НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і

спеціалізованих комп'ютерних систем

«На правах рукопису»
УДК __004.056.5__

До захисту допущено:
Завідувач кафедри
_____ Віталій РОМАНКЕВИЧ
«___»_____2025 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системне програмування та спеціалізовані комп'ютерні системи»

зі спеціальності 123 «Комп'ютерна інженерія»

на тему: «СПОСОБИ ТА ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД ФІШИНГ-АТАК У СОЦІАЛЬНИХ МЕРЕЖАХ»

Виконав :
студент II курсу, групи КВ-42 мп
Вінницький Владислав Олексійович _____
Науковий керівник:
к.т.н., доцент, доцент кафедри СПіСКС
Павловський Володимир Ілліч _____
Рецензент:
Посада, науковий ступінь, вчене звання,
Прізвище, ім'я, по батькові _____

Commented [AK1]: Треба заповнити

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2025 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)

Спеціальність – 123 «Комп'ютерна інженерія»»

Освітньо-професійна програма «**Системне програмування та спеціалізовані комп'ютерні системи»**

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Віталій РОМАНКЕВИЧ

«_01_»__жовтня____2024 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Вінницький Владислав Олексійович

1. Тема дисертації «СПОСОБИ ТА ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД ФІШИНГ-АТАК У СОЦІАЛЬНИХ МЕРЕЖАХ», науковий керівник дисертації Павловський Володимир Ілліч к.т.н., доцент СПіСКС, затверджені наказом по університету від «6» листопада 2025 р. №4836-с

2. Термін подання студентом дисертації 16 грудня 2025

3. Об'єктом дослідження є корпоративна поштова інфраструктура та способи навчання персоналу для підвищення обізнаності користувачів проти фішингу у корпоративній пошті.

4. Вихідні дані:

4.1Статистичні дані щодо фішингових атак
4.2Інформація про існуючі платформи навчання персоналу та проведення фішинг-симуляцій
4.3Вимоги компанії-замовника
4.4Початкові показники рівня обізнаності співробітників

5. Перелік завдань, які потрібно розробити:

5.1Проаналізувати проблему фішингу в електронному листуванні, класифікувати типи атак, методи маскування та техніки соціальної інженерії.
5.2Дослідити та порівняти існуючі технічні методи захисту від фішингових атак, зокрема сигнатурні механізми, методи поведінкового аналізу, комбіновані системи захисту та інструменти аналізу електронної пошти.
5.3Вивчити сучасні програмні рішення для навчання персоналу та фішинг-симуляцій (Terranova, KnowBe4, Cofense, PSAT, CSAT) та провести їх порівняльний аналіз.
5.4Обґрунтувати доцільність використання навчання персоналу як методу зменшення вразливості до фішингових атак у корпоративному середовищі.
5.5Розробити концепцію та методологію методу Train–Simulate–Measure (TSM) як способу підвищення кіберобізнаності співробітників.
5.6Визначити елементи, компоненти та механізми роботи методу TSM, включаючи підготовку навчальних матеріалів, створення симуляцій, оцінювання та актуалізацію користувацьких результатів.
5.7Розробити архітектуру системи TSM для інтеграції в корпоративну мережу, визначивши структуру сервісів, взаємодію модулів та інформаційні потоки.
5.8Визначити інфраструктурні вимоги та мережеві параметри для розгортання системи TSM у корпоративній інфраструктурі.
5.9Розробити покроковий план впровадження TSM у мережу замовника, включаючи часову шкалу, ресурси та відповідальних осіб.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу – презентація 17 сторінок

7. Перелік публікацій:

- ПМК-2025 «Способи та засоби підвищення ефективності захисту від фішинг-атак у соціальних мережах»
- Міжнародна науково-практична конференція «Сучасні тенденції та перспективи розвитку науки, освіти і суспільства» публікація на тему «Методи вдосконалення захисту від фішингових атак у середовищі соціальних мереж»

8. Дата видачі завдання 1 листопада 2024р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Узгодження керівника кваліфікаційної роботи (МД) та його затвердження	15.09.2025	
2	Визначення тематики (напряму) дослідження магістерської дисертації	20.09.2025	
3	Визначення структури магістерської дисертації	21.09.2025	
4	Перший розділ МД з висновками (робочі версія). Підготовка тез доповіді для виступу на конференції	01.10.2025	
5	Другий розділ МД з висновками (робочі версія)	19.10.2025	
6	Остаточне формування тематики кваліфікаційної роботи	20.10.2025	
7	Тема магістерської дисертації, заява на ім’я завідувача кафедри з точною назвою МД	20.10.2025	
8	Зміст та вступ до МД (остаточний варіант)	24.10.2025	
9	Реферат до МД (українською мовою) та перший розділ	30.10.2025	
10	Титульний аркуш, завдання та другий розділ МД з висновками	10.11.2025	
11	Залік з науково-дослідної практики	22.10.2025	
12	Попередній захист магістерської дисертації	24.11.22025	

Студент Владислав ВІННИЦЬКИЙ

Науковий керівник Володимир ПАВЛОВСЬКИЙ

РЕФЕРАТ

Актуальність теми. Електронна пошта лишається буденним і дуже зручним інструментом комунікації у бізнесі, держсекторі та приватній сфері. За статистикою, понад 80% успішних кібератак починаються саме з фішингових листів.

Сучасні поштові фільтри працюють, але не все виловлюють, адже сценарії злому постійно оновлюються і їх мімікрія під бренди стає акуратнішою. Тому розробка спеціальних методів навчання персоналу у боротьбі з соціальною інженерією та фітингом у електронній пошті є актуальною і важливою задачею з практичної точки зору яка буде використовуватися у всіх дотичних сферах.

Об’єктом дослідження є корпоративна поштова інфраструктура та способи навчання персоналу для підвищення обізнаності користувачів проти фішингу у корпоративній пошті.

Предметом дослідження процеси навчання користувачів і їхній вплив на поведінкові метрики.

Мета роботи: дослідження існуючих програмних реалізацій боротьби з фітинговою активністю; вивчення та аналіз методів фішинговий атак спрямоване на виявлення ознак та побудову дій для виявлення та протидії атаці; аналіз ефективності навчання у запобіганні переходам за шкідливими посиланнями та створення автоматизованої схеми розгортання програм у корпоративному сегменті для підвищення обізнаності користувачів пошти.

Наукова новизна полягає роботи полягає у створенні методики навчання персоналу яка буде полягати у постійному вдосконалені знань через постійні

курси та вебінари, а засвоєні знання та рівень ризику кожного співробітника буде досліджено на реальних контрольованих фітингові атаки. Впроваджена методика інтегрується з програмними засобами, які легко масштабуються під довільну кількість персоналу компанії та дозволяє безперервно поліпшувати кіберобізнаність користувачів як до нових так і старих схем атак.

Практична цінність досліджень допоможе не тільки комерційним компаніям а і звичайним користувачам за короткий час навчитися виявляти фишингове листування. Запропонований безперервний підхід Train–Simulate–Measure який полягає у мікро-тренінгах з підвищення кваліфікації клієнта, регулярних email-симуляції та вимірюванні індивідуальний/командний risk-score для адресної роботи з «групами ризику» дозволить комплексно оцінювати знання та компетенції користувачів у сфері соціальної інженерії та фішингу та зменшити кіберзагрози з боку пошти для компаній.

Апробація роботи. Ключові ідеї та здобуті результати доповідались і дискутувалися під час XVIII наукової конференції магістрантів та аспірантів «Прикладна математика та комп’ютинг» (ПМК-2025), Київ, 19–21 листопада 2025р. На міжнародна науково-практична конференція «Сучасні тенденції та перспективи розвитку науки, освіти і суспільства» опубліковано тези на тему «Методи вдосконалення захисту від фішингових атак у середовищі соціальних мереж».

Структура та обсяг роботи. Магістерська дисертація складається з вступу, чотирьох розділів та висновків.

У вступній частині представлено загальну характеристику роботи, проведено аналіз сучасного стану проблеми та доведено актуальність дослідження. Сформульовано мету й основні завдання, окреслено наукову новизну та практичну корисність здобутих результатів, наведено відомості щодо їх апробації та впровадження.

Перший розділ присвячено систематизації наявних рішень боротьбі х фішингом їх перевагам та недолікам, розглянуто можливі рішення інтеграції методу у існуючі програмні рішення та обрано на якому з них буде побудовано метод.

У другому розділі розроблено метод постійного навчання користувачів Train–Simulate–Measure.

У третьому розділі детально описано впровадження запропонованої методики протидії фішингу на базі обраного ПЗ, налаштування модулів, сценарії тренувань і метрики оцінювання.

Четвертий розділ описує етапи впровадження запропонованого підходу «Train–Simulate–Measure»

Висновки містять огляд досягнутих результатів і їх практичну значущість для організаційного захисту електронної пошти.

Ключові слова: фішинг, соціальна інженерія, електронна пошта, метод навчання, способи захисту, ризик група, техніки фішингу.

ABSTRACT

Relevance of the topic. Email remains an everyday and highly convenient communication tool in business, the public sector, and personal use. According to statistics, more than 80% of successful cyberattacks begin with phishing emails. Modern email filters are effective, but they cannot catch everything, since attack scenarios are constantly evolving and their mimicry of trusted brands becomes increasingly accurate. Therefore, the development of specialized methods for training personnel to counter social engineering and phishing in email is a relevant and important practical task that can be applied across all related fields.

The object of the study is the corporate email infrastructure and the methods of training personnel to improve user awareness against phishing in corporate email. The subject of the study is the processes of user training and their impact on behavioral metrics.

The aim of the work is: to study existing software implementations for combating phishing activity; to examine and analyze methods of phishing attacks in order to identify indicators and build actions for detecting and countering attacks; to analyze the effectiveness of training in preventing users from following malicious links; and to develop an automated deployment scheme for software in the corporate environment to enhance user awareness.

