніх консультантів, використання ліцензійного ПЗ та програми навчання за річною підпискою, та витрати на обладнання, що включені в вартість самого обладнання, капітальні витрати організації першого типу будуть дорівнювати:

$$К_1 = 10{,}84 + 110 + 60 = 180{,}84 \text{ тис. грн.}$$

Відповідно до рекомендацій, ефективним рішенням для компаній другого типу буде використати комплексну систему захисту від IRONSCALES, що включає в себе індивідуально розрубку політик безпеки, все необхідне ПЗ та програму з навчання працівників, вона поширюється по річній підписці, та коштує близько 185 тис. грн. на рік для компанії зі штабом 50 працівників. Враховуючи це, капітальні витрати організації другого типу будуть:

$$К_2 = 185 \text{ тис. грн.}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання системи протидії фішингу

До щорічних витрат на рекомендовані методи протидії фішингу можна віднести методи, що впроваджуються на умовах регулярної підписки. Для розрахунку річних експлуатаційних витрат потрібно скористатись формулою:

$$С = С_{навч} + С_{пз} + С_з \qquad (3.7)$$

де $С_{навч}$ – регулярні витрати на навчання працівників, тис. грн.;

$С_{пз}$ – регулярні витрати на продовження дії ліцензійного ПЗ, тис. грн.;

$С_з$ – річний фонд заробітної плати технічного персоналу, що обслуговує систему протидії фішинговим атакам, тис. грн.

Станом на 2023 рік, середня заробітна плата спеціаліста з інформаційної безпеки становить 180 грн на годину з урахуванням основної і додаткової заробітної плати, а також відрахування на соціальні потреби. Для обслуговування систем протидії фішингу вистачить одного спеціаліста, отже:

$$С_з = 180 * 160 * 12 = 345600 \text{ грн}$$

Відповідно до формули 3.7 та таблиці 3.1, річні експлуатаційні витрати для організації першого типу будуть дорівнювати:

$$С_1 = 60 + 348 + 345{,}6 = 753{,}6 \text{ тис. грн}$$

В наслідок того, що організація другого типу може використовувати технічну підтримку та програми навчання від компанії IRONSCALES, то її річні експлуатаційні витрати будуть складати:

$$С_2 = 185 \text{ тис. грн}$$

3.3 Визначення річного економічного ефекту від впровадження запропонованих рекомендацій з впровадження методів протидії фішингу

Для розрахунку економічного ефекту від впровадження запропонованих рекомендацій потрібно оцінити величину можливого збитку. Через неможливість стовідсотково передбачити наслідки атаки, для розрахунку вартості такого збитку можна використати наступну спрощену модель оцінки:

Необхідні вхідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла чи сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу персоналу, осіб;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

I – число атакованих вузлів або корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \tag{3.8}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної пошти, грн;

V – втрати від зниження обсягу продажів, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_{п} = \frac{\sum З_{с}}{F} \cdot t_{п} \quad (3.9)$$

де F – місячний фонд робочого часу (при 40-ка годинному робочому тижні становить 176 годин).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_{в} = П_{ви} + П_{пв} \quad (3.10)$$

де $П_{ви}$ – витрати на повторне введення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегменту корпоративної мережі.

Витрати на повторне введення інформації розраховуються за формулою:

$$П_{ви} = \frac{\sum З_{с}}{F} \cdot t_{ви} \quad (3.11)$$

Витрати на відновлення вузла або сегмента корпоративної мережів визначаються за формулою:

$$П_{пв} = \frac{\sum З_{о}}{F} \cdot t_{в} \quad (3.12)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента визначаючи виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{F_{г}} \cdot (t_{в} + t_{п} + t_{ви}) \quad (3.13)$$

де $F_г$ – річний фонд часу роботи організації (52 тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 годин.

Таким чином збитки від атаки на вузол або сегмент корпоративної мережі складе:

$$В = \sum_{i} \sum_{n} U \tag{3.14}$$

Для організації першого типу зі штабом 100 працівників, 3 з яких є обслуговуючим персоналом, відносно формул 3.10, 3.11, 3.12, витрати будуть складати:

$$П_{ви} = \frac{1455000}{176} \cdot 3 = 24801 \text{ грн}$$

$$П_{пв} = \frac{86400}{176} \cdot 3 = 1473 \text{ грн}$$

$$П_{в} = 24801 + 1473 = 26274 \text{ грн}$$

Втрати від зниження очікуваного обсягу за час простою вираховується за формулою 3.13 і буде дорівнювати:

$$V = \frac{43200000}{2080} \cdot (3 + 3 + 3) = 186923 \text{ грн}$$

А упущена вигода за формулою 3.8 буде складати:

