ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО—НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ ВІД ФІШИНГОВИХ АТАК ЗА ДОПОМОГОЮ CISCO EMAIL THREAT DEFESE»

Виконав студент 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Остафійчук В.О.
(прізвище та ініціали)

Керівник Марченко В.В.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер _____
(прізвище та ініціали)

КИЇВ - 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"24" лютого 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Остафійчуку Валентину Олеговичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту корпоративної пошти від фішингових атак за допомогою Cisco Secure Email Threat Defense»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна пошта;
програмний комплекс захисту пошти в реальному часі;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту від фішингових атак.
2. Сутність явища фішингових атак в історії інформаційних технологій
3. Методи реалізації фішингових атак та їх різновиди
4. Використання програмного забезпечення для захисту корпоративної пошти
5. Розробка рекомендацій щодо захисту корпоративної пошти

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3.Результати аналізу історії шкідливого програмного забезпечення та фішингових атак
4. Результати аналізу методів та засобів протидії з найпоширенішими видами фішингових атак.
5. Призначення та можливості рішення Cisco Email Threat Defence.
6. Рекомендації щодо покращення захищеності електронної корпоративної пошти від фішингових атак
7. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Аналіз теоретичних основ щодо захисту інформаційних активів в корпоративній інформаційній ситсемі	24.02.2023 р.	
2.	Дослідження методик фішингових атак на корпоративну мережу та визначення типології методів захисту від них.	11.03.2023 р.	
3.	Прикладне вирішення питання фішингових атак та визначення вектору можливого вирішення програмними та організаційними методами	26.03.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту електронної корпоративної пошти.	20.04.2023 р.	
5.	Оформлення результатів дослідження.	15.05.2023 р.	
6.	Підготовка доповіді до захисту.	29.05.2023 р.	

Студент Остафійчук В.О.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Остафійчука Валентина Олеговича
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту корпоративної пошти від фішингових атак за допомогою Cisco Secure Email Threat Defense»

Актуальність: На сьогодні корпоративна пошта є головним засобом передачі важливої інформації в середині середніх та великих організацій. Будь-яка організація прагне зберегти свої інформаційні активи в межах інформаційної системи та запобігти витокам інформації. Проте не будь-який співробітник розуміє що таке фішинг, так які методи протдії можуть бути використані для забезпечення безпеки даних.

Саме тому дослідження фішингу та протидії його реалізації є досить актуальною.

Позитивні сторони:

1. Було проведено аналіз розвитку фішингових атак, включаючи перші зареєстровані випадки та можливі засоби протидії.
2. Було досліджено методи та засоби захисту корпоративної пошти на основі програмного продукту Cisco Secure Email Threat Defense
3. Розроблення рекомендацій щодо програмних та організаційних засобів зменшення впливу фішингових атак.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково—технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. Використаний програмний продукт наданий на випробувальний період, та не надає повного функціоналу, що не дає можливості провести детальніші дослідження
2. Дослідження були проведені на тестовій пошті, що не дає можливості відобразити всі можливості програмного продукту.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **відмінно**, а студент **Остафійчук В.О.** — присвоєння кваліфікації: 3439. Фахівець з організації інформаційної безпеки.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект—частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Остафійчук В.О. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
Освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту корпоративної пошти від фішингових атак за допомогою Cisco Secure Email Threat Defense».
Бакалаврська робота і рецензія додаються.
Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Остафійчук В.О. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Остфійчук В.О.*** обрав тему роботи, метою якої було дослідження методів та засобів багатовимірного візуального аналізу та розроблення рекомендацій щодо їх застосування під час розслідування кіберінцидентів. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Горобець Р.В. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Остафійчука Валентпна Олеговича на оцінку **«відмінно»** та присвоїти йому кваліфікацію: 3439. Фахівець з організації інформаційної безпеки.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“_____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Остафійчук В.О.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ — програмне забезпечення

ШПЗ — шкідливе програмне забезпечення

ШІ — штучний інтелект

URL — Uniform Resource Locator

IP — Internet Protocol

DMARC — Domain-based Message Authentication, Reporting, and Compliance

CSV — Comma-Separated Values

SIM — Subscriber Identification Module

2FA — двохфакторна аутентифікація

MFA — мультифакторна аутентифікація

HTML — HyperText Markup Language

SMTP — Simple Mail Transfer Protocol

O365 — Ofice 365

SETD — Secure Email Threat Defense

TLS — Transport Layer Security

ЦС — центр сертифікації

IoT — інтернет речей

ВСТУП

*Актуальність теми***.** Кібербезпека зараз важлива як ніколи. Зростаючий розвиток технологій та Інтернету приніс великі переваги, але також і нові ризики. Більшість користувачів навіть не усвідомлюють цього. Кіберзлочинці продовжують вдосконалювати свою тактику, їхні атаки стають все більш витонченими, а експертам стає все складніше вирішувати проблеми. Однією з найважливіших проблем кібербезпеки сьогодні є збільшення числа кібератак і зростання кількості кіберзлочинців. Атаки варіюються від простих спроб фішингу до складного шкідливого програмного забезпечення та атак з вимогою викупу, які можуть завдати значної фінансової та репутаційної шкоди. Організації стають більш вразливими до кіберзагроз, оскільки інформація та технології сьогодні тісно інтегровані в повсякденну діяльність, а Інтернет речей (IoT) може підвищити вразливість систем, якщо їх не налаштувати належним чином. Але зростає і витонченість атак на інформацію та критичну інфраструктуру. Запобігання фішингу є критично важливим для бізнесу, оскільки фішингові атаки є широко розповсюдженою та значною загрозою для його безпеки.

Фішинг — вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані — наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів. Фішингові атаки стають все більш витонченими і часто прозоро відображають сайт, на який спрямована атака, що дозволяє зловмиснику спостерігати все, поки жертва займається власними справами.

Згідно статистичної інформації наданої компанією Egress, що спеціалізується на захисті від фішингових атак:

- викрадені або скомпрометовані облікові дані були основним вектором атаки у 19% витоків даних 2022 року;
- у 2022 році спостерігається незначне зниження цієї статистики порівняно з 2021 роком, коли викрадені або скомпрометовані облікові дані були основним вектором атаки у 20% випадків;
- порушення, спричинені викраденими або скомпрометованими обліковими даними, в середньому коштували $4,5 млн;
- цей тип порушень мав найдовший життєвий цикл — 243 дні на виявлення порушення та 84 дні на його локалізацію;
- це на 16,6% більше, ніж загальний середній час виявлення та локалізації витоку даних;
- фішинг був другою найпоширенішою причиною порушень (16%), що коштувало $4,91 млн.

Наслідки успішної фішингової атаки можуть нанести значну шкоду організації. Зловмисник може отримати доступ до конфіденційних даних, скомпрометувати корпоративні мережі та викрасти цінну інтелектуальну власність. Це може призвести до значних фінансових, репутаційних втрат та навіть юридичної відповідальності. Більше того, фішингові атаки можуть поставити під загрозу безпеку всієї організації, оскільки може призвести до ланцюгової реакції скомпрометованих облікових записів і систем. Ефективні заходи захисту від фішингу мають важливе значення для зменшення ризику таких атак. Організації повинні інформувати своїх співробітників про ризики і надавати їм інструменти та ресурси для виявлення та повідомлення про підозрілі електронні листи, посилання або повідомлення.

Метою дипломної роботи є дослідження можливого рішення підвищення рівня захищеності корпоративної мережі від фітингових атак.

Завдання дипломної роботи є:

дослідити сучасні способи фішингових атак та їх загрози корпоративній мережі;

- визначити необхідні навички спеціалістів кібербезпеки при протидії фішинговим атакам;
- визначити можливості застосування спеціалізованого програмного забезпечення для захисту від фітингових атак на основі програмного комплексу Cisco Secure Email Threat Defense;
- розробка рекомендацій щодо застосування програмного забезпечення для запобігання кіберінцидентів основою яких є фішингові атаки.

Об'єктом дипломної роботи є реагування на фішингові атаки на організації

Предметом дипломної роботи методи та засоби боротьби з фішинговими атаками

Методи дослідження: опрацювання експлуатаційної документації інформації інформації, міжнародні стандарти, практичне випробування.

1 АНАЛІЗ ТЕОРЕТИЧНИХ ОСНОВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1 Сутність шкідливого програмного забезпечення та його вплив на формування методів викрадення інформації.

Згідно з визначенням Федерального бюро розслідувань (ФБР), Програми-здирники — це тип шкідливого програмного забезпечення (ШПЗ), яке перешкоджає доступу до файлів, систем або мереж вашого комп'ютера та вимагає сплатити викуп за їхнє повернення. Атаки вірусів-здирників можуть призвести до значних перебоїв у роботі та втрати критично важливої інформації та даних

Шкідливе програмне забезпечення може приймати різні форми, включаючи віруси, хробаки, троянські програми, програми-вимагачі, шпигунські програми, рекламні програми та руткіти, серед інших [1].

Аналогічно, ESET описує шкідливе програмне забезпечення як програми створенні з зловмисним наміром та хоплює різні види шкідливих програм на комп’ютері. Серед найвідоміших форм — трояни, програми-вимагачі, віруси, черв’яки та банківські шкідливі програми [2].

Незалежно від своєї конкретної специфікації, шкідливе програмне забезпечення вважається серйозною загрозою для безпеки і конфіденційності комп'ютерних систем та їхніх користувачів. Як наслідок, було впроваджено численні закони та політики, спрямовані на запобігання, виявлення та покарання операцій, пов'язаних зі шкідливим програмним забезпеченням.

Головною метою ШПЗ є крадіжка даних або заподіяння шкоди і руйнування комп'ютерів і комп'ютерних систем. Існує кілька типів поширеного шкідливого програмного забезпечення. Існує безліч різновидів шкідливого програмного забезпечення, кожен з яких має свої особливості та функціональні можливості

Комп'ютерний вірус — це тип комп'ютерного програмного забезпечення, що при виконанні відтворює себе, модифікуючи інші комп'ютерні програми та вставляючи в них свій власний код. Якщо ця реплікація є успішною, то уражені

ділянки вважаються «інфікованими» комп'ютерним вірусом.. Комп'ютерні віруси, як зазначається, вимагають наявності хост-програми. Вірус записує свій власний код у хост-програму. Коли програма запускається, написана вірусна команда виконується першою, спричиняючи зараження та пошкодження.

Комп'ютерний черв'як — це шкідливе програмне забезпечення, що самовідтворюється і автономно поширюється на декілька комп'ютерних систем. Часто використовуючи комп'ютерну мережу для свого розповсюдження, це явище покладається на використання недоліків безпеки, наявних у цільовій комп'ютерній системі, як засобу проникнення в мережу. Цей комп'ютер виступає в ролі хоста для сканування та зараження інших пристроїв. Отримавши контроль над нещодавно інфікованими комп'ютерами, хробак продовжує своє розповсюдження, скануючи та заражаючи додаткові комп'ютери через свою хост-систему. Ця поведінкова модель зберігається, коли хробак продовжує розмножуватися і поширювати свою інфекцію безперервно. Комп'ютерні черв'яки використовують рекурсивну тактику, щоб увічнити процес свого розмноження без потреби в хост-програмі. Завдяки вигідному використанню експоненціального розширення, ці черв'яки швидко поширюються, в результаті чого досягають контролю над значною кількістю комп'ютерів за короткий період часу. Зазвичай спостерігається, що хробаки спричиняють помітні порушення в роботі мережевої інфраструктури, в першу чергу, через споживання пропускної здатності. І навпаки, віруси, як правило, призводять до пошкодження або зміни файлів, що знаходяться в комп'ютерній системі, яку вони атакують. Безліч черв'яків створюються з єдиною метою — розмножуватися, утримуючись від будь-яких спроб модифікувати системи, через які вони проникають. Хробаки Morris і Mydoom продемонстрували, що навіть позірно нешкідливі хробаки можуть спричинити серйозні збої, збільшуючи мережевий трафік і породжуючи непередбачувані наслідки [3-4].

Троянський кінь — це комп'ютерна програма, що відноситься до категорії шкідливого програмного забезпечення, широко відома як «троянська програма», яка обманює користувачів, видаючи себе за легітимну програму або файл, тоді як

насправді вона виконує шкідливі дії в комп'ютерній системі або мережі. Як правило, трояни отримують несанкціонований доступ до комп'ютера або мережі за допомогою методів соціальної інженерії — фішингових схем електронної пошти або представляючи себе як безпечний і надійний варіант завантаження програмного забезпечення. Його здатність уникати виявлення та непомітно проникати в системи робить його особливо потужною зброєю в руках кіберзлочинців. «Після успішної інсталяції в комп'ютерну систему троянський кінь здатен виконувати цілу низку шкідливих дій без явного відома користувача системи. Здатність троянського коня залишатися непомітним і непомітно проникати в системи підвищує його ефективність як інструменту в руках кіберзлочинців».

Програми-здирники — це категорія шкідливого програмного забезпечення, яке має унікальну структуру для шифрування цифрових файлів у системі, що належить жертві, роблячи їх неефективними та недоступними, доки не буде сплачено узгоджений викуп. Звичайний варіант програми-здирника — це спливаюче повідомлення з вимогою криптографічної компенсації, часто у формі Bitcoin або Ethereum, в обмін на ключ розшифрування, необхідний для розблокування даних. Поширення програм-вимагачів зазвичай відбувається за допомогою таких засобів, як фішингові електронні листи, шкідливі вкладення або використання вразливостей, знайдених у застарілому програмному забезпеченні. Після встановлення на цільову комп'ютерну систему програма-здирник має здатність швидко поширюватися мережею, здійснюючи шифрування на всіх інших підключених до неї комп'ютерних системах.

Шпигунське програмне забезпечення — це різновид шкідливого програмного забезпечення, призначеного для прихованого вивчення та накопичення інформації про роботу комп'ютерної системи користувача без його явного дозволу або усвідомлення. Термін «шпигунське програмне забезпечення» стосується групи комп'ютерних програм, які спостерігають за діями користувача і збирають конфіденційні, важливі дані, включаючи, але не обмежуючись ними, облікові дані для входу в систему, історію переглядів, натискання клавіш і

персональні дані. Проникнення шпигунського програмного забезпечення в комп'ютерну систему жертви може відбуватися різними способами, включаючи вкладення в електронних листах, завантаження безкоштовного програмного забезпечення та перехоплення браузера. Після встановлення шпигунське програмне забезпечення може непомітно працювати у фоновому режимі, збираючи інформацію та передаючи її на сервер зловмисника. Крім того, шпигунські програми можуть ініціювати завантаження додаткового програмного забезпечення, перенаправляти інтернет-трафік жертви в небажані напрямки, показувати настирливу спливаючу рекламу та виконувати інші зловмисні дії.