Scientific novelty lies in the creation of a personnel training methodology based on continuous knowledge improvement through regular courses and webinars, with acquired knowledge and individual employee risk levels evaluated using real controlled phishing attacks. The implemented methodology integrates with software tools that can easily scale to any number of employees and ensures continuous

improvement of cyber awareness regarding both new and traditional attack techniques.

Practical significance: The results of the research will help not only commercial organizations, but also regular users quickly learn to identify phishing emails. The proposed continuous Train–Simulate–Measure approach, which consists of micro-trainings, regular email simulations, and measuring individual/team risk scores for targeted work with "risk groups," provides a comprehensive assessment of user knowledge and competencies in social engineering and phishing, reducing email-related cyber risks for companies.

Implementation and verification. The key ideas and obtained results were presented and discussed at the XVIII Scientific Conference of Master's and PhD Students "Applied Mathematics and Computing" (AMC–2025), Kyiv, November 19–21, 2025. Abstracts on the topic "Methods for Improving Protection Against Phishing Attacks in Social Media Environments" were published at the international scientific-practical conference "Modern Trends and Prospects for the Development of Science, Education and Society."

Structure and scope of the work. The master's thesis consists of an introduction, four chapters, and conclusions.
The introduction presents the general characteristics of the work, analyzes the modern state of the problem, and justifies the relevance of the research. The aim and tasks are formulated, scientific novelty and practical usefulness are outlined, and information about implementation and testing is provided.

The first chapter is devoted to systematizing existing anti-phishing solutions, their advantages and drawbacks, and reviewing possible ways to integrate the method into existing software solutions, with a justification for the chosen technological base.

The second chapter develops the continuous user-training method Train–Simulate–Measure.

The third chapter provides a detailed description of implementing the proposed anti-phishing methodology using the selected software, including module configuration, training scenarios, and evaluation metrics.

The fourth chapter describes the stages of implementing the proposed Train–Simulate–Measure approach.

The conclusions summarize the achieved results and their practical significance for organizational email security.

Keywords: phishing, social engineering, email, training method, protection techniques, risk group, phishing techniques.

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

API (Application Programming Interface) – програмний інтерфейс, що дозволяє системам взаємодіяти між собою.

DKIM (DomainKeys Identified Mail) – технологія автентифікації електронної пошти, яка підтверджує достовірність домену відправника за допомогою криптографічного підпис

DMARC (Domain-based Message Authentication, Reporting & Conformance) – механізм захисту електронної пошти, який визначає політики перевірки SPF та DKIM, а також забезпечує репортування про невдалі спроби доставки.

EDR/XDR (Endpoint Detection & Response / Extended Detection & Response) – технології для виявлення, аналізу та реагування на загрози на рівні кінцевих точок (EDR) або в комплексі з іншими джерелами телеметрії (XDR).

LMS (Learning Management System) – система управління навчанням, платформа для доставки, обліку та оцінювання навчальних матеріалів.

REST API (Representational State Transfer API) – архітектурний стиль веб-інтерфейсів, де взаємодія здійснюється через стандартні HTTP-запити.

SIEM (Security Information and Event Management) – система централізованого збору, кореляції та аналізу логів безпеки з різних джерел.

Конектор (Connector) – компонент інтеграції, який забезпечує передачу даних між системами (наприклад, між ITS, SIEM, LMS або Defender).

ВСТУП

У сучасному світі ми не можемо уявити життя без використання соціальних мереж. Саме поглиблена і швидка цифровізація світу зробила людей залежними від онлайн комунікацій. У більшості людей є по два-три акаунти для соціальних мереж, і хоча б одна електронна пошта, яка використовується для зв'язування/поєднання цих мереж та підключається як резервний спосіб/засіб відновлення акаунту. І саме через те, що електронна пошта лишається буденним і дуже зручним інструментом комунікації у бізнесі, держсекторі та приватній сфері, злочинці масово націлюються та цілеспрямовано намагаються зламати поштові акаунти. Використовуючи інколи досить неетичні методи, які націлені на маніпулюванням довірою, примус або шахрайські техніки, кіберзлочинці викрадають облікові дані, платіжну інформацію чи встановлюють шкідливе ПЗ без відома.

За статистикою понад 80% успішних кібератак на компанії починаються саме з фішингових листів [1].

Сучасні поштові фільтри працюють, але не все виловлюють, адже сценарії злому/зламування постійно оновлюються і їх мімікрія під відомі бренди стає акуратнішою/досконалішою. А у сучасні часи зловмисники масово почали застосовувати генеративні мовні моделі для створення правдоподібних листів і фішингових лендінгів.

Тема роботи доволі актуальна у нинішні часи, бо в більшості випадків протидія фішингу у організаціях все ще зводиться до простих інформаційних попереджень раз на пів року, а весь інший захист покладається на технічні фільтри пошти або внутрішні політики безпеки. Додатковим фактором ризику є нерівномірність розподілу ризику для різних ролей та підрозділів, вони взаємодіють з поштою по-різному, однак все одно отримують однотипне навчання, що призводить до перевантаження чи недостатнього навчання персоналу.

Для проведення дослідження та отримання результатів проаналізовано як користувачі взаємодіють з соціальними мережами та електронною поштою. Аналіз існуючого навчального матеріалу показав ключові аспекти, які допомагають у створенні змістовно логічного та інформативного змісту. Досягнення мети роботи очікується у розробці цілісного та масштабованого підходу до навчання персоналу у протидії фішинговим атакам різної складності та направленості. Підхід включає в себе мікро-тренінги з підвищення кваліфікації клієнта, регулярні email-симуляції та створення єдиної метрики ризиків та обчислення індивідуальний/командний risk-score для адресної роботи з «групами ризику».

Наукова новизна очікуваних результатів полягає у створенні комплексного захисту, який буде мати можливість швидко та легко інтегруватися з існуючими процесами та системами. Практична частина роботи пропонує механізм впровадження розробленого підходу в організаціях різного масштабу, яке дасть змогу зменшити частку кліків на фішингові посилання у електронній пошті, підвищити частку коректних користувацьких репортів, знизити кількість успішних спроб захоплення кабінетів користувачів і відновлень доступу через пошту.

Ключовим принципом запропонованого підходу є безперервність і циклічність підвищення обізнаності співробітників. Підхід Train–Simulate–Measure, зосереджений більше на електронній пошті як критичному каналі, основним завданням якого буде статистичне зменшення ймовірностей успішної компрометації акаунтів у соціальних мережах та зниженні середніх збитків від атак.

Структурно робота побудована наступним чином: у першому розділі розглянуто сучасний стан проблем фішингу у електронному листуванні із детальним аналізом недоліків відомих методів протидії фішингу, другий розділ розповідає про проведення дослідження впливу обізнаності користувачів та створенню методу Train–Simulate–Measure як боротьби з фішингом через безперервне навчання персоналу, у третьому розділі сформовано технологію та спосіб реалізації побудови циклу Train–Simulate–

Measure, наведено архітектуру рішення, конструктор мікро-тренінгів і систему метрик ризику, а вже в четвертому розділі опрацьовано результати експериментальної апробації методики, здійснено порівняння з альтернативними підходами та оцінку ефективності за обраними KPI. У висновку роботи узагальнено отримані результати, визначено обмеження і наведено практичні рекомендації щодо впровадження та посилення кібербезпеки і обізнаності користувачів в організаціях різного масштабу.

1 АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд проблеми фішингу у електронному листуванні

Фішинг в електронному листуванні є однією з найпоширеніших загроз сучасного цифрового середовища. Суть кіберзлочину полягає у обмані користувачів шляхом надсилання підроблених або схожих на реальні листи, які імітують повідомлення від легітимних компаній, установ чи окремих персон. Основною метою діяльності кіберзлочинців є отримання конфіденційної та персональної інформації, такої як: логіни, паролі, номери банківських карток або інші персональні дані користувача. Особливість фішингу полягає у використанні людського фактору, адже саме користувач, який відкриває, читає лист і виконує вказівки у ньому, стає останньою та найслабшою ланкою, що визначає успіх або провал злочинної атаки та викрадення даних.

Історично електронна пошта створювалась як відкритий та доступний канал комунікації, він не мав вбудованих механізмів перевірки справжності відправника або змісту повідомлення. Через масштабоване використання злочинці почали використовувати можливість надсилати листи, які виглядають правдоподібно та переконливо. Вони масово та майстерно підробляють електронні адреси, логотипи компаній, підписи керівників, стиль ділового спілкування, а також інколи використовують соціально-психологічні прийоми для маніпуляції емоціями людини та цим спонукають її на необдумані дії. Найчастіше зловмисники намагаються керувати почуттям терміновості, страху, вигоди або авторитету, щоб змусити отримувача діяти імпульсивно, без перевірки та підтвердження правдивості інформації.

Фішиг став всесвітньою проблемою безпеки, яка прямо впливає на фінансові результати компаній і державних установ. Щоб наглядно продемонструвати реальний масштаб втрат, я підготував зведену таблицю 1.1 з резонансними кейсами за останні роки, де всі суми було приведено до долара США. Дані демонструють, що збитки вимірюються мільйонами, іноді десятками мільйонів доларів, а розробки атак залишаються відносно дешевими для зловмисників, тому робити ставку тільки на фільтри пошти замало, потрібно впроваджувати додаткові рівні захисту.