$$U = 26274 + 186923 = 213197 \text{ грн}$$

Таким чином, при 14 атаках на рік, збитки для організації першого типу лише внаслідок простою складуть:

$$B_1 = 14 * 213197 = 2984758 \text{ грн}$$

А для організації другого типу в результаті таких самих розрахунків:

$$B_2 = 14 * 106600 = 1492400 \text{ грн}$$

Загальний ефект від слідування рекомендаціям щодо впровадження методів протидії фішингу визначається з урахуванням ризиків порушення інформаційної безпеки становить:

$$E = B \cdot R - C \tag{3.15}$$

Відповідно до формули 3.15, загальний ефект від слідування рекомендаціям для організації першого типу складе:

$$E_1 = 2984758 \cdot 0{,}66 - 753600 = 1216340 \text{ грн}$$

А для організації другого типу:

$$E_2 = 1492400 \cdot 0{,}66 - 185000 = 799984 \text{ грн}$$

3.3 Визначення та аналіз показників економічної ефективності запропонованих рекомендацій з впровадження методів протидії фішингу

Для проведення оцінки економічної ефективності запропонованих рекомендацій з впровадження методів протидії фішингу, необхідно визначити та проаналізувати наступні показники:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає ROSI;

б) термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Для обчислення ROSI необхідно скористатись формулою:

$$ROSI = \frac{E}{K}, \text{частки одиниці} \tag{3.16}$$

де Е – загальний ефект від слідування рекомендаціям (формула 3.15), тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Отже відповідно до формули 3.16, ROSI для організацій першого і другого типів буде дорівнювати:

$$ROSI_1 = \frac{1216,3}{180,84} = 6,73$$

$$ROSI_2 = \frac{800}{185} = 4,32$$

Термін окупності капітальних інвестицій T_o показує за скільки років окупаються капітальні інвестиції за рахунок отриманого ефекту від впровадження рекомендованих методів протидії фішинговим атакам, та обчислюється за формулою:

$$T_o = \frac{K}{E} \tag{3.17}$$

Отже відповідно до формули 3.17, термін окупності для організації першого і другого типів буде дорівнювати:

$$T_{o1} = \frac{180,84}{1216,3} = 0,15 \text{ років} = 2 \text{ місяці}$$

$$T_{o2} = \frac{185}{800} = 0,23 \text{ років} = 3 \text{ місяці}$$

3.4 Висновок про економічну доцільність запропонованих рекомендацій

В економічному розділі кваліфікаційної роботи була визначена економічна ефективність від впровадження рекомендацій щодо використання методів протидії фішингу. Було розраховані капітальні витрати для двох тип організацій, залежно від архітектури їх сервісу електронної пошти, результати склали 180,84 тис. грн. для організації з власним сервером, та 185 тис. грн для організацій, що використовують орендований сервіс корпоративної пошти. Було проведено оцінку можливих наслідків вразі проведення успішних фішингових атак для цих організацій, результати відповідно 2984,8 та 1492,4 тис. грн. Визначений термін окупності склав 2 та 3 місяці. Враховуючи це, можна вважати, що впровадження запропонованих рекомендацій щодо використання методів протидії фішингу в корпоративній пошті є економічно ефективним рішенням.

ВИСНОВКИ

На фоні зростаючої кількості фішингових атак, та економічних наслідків від них, для будь-якої сучасної компанії важливо впроваджувати методи для протидії ним та захисту своїх сервісів корпоративної пошти. Велика кількість методів протидії фішинговим атакам часто ставить під питання доцільність їх використання, та потрібність і сумісність з тими методами, що вже використовуються.

В кваліфікаційній роботі було проаналізовано дослідження наслідків фішингових атак, проаналізовано найпопулярніші архітектури сервісів корпоративної пошти, актуальні фішингові загрози та їх наслідки для організацій.

В спеціальному розділі проаналізовано методи протидії фішинговим атакам, проведено класифікацію організацій відповідно до архітектури корпоративної пошти. Проведено пошук та аналіз існуючих комплексних рішень з протидії фішингу. На основі отриманих результатів було розроблено рекомендації, щодо впровадження методів протидії фішинговим атакам в сервісах електронної пошти для кожного типу організацій.

В економічному розділі визначено економічну доцільність впровадження методів протидії фішингу в інформаційні системи різних організацій відповідно до запропонованих рекомендацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП» 2020.

2. Методичні рекомендації до економічної частини дипломного проекту зі спеціальності 125 кібербезпека / Упоряд.: Д.П. Пілова – Дніпро: НТУ «ДП» 2019.

3. Tessian Spear phishing threat landscape 2021 (Електрон. ресурс) / Спосіб доступу: URL: https://www.tessian.com/research/spear-phishing-threat-landscape/ - Загол. з екрана.