Рекламне ПЗ — це клас програм, спеціально розроблених для показу рекламного контенту на комп'ютерному пристрої користувача. Поєднання рекламного ПЗ з безкоштовним або умовно—безкоштовним програмним забезпеченням та його потенційна інтеграція з небажаними програмами є поширеним явищем. Основною метою рекламного ПЗ є отримання доходу для його розробника шляхом показу реклами користувачам. Було розроблено безліч механізмів для впровадження рекламного ПЗ — явища, яке охоплює різні форми небажаної реклами, такі як спливаючі вікна, банери та транзакції в додатках. Певні форми рекламного ПЗ мають здатність відстежувати шаблони інтернет-перегляду користувача і згодом показувати персоналізовану рекламу, яка відповідає його інтересам. Незважаючи на те, що рекламне ПЗ часто розглядається як подразник, воно не обов'язково становить значну загрозу. Деякі рекламні програми демонструють вищий рівень напористості, показуючи небажану рекламу або перенаправляючи користувачів на незахищені веб-сайти. За певних обставин рекламне ПЗ здатне приховано збирати конфіденційні дані користувачів без їхньої явної згоди або усвідомлення.

Небезпека ШПЗ може відрізнятися залежно від його типу та цілей зловмисника. Шкідливе програмне забезпечення може завдати шкоди комп'ютерним системам, мережам і пристроям, викрасти конфіденційну інформацію, поставити під загрозу особисту конфіденційність і навіть використовуватися як інструмент для кібершпигунства або кібервійни.

Кібершахрайство стало зростаючою проблемою з перших днів існування Інтернету і за останні три десятиліття зазнало значної еволюції. Ось деякі ключові зміни у сфері кібершахрайства з 1990 року: Шкідливе програмне забезпечення та програми-вимагачі: У 2010-х роках кіберзлочинці почали використовувати шкідливе програмне забезпечення та програми-вимагачі для зараження комп'ютерів і мереж, шифруючи файли і вимагаючи оплату в обмін на ключ до розшифровки. Ці атаки стають все більш витонченими і поширеними, вражаючи як окремих осіб, так і великі організації.

Зі зростанням інтернету в 1990-х і 2000-х роках все більше людей почали користуватися онлайн-банкінгом і здійснювати покупки онлайн. Це створило нові можливості для кіберзлочинців викрадати особисту та фінансову інформацію.

На початку 2000-х років фішингові атаки стали більш поширеними, використовуючи шахрайські електронні листи та веб-сайти, що змушували людей вводити свою персональну інформація. Також стали популярними методи соціальної інженерії, наприклад видавання себе за авторитетну особу, якій довіряють, або створення відчуття терміновості.

Зі зростанням популярності смартфонів і мобільних пристроїв кіберзлочинці також націлилися на ці платформи, використовуючи підроблені додатки та інші методи для крадіжки особистої та фінансової інформації.

Зростання популяронсті криптовалют, таких як біткоін, також створило нові можливості для кіберзлочинців займатися шахрайством, наприклад, використовувати фальшиві криптовалютні біржі або фішингові атаки, спрямовані на власників криптовалют. Незважаючи на всі ці зміни, кібершахрайство залишається постійною загрозою, що еволюціонує. З розвитком технологій, ймовірно, з'являться нові форми кібершахрайства, і для приватних осіб та організацій буде важливо зберігати пильність і вживати заходів для захисту від цих загроз.

Потенційна небезпека, притаманна шкідливому програмному забезпеченню, може відрізнятися залежно від конкретного типу шкідливого програмного забезпечення та конкретних цілей зловмисника. Шкідливий вплив шкідливого

програмного забезпечення включає в себе здатність завдавати шкоди комп'ютерним системам, мережам і пристроям, а також несанкціонований доступ до конфіденційної інформації та посягання на особисту приватність. Крім того, нерідко воно використовується як потенційний інструмент для кібершпигунства або ведення війни. Проблема кібершахрайства постійно зростала з моменту появи Інтернету і зазнала суттєвих змін протягом попередніх трьох десятиліть. Подальший дискурс висвітлює основні зміни у сфері кібершахрайства після 1990 року.

Протягом 2010-х років кіберзлочинці все частіше використовували шкідливе програмне забезпечення та програми-вимагачі (особливо поширені останні) для проникнення в комп'ютери та мережі, шифрування цінних даних і вимагання винагороди за видачу ключа для розшифрування. Вищезгадані атаки поступово еволюціонують у своїй складності та поширеності, впливаючи як на окремі організації, так і на великі конгломерати. На хвилі експоненціального розвитку Інтернету в 1990-х і 2000-х роках дедалі більше людей почали користуватися послугами онлайн-банкінгу та здійснювати покупки в Інтернеті. Поява нових технологічних досягнень створила для кіберзлочинців нові можливості для викрадення конфіденційних персональних і фінансових даних.

У перші роки 21-го століття помітно зросла кількість фішингових атак, які характеризуються використанням підроблених електронних листів і веб-сторінок, щоб обманом змусити людей розкрити їхні персональні дані. Широкої популярності набули стратегії соціальної інженерії, що включають такі методи, як видавання себе за надійну та авторитетну особу або створення відчуття нагальної потреби. Зростаюче поширення смартфонів і мобільних пристроїв ненавмисно надало кіберзлочинцям розширений пул жертв, тим самим спонукаючи до використання шахрайських додатків та інших хитромудрих схем, спрямованих на незаконний збір приватних і грошових даних. Різке зростання популярності цифрових валют, таких як біткойн, також створило нові можливості для зловмисників здійснювати обман, що включає в себе розгортання фальшивих бірж цифрових валют або фішингових експедицій, націлених на власників

криптовалют. Незважаючи на безліч заходів, спрямованих на боротьбу з кіберзлочинністю, явище кібершахрайства залишається постійною і динамічною загрозою, яка постійно еволюціонує. З кожним технологічним досягненням очікується поява нових проявів кібершахрайства. Відповідно, як фізичним, так і юридичним особам вкрай важливо зберігати пильність і вживати заходів для захисту від цих небезпек.

1.2 Кореляція змін методик кібератак на конфіденційні дані до технологічного розвитку.

Розвиток інформаційних технологій починаючи ще 70-х років попереднього століття вражав людей. Звичайно, людство розвивало нові технології впродовж усього існування, проте на даний момент науковцями виділяється 4 етапи історичної інформаційної революції:

- перша інформаційна революція пов'язана з появою писемності. З'явилася можливість фіксувати знання на матеріальному носії, тим самим відчужувати їх від виробника і передавати від покоління до покоління через її фіксацію в знаках та зруйнувала монополію вузького кола людей на знання;
- друга інформаційна революція була викликана винаходом та поширенням книгодрукування в XV ст. і розширила доступ до інформації широким верствам населення завдяки тиражуванню знань. Ця революція радикально змінила суспільство, створила додаткові можливості прилучення до культурних цінностей відразу великих верств населення;;
- третя інформаційна революція (кінець XIX — початок XX ст.) пов'язана з винаходом телеграфу, телефону, радіо, телебачення, що дозволяло оперативно, у великих обсягах передавати і накопичувати інформацію, передавати звукові та візуальні образи на великі віддалі. Останнє створило передумови ефекту «стискання простору»;
- четверта інформаційна революція (70-ті роки XX ст.) зумовлена винаходом мікропроцесорної технології і персонального комп'ютера. Вона характеризується переходом від механічних, електричних засобів перетворення

інформації до електронних та створення програмного забезпечення цього процесу. «Вінцем» цієї хвилі революції є поява всесвітньої мережі - інтернету, що уможливило інформаційний обмін в глобальних масштабах [5].

У 1971 році Джон Дрейпер виявив, що може використовувати іграшковий свисток з коробки з-під пластівців для безкоштовних міжміських телефонних дзвінків, скориставшись недоліком у сигнальній системі телефонної компанії. Він поділився цією інформацією з групою хакерів, які почали використовувати її для безкоштовних телефонних дзвінків і продавати інформацію іншим. Дрейпер та його однодумці стали відомі як «телефонні фрики», а їхня діяльність стала предметом статті 1971 року в журналі «Есквайр». Цю статтю часто цитують як одну з перших публікацій про комп'ютерний злом і кіберзлочинність.

Серед інших прикладів кіберзлочинності цього часу включають крадіжку конфіденційних даних з комп'ютерних мереж 1970-х і 1980-х роках. Наприклад, у 1986 році група хакерів, відомих як «414», зламала комп'ютерні системи кількох великих корпорацій та урядових установ, включаючи Лос-Аламоську національну лабораторію.

У 1990-х роках інтернет став більш доступним для широкого загалу, що створило нові можливості для втілення у реальність нових технологій кібершахрайства. Поки деякі організації лише починали переходити на форму бізнесу з використанням інтернет-технологій. Оскільки все більше людей і підприємств почали підключатися до інтернету, потенційна кількість жертв для атаки розширювалась.

Саме недостатній рівень знань нових користувачів інтернету полегшив завдання атаки фізичних та юридичних осіб за допомогою фішингових атак, шкідливого програмного забезпечення та інших видів кібератак. Електронна пошта стала популярним способом спілкування в 1990-х роках, але напротивагу вона стала однією з найбільш ефективних методів кібератак.

У 2000-х роках фішинг-атаки часто призводили до надсилання підроблених електронних повідомлень, які були схожі на ті, що розповсюджувалися авторитетними організаціями, такими як фінансові установи, провайдери

кредитних карток або соціальні мережі в Інтернеті. Такі електронні повідомлення, як правило, містили гіперпосилання на підроблену онлайн-платформу, яка вимагала від користувача розкрити свої облікові дані для входу в систему або інші особисті дані. Згодом кіберзлочинці викрадали цю інформацію. У 2000-х роках фішингові електронні листи часто можна було розпізнати завдяки неправильному написанню або граматиці; однак траплялися випадки, коли вони були більш складними для розпізнавання.

У наш час поширеним методом фішингу є використання вразливостей міжсайтового скриптингу (XSS) у веб-додатках, коли кіберзловмисники можуть вставляти шкідливий код у веб-сторінки, до яких мають доступ інші користувачі. Використання кіберзлочинцями міжсайтового скриптингу (XSS) полегшило створення фішингових сторінок, які імітують справжні веб-сайти, але при цьому приховано збирають облікові дані користувачів.

Водночас, поява таких веб-браузерів, як Internet Explorer та Firefox, відкрила кіберзлочинцям нові можливості для здійснення фішингових атак. Використовуючи вразливості браузерів або виготовляючи підроблені розширення, користувачів спокушали ненавмисним завантаженням шкідливого програмного забезпечення або підневільним наданням їхніх персональних даних.

Протягом десятиліття 2010-х років фішингові атаки стали більш витонченими та специфічними, коли зловмисники використовували тактику соціальної інженерії, щоб змусити людей надати свої персональні дані або встановити шкідливе програмне забезпечення. Останнім часом все більшого поширення набуває практика фішингу, що включає в себе цілеспрямовані спроби, спрямовані на конкретних осіб або організації. Зловмисники, що діють у сфері кіберзлочинності, використовували накопичені дані, що стосуються відповідного суб'єкта, щоб сфабрикувати електронний лист або повідомлення з високим ступенем достовірності, що відображає повідомлення авторитетного суб'єкта, наприклад, знайомого або клієнта.

На початку 2000-х років ідентифікація спаму часто не вимагала особливих зусиль через його загальний і нерелевантний характер. Протягом десятиліття

2010 року у сфері спаму відбулася помітна еволюція, в результаті якої характер таких електронних повідомлень став більш витонченим і специфічним, спрямованим на конкретні цілі. У наш час кіберзлочинці застосовують тактику інтелектуального аналізу даних як засіб збору інформації про вразливі цілі, включаючи, зокрема, їхні особисті інтереси та купівельні вподобання, щоб створювати більш переконливі та достовірні за своєю природою спам-повідомлення. Ці електронні листи можуть виглядати як такі, що походять від справжнього джерела, наприклад, від продавця або мережевого сайту, і містити індивідуалізовані матеріали, сформульовані таким чином, щоб спокусити одержувача натиснути на гіперпосилання або отримати документи.

Поширення смартфонів і планшетів у 2010-х роках призвело до відповідної ескалації схильності кіберзлочинців до фішингових атак, спрямованих на цю когорту користувачів. Використовуючи підроблені додатки або фішингові повідомлення, що надсилаються через служби коротких повідомлень та платформи обміну повідомленнями, зловмисники застосовували стратегічне використання тактики соціальної інженерії, щоб заманити нічого не підозрюючих користувачів до встановлення на їхні персональні пристрої програм-вимагачів або використання вразливостей безпеки, притаманних програмам-месенджерам, і таким чином отримати несанкціонований доступ до пристрою жертви.

Вищезгадані атаки часто включали в себе передачу оманливих електронних повідомлень, які мали видимість автентичності, що походили від надійних суб'єктів, таких як фінансові установи або державні органи. Поширення HTML полегшило здійснення такої оманливої тактики. HTML — це повсюдна мова розмітки, яка полегшує створення веб-документів. У 1990-х роках кіберзлочинці почали використовувати мову гіпертекстової розмітки (HTML) для створення оманливих фішингових електронних листів, схожих на справжні повідомлення від авторитетних фінансових установ та інших організацій, яким довіряють. Використання HTML сприяло підвищенню переконливості електронних листів, тим самим підвищуючи ймовірність того, що користувачі здійснять такі дії, як перехід за посиланнями або розголошення особистої інформації, надання доступу

до облікових даних для входу в систему або отримання іншої не менш чутливої інформації.

У 1990-х роках з'явилася особлива форма атак на електронну пошту, що отримала назву "спам". Вона полягала у надсиланні великої кількості необґрунтованих електронних листів одержувачам без їхньої згоди. Часто виявлялося, що така кореспонденція рясніє оманливим або неправдивим змістом, починаючи від пропозицій підроблених товарів або послуг і закінчуючи проханнями про пожертвування на благодійні цілі, які були повністю фіктивними за своєю природою. Передача небажаних масових електронних повідомлень, широко відомих як спам, представляє додаткову і значну загрозу для користувачів, окрім простого роздратування. Це пов'язано з наявністю шкідливих кодів, таких як шкідливе програмне забезпечення або віруси, які можуть бути приховано вбудовані у вміст таких повідомлень. Перейшовши за гіперпосиланням або завантаживши вкладення, користувач може ненавмисно спровокувати активацію цих шкідливих кодів, що в кінцевому підсумку призведе до порушення роботи та безпеки його комп'ютерної системи.