Таблиця 1.1 - Перелік компаній та завдані їм збитки

Company	Country	Year	Incident_Type	Loss_USD
Facebook (Meta)	USA	2013	BEC/vendor impersonation (Rimasauskas)	99000000
Google (Alphabet)	USA	2015	BEC/vendor impersonation (Rimasauskas)	23000000
FACC AG	Austria	2016	CEO fraud / fake president	46450979
Leoni AG	Germany	2016	CEO fraud / BEC	44239028
Crelan Bank	Belgium	2016	CEO fraud / BEC	77418299
Ubiquiti Networks	USA (HK subsidiary)	2015	Executive spoofing / BEC	46700000
MacEwan University	Canada	2017	Vendor bank details change (phishing)	9086709
Pathé Netherlands	Netherlands	2018	CEO fraud / BEC	22653771

Продовження таблиці 1.1

Company	Country	Year	Incident_Type	Loss_USD
Toyota Boshoku	Japan/EU	2019	Email fraud / BEC	36856169
Nikkei America	USA/Japan	2019	Executive impersonation / BEC	29000000
PRIDCO	Puerto Rico (US)	2020	Phishing-led bank change / BEC	2600000
City of Naples, Florida	USA	2019	Spear-phishing vendor payment change	700000
Barbara Corcoran / The Corcoran Group	USA	2020	Invoice fraud via phishing	388700
Scoular Company	USA	2014	Spear-phishing CFO/Controller	17200000

Одним із найпоширеніших прийомів фішингу виступає надсилання посилання на фальшиву імітовану сторінку входу до поштової скриньки або банківського акаунта. Ззовні підроблену сторінку не відрізнити від справжніх, але всі дані, які вводить користувач, перенаправляються і потрапляють безпосередньо до рук злочинців. Найменш поширеним способом є атака, яка передбачає використання вкладених файлів у повідомленнях, в яких вставляють шкідливий код. Після відкриття отриманого файлу відбувається зараження системи, яке може призвести до крадіжки даних, блокування доступу або подальшого розповсюдження шкідливого ПЗ через корпоративну пошту.

Окрему небезпеку становлять спрямовані персональні фішингові атаки, або так званий спірфішинг. Їх суть полягає у підготовленому повідомленні спеціально для певної компанії, департаменту чи, навіть, конкретної людини.

Надіслані листи виглядають максимально реалістично, містять справжні імена співробітників, інколи містять внутрішні формулювання та навіть підроблені документи. Працівники бухгалтерії, служби кадрів чи технічної підтримки часто стають першими та основними жертвами спірфішингових атак саме через свій рівень критичності.

Фішингові кампанії швидко та постійно еволюціонують. Зловмисники змінюють шаблони листів, використовують штучний інтелект, нові домени, шифрують вкладення, маскують посилання через елементи html коду або вбудовані кнопки. Фішинг вже настільки розвинувся, що застосовуються такі просунуті методи як оминання антивірусних систем за допомогою псевдобезпечних форматів файлів, які здаються звичайними документами, але містять прихований код. Складність захисту електронної пошти наразі полягає у тому, що навіть найкращі та найдорожчі поштові шлюзи, спам-фільтри та антивірусні рішення не здатні забезпечити абсолютний захист від вірусних повідомлень, оскільки людський фактор залишається ключовим елементом атаки та ланкою, що найчастіше використовується у проникненні.

Щоб кількісно показати, як описані вище прийоми зловмисників у поєднанні з людським фактором перетворюються на реальний ризик, розглянемо типову «воронку» взаємодії користувача з фішинговим листом. Отримані результати (рисунок 1.1) демонструють типовий “ризиковий профіль” фішингової кампанії.

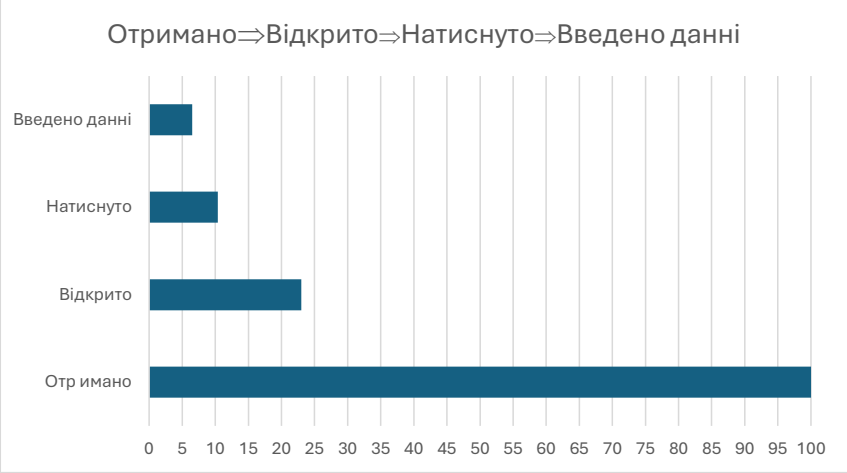

Рисунок 1.1 - Статистика взаємодії користувача з фішинговим листуванням

На сьогоднішній день існує багато методів захисту від фішингу. Їх поділяють на три основні групи: сигнатурні, поведінкові (аномальні) та комбіновані методи [2].

1.1.1 Сигнатурні методи захисту

Суть методів базуються на пошуку відомих зразків (сигнатур) у тексті листа, заголовках або вкладення. Типовим прикладом є антиспам-фільтри, які перевіряють наявність шкідливих URL-адрес, що вже внесені до Blacklist, аналізують контент для виявлення ключових фраз, підозрілих вкладень. Сигнатурні підходи ефективні для масових атак, однак безсилі проти персоналізованих spear phishing і whaling-кампаній [3], а також залежать від бази сигнатур, яку потрібно постійно оновлювати.

1.1.2 Виявлення поведінкових аномалій

Поведінкові методи захисту орієнтуються не на самі атаки, а на відхилення від «нормальної» поведінки користувачів і систем. Використання такої методики передбачає аналіз поведінки листа чи користувача: незвичний час відправлення, невідповідність адреси відправника та домену (DKIM, SPF), нетипові вкладення тощо. Не ефективність цих методів полягають у швидкому поширені нових доменів, що ускладнює налаштування правильного аналізу.

1.1.3 Комбіновані методи захисту

Методи поєднують сигнатурний та поведінковий підходи до захисту. Подібні засоби здатні не лише фіксувати відомі загрози, а й адаптуватися до нових сценаріїв атак. Вони вважаються найбільш перспективними у сфері захисту електронної пошти [4]. Хоча ефективність комбінованих методів доведена, велика коштовність їх впровадження та підтримки робить їх доступними лише великим компаніям.

1.1.4 Технічні методи боротьби з фішингом

Технічні методи боротьби з фішингом, такі як протоколи SPF, DKIM та DMARC, при правильному налаштуванні дають змогу частково фільтрувати підроблені домени і зменшувати ризики потрапляння шкідливих листів до скриньки користувача. Проте, навіть за наявності цих дорогих та громіздких механізмів, користувач сам може стати причиною інциденту, якщо не зверне увагу на дрібні ознаки підробки.

Економічні наслідки фішингових атак можуть бути катастрофічними навіть для ентерпрайз компаній. Організації зазнають не лише грошових втрат, а й погіршують свою важко зароблену репутацію, отримують штрафи за порушення законодавства про захист персональної інформації та значну часову зупинку бізнес-процесів. Для державного та освітнього секторів ситуація стає дедалі складніша, оскільки успішна атака може призвести до компрометації внутрішніх мереж, підміни офіційних повідомлень або втратою критичних конференційних даних. У військовий час країна агресор не цурається знищувати дані критично важливих сервісів, що є величезною проблемою. З кожним роком масштаби збитків, пов’язаних із фішингом, лише зростають, що підтверджують звіти провідних аналітичних компаній у сфері кібербезпеки (рисунок 1.2).

APWG рахує «унікальні фішингові сайти/атаки» за базовими URL, інколи звіти дають сумарне квартальне число, інколи лише помісячні значення. Там, де лише наявні помісячні данні самостійно було обчислено квартальну суму.

Побудовано на основі звітів з APWG Phishing Activity Trends Reports

Рисунок 1.2 - Статистичні дані кількості фішинговий атака

Фішинг наглядно демонструє наскільки вразливими залишаються люди перед психологічними маніпуляціями навіть у цифровому середовищі. Кожен користувач електронної пошти повинен чітко усвідомлювати, що навіть звичайний на перший погляд лист, може стати початком серйозної фішингової атаки. Тому головним завданням сучасного користувача електронної пошти повинно бути формування культури обережності, довіри, але водночас критичного мислення при роботі з електронною кореспонденцією.

Фішинг настільки глобальна проблема, що лише технічними засобами повністю її не усунути, жоден із існуючих інструментів не дає ідеального захисту. Навіть найсучасніші поштові шлюзи, антиспам або блоклист-системи, ML-класифікатори, працюють із ймовірностями та не можуть гарантувати повністю безпечне використання електронної пошти. Навіть при ретельному налаштуванні вони або пропускають частину атак (false negatives), або

блокують легітимні листи (false positives), що вбиває довіру бізнесу до систем безпеки. При попередньому аналізі застосованих механізмів захисту зловмисники швидко адаптуються. Існує багато схем вже відомих систем зміни домену, стилю повідомлень або використання легального хмарного сервісу для хостингу фішингових форм, шифрування вкладень та вставка QR-кодів дозволяють частково або повністю обходити перевірку систему захисту. У такому динамічно мінливому середовищі технічні засоби відіграють ключову роль , але недостатні; без навчання та регулярних симуляцій ризик «людської помилки» залишається високим.

Для забезпечення надійної системи захисту при роботі з електронною поштою організації будують багатошарову систему захисту, кожен етап захисту якої має свій унікальний механізм та націлений на позбавлення слабкості та закриття дірок у захисті від проникнення неавторизованого листа у корпоративний сегмент пошти.