4. ESET THREAT REPORT T2 2021 (Електрон. ресурс) / Спосіб доступу: URL: https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf (дата звернення: 10.05.2023) - Загол. з екрана.

5. IBM Security X-Force Threat Intelligence Index 2023 (Електрон. ресурс) / Спосіб доступу: URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 10.05.2023) - Загол. з екрана.

6. CISCO 2021 Cyber security threat trends: phishing, crypto top the list (Електрон. ресурс) / Спосіб доступу: URL: https://cloudmanaged.ca/wp-content/uploads/2021/09/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.pdf (дата звернення: 12.05.2023) - Загол. з екрана.

7. Verizon 2021 Data Breach Investigations Report (Електрон. ресурс) / Спосіб доступу: URL: https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf (дата звернення: 12.05.2023) - Загол. з екрана.

8. IC3 Internet crime report 2020 (Електрон. ресурс) / Спосіб доступу: URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата звернення: 12.05.2023) - Загол. з екрана.

9. OMB M-22-09 Zero Trust (Електрон. ресурс) / Спосіб доступу: URL: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (дата звернення: 13.05.2023)

10. Mitnick K. D. Ghost in the wires: My adventures as the world's most wanted hacker. New York : Little, Brown and Company, 2011. 413 c.

11. Phishing (Електрон. ресурс) / Спосіб доступу: URL: https://www.phishing.org/what-is-phishing (дата звернення: 14.05.2023)

12. Anti-Phishing Certification Bitdefender 2022 (Електрон. ресурс) / Спосіб доступу: URL: https://www.av-comparatives.org/tests/anti-phishing-certification-bitdefender-2022/ (дата звернення: 14.05.2023)

13. Bitdefender (Електрон. ресурс) / Спосіб доступу: URL: https://www.bitdefender.com/ (дата звернення: 24.05.2023)

14. Configure anti-phishing policies in Microsoft Defender for Office 365 (Електрон. ресурс) / Спосіб доступу: URL: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-mdo-configure?view=o365-worldwide (дата звернення: 26.05.2023) - Загол. з екрана.

15. Tessian (Електрон. ресурс) / Спосіб доступу: URL: https://www.tessian.com/ (дата звернення: 26.05.2023)

16. IRONSCALES (Електрон. ресурс) / Спосіб доступу: URL: https://ironscales.com/ (дата звернення: 26.05.2023)

17. ESET (Електрон. ресурс) / Спосіб доступу: URL: https://www.eset.com/ua/ (дата звернення: 31.05.2023)

18. INFOSEC (Електрон. ресурс) / Спосіб доступу: URL: https://www.infosecinstitute.com/ (дата звернення: 31.05.2023)

19. Phishing trends and techniques (Електрон. ресурс) / Спосіб доступу: URL: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/phishing-trends?view=o365-worldwide (дата звернення: 31.05.2023) - Загол. з екрана.

20. Examples of Common Phishing Emails (Електрон. ресурс) / Спосіб доступу: URL: https://terranovasecurity.com/top-examples-of-phishing-emails/ (дата звернення: 01.06.2023) - Загол. з екрана.

21. Work.ua (Електрон. ресурс) / Спосіб доступу: URL: https://www.work.ua/ 03.06.2023

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	20	
6	А4	Спеціальна частина	24	
7	А4	Економічний розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Презентація Іванов_СС_125_19_1_КВ_РОБ.pptx
2. Іванов_СС_125_19_1_КВ_РОБ.docx
3. Іванов_СС_125_19_1_КВ_РОБ.pdf
4. Іванов_СС_125_19_1_КВ_РОБ.pdf.p7s

ДОДАТОК В. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 95 б. («відмінно»).

Керівник розділу _____ _____

(Підпис) (ініціали прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-1
Іванова Станіслава Сергійовича
на тему: «Методи протидії фішингу в корпоративній пошті»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на ___ сторінці.

Метою кваліфікаційної роботи є підвищення ефективності протидії фішинговим атакам на корпоративні сервіси електронної пошти.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз актуальності проблеми фішингових атак; аналіз технологій корпоративного сервісу електронної пошти; аналіз методів протидії фішингу в корпоративній пошті; аналіз комплексних рішень для протидії фішингу в корпоративній пошті.

Розроблено рекомендації щодо впровадження методів протидії фішингу.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності протидії фішинговим атакам на корпоративні сервіси електронної пошти, за рахунок розробки рекомендацій щодо впровадження методів протидії фішингу.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Іванов С.С. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи **д.т.н., проф. В.І. Корнієнко**

Керівник спец. Розділу **ст. викл. Д.С. Тимофєєв**