У 1990-х роках кіберзлочинці використовували електронну пошту не лише для фішингу та спам-атак, але й як засіб поширення шкідливого програмного коду, який зазвичай називають шкідливим програмним забезпеченням, а також вірусів. Як ілюстрація, одним із можливих способів проникнення шкідливого програмного забезпечення на комп'ютер користувача є електронне повідомлення, яке містить пошкоджене вкладення, включаючи, але не обмежуючись, документи Word або PDF-файли. Якщо одержувач такого повідомлення вирішить отримати доступ до вкладеного файлу, шкідливе програмне забезпечення буде інстальоване в його систему.

На той час технологія Common Gateway Interface (CGI) широко використовувалася для створення динамічних веб-сторінок, які полегшували взаємодію з користувачем. Використання кіберзлочинцями CGI-скриптів уможливило створення підроблених сторінок для входу в систему, призначених для відомих веб-сайтів [6].

1.3 Аналіз фішингових атак як однієї з найбільш ефективних методик викрадення інформаційних активів організації.

Фішингові атаки є справжньою проблемою для людей та бізнесу. Цей вид атак включає в себе обман жертви з метою розкриття індивідуальних даних, таких як імена користувачів, паролі та дані кредитних карток, які її цікавлять. Згодом фішингові атаки стали більш успішними та складними для розпізнавання та припинення. Фішингові атаки можуть відбуватися за допомогою електронної пошти, соціальних мереж, інформування адміністрацій, телефонних дзвінків тощо. Цільовий фішинг, клон фішинг, «вішинг» та «смішинг» — ось кілька найпоширеніших видів фішингових атак.

Цільовий фішинг — це навмисна і цілеспрямована форма кібератаки, яка зосереджена на конкретних особах або організаціях. Зловмисники беруть участь у процесі збору відповідних даних про свої цілі, включаючи їхні назви, професійні позначення та ідентифікатори електронної пошти, які вони згодом використовують для створення спеціальних і переконливих електронних листів, що імітують електронну пошту, яка походить з надійного і достовірного джерела. Електронні повідомлення зазвичай містять гіперпосилання або вкладення, які після доступу до них приховано поширюють шкідливе програмне забезпечення на електронний пристрій одержувача, який нічого не підозрює, або перенаправляють його на фальшивий портал, призначений для отримання облікових даних для входу в систему.

Клон-фішинг — це цілеспрямована техніка фішингу, яка полягає в копіюванні справжньої електронної пошти або веб-сайту. Зловмисники копіюють електронну пошту або цифрове місцезнаходження, а потім вносять до них незначні зміни, перш ніж передати їх відповідній особі, на яку спрямована атака. Електронна пошта або онлайн-платформа, про яку йде мова, має вигляд справжньої, але після того, як одержувач переходить за гіперпосиланням або надає облікові дані для входу, дані беззастережно передаються зловмиснику.

«Вішинг» — це варіант фішингової атаки, спеціально спрямований на керівників високого рангу, а саме на генерального директора (CEO) та

фінансового директора (CFO). Зловмисники видають себе за надійну організацію, наприклад, корпоративного юриста або офіційну державну установу, і надсилають переконливі електронні повідомлення, які створюють відчуття терміновості або важливості. Зазначені електронні повідомлення часто містять гіперпосилання або вкладені файли, які після доступу до яких запускають шкідливе програмне забезпечення або перенаправляють жертву на фальшивий портал автентифікації, який незаконно отримує її облікові дані для входу [7].

Статистичні дані щодо кількості та типів атак, починаючи з 2000-х років, згідно зі звітом APWG, наведені в Таблиці 1.1 [8-9].

Фішингові атаки становлять значну загрозу для компаній, про що свідчить той факт, що 64% організацій стикалися з такими атаками протягом 2020 року. Збитки, завдані середнім та великим компаніям в результаті успішних фішингових атак, в середньому становлять $1,6 млн та до $14,8 млн відповідно. Вищезгадані атаки не мають особливих обмежень щодо цільових галузей або географічного розташування, при цьому найбільше вони поширені у фінансовому, медичному та виробничому секторах. Сполучені Штати, Великобританія та Індія — три країни, які повідомили про найбільшу кількість фішингових атак.

Сучасні дослідження показують, що фішингові зловмисники поступово вдосконалюють свої методи. Використання фішингових сайтів на основі HTTPS суттєво зросло на 220% у 2020 році. Крім того, в умовах пандемії COVID-19 зловмисники скористалися сплеском дистанційної роботи, щоб продовжити кібератаки. У 2020 році кількість фішингових атак з використанням інструментів, пов'язаних з COVID-19, зросла на вражаючі 600%.

Щоб зменшити ймовірність фішингових атак, необхідно підкреслити важливість профілактики та освіти. Сучасні підприємства можуть запровадити двофакторну перевірку, надати працівникам належну освіту щодо виявлення та повідомлення про шахрайські електронні листи, а також постійно оновлювати антивірусне програмне забезпечення, щоб захиститися від порушень безпеки. Як фізичні, так і юридичні особи повинні володіти знаннями про правові наслідки

фішингових атак, оскільки вони можуть призвести до значної фінансової та репутаційної шкоди.

Таблиця 1.1

Статистика фішингових атак

Рік	Кількість атак	Найбільш популярні типи атак
2005	173 063	Таргетований фішинг
2006	268 126	
2007	327 814	Фішинг в соц. Мережах
2008	335 965	Таргетований фішинг
2009	412 392	Фішинг в соц. Мережах
2010	313 517	Таргетований фішинг
2011	284 445	Фішинг електронної пошти
2012	320 081	Соціальна інженерія
2013	491 399	
2014	704 178	Фішинг електронної пошти
2015	1 413 978	
2016	1 313 771	Таргетований фішинг
2017	1 122 156	Фішинг електронної пошти
2018	1 040 654	Таргетований фішинг
2019	475 369	Фішинг електронної пошти
2020	1 031 347	Соціальна інжеренрія
2021	372 581	Фішинг даних карток

Висновок до розділу 1 — Історія фішингових атак включає в себе різні періоди, проте завжди існує загроза втрати інформації через хакерські атаки, а їх ефективність та кількість щороку зростають .

2 ДОСЛІДЖЕННЯ МЕТОДИК ФІШИНГОВИХ АТАК НА КОРПОРАТИВНУ МЕРЕЖУ ТА ВИЗНАЧЕННЯ ТИПОЛОГІЇ МЕТОДІВ ЗАХИСТУ ВІД НИХ

2.1 Дослідження можливих методів вирішення викрадення даних через фішингові атаки

З моменту перших спроб фішингу наприкінці 1990-х років існують різні стратегії захисту від цього виду атак, але темпи вдосконалення спочатку були скромними. Одним із перших кроків у запобіганні фішингу було навчання користувачів методам виявлення, ідентифікації та уникнення фішингу. Це було відповіддю на реальність, що найслабшою ланкою будь-якого рішення з безпеки завжди є кінцевий користувач. На початку 2000-х років кілька компаній почали проводити інформаційні кампанії, щоб навчити клієнтів, як виявляти фішингові електронні листи та веб-сайти й уникати їх. На цих курсах учасників навчали, як розпізнавати фальшиві електронні листи та веб-сайти, не переходити за посиланнями в сумнівних електронних листах і перевіряти веб-сайти. Щоб допомогти співробітникам розпізнавати фішингові електронні листи, знати, що робити, якщо вони отримали дивний лист, і повідомляти про будь-які фішингові атаки в ІТ-відділ, роботодавці можуть організувати для своїх працівників тренінги з е-безпеки. Освітні кампанії, які інформують як працівників, так і широку громадськість про небезпеку фішингових атак, є ще однією важливою стратегією підвищення обізнаності. Для інформування громадськості про численні спроби фішингу та про те, як їх уникнути, ці кампанії можуть використовувати брошури, буклети, фільми та інші засоби масової інформації. Глибшого розуміння проблеми можна досягти, створивши симулятори фішингу, щоб оцінити досвід персоналу. Під час таких симуляцій працівникам надсилають фальшиві фішингові електронні листи, щоб визначити, чи піддадуться вони на шахрайство, і повідомити про це свій ІТ-відділ. Крім того, компанії можуть розробити політику

для персоналу, яка описує найкращі практики безпеки електронної пошти і те, як реагувати на підозру в спробі фішингу [15].

Розробка чорних списків була ще однією формою захисту. «Чорний список» — це колекція відомих шкідливих IP-адрес, доменних імен, URL-адрес або адрес електронної пошти, які були заблоковані або позначені як потенційно небезпечні. Щоб визначити відоме джерело фішингової атаки, рішення для захисту електронної пошти, яке її отримує, аналізує адресу електронної пошти або доменне ім'я відправника на предмет наявності в чорному списку. Користувачі отримують попередження не відкривати і не відповідати на електронні листи, якщо адреса електронної пошти або веб-сайт відправника знаходяться в чорному списку, а сам лист заборонений або позначений як спам. Чорні списки допомагають боротися зі спробами фішингу, обмежуючи доступ до розпізнаних фішингових сайтів, запобігаючи ненавмисному переходу користувачів на ці сайти. Використовуючи дані користувачів для розпізнавання та повідомлення про підозрілу активність, компанії з безпеки електронної пошти та громадські організації часто покладаються на оновлення чорних списків у режимі реального часу. Чорні списки є чудовим методом захисту від відомих фішингових атак, але оскільки хакери постійно змінюють свої методи, щоб уникнути виявлення, вони можуть бути неефективними проти нових або нещодавно виявлених фішингових атак. Чорні списки найкраще використовувати в поєднанні з іншими заходами безпеки електронної пошти, включаючи фільтри спаму, антивірусне та антишкідливе програмне забезпечення, навчання персоналу та освітні кампанії, щоб створити багаторівневий захист від фішингових атак. Починаючи з 2000-х років, чорні списки є однією з основних ліній захисту для веб-браузерів. Наприклад, щоб визначити, чи є веб-сайт шкідливим, розробники браузерів все частіше використовують алгоритми машинного навчання та штучний інтелект для оцінки URL-адрес і вмісту веб-сайтів [16].

У міру того, як спроби фішингу вдосконалювалися технологічно, розроблялися нові тактики захисту. Однією з таких стратегій стало впровадження двофакторної автентифікації (2FA). Двофакторна автентифікація, або 2FA, яка

вводить додатковий рівень захисту облікових записів користувачів на додаток до пароля, є популярним методом запобігання спробам фішингу. Користувачі, які використовують 2FA, повинні надати дві форми автентифікації, такі як пароль і спеціальний код, згенерований додатком-автентифікатором або надісланий електронною поштою на телефон, щоб отримати доступ до свого облікового запису. Користувачів часто переконують розкрити свої дані для входу, включаючи пароль, у фішингових шахрайствах. Навіть якщо пароль користувача розкрито, отримати доступ до облікового запису набагато складніше за допомогою 2FA, оскільки зловмисникові все одно потрібно надати другу форму перевірки. Для реалізації 2FA можна використовувати SMS-коди, програми-автентифікатори, фізичні ключі безпеки та біометричну автентифікацію. Деякі рішення для захисту електронної пошти пропонують можливості 2FA для облікових записів електронної пошти, щоб гарантувати, що тільки авторизовані користувачі можуть отримати доступ до електронної пошти. Незважаючи на те, що 2FA є надійним захистом від фішингу, важливо пам'ятати, що вона не є бездоганною. Інші види біометричної автентифікації можуть бути вразливими до підроблених атак, а певні методи, такі як підробка SIM-карт, можуть обійти 2FA на основі SMS. Важливо використовувати 2FA разом з іншими заходами безпеки електронної пошти, щоб забезпечити багаторівневий захист від фішингових атак [17].

DMARC (Domain-based Message Authentication, Reporting, and Compliance — автентифікація, звітування та відповідність повідомлень на основі домену) дозволяє власникам доменів публікувати політики, які вказують постачальникам послуг електронної пошти, як обробляти повідомлення, що не пройшли автентифікацію. Поштовий сервер, який отримує повідомлення, звіряється з політикою DMARC домену відправника, щоб визначити, як його обробити. Якщо перевірка DMARC не пройшла успішно, політика може вказати поштовому провайдеру помістити повідомлення в карантин, відправити його в спам або повністю відхилити. Крім того, стандарти DMARC можуть містити інструкції щодо звітності, що дозволяє власникам доменів отримувати інформацію про

трафік електронної пошти, в тому числі про будь-яке незаконне використання їхніх доменів. Такий зворотній зв'язок може допомогти компаніям швидко виявляти спроби фішингу та зменшувати їхні наслідки. Підміна електронної пошти, коли зловмисник надсилає лист, який виглядає як лист від надійного відправника, але насправді є підробленою або фальшивою електронною адресою, є однією з головних переваг DMARC. Такі листи можуть бути ідентифіковані DMARC і заблоковані, не даючи їм потрапити до адресата, якому вони призначені, і потенційно викриваючи критичні дані. Загалом, DMARC є важливим інструментом для компаній, які бажають захистити свої електронні адреси від фішингових атак. DMARC пропонує надійний захист від спуфінгу та інших форм фішингу, дозволяючи власникам доменів встановлювати політики та отримувати зворотній зв'язок щодо активності електронної пошти. Останніми роками фішингові атаки стають дедалі легше виявляти та запобігати їм завдяки штучному інтелекту та машинному навчанню. Ці інструменти можуть аналізувати величезні обсяги даних і виявляти тенденції та аномалії, які можуть вказувати на фішингову атаку.