Базовий шар захисту становлять механізми захисту від неправомірної аутентифікації пошти: SPF дозволяє визначити, які сервери мають право надсилати пошту від імені домену, за допомогою DKIM криптографічно підписується вміст листа, а DMARC вимагає сурової узгодженості доменів та дозволяє задавати політику поводження з невдалими перевірками. На практиці ж багато організацій роками нехтують найпростішими механізмами та тримають політики не налаштованими, мають прогалини на піддоменах або некоректні записи, і саме така ситуація дозволяє частині ретельно підробленим листам проходити базовий рівень захисту.

Наступним шаром захисту виступають поштові шлюзи безпеки й ML-фільтри. Їх суть в комбінації репутаційних баз, статистичних моделей, евристики, OCR для зображень із текстом і переписуванні посилань із перевіркою під час кліку. Найлегший спосіб обійти їх та основна проблема в

тому, що зловмисники просто переходять на хостинг легальних платформ, активують шкідливий контент уже після доставки або ховають посилання в кнопках, зображеннях та QR-кодах. Налаштування жорстких політик суттєво зменшують пропуск загроз, але підвищують частку помилкових спрацьовувань і породжують затримки, втрачені листи клієнтів, обхідні канали комунікації поза контролем безпеки.

Додатковим технічним рівнем захисту може бути антивірус, EDR/XDR, політики макросів та блоки небезпечних форматів на робочих станціях, вони дозволяють обмежувати експлуатацію вкладень, але не можуть зупинити крадіжку облікових даних через фальшиві сторінки входу. Навіть із MFA користувачі вразливі до «MFA-fatigue» і push-бомбардувань, до фішингу токенів через проксі (reverse-proxy phishing) та OAuth-консенсу, коли жертва сама надає додатку стороннього розробника доступ до електронної пошти та файлів. У багатьох організаціях відсутня налагоджена політика реагувань на сценарії «зміни реквізитів» і «термінових виплат», тож BEC обходить технічні методи безпеки.

Через існуючі обмеження технічних засобів саме персональне навчання(рисунок 1.3) та реалістичні симуляції дають те, чого не може дати жоден фільтр, потрібна поступова зміна поведінки користувачів і виконання послідовно відпрацьованого алгоритму дій у моменті прийняття рішення. Реальні симуляції дають можливість людині бачити той самий інтерфейс пошти, ті самі бренди та формулювання, що й під час реальної атаки. Після навчання ці навички допомагають діяти правильно та послідовно перевіряти домен і адресу відправника, не переходити за натиском терміновості та звіряти реквізити іншим каналом, який підтверджує достовірність.

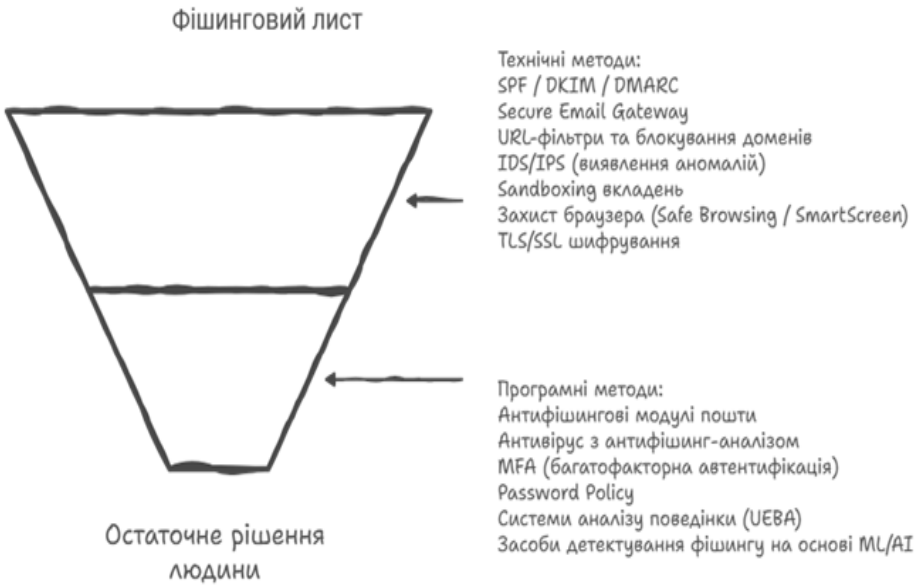

Рисунок 1.3 – Схема багатошарового захист у корпоративній мережі

Реальні симуляції переважають за теоретичні курси ще й тим, що дають вимірюванність. Після кожної активності організація бачить частку натискань на вкладення, хто повідомляє замість натискати, які підрозділи стійкіші або вразливіші, та на основі отриманих даних може формувати ризик групу. Здобуті дані одразу застосовуються на практиці та обирається відповідний курс для покращення знань. Отже, поєднання регулярних, правдоподібних і рольових симуляцій із миттєвим персоналізованим фідбеком та чіткими процесами верифікації платежів дає стійкі результати: менше кліків, швидше виявлення інцидентів і менші фінансові втрати навіть тоді, коли частина листів неминуче обходитиме будь-які фільтри.

1.3 Засоби навчання протидії фішингу та фішинг-симуляцій

Для реалізації безупинного навчання та реальних симуляцій було проаналізовано та розглянуто відомі платформи, які мають змогу забезпечити виконання запропонованого методу: Terranova, KnowBe4, Cofense, Proofpoint є авторитетними рішеннями для підвищення обізнаності з кібербезпеки, кожне зі своїм підходом. У Додатку А наведено детальний категоризований розбір функціональності обраних додатків.

1.3.1 Terranova

Terranova Security – канадський провайдер платформи Security Awareness Training, що виділяється багатим мультимедійним контентом і глобальним охопленням. Платформа Terranova повністю хмарна (SaaS), розроблена з урахуванням потреб великих міжнародних компаній.

Terranova Security Fortra поєднує повний цикл формування знань практичного відпрацювання та кількісної оцінки результатів тестів. У платформі присутня широка бібліотека навчального контенту з короткими мікроуроками та поглибленими курсами різними форматами від відео і інтерактивів до ігор та коміксів. База знань дозволяє повністю сформувати базовий рівень кібергігієни у всіх підрозділів та адресно посилити теми для груп підвищеного ризику. Засоби автоматизації вже допомагають побудувати навчальні траєкторії без ручної рутини.

Для симуляцій у Terranova присутній конструктор шаблонів, він дає змогу відтворювати правдоподібні ситуації з діловими інвойсами, запитами кадрового відділу, нотифікаціями служб доставки та службою єдиного входу з

урахуванням локальних деталей і мов. Плюсом є вбудована кнопка Report Phishing, повідомлення про підозрілі листи при її натисканні надходять напряму до команди безпеки або до сервісів аналізу Fortra буквально у момент проходження симуляції.

Інструменти звітності дають змогу відстежувати ключові показники у реальному часі, зокрема, відсоток клацань на симуляціях, частку і швидкість повідомлень про підозрілі листи, повторюваність помилок, рівень завершення курсів. Дані можна експортувати до систем бізнес аналітики і представити у вигляді виконавчих дашбордів, що підсилює аналітичну частину дослідження.

Водночас необхідно врахувати обмеження. Без продуманої методики адміністратори можуть перевантажити користувачів контентом, що знижує ефективність. Локалізація українською поки не ідеальна тож скоріш за все частину матеріалів доведеться адаптувати самостійно. Питання розміщення даних вирішується індивідуально, адже рішення працює у хмарі, що не завжди відповідає політикам великих підприємств. Вартість у глобального постачальника теж може бути високою, тож важливо показати реальний вплив на зниження ризиків.

1.3.2 KnowBe4

KnowBe4 – найвідоміша у світі платформа тренінгів з кібербезпеки, заснована відомим експертом Кевіном Митником. Вона неодноразово визнавалася лідером Gartner Magic Quadrant і має найбільшу ринкову частину.

Платформа пропонує величезний вибір мікроуроків, інтерактивних курсів і симуляцій на теми від фішингу паролів до приватності та цифрової безпеки. Персоналізовані вбудовані алгоритми мають змогу гнучко підлаштовувати складність завдань під рівень користувача.

Найсильнішою стороною KnowBe4 треба вважати розроблені інтеграції та зручність налаштування додатку. Платформа легко працює з корпоративною поштою, добре масштабується і спрощує операційну роботу завдяки автоматичним планам навчання і динамічним групам які діють за правилами та готовими рекомендаціями. Для адміністраторів передбачено автоматичні плани навчання, динамічні групи та рекомендації з частоти кампаній.

Найбільшою перешкодою для впровадження платформи є її розташування у хмарі, у компаніях із жорсткими політиками, такі як банкові установи, питання дуже гостре.

1.3.3 Cofense (PhishMe)

Cofense PhishMe відомий нащадок однієї з перших платформ фішинг-симуляцій (PhishMe, запущеної ще у 2008 році). Наразі велика частина екосистеми Cofense зосереджена на повному циклі боротьби з фішингом, що включає в себе від навчання до виявлення і знешкодження атак.

Cofense PhishMe вирізняється реалістичністю підходу та глибиною у векторі email загроз. Сценарії базуються на реальних атаках, які щоденно фіксуються та оновлюються за допомогою глобальної мережі користувачів кнопки Reporter та інтеграції з поштовими шлюзами. Як результат симуляції дуже схожі на реальні загрози й чудово тренують увагу. Після кожної симуляції користувач отримує короткий відеоурок або мінікурс, що допомагає швидко усунути прогалини у знаннях. Хоча, нажаль, база знань по курсам дуже обмежена порівняно з іншими додатками.