Раннє використання антифішингового програмного забезпечення було ще однією формою безпеки. Вивчаючи вміст електронних листів і веб-сторінок, було створено антифішингове програмне забезпечення для виявлення і припинення фішингових атак. Одним з його режимів роботи було сканування електронних листів і веб-сторінок на наявність термінів або фраз, які часто використовувалися у фішингових шахрайствах. Цей метод добре працював для зупинки відомих фішингових спроб, але він був непридатний для зупинки абсолютно нових або неідентифікованих атак. Антифішингове програмне забезпечення з часом вдосконалювалося і на сьогоднішній день використовує низку методів для виявлення та зупинки фішингових атак. Серед них:

Аналіз у режимі реального часу є ключовим компонентом багатьох антифішингових програм. Він передбачає безперервне сканування вхідних електронних листів та інших онлайн-повідомлень на наявність ознак фішингу і швидке визначення того, чи є вони справжніми або підробленими. Після

отримання електронного листа або іншого повідомлення антифішингове програмне забезпечення негайно перевіряє різні компоненти, включаючи адресу електронної пошти відправника, тіло повідомлення, а також будь-які посилання або вкладення. Програма порівнює цю інформацію з відомими методами фішингу та іншими ознаками шахрайства, такими як вірусні підписи, сумнівні IP-адреси та відомі фішингові URL-адреси. Програма ідентифікує повідомлення як можливе шахрайство і вживає заходів для захисту користувача, якщо виявляє підозрілу поведінку або вміст. Залежно від того, як налаштована програма, це може призвести до повного блокування повідомлення, поміщення його в карантин для подальшого розслідування або попередження користувача про те, що повідомлення може бути шахрайським, і рекомендації не переходити за посиланнями та не надавати жодної особистої інформації. Для того, щоб програмне забезпечення швидко та ефективно реагувало на можливі загрози, для захисту від фішингу необхідний аналіз у режимі реального часу. Програма може ідентифікувати та зупинити фішингові спроби, оцінюючи повідомлення в режимі реального часу до того, як вони можуть завдати шкоди, захищаючи людей та компанії від згубного впливу фішингових атак.

Підгалузь штучного інтелекту (ШІ) та комп'ютерних наук під назвою «машинне навчання» має на меті імітувати те, як люди навчаються, використовуючи дані та алгоритми, поступово підвищуючи їхню точність. Алгоритми машинного навчання можна використовувати в антифішинговому програмному забезпеченні для розпізнавання і припинення фальшивих електронних листів та інших онлайн-взаємодій. Великі масиви даних аналізуються за допомогою машинного навчання, щоб знайти закономірності та кореляції. У випадку з антифішинговим програмним забезпеченням дані можуть містити інформацію про відомі методи фішингу, фальшиві URL-адреси, сумнівні IP-адреси та інші ознаки шахрайства. Ці дані будуть проаналізовані системою машинного навчання, щоб знайти закономірності та зв'язки, які вказують на фішингові дії. Після навчання на цих даних алгоритм може бути використаний для виявлення та запобігання спробам фішингу в режимі реального часу.

Алгоритм може продовжувати навчатися і коригуватися при розробці нових стратегій і методів фішингу, підвищуючи свою ефективність з часом і випереджаючи нові загрози. Однією з головних переваг машинного навчання в антифішинговому програмному забезпеченні є те, що воно може розпізнавати і зупиняти фішингові атаки або атаки нульового дня, які раніше не були виявлені. Традиційні антифішингові стратегії часто покладаються на системи, засновані на правилах або чорних списках, які зловмисники можуть обійти, використовуючи нові стратегії або підходи. На противагу цьому, машинне навчання може виявити шаблони та зв'язки, які люди не можуть миттєво розпізнати, що дає змогу зупинити навіть найскладніші фішингові атаки [18].

Антифішингове програмне забезпечення використовує поведінковий аналіз як метод виявлення та припинення фішингових атак шляхом вивчення поведінки користувача. За допомогою цього методу відстежується активність користувачів і виявляються відхилення, які можуть вказувати на можливу фішингову атаку. Спочатку збираються дані про активність користувачів, наприклад, як часто вони відвідують певні програми або які електронні листи регулярно отримують. Потім, щоб знайти тенденції та відхилення, які можуть вказувати на фішинг, ці дані досліджуються за допомогою алгоритмів машинного навчання. Наприклад, програма поведінкового аналізу може визначити діяльність людини як підозрілу, якщо вона раптом починає отримувати багато листів від невідомих відправників або відвідувати дивні веб-сайти, і або повідомити про це користувача, або повністю припинити його активність. Контекстні дані, такі як місцезнаходження користувача або час доби, можуть бути включені в аналіз на основі поведінки для подальшого покращення та підвищення точності. Поведінковий аналіз може бути ефективним методом для запобігання спробам фішингу шляхом швидкої оцінки поведінки користувачів і швидкого пристосування до нових загроз. Однією з переваг поведінкового аналізу є те, що він може краще виявляти нові та витончені фішингові атаки, ніж звичайні методи, засновані на правилах. Поведінковий аналіз використовує алгоритми машинного навчання для пошуку тенденцій і відхилень, які можуть вказувати на спробу фішингу, а не застосовує заздалегідь

визначені критерії або чорні списки. Це дозволяє розпізнавати та запобігати спробам фішингу, які інші методи можуть пропустити. Загалом, поведінковий аналіз є важливим методом запобігання фішинговим атакам. Поведінковий аналіз може допомогти запобігти тому, щоб окремі особи та організації ставали жертвами таких атак, відстежуючи поведінку користувачів та оцінюючи її в режимі реального часу.

Програмне забезпечення для захисту від фішингу часто має функцію інтеграції з веб-браузерами. Це дозволяє програмному забезпеченню аналізувати веб-сайти та онлайн-контент під час їх відвідування через браузер, забезпечуючи захист від фішингових атак у реальному часі. Антифішингове програмне забезпечення, інтегроване з онлайн-браузером, може відстежувати поведінку користувачів і миттєво аналізувати веб-матеріали, щоб знайти ознаки фішингової активності. Наприклад, воно може перевіряти URL-адресу веб-сайту на наявність помилок або шукати ознаки підробленої сторінки входу, яка може бути використана для крадіжки облікових даних. Коли користувачі намагаються отримати доступ до відомого фішингового веб-сайту, антифішингове програмне забезпечення може забезпечити захист у режимі реального часу, а також сповіщення та попередження. Ці попередження, які можуть з'являтися у вигляді спливаючих вікон або сповіщень браузера, можуть зупинити користувачів від ненавмисного відвідування веб-сайтів, призначених для крадіжки їхньої особистої інформації.

Звертаючи увагу на ці вказівки, які можуть з'являтися у вигляді спливаючих вікон або сповіщень у браузері, користувачі можуть уникнути ненавмисного відвідування ризикованого веб-сайту. Ще одна перевага антифішингового програмного забезпечення, інтегрованого з веб-браузерами, полягає в тому, що воно може надати користувачам більше контексту та інформації, коли вони стикаються з сумнівним контентом. Наприклад, програма може запропонувати детальну інформацію про репутацію веб-сайту або поради щодо того, як бути в безпеці в Інтернеті. Антифішингові програми часто використовують плагіни або розширення для браузерів, які встановлюються на комп'ютер користувача для

взаємодії з веб-браузерами. Щоб ці розширення працювали коректно, користувачам може знадобитися надати певні права або змінити налаштування.

2.2 Дослідження ринку програмного забезпечення націленого на захист корпоративної пошти.

Серед описаних раніше засобів захисту інформації можна звернути особливу увагу на автоматизовані програмні комплекси для захисту корпоративної пошти. Корпоративна електронна пошта вважається важливим інструментом комунікації для компаній будь-якого розміру. Це основний засіб, за допомогою якого співробітники обмінюються інформацією, співпрацюють над проектами та спілкуються з клієнтами і постачальниками. Однак в зв'язку з кількістю інформації що проходить черех неї, пошта є й найбільш важдивою ціллю атаки для кіберзлочинців, які прагнуть отримати доступ до конфіденційних корпоративних даних або організувати фішингові атаки або надіслати шкідливе програмне забезпечення. Для захисту корпоративної електронної пошти від цих загроз існують програмні рішення, що розроблені для запобігання несанкціонованому доступу, виявлення та блокування шкідливих електронних листів, а також для забезпечення інших функцій безпеки.

Першим кроком у дослідженні програмних рішень для захисту корпоративної електронної пошти є визначення ключових необхідних функцій. Сюди входять такі функції, як шифрування електронної пошти, захист від фішингу та шкідливих програм, фільтрація спаму, архівування електронної пошти та запобігання втраті даних. Конкретні потреби організації та вимоги до відповідності визначатимуть, які функції є важливими.

Програмні рішення для захисту корпоративної електронної пошти можуть варіюватися від базових до просунутих, з відповідним діапазоном цін. Визначення бюджету має вирішальне значення для звуження доступних варіантів і вибору найкращого рішення, яке відповідає фінансовим можливостям організації. Серед вибору цін може бути присутній варіант обрати безкоштовне ПЗ. Безкоштовному програмному забезпеченню для захисту електронної пошти може бракувати

важливих функцій і можливостей, необхідних для захисту корпоративної електронної пошти від складних кіберзагроз. Наприклад, воно може не мати сучасних функцій, таких як алгоритми машинного навчання, шифрування електронної пошти, запобігання втраті даних та інших важливих заходів безпеки. Іншим недоліком можна вважати відсутність регулярних оновлень, технічної підтримки та обслуговування, що робить його вразливим до нових загроз. Це може призвести до значних прогалин у захисті, якими можуть скористатися кіберзлочинці.

Після звуження кола доступних рішень слід оцінити кожне з них на відповідність конкретним потребам і вимогам підприємства. Це передбачає тестування функціональності, зручності використання, продуктивності та сумісності програмного забезпечення з наявною інфраструктурою. Це може включати перевірку концепції, перегляд технічної документації та розмови з представниками постачальника.

Провівши загальний розгляд ринку, серед фаворитів в сфері забезпеченні безпеки корпоративної пошти можна виділити наступні продукти:

1. Microsoft 365 Defender — це хмарне рішення для забезпечення безпеки, яке надає комплексний набір засобів захисту від широкого спектра загроз для електронної пошти, кінцевих точок, ідентичностей і хмарних додатків.

Точки захисту:

- кінцеві точки за допомогою Defender
- активи за допомогою Defender Vulnerability Management
- електронна пошта та співпраця
- захист ідентичностей і Azure Active Directory (Azure AD)
- програми з Microsoft Defender для хмарних додатків

Переваги:

- комплексний захист: Microsoft 365 Defender забезпечує комплексний підхід до захисту, який охоплює електронну пошту, кінцеві точки, ідентичності та

хмарні програми, що робить його єдиним рішенням для всіх потреб у сфері безпеки.

- інтеграція з Microsoft 365: Оскільки Microsoft 365 Defender є продуктом корпорації Майкрософт, він легко інтегрується з іншими службами Microsoft 365, що спрощує його налаштування та керування.
- удосконалений захист від загроз: Microsoft 365 Defender використовує передові засоби захисту від загроз, зокрема штучний інтелект і машинне навчання, щоб виявляти загрози та реагувати на них у режимі реального часу, знижуючи ризик витоку даних.
- зручне керування: Microsoft 365 Defender надає централізовану консоль керування, яка дає змогу адміністраторам керувати всіма аспектами безпеки, зокрема політиками, оповіщеннями та усуненням загроз.

Недоліки:

- обмежена інтеграція зі сторонніми програмами: Хоча Microsoft 365 Defender добре інтегрується з іншими службами Microsoft, він може не так легко інтегруватися зі сторонніми рішеннями для захисту.
- обмежені можливості налаштування: Microsoft 365 Defender надає стандартний набір політик безпеки, але він може не дозволяти широко налаштувати ці політики, що може бути недоліком для організацій з унікальними вимогами до безпеки.
- вартість: Microsoft 365 Defender може бути дорогим для невеликих організацій або організацій з обмеженим бюджетом, особливо якщо їм потрібні додаткові функції, які не входять до базового пакета.
- обмежений контроль: Microsoft 365 Захисник — це хмарна служба, а це означає, що організації можуть мати обмежений контроль над своїми даними та політиками безпеки.

2. Proofpoint Email Protection — що позиціонується як провідний у галузі поштовий шлюз, який можна розгорнути як хмарний сервіс або локально, що

забезпечує захист від різних загроз електронної пошти, таких як фішинг, шкідливе програмне забезпечення та спам.

Точки захисту:

- захист від спаму та фішингу, знижуючи ризик шахрайства та кіберзагроз через електронну пошту.
- захист URL-адрес завдяки скануванню URL-адрес в електронних листах, щоб виявити і заблокувати шкідливі посилання, знижуючи ризик ненавмисного переходу користувачів на небезпечні посилання.
- захист через сканування вкладення електронної пошти на наявність шкідливого програмного забезпечення та інших загроз, не дозволяючи користувачам відкривати або завантажувати шкідливі файли.
- Proofpoint Email Protection надає функції запобігання втраті даних, які дозволяють організаціям виявляти і захищати конфіденційні дані, знижуючи ризик витоку даних і порушень нормативних вимог.

Переваги:

- удосконалений захист від загроз завдяки передовим технологіям, таким як машинне навчання та штучний інтелект, для виявлення та реагування на загрози в режимі реального часу, знижуючи ризик атак через електронну пошту.
- легка інтеграція з різними поштовими платформами, такими як Microsoft Office 365, Exchange і Google Workspace, що робить його простим у налаштуванні та управлінні.
- Proofpoint Email Protection надає можливості шифрування, які дозволяють організаціям захистити свої конфіденційні дані та забезпечити відповідність галузевим нормам.
- просте керування чкркз централізовану консоль управління, яка дозволяє адміністраторам керувати всіма аспектами безпеки електронної пошти, включаючи політики, оповіщення та виправлення.

Недоліки:

- вартість: Proofpoint Email Protection може бути дорогим для невеликих організацій або організацій з обмеженим бюджетом, особливо якщо їм потрібні додаткові функції за межами базового пакету, та відсутність тестового періоду для ознайомлення з функціоналом ПЗ
- обмежена гнучкість налаштувань: ПЗ надає стандартний набір політик безпеки, але не дозволяє широко налаштовувати ці політики, що може бути недоліком для організацій з унікальними вимогами до безпеки.
- хибні спрацьовування: Proofpoint Email Protection може генерувати хибні спрацьовування, що може спричинити незручності та розчарування користувачів.

3. BrandShield Anti-Phishing: надає повну карту цифрових загроз, здійснюючи моніторинг Інтернету, включаючи соціальні мережі, для виявлення фішингових сайтів і сторінок, видачі себе за іншу особу та шахрайства в Інтернеті. Наші послуги з усунення загроз ефективні та швидкі, прозорі для вас у будь-який час.

Точки захисту:

- BrandShield Anti-Phishing забезпечує захист від фішингових атак, спрямованих на бренд організації, знижуючи ризик репутаційних та фінансових втрат.
- моніторинг доменів відстежує домени та виявляє несанкціоноване використання бренду або торгових марок організації, знижуючи ризик зловживання брендом.
- ПЗ відстежує платформи соціальних мереж і виявляє шахрайські акаунти, які використовують бренд організації для проведення фішингових атак, знижуючи ризик атак соціальної інженерії.
- моніторинг мобільних додатків виявляє шахрайські мобільні додатки, які використовують бренд організації для проведення фішингових атак, знижуючи ризик мобільних загроз.

Переваги:

- комплексні можливості захисту бренду, які допомагають організаціям виявляти та запобігати фішинговим атакам, націленим на їхній бренд.
- BrandShield Anti-Phishing використовує передові технології машинного навчання та штучного інтелекту для виявлення та запобігання фішинговим атакам, знижуючи ризик шахрайства через електронну пошту та кіберзагроз.
- легка інтеграція з різними поштовими платформами та веб-браузерами, що полегшує його налаштування та керування.
- сповіщення в режимі реального часу дозволяє організаціям швидко реагувати на фішингові атаки та захищати свій бренд.

Недоліки:

- вартість: BrandShield Anti-Phishing може бути дорогим для невеликих організацій або організацій з обмеженим бюджетом, особливо якщо їм потрібні додаткові функції за межами базового пакету.
- обмежене налаштування: ПЗ надає стандартний набір політик безпеки, але може не дозволяти широко налаштовувати ці політики, що може бути недоліком для організацій з унікальними вимогами до безпеки.
- хибні спрацьовування: BrandShield Anti-Phishing може генерувати хибні спрацьовування, що може спричинити дискомфорт і невдоволення користувачів.

4. Cisco Secure Email Threat Defense — розширений захист електронної пошти, що захищає співробітників та організацію, одночасно розширюючи можливості реагування на загрози.

Точки захисту:

- захист URL-адрес і вкладень: Cisco Secure Email Threat Defense сканує URL-адреси та вкладення електронної пошти на наявність шкідливого програмного забезпечення та інших загроз, запобігаючи відкриттю або завантаженню шкідливих файлів.

- автентифікація електронної пошти: ПЗ використовує різні методи автентифікації електронної пошти, такі як SPF, DKIM і DMARC, щоб запобігти підробці та імітації електронної пошти.
- захист на основі поведінки: Cisco Secure Email Threat Defense використовує поведінкову аналітику для виявлення та запобігання атакам на основі електронної пошти, які не можуть бути виявлені традиційними методами на основі підписів.
- розширена аналітика загроз: Cisco Secure Email Threat Defense використовує аналітику загроз Talos від Cisco, щоб надавати інформацію про загрози в режимі реального часу та захищати від нових загроз.

Переваги:

- удосконалений захист від загроз: Cisco Secure Email Threat Defense використовує передові технології, такі як машинне навчання, штучний інтелект і поведінкова аналітика, для виявлення та реагування на загрози в режимі реального часу, знижуючи ризик атак через електронну пошту.
- інтегрований захист: Cisco Secure Email Threat Defense є частиною платформи Cisco SecureX, яка забезпечує комплексну архітектуру безпеки, що інтегрується з іншими продуктами Cisco, забезпечуючи більш повне рішення безпеки.
- просте керування: Програмен рішення надає централізовану консоль управління, яка дозволяє адміністраторам керувати всіма аспектами безпеки електронної пошти, включаючи політики, оповіщення та усунення.
- шифрування електронної пошти: Cisco Secure Email Threat Defense надає можливості шифрування, які дозволяють організаціям захистити свої конфіденційні дані і забезпечити відповідність галузевим нормам.

Недоліки:

- вартість: Cisco Secure Email Threat Defense може бути дорогим для невеликих організацій або організацій з обмеженим бюджетом, особливо якщо їм потрібні додаткові функції за межами базового пакету.

- складність: Розширені функції та інтеграційні можливості Cisco Secure Email Threat Defense також можуть зробити його складнішим у впровадженні та управлінні великими організаціями.

Унікальні технології:

- SecureX що забезпечує узгоджену, вбудовану роботу з усіма продуктами, та дозволяє:
  - автоматизовувати завдання
  - подання результатів в єдиній формі
  - інвентаризація пристрохв
  - єдиний вхід з всіх додактів Cisco
- Cisco Secure Cloud Analytics що підтримує:
  - автоматичне виявлення загроз
  - автоматизовані сповіщення про загрози
  - шібридну мережеву безпеку

Висновок до розділу 2 — Ринок програмного забезпечення надає широкий спектр варіантів захисту від різних типів шахрайських атак, в тому числі від фішингових листів.

3 ПРИКЛАДНЕ ВИРІШЕННЯ ПИТАННЯ ФШИНГОВИХ АТАК ТА ВИЗНАЕННЯ ВЕКТОРУ МОЖЛИВОГО ВИРІШЕННЯ ПРОГРАМНИМИ ТА ОРГАНІЗАЦІЙНИМИ МЕТОДАМИ

3.1 Розгортання програмного засобу Cisco Secure Email Threat Defense та особливості експлуатації

Як вже було сказано раніше, Cisco Secure Email Threat Defense — це дуже потужне хмарне рішення для захисту електронної пошти, яке пропонує неперевершений захист від різноманітних шкідливих загроз, таких як фішинг, шкідливе програмне забезпечення та атаки з вимогою викупу. Однією з його головних переваг є те, що ця передова технологія базується на хмарній архітектурі, яка пропонує низку переваг для компаній будь-якого розміру. Завдяки тому, що Cisco Secure Email Threat Defense базується на хмарних технологіях, процедура впровадження, зокрема, значно відрізняється від традиційних рішень. Передбачається, що ця спрощена процедура розгортання буде більш ефективною та результативною, дозволяючи компаніям швидко і просто інтегрувати рішення в свою поточну інфраструктуру. Використовуючи можливості хмарних технологій, Cisco Secure Email Threat Defense є високомасштабованим і адаптованим рішенням, яке можна легко пристосувати до конкретних потреб і вимог будь-якого підприємства. Cisco Secure Email Threat Defense, при правильному впровадженні та налаштуванні, є найкращим варіантом для захисту вашої компанії від новітніх загроз електронної пошти, незалежно від розміру організації.

Початок роботи з Cisco Secure Email Threat Defense починається з веб-сайту де можна ознайомитись з продуктом. Вигляд сайту наведений на Рис 3.1.

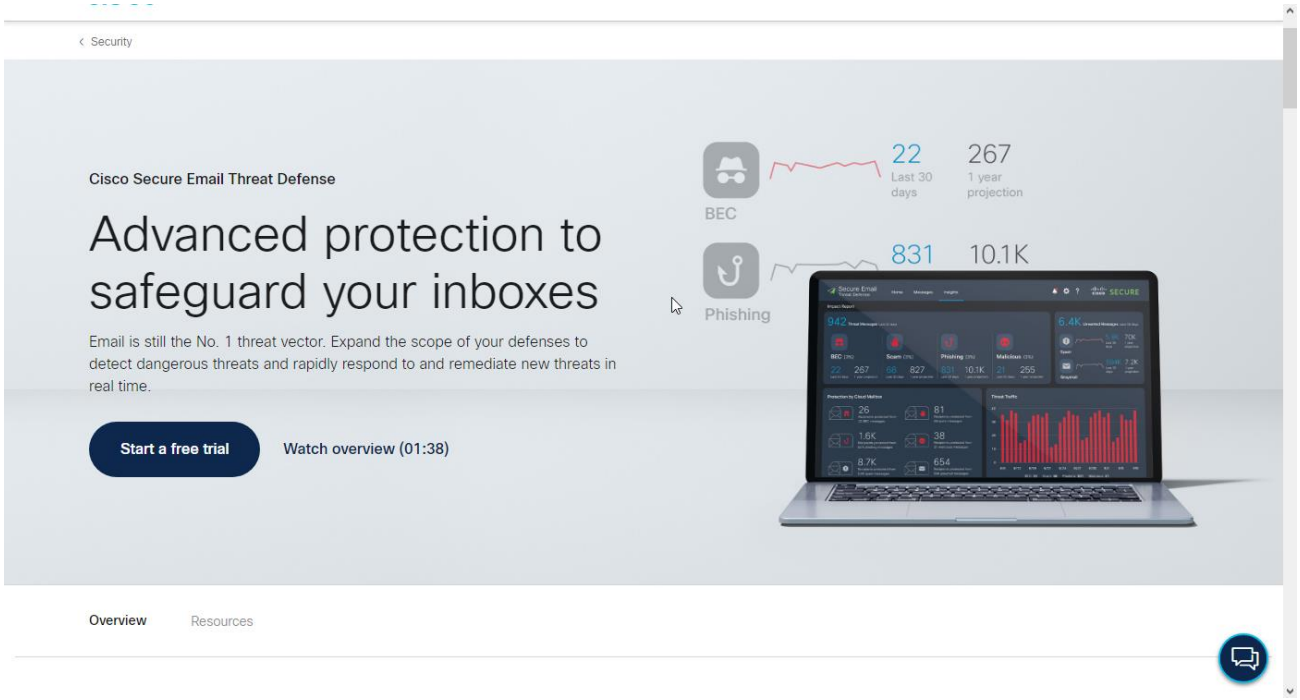

Рис. 3.1. Ознайомча сторінка Cisco Secure Email Threat Defense

Надаючи тимчасову демо-версію, Cisco пропонує практичне рішення, яке дозволяє кожному співробітнику підприємства ознайомитися з продуктом. Це дає змогу ретельно дослідити та оцінити продукт, перш ніж прийняти рішення про його купівлю. Персонал технічної підтримки Cisco постійно готовий запропонувати допомогу та відповіді у разі виникнення будь-яких нагальних технічних проблем. Крім того, завжди є можливість перейти на більш просунуту версію продукту, якщо тимчасової демо-версії недостатньо для потреб вашої організації. Таким чином, ви можете бути впевнені, що ваша компанія отримає доступ до найновіших і найсучасніших функцій і можливостей Cisco. Cisco прагне забезпечити найкращий користувацький досвід та підтримку, щоб задовольнити потреби клієнтів. Різниця між версіями наведена в таблиці 3.1.

Таблиця 3.1.

Пакети «Secure Email»

Можливості програмного забезпечення	“Secure Email Essentials”	“Secure Email Advantage”	“Secure Email Premier”
Антиспам, репутація домену відправника та URL-фільтрація	+	+	+
Фільтри для запобігання проривам	+	+	+
Антивірус	+	+	+
Безпечний захист електронної пошти від шкідливого програмного забезпечення та аналітика	Присутня обмежена версія	Присутня обмежена версія	Присутня обмежена версія
Cisco SecureX	+	+	+
Виявлення шантажу	+	+	+
Запобігання втраті даних	Лише з додатком	+	+
Послуга безпечного шифрування електронної пошти	Лише з додатком	+	+
Безпечна відписка	Лише з додатком	+	+
Ознайомчий тренінг з безпеки**	Лише з додатком	Лише з додатком	+
Безпечний захист від загроз електронної пошти	Лише з додатком	Лише з додатком	Лише пошта Microsoft365
Безпечний захист домену електронної пошти**	Лише з додатком	Лише з додатком	Лише з додатком
Інтелектуальне мультисканування**	Лише з додатком	Лише з додатком	Лише з додатком
Аналізатор зображень**	Лише з додатком	Лише з додатком	Лише з додатком
"McAfee" - захист від шкідливого програмного забезпечення	Лише з додатком	Лише з додатком	Лише з додатком

Продовження таблиці 3.1

Пакети «Secure Email»

Можливості програмного забезпечення	“Secure Email Essentials”	“Secure Email Advantage”	“Secure Email Premier”
Керування безпечною електронною поштою Cisco*	Лише з додатком	Лише з додатком	Лише з додатком

* — Потрібно лише для локальних та гібридних ліцензій. Входить до складу хмарних ліцензій.

** — Можна придбати як окремі пропозиції.

Ознайомившись з різними доступними планами підписки, ви можете продовжити процес реєстрації, щоб отримати тимчасову 30-денну ознайомчу ліцензію на програмний продукт, що дозволяє вам отримати практичний досвід і розуміння функціональності та можливостей програмного продукту перед тим, як оформити довгострокову підписку. Сторінку реєстрації можна побачити на Рис. 3.2.

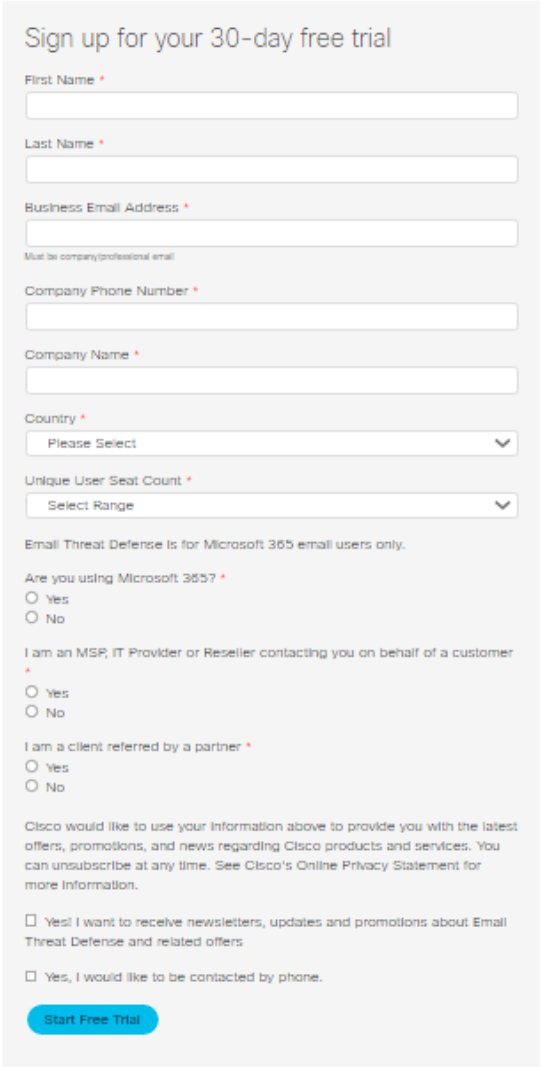

Рис. 3.2. Вигляд форми заповлення для контакту служби підтримки Cisco

Оскільки рішення Cisco для захисту корпоративних мереж створені для того, щоб задовольняти складні та комплексні вимоги організацій до безпеки, важливо усвідомлювати, що для реєстрації та подачі заявок необхідно використовувати корпоративну адресу електронної пошти. Варто усвідомлювати суттєві відмінності між особистим обліковим записом електронної пошти та корпоративною електронною адресою. Особиста електронна адреса часто використовується для персональної взаємодії, зокрема для спілкування в соціальних мережах, листування та здійснення покупок в Інтернеті. Зазвичай вона пов'язана з особовим обліковим записом людини. Корпоративна електронна адреса, з іншого боку, надається роботодавцем і призначена лише для

внутрішнього ділового листування. Корпоративні адреси електронної пошти зазвичай обслуговуються IT-відділом вашої компанії, і на них поширюються особливі правила безпеки та контролю за дотриманням нормативних вимог для захисту від кібератак і захисту конфіденційних даних. Реєструючись на рішення Cisco для захисту корпоративних мереж з використанням корпоративної адреси електронної пошти, компанії можуть забезпечити повний контроль над своєю інфраструктурою безпеки, відстежувати, як рішення використовується всередині компанії, і впроваджувати необхідні політики і процедури безпеки для захисту своїх даних і активів.