Також треба зазначити інтеграцію з SOC, зазвичай механізм роботи системи, такий як Reporter робить співробітників “сенсорами безпеки”, Triage

автоматизує обробку повідомлень у SOC, Vision видаляє небезпечні листи з поштових скриньок, а Intelligence додає аналітику про нові кібератаки. Як результат, платформа демонструє себе найкраще у компаніях, які вже інвестують у SOC, мають інтеграції з SIEM, та прагнуть з'єднати навчання з реальними інцидентами, щоб вимірювати ефект не лише за відсотком кліків, а й за швидкістю репортів і скороченням шкоди. Якщо ж потрібна максимально широка тематика навчання та висока ступінь автоматизованих сценаріїв змішаної складності, варто передбачити додаткові джерела контенту або порівняти сумарну цінність із більш універсальними платформами.

1.3.4 Proofpoint Security Awareness Training (PSAT)

Proofpoint один з відомих постачальників рішень кібербезпеки для підприємств, особливо у галузі email-захисту. У сферу навчання з кібербезпеки Proofpoint увійшов у 2018 році, придбавши компанію Wombat Security (піонера у цьому напрямку). Тепер їхній продукт називається Proofpoint Security Awareness Training і є частиною стратегії "People-Centric Security". Що вирізняє Proofpoint SAT:

Proofpoint Security Awareness Training є платформою, що поєднує навчання з реальними загрозами електронної пошти завдяки тісній інтеграції з екосистемою Proofpoint. Завдяки інтеграції з екосистемою Proofpoint платформа використовує аналітику Targeted Attack Protection та концепцію "Very Attacked People", тобто навчає саме тих, хто найчастіше стає мішенню.

Платформа підтримує персоналізовані траєкторії, автоматичний добір курсів і симуляцій відповідно до ролі користувача, рівня вразливості та історії взаємодії з фішинговими листами. Доступна велика бібліотека мультимовного

контенту, від мікроуроків до повноцінних інтерактивних модулів, а також навчальні матеріали на випадок помилки користувача у форматі just in time, що допомагає закріплювати навички в момент поведінкової події. Аналітичні панелі орієнтовані на зміни поведінки, є зручні звіти для керівництва, можливість відслідковувати динаміку кліків, частку повідомлень про підозрілі листи, завершення курсів, порівнювати підрозділи та будувати обґрунтування ефективності програми в категоріях ризику.

Основним недоліком програми виступає складність та ціна. Через широку функціональність метрик навчання для адміністраторів доволі крута, а без продуманої стратегії кампанії можуть втратити темп. Повна ефективність PSAT розкривається у зв'язці з іншими продуктами Proofpoint, що збільшує загальну вартість. Локалізація українською поки не завжди глибока, тому матеріали доведеться адаптувати під місцевий контекст. Також хмарна модель може вимагати погоджень щодо зберігання даних.

Загалом, Proofpoint SAT найкраще підходить компаніям, які вже користуються продуктами Proofpoint і прагнуть поєднати дані про реальні загрози з навчанням. Для локальних рішень на кшталт ITS CSAT цей приклад демонструє, як ефективно об'єднувати аналітику, адаптивність і масштаб. Водночас, спрощені локальні аналоги можуть вигравати за швидкістю впровадження, зручністю і ціною.

1.3.5 ITS CSAT

ITS CSAT (Cybersecurity Awareness Tracker) – це платформа українського походження для навчання співробітників кібербезпеці, яка надає персоналізоване навчання, симуляції кібератак (наприклад, фішингові

розсилки), аналітику знань користувачів, моніторинг прогресу та автоматизацію планування навчальних кампаній.

Застосунок містить все необхідне для ефективного навчання: від планування навчальних активностей та розподілу матеріалів до проведення симульованих фішингових атак і детальної аналітики результатів.

ITS CSAT автоматично визначає рівень ризику кожного співробітника, створює персоналізовані програми навчання та відстежує прогрес у реальному часі.

Основними перевагами додатку ITS CSAT можна вважати:

— контрольовані симуляції реальних загроз у захищеному середовищі, співробітники вчаться на помилках без ризику, а ви отримуєте картину готовності до реальних атак;

— планування активностей з між підрозділами та оптимізацією навантаження на співробітників;

— єдина точка контролю всіх навчальних процесів;

— створення тестів, розсилка унікальних посилань, відстеження проходження курсу користувачами та з миттєвою синхронізацією результатів;

— Real-time дашборди з ключовими метриками, рекомендації щодо активностей на основі рівнів обізнаності та ризику;

— система сама визначає наступні кроки та формує звіти;

— взаємодія з багатьма джерелами даних для інформації про співробітників;

— синхронізація результатів з HR системами, експорт звітів через API;

— HR бачить навчання, безпека керує симуляціями, керівництво отримує аналітику.

Повністю українська onpremis розробка, яка включає переваги минулих рішень та не має недоліків у вигляді ціни.

Висновки до першого розділу МД

Проведений аналіз показав, що фішинг в електронному листуванні залишається однією з найактуальніших і найнебезпечніших загроз у сфері інформаційної безпеки. Його природа постійно змінюється — зловмисники вдосконалюють технічні прийоми, використовують соціальну інженерію та психологічні маніпуляції, що робить традиційні технічні методи захисту недостатніми. Навіть найсучасніші фільтри та системи виявлення загроз працюють із певною похибкою, тому головним елементом безпеки залишається людина. Саме людський фактор визначає успіх або провал захисту організації від фішингових атак.

Розгляд сучасних підходів до протидії фішингу дозволив зробити висновок, що ефективне рішення можливе лише за умови поєднання трьох складових: технічних інструментів захисту, системного навчання персоналу та впровадження внутрішніх політик безпеки. Комплексний підхід, у якому працівники не є “слабкою ланкою”, а виступають активними учасниками процесу захисту, дає змогу істотно зменшити ризик успішної атаки. Регулярне навчання, симуляції фішингових листів, негайний персоналізований зворотний зв’язок і вимірювання поведінкових показників сприяють формуванню стійких звичок безпечної поведінки.

Порівняльний аналіз провідних світових платформ показав, що кожне рішення має власну концепцію й фокусується на різних аспектах проблеми.

Terranova Security вирізняється гнучкістю, мультимедійністю та орієнтацією на великі підприємства з міжнародною структурою. KnowBe4 є наймасштабнішим рішенням із величезною бібліотекою контенту, високим рівнем автоматизації та простотою впровадження, хоча потребує адаптації до локальних умов. Cofense PhishMe демонструє глибоку інтеграцію з операційними процесами SOC, забезпечує найреалістичніші фішингові симуляції та замкнений цикл реагування, проте має вузьку тематику. Proofpoint SAT поєднує навчання з реальною аналітикою загроз, орієнтуючись на організації з високими вимогами до безпеки, однак є складним і дорогим у розгортанні.

На тлі цих глобальних рішень ITS CSAT займає перспективну нішу локального, персоналізованого продукту. Його потенціал полягає у поєднанні кращих практик провідних систем (інтерактивне навчання, фішинг-симуляції, поведінкова аналітика) з перевагами локалізації — підтримкою української мови, культурною релевантністю та гнучким налаштуванням під конкретні потреби компаній. Подальший розвиток ITS CSAT може включати розширення бібліотеки контенту, впровадження автоматизованих рекомендацій на основі оцінки ризиків, інтеграцію з інфраструктурою безпеки (SOC/SIEM) і вдосконалення користувацького досвіду.

Узагальнюючи, можна стверджувати, що жодна система не забезпечує повного захисту від фішингу окремо. Лише поєднання технологічних рішень, адаптивного навчання та побудови культури безпеки створює надійний бар’єр проти сучасних загроз. Саме в цьому контексті подальший розвиток і позиціонування ITS CSAT як гнучкої, локально орієнтованої та ризик-адаптивної платформи є логічним і перспективним напрямом для підвищення стійкості українських організацій до фішингових атак.

2 ЗАПОБІГАННЯ ВРАЗЛИВОСТІ ВІД ФІШИНГ-АТАК НА КОРПОРАТИВНИХ КЛІЄНТІВ МЕТОДОМ НАВЧАННЯ ПЕРСОНАЛУ

2.1 Навчання персоналу як спосіб захисту від фішингових листів

Зважаючи на те, що технічні засоби не мають сто відсоткової гарантії захисту, а також інколи можуть мати недоліки у вигляді навантаження трафіку, зниження швидкості або блокування доставки електронних листів. Фільтри спаму або блеклисти, антифішингові механізми, політики SPF/DKIM/DMARC, ізоляція вкладень у «пісочницях», репутаційні перевірки доменів і переписування URL звісно допомагають з боротьбою, але їх налаштування та підтримка коштує великих грошей. Для малих або середніх організацій багатошарове налаштування описаних вище систем стає непідйомним по грошам та неможливим з точки зору найму спеціалістів для підтримки та оновлення встановлених систем.

Злочинці також не стоять на місці і вигадують нові способи обійти сучасні технічні засоби захисту. Вже не можна з’ясувати чи підроблений лист по грамотності напису змісту, а з додаванням генеративних моделей це стає неможливим. Саме через це навчання персоналу дає змогу закрити критичні прогалини оборони за допомогою простих та дієвих методів. Підвищення обізнаність, формування стійких навичок розпізнавання ризиків і набуття правильних навичок стає ще одним захисним шаром безпеки для організацій різного рівня. У поєднанні з технічними контролями якісно організоване навчання перетворює користувача з «останньої лінії» на повноцінний датчик

безпеки, який вчасно дає змогу розпізнавати, утримувати від кліку та повідомляти про підозрілі листи.

Основна суть політик навчання полягає у безпосередній передачі знань та зміни поведінки користувачів під час використання такого вразливого елементу як електронна пошта. Співробітник після проходження курсу навчається швидко оцінювати ризик, діяти за простим алгоритмом і автоматично застосовувати його під тиском терміновості та авторитету відправника. Для того, щоб сформувати такі навички, потрібно безперервно розробляти адаптивні та пізнавальні курси та міні-квізи, які дозволять закріплювати навички через повторення у реальних або наближених до реальних умовах. Саме через це програми протидії мають включати реальні симуляції фішингових листів, які формують практичну навичку розпізнавання ризиків і правильних дій у природному робочому середовищі. Але, нажаль, таких програм обмаль, та їх адаптивність складна у налаштуванні та оновлення не є періодичним. Симуляції не можуть підміняти технічні контролі, але за допомогою поєднання дають змогу закривати прогалини саме там, де автоматичний фільтр пропускає лист. Досвідчено навчене око і відточений рефлекс користувача зупиняють інцидент. Такий сценарій є ідеальною складовою захисту.