Після заповнення форми впродовж певного часу на вашу електронну пошту звернеться менеджер компанії Cisco проінформувавши про успішність надання ознайомчої версії чи відмову. У випадку успіху буде надано посилання на внутрішній сервіс компанії Cisco - SecureX. Вигляд вікна реєстрації на Рис 3.3.

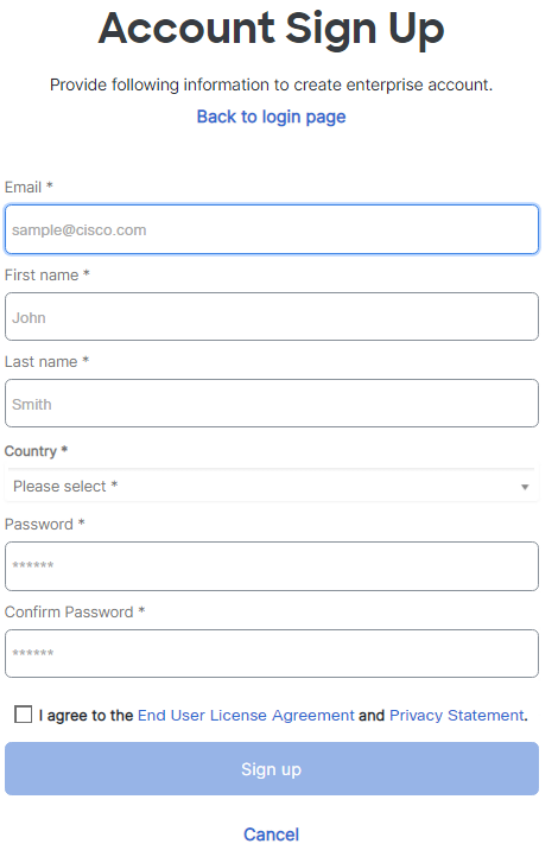

Рис. 3.3. Форма реєстрації в Cisco SecureX

Складність пароля та обрана адреса електронної пошти є двома важливими факторами при заповненні необхідних форм для реєстрації користувача. Пароль повинен відповідати ряду вимог, зокрема мати довжину не менше 8 символів і включати щонайменше одну цифру, одну малу літеру та одну велику літеру. З метою запобігання несанкціонованому доступу та захисту від кібернетичних загроз, пароль також не повинен містити літер, цифр або інших символів з імені, прізвища або адреси електронної пошти користувача. Дотримуючись цих рекомендацій і використовуючи надійний, унікальний пароль, користувачі можуть значно знизити ймовірність того, що їхній обліковий запис буде зламано, а конфіденційна інформація стане надбанням громадськості.

Після заповнення всіх необхідних полів система покаже спливаюче вікно з проханням встановити багатофакторну автентифікацію (MFA). Змушуючи користувачів вводити додаткову перевірку на додаток до пароля, цей крок забезпечує додатковий рівень захисту процесу входу в систему. MFA можна налаштувати за допомогою спеціального додатку та номера телефону. Навіть якщо їхній пароль буде зламано, користувачі можуть бути впевнені, що тільки авторизовані особи зможуть отримати доступ до їхнього облікового запису, встановивши MFA. MFA відіграє важливу роль у запобіганні небажаному доступу та забезпеченні безпеки і конфіденційності конфіденційних даних, що є надзвичайно важливим у сучасному цифровому світі, де кіберзагрози постійно змінюються. Вигляд на Рис. 3.4.

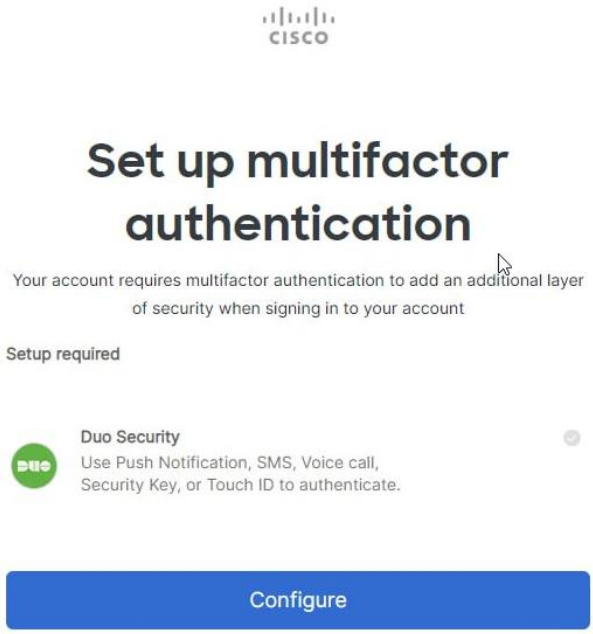

Рис. 3.4. Налаштування мультифакторної аутентифікації

Користувачі системи SecureX повинні використовувати або Push-повідомлення, або спеціальний код, який відображається у вікні додатку на смартфоні при кожній наступній спробі входу в систему після успішного завершення процесу верифікації телефону та встановлення додатку для підтвердження входу в систему. Цей додатковий рівень безпеки має важливе значення для запобігання прогалин у системі безпеки та незаконного доступу до системи SecureX. Cisco знижує ризик витоку даних і кібератак, застосовуючи ці складні методи аутентифікації, щоб гарантувати, що доступ до системи отримають лише авторизовані користувачі. Підтверджуючи, що користувачі мають фізичний доступ до свого зареєстрованого смартфону і що він не перебуває у володінні сторонніх осіб, метод push-повідомлень або унікального коду забезпечує додатковий рівень захисту. Таким чином, Cisco може надати своїм клієнтам високонадійне і безпечне рішення для захисту їх безцінних даних і гарантувати безперервність бізнесу. Вигляд на Рис. 3.5

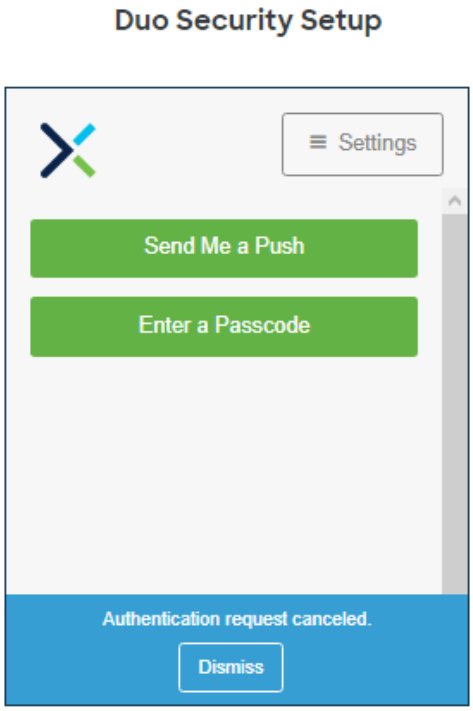

Рис. 3.5. Вигляд вікна вибору типу підтвердження особистості

Після налаштування основних функцій безпеки для доступу до системи SecureX вас буде перенаправлено на портал додатків SecureX - комплексний сервіс, який об'єднує всі додатки Cisco Security в єдину інтегровану платформу. За допомогою цього креативного рішення користувачі можуть легко і зручно отримати доступ до широкого спектру продуктів і послуг безпеки з одного місця.

Користувачі можуть легко отримати доступ до будь-яких додатків Cisco Security, на які вони підписалися, в межах одного підприємства, використовуючи портал додатків SecureX, який діє як центральний вузол. Об'єднавши всі програми в єдиному обліковому записі, користувачі можуть оптимізувати свої операції з безпеки і зменшити складність обслуговування різних систем. Користувачі можуть краще розуміти можливі ризики і вразливості в архітектурі безпеки своєї організації завдяки єдиному баченню загроз безпеки на порталі SecureX Application Portal.

Користувачі можуть скористатися різноманітними передовими функціями та можливостями безпеки, включаючи виявлення загроз, реагування на інциденти

та аналітику безпеки, серед іншого, за допомогою Порталу додатків SecureX. Використовуючи цю надійну платформу, компанії можуть посилити свою систему безпеки, підвищити стійкість до кібератак і захистити свої безцінні дані та активи від можливих порушень. Вигляд панелі на Рис. 3.6.

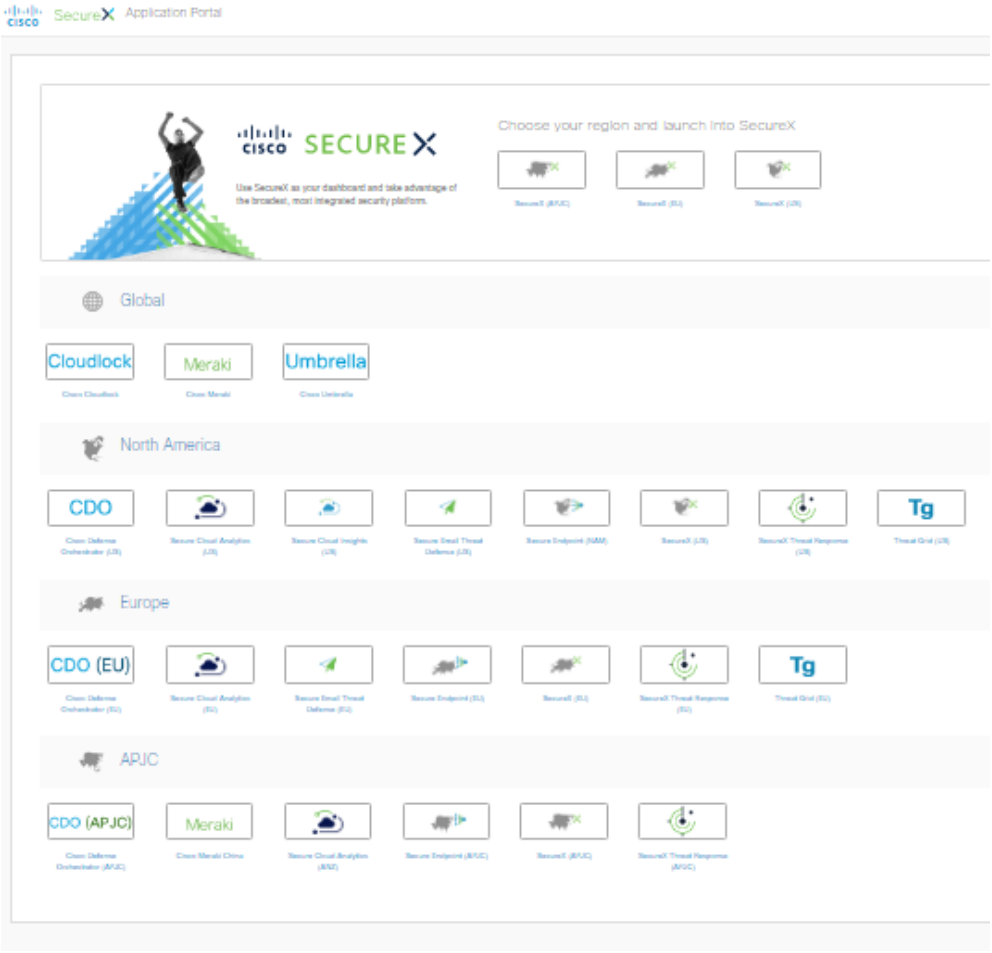

Рис. 3.6. Вигляд центру доступу SecureX

Визначення того, чи встановлено захищений шлюз електронної пошти (SEG) в поштовій системі користувача, є одним з основних процесів, необхідних для налаштування Secure Email Threat Defense (SETD). SEG на платформі SETD є важливим компонентом, який виступає першою лінією захисту від атак через електронну пошту. До її обов'язків входить перевірка вхідного та вихідного електронного трафіку, виявлення можливих небезпек і запобігання потраплянню шкідливих листів до поштової скриньки користувача.

SEG аналізує вміст електронної пошти, вкладення, посилання та інформацію про відправника, використовуючи найсучасніші алгоритми та дані

про загрози, щоб вирішити, чи є електронний лист безпечним чи небезпечним. Залежно від ймовірної загрози, SEG може помістити повідомлення в карантин, заблокувати або передати його службі безпеки користувача для додаткового розслідування.

Налаштування SETD передбачає з'єднання двох платформ, щоб гарантувати безперебійну інтеграцію та максимальну продуктивність, якщо SEG вже встановлено в поштовій системі користувача. Конфігурація SEG і SETD буде покроково пояснена користувачам, щоб вони могли скористатися всіма можливостями і функціями, доступними на платформі SETD.

Використовуючи можливості SEG та SETD, організації можуть значно покращити рівень безпеки електронної пошти та захистити свої важливі дані й активи від різноманітних кіберзагроз. Вигляд на Рис. 3.7.

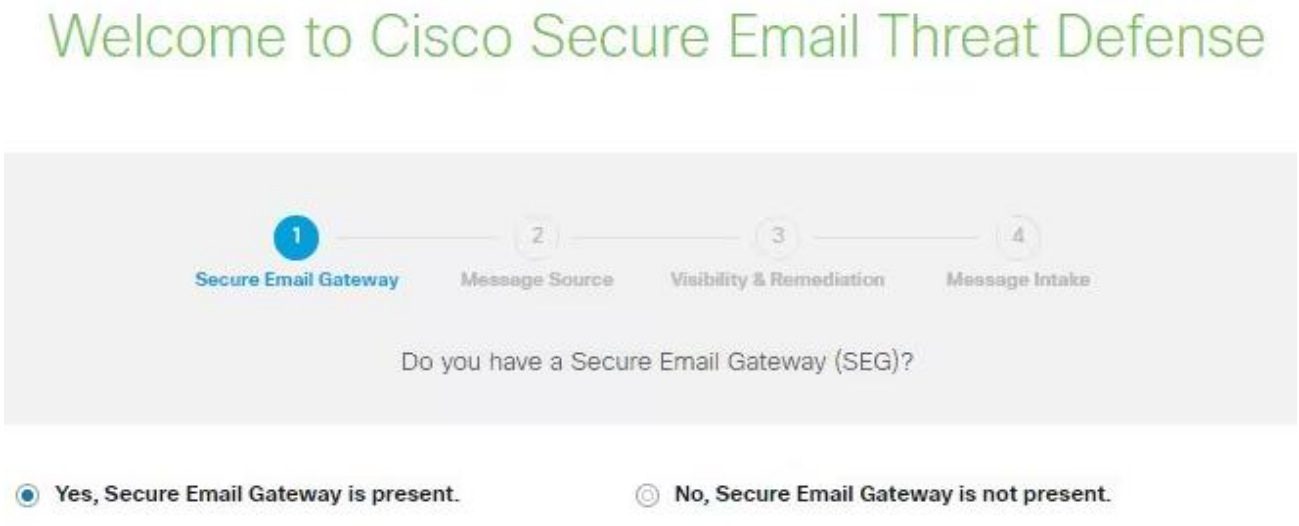

Рис. 3.7. Вікно вибору налаштування SEG

Після налаштування SEG, якщо обрано відсутніть такого, SETD запропонує обрати видимість та виправлення

Режим видимості та виправлення визначає тип політики виправлення, яку ви можете застосувати.