Безперервне навчання вимагає також постійного оновлення матеріалу курсів, а деякі замовники бажають мати змогу створювати особисті курси для навчання свого персоналу. При власноручному створенні курсі варто врахувати етичні норми, хоча ми намагаємося створювати реальні кейси, не потрібно використовувати надмірно чутливі теми або персональні данні, які неможливо знайти у відкритих джерелах(рисунок 1.4).

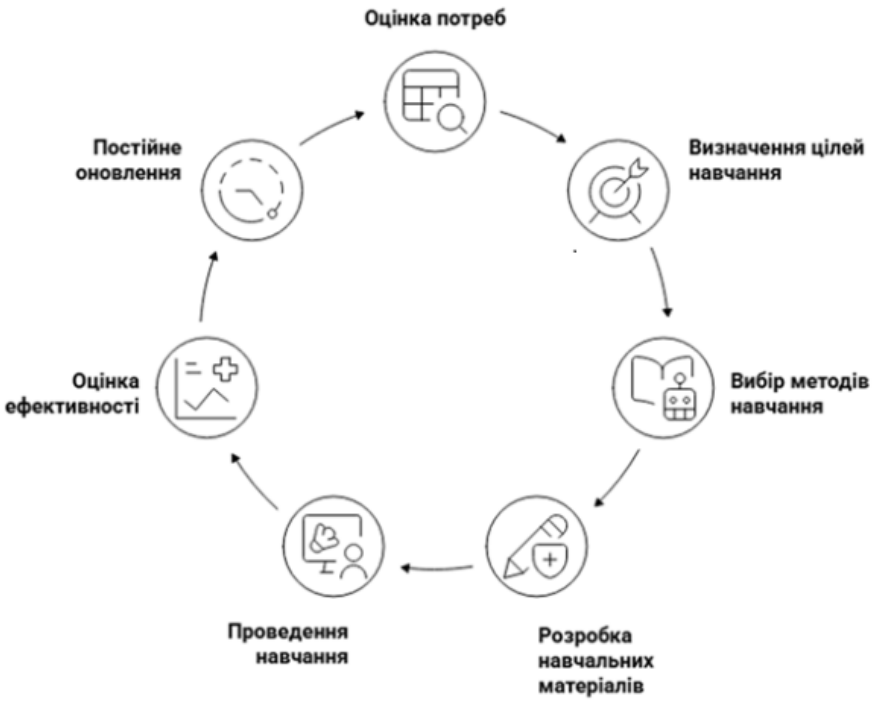

Рисунок 1.4 – Цикл безперервного навчання персоналу

Для перевірки засвоєння знань пропонується впровадження фішингових симуляцій. Ефективності проходження курсів якраз буде оцінюватися цими симуляціями. Також увагу слід приділити створенню ранжування курсів в залежності від підрозділу компанії, бо робітники можуть по різному реагувати на одні й тіж самі листи, наприклад, при надсиланні якогось підробного кредитного обліку або звіту за місяць до бухгалтера результат фішингу може мати успішний шанс на спрацювання, а вже менеджер з проектів поставиться до листа з підозрою та може не відкривати та уникнути фішингу. Навпаки, ж ситуація з листом, який містить розширення .logs може привернути увагу аналітика безпеки і він, не перевіряючи, відкриє його, а

звичайний офісний працівник буде вважати це спамом та повідомить про інцидент відділ безпеки.

Об’єднавши разом симуляції з навчальними модулями в один безперервний цикл, ми маємо змогу досягти краще результатів у захисті електронної пошти. Технічно це реалізується через інтеграцію симулятора, поштового клієнта та системи управління навчанням (LMS). На основі risk-score користувача LMS автоматично призначає релевантні модулі (базові пояснення, рольові кейси, тренажери перевірки URL, вправи з «OAuth-згоди» чи QR-фішингу) і планує повторні симуляції з поступовим ускладненням.

У підсумку, правильно розроблена система, яка буде включати періодичні реальні фішинг симуляції з використанням сучасних електронними листами, так і навчання по протидії різним тактикам, створених зловмисниками може дозволити поліпшити захист пошти. Створення методу, який об’єднує дві технології разом та самостійно визначає ризик людини і згідно нього назначає проходження курсу або симуляції фішингових атак є інноваційним та важливим рішенням, яке потребують сучасні компанії.

2.2 Метод Train–Simulate–Measure боротьби з фішингом через навчання персоналу

2.2.1 Концепція методу Train Simulate Measure

У багатьох сучасних компаніях електронна пошта залишається основним засобом ідентичності та службових дій, бо саме через цей поштовий канал відбуваються підтвердження входу, відновлення паролів, сповіщення від соціальних мереж і хмарних сервісів, узгодження внутрішніх операцій. Як

висновок, будь-яка програма протидії фішингу повинна починатися з електронної пошти і завершуватися у ній. Метод Train Simulate Measure (TSM) пропонує цілісний і керований цикл, що об’єднує технічну інфраструктуру симуляцій, вимірювання, прогнозування поведінки користувачів та їх персоналізоване навчання. Основним джерелом методу є власна інфраструктура розсилок і телеметрії, що створює реалістичні сценарії і автоматично перетворює кожну взаємодію співробітника з листом на матеріал для аналізу ризиків та прогнозування подальших дій. Даний метод працює постійно, на відміну від епізодичних лекцій або разових інформаційних кампаній, адаптується до змін різних тактик зловмисників і забезпечує постійний зворотний зв’язок, що закріплює правильну поведінку користувачів.

Базова суть методу TSM полягає в тому, що навіть найкращі технічні рішення не можуть гарантувати абсолютну безпеку. В сучасному середовищі зміст листів стає грамотно написаним, стилістика копіює внутрішні шаблони, ланцюжки доменів вибудовуються так, щоб пройти репутаційні перевірки, і тому людина лишається останнім бар’єром, бо саме її навички та звички впливають на результат. Метод TSM перетворює користувача з слабкої ланки на активний запобіжник небезпеки. Для цього кожен етап тісно пов’язаний із наступним: симуляція запускає вимірювання, результат вимірювання автоматично призначає курс, курс завершується цільовою перевіркою, а агреговані підсумки формують оновлену програму наступної хвилі. Таким чином система сама безперервно навчається на власних даних, аналізує їх і поступово знижує сукупний ризик організації.

2.2.2 Складові ефективності використання методу TSM

Першою складовою і умовою ефективності використання методу TSM є володіння власним SMTP середовищем для розсилки симуляційних листів. Саме контроль над поштовою інфраструктурою дозволяє створювати сценарії, що максимально наближені до реальних, а також керувати технічними параметрами, саме тут можна використовувати домени, подібні до внутрішніх або партнерських, варіювати таймінги доставок, моделювати типове навантаження на співробітників у робочий день. Це дозволяє готувати варіанти листів, що імітують сповіщення соціальних мереж про порушення політик, попередження рекламних кабінетів, документи від відділу кадрів, повідомлення фінансового відділу про звірку рахунків. Контрольованість SMTP шляху дає можливість коректно працювати з DKIM і SPF, що завжди підвищує правдивість симуляцій і одночасно не порушує правил внутрішньої безпеки компаній. При належному маркуванні та ізоляції доменів симуляцій організація не змішує тренувальний трафік з реальним, але зберігає необхідний рівень реалістичності.

Другою складовою ефективності використання методу TSM є система детекції і повної телеметрії дій користувачів з симуляційними листами. Завжди потрібно фіксувати факт відкриття листів, переходи за посиланнями, введення даних на підроблених формах, завантаження різних вкладень, будь-які спроби пройти двофакторну перевірку. Потрібно використовувати для цього пікселі відстеження для відкриттів, параметризовані посилання, які генерують унікальний маршрут для кожного адресата, а також тренувальні цільові сторінки із захищеним збиранням подій. У випадку сценаріїв із псевдоформами автентифікації потрібно налаштувати окремий набір телеметрії, коли користувач не лише переходить за посиланням, а й вводить логін, пароль, коди з додатків або підтвердження в системі багато факторної перевірки. Усі події, що відбуваються, повинні записуватися у актуальному

часовому розрізі, оскільки швидкість реакції є так само важливим індикатором, як факт неправильної дії. Відлік моменту до отримання листа до кліку та від кліку до введення даних можна оцінювати як ризики терміновості та важіль соціально інженерних тригерів.

Тертою складовою ефективності використання методу TSM стає звітність, яка складається на основі зібраної телеметрії. Система може автоматично генерувати звітність за кожну хвилю симуляцій, в ній відображається рівень ризику для кожного користувача, команди і підрозділу. Кожен ризик вираховується з урахуванням різних даних, потім вираховується окремий індекс ризику, командний індекс і агрегації, усі ці індекси прив'язані до порогових значень, що запускають навчальні програми.

Четвертою складовою ефективного використання методу TSM є автоматизована система координації навчання користувачів на основі аналізу опрацьованих ризиків. Після кожної хвилі симуляцій і публікації звіту система управління навчанням отримує дані і призначає інтервенції: для одних користувачів із низьким ризиком достатнім є невеликий мікротест і заохочення за швидкі правильні рішення, для профілів середнього ризику заплановано короткий курс навчання із практичними вправами, що відповідають саме тим діям, які були проігноровані, а вже для користувачів з високим ступенем ризику призначається навчальний модуль з інтерактивними вправами і тестуванням отриманих навичок. Визначення рівнів навчання відбувається швидко, без затримок, поки подія ще в пам'яті користувача, адже навчання в момент виниклої потреби закріплює правильні реакції краще за абстрактні лекції. Після завершення навчання система надає перевірочний тест, що копіює схожу схему атаки, якою користувач раніше був вражений. У тому випадку, якщо поведінка правильна і користувач розпізнає спробу фішингу, можливі ризики переглядаються, то профіль користувача повертається до нормального рівня.

У випадку повторення помилкової поведінки, відбудеться перерозподіл основних завдань на рольовому рівні та додаткові навчальні тренінги.

Для забезпечення реалістичності симуляцій фішингових атак на корпоративні мережі у листах використовується окремі вимоги: усі листи повинні створювати структуру і копіювати стиль реальних повідомлень, це стосується не лише адрес відправника, а і відображуваного імені, макета, мови, часу, підпису тощо. Потрібно повторювати загальні теми, що атакують соціальні мережі та пов'язані з ними сторінки, також це може бути повідомлення про порушення політик спільноти, заклики про призупинення рекламних кампаній, повідомлення про оновлення платіжних та персональних даних, сповіщення про підозрілу активність із пропозицією негайно пройти ідентифікацію. Різні варіанти ідуть далі за один крок і запускають ланцюжок подій: наприклад, перший лист готує користувача психологічно, другий підштовхує до дії, третій імітує підтримку у приватних повідомленнях. Саме такий формат повинен розвивати уважність та критичність мислення у динаміці, вчить перевіряти інформацію лише в офіційних кабінетах, не сподіватися на достовірність посилання з листа. Обрана програма ITS CSAT має вбудований механізм завантаження реального листа фішингу, який перевіряється системою і на місцях IoC (індикатори компрометації) ставлять теги, на які програма буде посилатися і підставляти туди вже самостійно створені дані, саме це забезпечує максимальну реалістичність.

Основним показником в методиці є зворотний зв'язок з користувачем: після будь-якої дії в симуляції система усе аналізує та повинна надавати короткий розбір помилок і, якщо користувач натиснув на посилання або виконав неправильні дії, то він у кінці симуляції одразу бачить пояснення: які ознаки ризику були в листі, де саме у макеті вони розташовані, як розрізнити підміну адреси відправника, як критично оцінити запит на терміновість, яке

посилання є небезпечним. У випадку, коли користувач все правильно виконав, тоді він після закінчення симуляції отримає повідомлення у вигляді подяки і мініпідказки з корисною практикою. Саме такий розбір та аналіз дій користувача перетворює помилки на навчальні моменти, а правильні дії на закріплену звичку, а також знижує тривожність і надає відчуття контролю над ситуацією.

2.2.3 Основні елементи методу TSM

Система оцінки ризиків є центральною частиною Measure. Завжди варто застосовувати математичну модель, яка комбінує поведінкові метрики, кількість доступів і всю історію навчання. Як, наприклад, кожен клік за симуляцією має певну вагу, введення облікових даних підвищує вагу, а проходження перевірки у двофакторному сценарії ще вище важить, і якщо швидкість кліку підвищує вагу події, то швидкість повідомлення знижує. Далі потрібно застосовувати коефіцієнт ролі, що враховує вартість потенційної помилки для бізнесу, бо на виході модель повертає бал, який порівнюється з порогами для навчальних дій. Дуже важливо враховувати, що скоринг не є вироком, це механізм пріоритезації навчання і підтримки. Тому пізніше, якщо користувач демонструє свою правильну поведінку у тестових листах, бал ризику знижується і профіль повертається у безпечну зону.

Цей метод може також передбачати планові перевірки поза циклом навчання, організація деколи проводить незалежні хвилі перевірочних листів без попередніх курсів. Мета цієї дії полягає у перевірці довготривалої пам’яті помилок і виявленні нових патернів вразливості системи. Завжди результати таких хвиль аналізуються та порівнюються з попередніми випадками, якщо

спостерігається сплеск кліків на певну тему - контент навчання оновлюється, а наступна хвиля симуляцій адаптується під нову тактику зловмисників. В такому стані перевіряється актуальність програми безпеки навіть у сучасному мінливому середовищі.

Системність підходу полягає у з’єднанні усіх трьох складових у безперервний цикл: Train відповідає за розвиток навичок через мікрокурси, інтерактивні кейси, рольові вправи, Simulate вносить реальність у тренажер, створює безпечне поле для перевірки поведінки у звичних інструментах, Measure перетворює події на дані, а дані на рішення, забезпечуючи адресність і персоналізацію навчання. Коли усі ці компоненти працюють разом, то організація отримує результат, що не дає жодна частина окремо. Коли користувач відкриває електронну пошту та бачить лист, то у нього вже сформована звичка перевіряти адресу відправника, він уважно дивитися на домен, знає, що не потрібно виконувати дії з посилання листа, а завжди використовувати офіційні кабінети і кнопки повідомлення. Лише так формується культура безпеки, що тримається на системі, а не на разових кампаніях. Основні елементи системи та їх призначення наведено на рисунку 2.1.

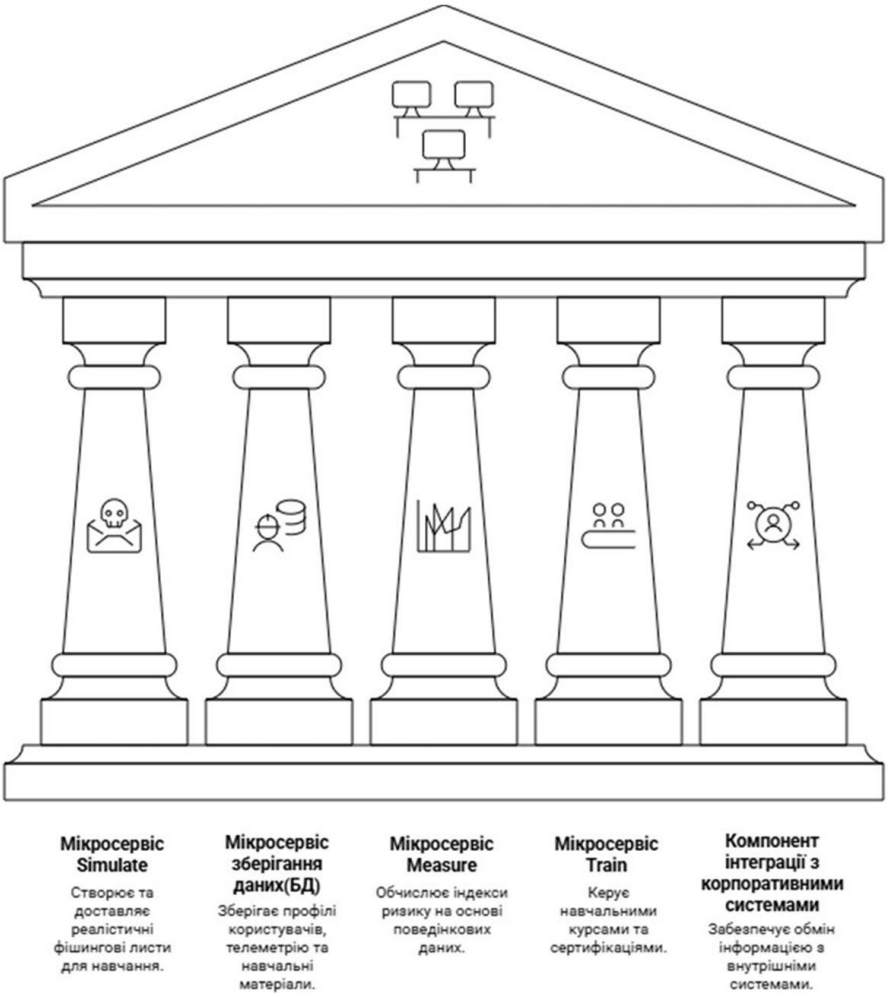

Рисунок 2.1 – Основні компоненти методу TSM

Дуже важливо використовувати стратегію контент оновлень. У сучасному світі навчальні матеріали мають прогресувати, бо методи фішингу змінюються. Відповідальні за безпеку аналізують реальні інциденти, готують доповіді з новими прикладами, проводять тематичні хвилі симуляцій,

наприклад, присвячені новим тактикам кібератак у соціальних мережах. Завжди використовуються короткі інформаційні оголошення на корпоративних ресурсах із прикладами червоних прапорців, але вони повинні доповнюватися практикою у вигляді таргетованих симуляцій і мінікурсів, коли теорія підкріплюється дією, то шанс перенесення отриманих знань у щоденні звички стрімко зростає.

Результативність методів програми потрібно оцінювати не лише за часткою кліків і введень, потрібно дивитися на загальний результат: швидкість і якість користувацьких репортів, частоту повторних помилок, стійкість результатів після перерв між хвилями, перенос навичок у суміжні канали. Завжди показово, коли після впровадження системної програми зростає число повідомлень про підозрілі листи до запуску чергової симуляції, це значить, що користувачі стали більш навченими. Гарним маркером успіху є зменшення кількості випадків зміни облікових даних або втрати контролю над ресурсами у соціальних мережах, дуже важливо фіксувати ці показники та порівнювати їх із попередніми періодами.

2.2.4 Актуалізація та вимір результатів

Метод Train Simulate Measure забезпечує окремі переваги для організації: по-перше, він переводить розмову про обізнаність з площини вражень у площину даних - керівник завжди отримує конкретні цифри і може планувати ресурси навчання раціонально; по-друге, він формує в користувачів стійкі навички, які працюють у стресових ситуаціях; по-третє, він підвищує загальну культуру безпеки, де кожен співробітник розуміє свою роль, не боїться повідомляти про підозрілі випадки і має інструменти, щоб зробити це

швидко; і по-четверте, метод робить технічні контролі ефективнішими, адже симуляції допомагають виявляти прогалини у правилах фільтрації та налаштуваннях поштових шлюзів.