- Читання/запис — Дозволяє переглядати та виправляти на вимогу або автоматично (тобто переміщати або видаляти підозрілі повідомлення). Дозволи на читання/запис буде запитано в Microsoft 365.
- Читання — Дозволяє лише перегляд, але не виправлення. У Microsoft 365 буде запитано дозволи лише на читання.

Якщо обрано Читання/Запис, необхідно буде ввімкнути політику автоматичного виправлення в налаштуваннях політики після завершення налаштування. Щоб застосувати автоматичне виправлення до всіх внутрішніх електронних листів потрібно щоб в полі «Застосовувати автоматичне виправлення до доменів, яких немає в списку доменів» на сторінці політики встановлено відповідний прапорець

- Без автентифікації — доступний, якщо Cisco SEG використовується як джерело повідомлень. Він забезпечує лише видимість, а виправлення повідомлень буде недоступне.

Далі необхідно авторизуватись в поштовому сервісі Microsofr 365 з правами адміністратора.

Наступним кроком налаштування буде встановлення коректних налаштувань пошти. В залежності від налаштувань SEG існує 2 сценарія налаштування:

Перший сценарій: Для користувачів із захищеним шлюзом електронної пошти (SEG) : Потрібно додати коннектор у Microsoft 365.

Щоб журнали надсилалися безпосередньо з Microsoft 365 до Secure Email Threat Defense, не проходячи через шлюз, рекомендуємо додати в Microsoft 365 коннектор вихідних даних. Коннектор потрібно додати до того, як ви налаштуєте ведення журналів.

В Центрі адміністрування Microsoft 365 Exchange створіть новий коннектор, використовуючи такі параметри в майстрі додавання коннектора:

- Підключення з : Office 365
- Підключення до : Організація-партнер

- Ім'я коннектора : Вихідний до Cisco Secure Email Threat Defense
- Використання коннектора : Тільки коли повідомлення електронної пошти надсилаються на ці домени (додайте mail.cmd.cisco.com)
- Маршрутизація : Використовувати MX-запис, пов'язаний з доменом партнера
- Обмеження безпеки : Завжди використовуйте безпеку транспортного рівня (TLS) для захисту з'єднання (рекомендується); Виданий надійним центром сертифікації (ЦС)
- Email для перевірки : Адреса вашого журналу зі сторінки налаштування Secure Email Threat Defense

Перевірка з'єднання може не спрацювати, якщо у користувачів O365 вже налаштовано умовну маршрутизацію пошти за допомогою транспортного правила Exchange для перенаправлення вихідної пошти на наявне з'єднання. Хоча повідомлення журналу є системними привілеями і на них не впливають транспортні правила, тестовий лист перевірки коннектора не є привілейованим і на нього впливають транспортні правила.

Щоб вирішити цю проблему з перевіркою, слід знайти попереднє транспортне правило і додати виняток для адреси журналу Secure Email Threat Defense. Після того, як зміни набудуть чинності, необхідно повторити перевірку нового з'єднувача.

Другий сценарій: Налаштування Microsoft 365 для надсилання журналів до Secure Email Threat Defense. Для цього необхідно додати правило для журналу.

Необхідно скопіювати адресу журналу зі сторінки налаштування Secure Email Threat Defense. Якщо потрібно повторити цей процес пізніше, то адресу журналу також можна знайти на сторінці «Адміністрування».

На порталі відповідності Microsoft Purview: https://compliance.microsoft.com/homepage Треба перейти в розділі Рішення > Керування життєвим циклом даних > Exchange (застарілі) > Правила журналу.

Якщо цього ще не зроблено то потрібно додати одержувача Exchange у полі «Надсилати недоставлені звіти журналу до», а потім натиснути кнопку «Зберегти».

Кнопку «+» на сторінці «Правила журналу» щоб створити нове правило журналу.

Потрібно вставити адресу журналу зі сторінки налаштування Secure Email Threat Defense у поле Надсилати звіти журналу до.

У полі Ім'я правила журналу — Cisco Secure Email Threat Defense.

У розділі Журнал повідомлень, надісланих або отриманих від — «Усі».

У розділі Тип повідомлення для журналу — «Усі повідомлення».

Потрібно перевірити вибрані варіанти, а потім натиснути кнопку «Надіслати», щоб завершити створення правила.

Також важливим кроком буде налаштування джерела повідомлень шлюзу

- Якщо обрано шлюз як джерело повідомлень, треба увімнути коннектор захисту від загроз шлюзу Cisco Secure Email Cloud Gateway, щоб надсилати повідомлення до Secure Email Threat Defense. Для цього потрібно:
- Потрібно скопіювати адресу отримання повідомлень зі сторінки налаштування Secure Email Threat Defense. Якщо вам потрібно повторити цей процес пізніше, ви можете знайти свою адресу отримання повідомлень на сторінці Адміністрування.
- В інтерфейсі Secure Email Cloud Gateway виберіть Служби безпеки > Коннектор захисту від загроз.
- Установити прапорець «Увімкнути коннектор захисту від загроз».
- Далі необхідно ввести адресу отримання повідомлень, яку було скопійовано з «Secure Email Threat Defense».
- Натиснувши кнопку «Надіслати, щоб зберегти зміни» можна повернутись на сторінку налаштування та переглянути політику

Після цього базові налаштування Secure Email Threat Defense завершено та можна перейти до інтерфейсу SETD. Вигляд на Рис. 3.8.

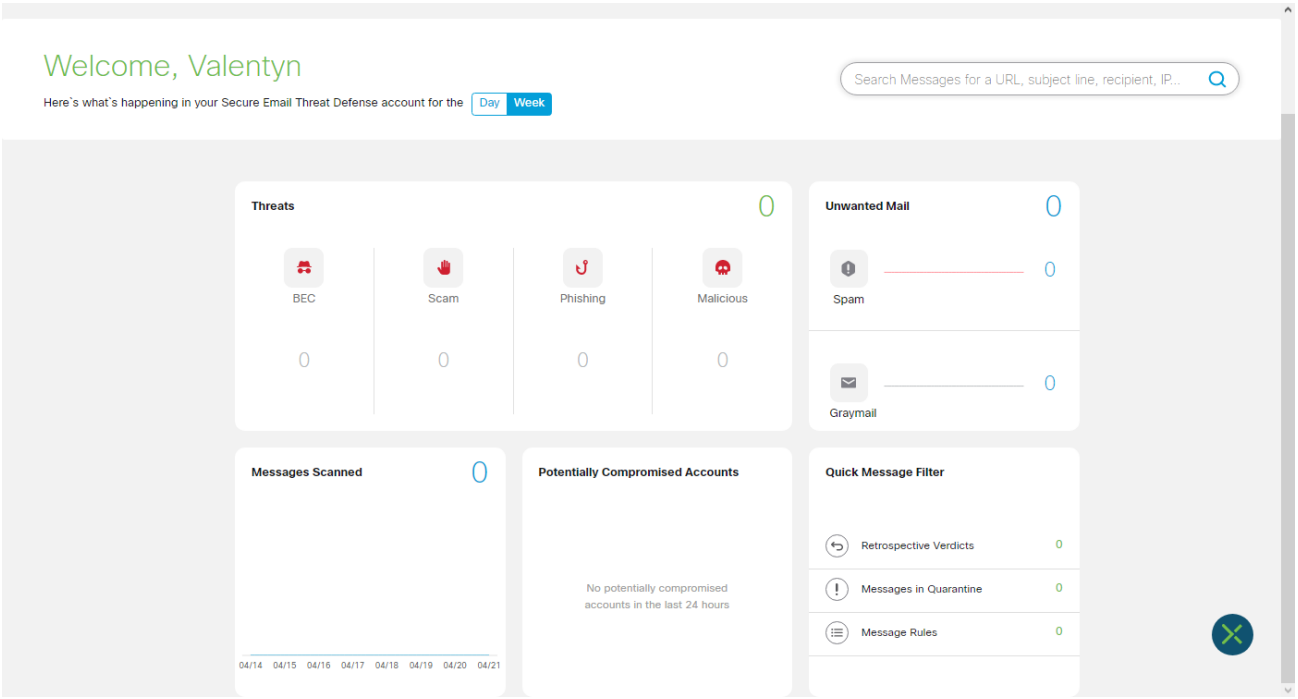

Рис. 3.8. Вигляд узагальнюючого інформаційного дашборду SETD

Для більш детальної інформації щодо загроз можна перейти на вкладення «Insights», де відображена наступна інформація:

- Загальна кількість відсканованих повідомлень (внутрішні, вхідні, вихідні, змішані)
- Загрозливий трафік
- Спам-трафік
- Трафік шантажу
- Інформація про повідомлення: вирок, дані про відправника та отримувача, інформація про вкладення, URL-адреса
- Інформація про вирок (чому повідомлення було визнано винним, які детектори були використані, які докази були знайдені)
- Перегляд бесіди — кому було надіслано електронний лист
- Перегляд часової шкали — з моменту отримання, засудження тощо.

Вигляд вкладки «Insights» на Рис. 3.9

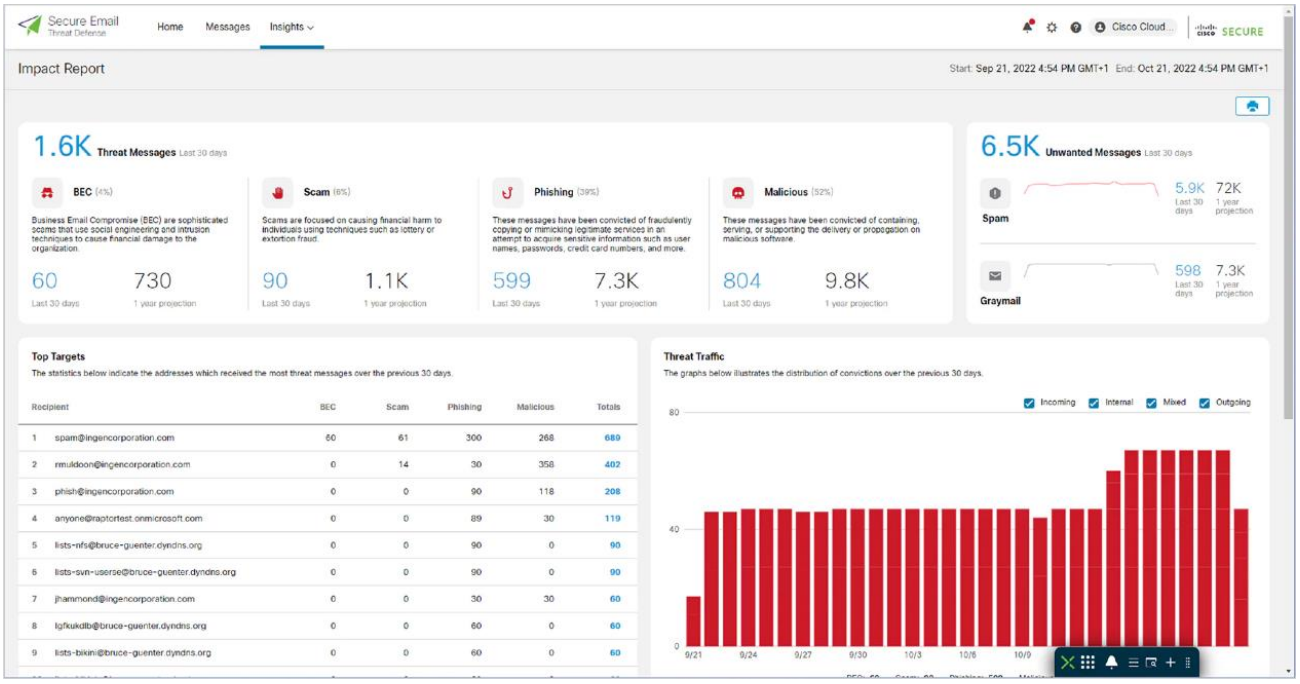

Рис. 3.9. Вигляд дашборду «Insights» з прикладами виявлених порушень

Для того щоб переглянути роботу фільтра можна скористатися вкладенням «Messages» де всі отримані повідомлення вже будуть відсортовані та помічень за потреби. Повідомлення можна сортувати за:

- Відправник
- Одержувач
- Тема
- Конверт З адреси
- Відповісти на
- IP-адреса SMTP-сервера
- IP-адреса SMTP-клієнта
- X-відправник IP
- Організація-BCC
- URL
- Назва вкладення
- Ідентифікатор повідомлення MS

Вигляд вкладки «Messages» на Рис. 3.10

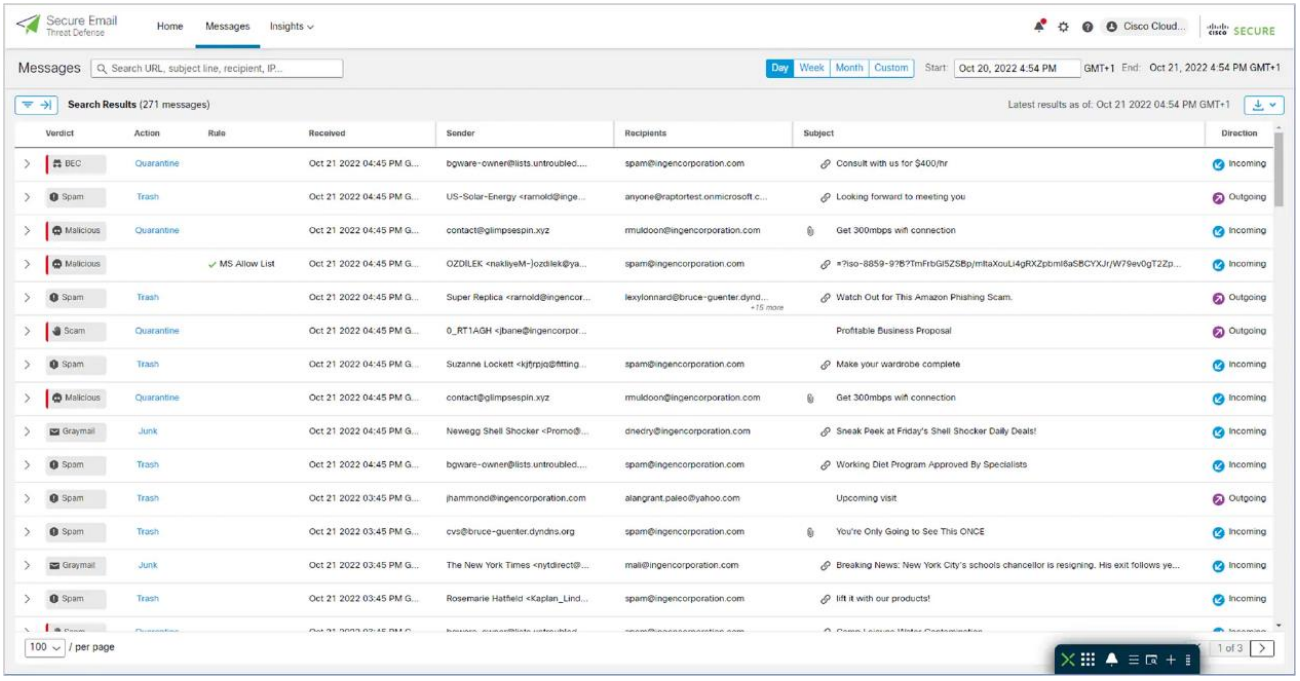

Рис. 3.10. Вигляд вкладення «Messages» з прикладами отриманих фішингових листів

Secure Email Threat Defense (SETD), окрім того, що пропонує найсучасніші заходи захисту електронної пошти, також надає можливість створювати докладні звіти про поведінку користувачів і продуктивність системи.

Можливість створення файлу a.csv з вичерпними даними про користувачів, які входили в панель керування, є однією з основних можливостей SETD для створення звітів. У цьому файлі міститься безліч даних про поведінку користувачів, включаючи час входу в систему, IP-адреси та іншу важливу інформацію. Ці дані можна використовувати для виявлення потенційних ризиків для безпеки, виявлення дивної поведінки користувачів і відстеження продуктивності системи з плином часу.

Команди безпеки можуть провести глибоке дослідження і отримати корисну інформацію про поведінку користувачів і продуктивність системи, просто імпортувавши файл .csv, створений SETD, в ряд аналітичних інструментів і платформ. Використання цих даних дозволяє компаніям передбачити можливі ризики безпеки та вжити заходів для їх зменшення до того, як вони матеріалізуються у злом або іншу проблему безпеки.

Загалом, функції звітності SETD є важливою частиною загальної системи безпеки платформи, оскільки вони надають користувачам інструменти та інформацію, необхідні для управління інфраструктурою безпеки електронної пошти та захисту важливих даних і активів від різноманітних онлайн-загроз.

Завантажити .csv файл можна за посиланням «Settings»> «Administration»> «Download CSV»

Secure Email Threat Defense, окрім складних заходів захисту електронної пошти та можливостей звітування, надає користувачам потужні інструменти статистичного аналізу, які дозволяють відстежувати час безвідмовної роботи та продуктивність системи в режимі реального часу.

Здатність відстежувати час безвідмовної роботи системи захисту і представляти цю інформацію користувачам у стислій і зрозумілій формі є однією з основних статистичних функцій SETD. Ця інформація може бути використана для виявлення можливих системних проблем, моніторингу продуктивності системи в часі та коригування системних налаштувань для оптимальної ефективності та безпеки.

Користувацький інтерфейс платформи спрощує клієнтам доступ до статистичних даних, які пропонує SETD, інформуючи їх про продуктивність системи та дозволяючи їм робити вибір на основі даних щодо своєї архітектури безпеки електронної пошти. Користувачі можуть передавати статистику продуктивності системи і часу безвідмовної роботи важливим зацікавленим сторонам і особам, які приймають рішення, використовуючи цю інформацію для створення спеціальних звітів і візуалізацій.

Вигляд звіту безвідмовної роботи на Рис 3.11.

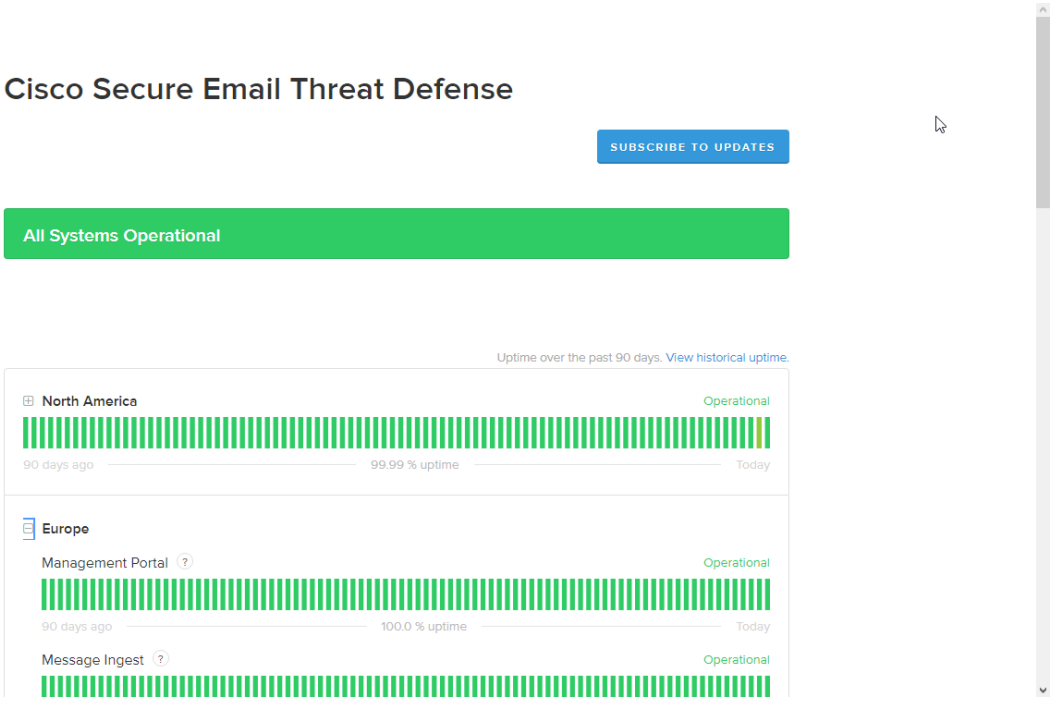

Рис. 3.11. Вигляд звітності щодо часу роботи системи та збоїв

3.2 Розробка рекомендацій щодо актуальності використання комплексних методів боротьби з фішингом

Стає все більш очевидним, що існують різні дуже ефективні методи захисту від цих видів кіберзагроз, що є наслідком постійної еволюції фішингових атак і значних досліджень у цій галузі. Для того, щоб залишатися на крок попереду нових загроз, дуже важливо застосовувати проактивний підхід до безпеки електронної пошти та регулярно перевіряти й оновлювати політики безпеки. Експерти радять поєднувати кілька антифішингових методів, таких як моніторинг у режимі реального часу, машинне навчання та поведінковий аналіз, щоб успішно протистояти небезпеці фішингових атак. Організації повинні мати надійні заходи безпеки електронної пошти, щоб зменшити ймовірність стати жертвою фішингових атак. Це може включати використання таких програм, як Secure Email Threat Defense (SETD), що надає найсучасніші можливості захисту від численних атак, пов'язаних з електронною поштою. Впровадивши ефективні заходи безпеки електронної пошти, організації можуть значно знизити ймовірність стати жертвою фішингових атак. Важливо пам'ятати, що жоден захід безпеки не є непроникним і що хакери постійно змінюють свої стратегії ухилення. Для того,

щоб випереджати нові загрози, підприємствам вкрай важливо дотримуватися пильного та проактивного підходу до безпеки електронної пошти, а також регулярно перевіряти та оновлювати свої заходи безпеки. Для цього потрібно ретельно вибирати компанію та програмний продукт, який ви будете використовувати.

З іншого боку, як вже було встановлено, неграмотна людина є найслабшим компонентом будь-якої системи безпеки. Недостатня підготовка персоналу щодо того, як поводитися з фішинговими електронними листами, ускладнює для корпорації захист від таких атак. Дуже важливо інформувати кінцевих користувачів про ризики, пов'язані з цими атаками, а також надати їм знання та навички, необхідні для виявлення та повідомлення про підозрілі електронні листи. Для підвищення обізнаності та просування найкращих практик безпеки електронної пошти ця процедура може включати тренінги, імітацію фішингових атак та освітні програми. Організації повинні бути в курсі останніх тенденцій і стратегій фішингу, щоб підтримувати надійну систему захисту електронної пошти та захищатися від постійно еволюціонуючих фішингових атак. Щоб випереджати нові загрози, політики безпеки повинні регулярно переглядатися і оновлюватися. IT-спеціалісти можуть виявити можливі вразливості та проактивно усунути їх до того, як вони будуть використані, якщо будуть в курсі останніх тенденцій та стратегій фішингу. Частиною цього є відстеження нових векторів атак, стратегій соціальної інженерії та інших небезпек, пов'язаних з фішингом.

Щоб переконатися, що заходи безпеки, такі як обмеження паролів, контроль доступу та системи автентифікації, залишаються ефективними проти нових і нових загроз, також важливо регулярно оцінювати та оновлювати їх.Організації можуть значно знизити ймовірність стати жертвою фішингових атак та інших форм кіберзагроз, застосувавши проактивний підхід до безпеки електронної пошти та запровадивши повний комплекс заходів безпеки. Це може включати багатофакторну автентифікацію (MFA) для захисту облікових записів користувачів, а також використання складних технологій безпеки, таких як SEG і SETD, для виявлення і блокування небезпечних повідомлень.

Загалом, безпека електронної пошти має бути проактивною та всеохоплюючою стратегією, щоб захистити від зростаючої небезпеки фішингових атак. Організації можуть зменшити ризик стати жертвою таких атак і забезпечити безпеку та надійність своїх систем електронної пошти, якщо будуть постійно оцінювати та вдосконалювати заходи безпеки, а також впроваджувати найкращі практики.

Висновок до розділу 3 — Cisco Email Threat Defence потужний програмний засіб, що полегшує роботу IT спеціалістів організації по моніторингу та відсіюванню спам або фішинг листів. .

ВИСНОВКИ

З дослідження теоретичних основ захисту інформаційних активів в інформаційній системі бізнесу стає зрозуміло, що шкідливе програмне забезпечення та кіберзлочинність стають все більш поширеними проблемами, які загрожують безпеці конфіденційних даних. Очевидно, що ефективні заходи захисту повинні йти в ногу з новітніми технологіями, враховуючи зв'язок між змінами в кібератаках і технічним прогресом. Одним з найефективніших способів викрадення інформаційних активів компанії є фішингові атаки, які, як виявилося, завдають значних фінансових збитків. В результаті досліджень було створено типологію захисту від фішингових атак, і було доведено, що програмне забезпечення Cisco Secure Email Threat Defense перевершує своїх конкурентів.

Розгортання цього програмного інструменту та пропозиції щодо впровадження інтегрованих антифішингових методів, таких як навчання та підвищення кваліфікації персоналу, є частиною рішення проблеми фішингу. Організації можуть успішно захистити свої інформаційні активи від кібератак, запровадивши ретельні процедури захисту від фішингу та слідкуючи й використовуючи новимітні технології.

ПЕРЕЛІК ПОСИЛАНЬ

1. Scams And Safety URL: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (дата звернення: 12.02.2023).
2. Шкідливі програми URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/ (дата звернення: 12.02.2023).
3. Eugene Spafford The Internet Worm Program: An Analysis — Department of Computer Sciences Purdue University URL: http://www.textfiles.com/100/tr823.txt (дата звернення: 19.02.2023).
4. Newsweek Web Exclusive. 2004 URL: https://web.archive.org/web/20090302181536/http://www.newsweek.com/id/52912 (дата звернення: 19.02.2023).
5. The Common Gateway Interface URL: https://web.archive.org/web/20100127161358/http://hoohoo.ncsa.illinois.edu/cgi/ (дата звернення: 26.02.2023).
6. Christopher Hadnagy Social Engineering: The Art of Human Hacking / Christopher Hadnagy John Wiley & Sons, Inc. 298 pages.
7. APWG Phishing Activity Trends Reports URL: https://apwg.org/trendsreports/ (дата звернення: 8.03.2023).
8. FBI Internet Crime Complaint Center (IC3) URL: https://www.ic3.gov
9. History of Phishing URL: https://inspiredelearning.com/blog/history-of-phishing/
10. Anatomy of an Attack — RSA FraudAction Research Labs. 2011 URL: https://web.archive.org/web/20141006071018/https://blogs.rsa.com/anatomy-of-an-attack/

11. Report: Email phishing scam led to Target breach — BMTN STAFF. 2014 URL: https://bringmethenews.com/minnesota-news/report-email-phishing-scam-led-to-target-breach

12. D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump — The New York Times URL: https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html

13. Lessons From a Real WorldEvaluation of Anti-Phishing Training. 13 pages URL: https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Lessons_From_a_Real_World_Evaluation_of_Anti-Phish.pdf.

14. Employee education, training is key to curtailing risk of phishing attack URL: https://www.propertycasualty360.com/2019/05/24/how-effective-employee-education-and-training-combats-phishing-attack-risk-414-155823/?slreturn=20230322131231 (дата звернення: 8.03.2023)

15. Christian Ludl On the Effectiveness of Techniques to DetectPhishing Sites/ Christian Ludl, Sean McAllister, Engin Kirda, Christopher Kruegel URL: https://sites.cs.ucsb.edu/~chris/research/doc/dimva07_phishing.pdf (дата звернення: 15.03.2023)

16. Hochschule Wismar Security Evaluation of Multi—Factor Authentication in Comparison with the Web Authentication API URL: https://it-forensik.fiw.hs-wismar.de/images/b/bc/MT_TimBrust.pdf (дата звернення: 19.03.2023)

17. Fatima Salahdine Phishing Attacks DetectionA Machine Learning-Based Approach / Fatima Salahdine, Zakaria El Mrabet, Naima Kaabouch URL: https://arxiv.org/ftp/arxiv/papers/2201/2201.10752.pdf (дата звернення: 21.03.2023)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)