Як висновок, метод Train Simulate Measure це практичний і перевірений для зниження ризику фішингових атак через канали електронної пошти: власні SMTP сервери забезпечують реалістичні розсилки і контрольовану телеметрію, система детекції збирає події відкриттів, переходів, введень і спроб проходження багатофакторної перевірки, звіти перетворюють події на індекси ризику для людей і команд, навчальна платформа призначає мікрокурси, рольові модулі і перевірочні листи відповідно до реальної поведінки, регулярні позапланові хвилі підтримують готовність і вимірюють довготривалу пам’ять. Усе це працює як єдина система, у якій кожна дія користувача стає шансом навчитися, а кожен навчальний крок перевіряється в реалістичному моделюванні. Лише така взаємодія навчання та симуляцій закриває прогалини, що неминуче проходять крізь технічні фільтри, й забезпечує стабільне зниження імовірності успішної компрометації поштових облікових записів та пов’язаних із ними ресурсів у соціальних мережах і корпоративних сервісах.

2.3 Умови ефективного впровадження методу навчальної програми

Ефективне впровадження навчальної програми протидії фішингу в компанії починається із чіткого плану та узгоджених цілей, керівництво має формально закріпити мету програми, очікувані результати та відповідальних за їх досягнення. Це говорить про вимірювані орієнтири, які зрозумілі всім учасникам процесу, але коли очікування щодо зниження ризику, підвищення частки користувацьких репортів і скорочення часу реагування описані і

доведені до команд, то навчання з інструменту безпеки перетворюється на частину операційної моделі організації. Дуже важливо також зафіксувати зв'язок із цілями бізнесу, адже програма має не лише захищати від інцидентів, а й підтримувати безперервність операцій, зберігати репутацію і контроль над безпекою.

Другою важливою умовою є грамотне управління змінами: навчальна програма змінює звичну поведінку співробітників, а будь-які зміни викликають природний опір. І в цій ситуації потрібно зменшити тертя, необхідна прозора комунікація і зрозуміла відповідь на питання навіщо, що саме відбуватиметься, як це вплине на повсякденну роботу і які вигоди отримає кожна роль. Потрібно заздалегідь показати як виглядає взаємодія з навчальними модулями, як виглядають симуляційні листи, і як використовувати алгоритм дій при підозрілих повідомленнях.

Третя передумова забезпечується підготовкою інфраструктури і процесів ще до запуску навчання. Потрібно впровадити не лише технічну готовність поштового середовища до інтеграції з симулятором, а і систему телеметрії для фіксації дій користувача, і платформу управління навчальним контентом, а також канали зворотного зв'язку. Необхідно обов'язково протестувати систему: як швидко сповіщення доходять до відповідальної команди, які дані передаються автоматично, та чи достатньо їх для розслідування, чи не відсічуть поштові шлюзи тренувальний трафік завчасно. Також на рівні взаємодії процесів важливо розподілити хто і коли інформує підрозділи про результати, як часто плануються наступні хвилі і хто ухвалює рішення щодо зміни напрямків навчальної траєкторії.

Зокрема, особливої уваги потребує питання приватності, законності та етики: інформація про кліки, введення облікових даних і поведінку співробітників у симуляціях є персональними і організація повинна

насамперед визначити перелік даних, які збираються, строки зберігання, коло осіб з доступом. У внутрішніх документах потрібно визначити, що метою програми є навчання та зниження ризиків кібератак, а не дисциплінарні заходи, бо саме цей простір створює передбачувані правила і підвищує довіру.

Однією з важливих засад успіху є локалізації контенту і культурної релевантності, застосовані навчальні приклади повинні говорити мовою співробітників і віддзеркалювати реалії конкретного бізнес домену. При виборі програми, де можна реалізувати метод, саме через це питання стало вагомим приводом використовувати CSAT. При запровадженні завжди потрібно враховувати внутрішній стиль комунікації, часові проміжки, поширені теми і жаргон. Усі візуальні зразки листів мають відповідати тим інструментам, якими реально користуються команди, бо коли навчання впізнаване і близьке до щоденного досвіду, йому довіряють і його легше адаптувати у реальну поведінку.

Не менш важливою передумовою є закладання часового бюджету і управлінських стимулів на рівні керівників. Бо саме навчання, симуляції і короткі розбори дій займають час, тож це має бути офіційно відведений ресурс, а не додаткове завдання після всього. Саме коли керівники планують навчальні активності у робочому календарі і демонструють власну участь, програма отримує необхідний пріоритет, тому доцільно сформувати прості індикатори, які входять у регулярні огляди. Ці схеми дій насамперед говорять про відповідальність за культуру безпеки в команді.

Для більшої масштабованості програми потрібно обирати модульну архітектуру контенту і сценаріїв, а замість тривалих курсів краще мати короткі блоки, що складаються у гнучкі траєкторії. Якщо телеметрія показує вразливість до певної ознаки, призначається саме той модуль, який її адресує, бо це зменшує когнітивне навантаження і підвищує відсоток завершення.

Модульність полегшує оновлення навчальних матеріалів і дозволяє швидко реагувати на появу нових сучасних тактик зловмисників.

Ефективність навчальної програми завжди залежить від якості зворотного зв'язку, тому розбір помилки чи правильного рішення повинен бути коротким, конкретним і спрямованим на дію. Якщо співробітник одразу отримує пояснення та навички на що звернути увагу наступного разу і як перевірити сумнівне посилання без ризику, тоді він відчуває контроль і прагне поліпшити свій попередній результат. Для скорішого закріплення здобутих знань варто використовувати прості приклади з реальних інцидентів в компанії, які очищені від чутливих даних, бо такий підхід створює відчуття практичної корисності і формує пам'ять через емоційне залучення.

Важливо забезпечити узгодженість та взаємодію навчальної програми з іншими елементами кібергігієни: якщо в пошті впроваджено маркування зовнішніх відправників, то у навчанні має бути пояснення того, як ним користуватися; якщо змінилися політики паролів або впроваджено апаратні ключі, то тренажери повинні відпрацьовувати саме ці нові правила. Симуляції виявляють технічні прогалини, наприклад, надто лояльні правила пропуску вкладень, і тоді сигнали з навчальної програми повинні спрямовуватися до команди, яка підтримує поштові шлюзи, так діє контур взаємопідсилення, де організація одночасно навчає людей і вдосконалює системи безпеки.

Одним з основних етапів є питання пілотування і поступового розгортання: саме запуск цієї програми на невеликій вибірці підрозділів допомагає зняти початкові ризики і налаштувати логіку. Саме пілот дозволяє оцінити зрозумілість інструкцій, роботу кнопки репорту, релевантність сценаріїв, навантаження на службу підтримки і час, який потрібен користувачу для завершення навчальних кроків.

Важливо уникати втоми від навчання, завжди потрібно керувати ритмом і різноманіттям форматів, навіть найякісніший контент може викликати перевантаження, якщо йде хвиля за хвилею без пауз і чергувань. Варто комбінувати короткі мікроуроки з рідшими, але глибшими практичними кейсами, іноді доречно замість листа із симуляцією надати коротке інтерактивне завдання або відеорозбір нового трюку зловмисників.

Ще одна важлива умова пов'язана з аналітикою на рівні організації - оглядові панелі, що показують динаміку ключових показників у часі, в розрізі підрозділів і ролей. Отриману інформацію потрібно систематизувати відносно обсягу поштового трафіку і змін у бізнес процесах, ще варто відстежувати опосередковані показники, наприклад, скорочення кількості інцидентів, які доходять до етапу блокування доступів, або зменшення витрат на реагування. Будь-яка аналітика є інструментом ухвалення рішень, а не лише ретроспективним звітом, коли керівництво бачить кореляцію між навчальними інтервенціями та зниженням ризику, то програма отримує стабільне фінансування і підтримку.

Завжди необхідно дбати про кадрове забезпечення програми, бо навіть за наявності новітніх платформ і повної автоматизації потрібні люди, які курирують контент, розробляють сценарії, аналізують результати, комунікують з підрозділами і налаштовують інтеграції. Доцільно створити невелику багатофункціональну групу, куди входять представники безпеки, IT інфраструктури, навчання і комунікацій, вона зменшуватиме час на узгодження і швидко перетворить дані на дії. Стійкість програми постійно підсилюється, якщо у кожному підрозділі є людина, відповідальна за локальну адаптацію матеріалів і підтримку колег.

Надійність впровадження програми залежить і від якості взаємодії з постачальниками технологій: якщо використовується зовнішня платформа для

симуляцій або навчання, то необхідно з’ясувати вимоги до інтеграції, умови зберігання даних, можливості експорту телеметрії та гнучкість у налаштуванні сценаріїв. Важливо забезпечити чіткі зобов’язання щодо доступності сервісів і часу реакції на інциденти в договірних відносинах. Для впровадження мною розробленого методу використовувався продукт компанії ITSpecialist, де я безпосередньо працюю.(можна ще пару рядків води про продукт або компанію якщо не буде вистачати змісту)

На завершення, як висновок, варто підкреслити роль позитивної мотивації - люди краще навчаються, коли бачать сенс, отримують визнання і мають простір для безпечної помилки. Невеликі заохочення за вчасні дедлайни, історії успіху у внутрішніх каналах, подяки від керівництва завжди формують культуру, де безпека сприймається як спільна справа. Коли співробітник усвідомлює, що його уважність та знання реально запобігли інциденту, навчання перестає бути рутинним і стає частиною його професійної гордості.

Сукупність описаних умов створює систему, де навчальна програма не просто існує, а дає відчутний результат. Чіткі визначені цілі і постійна підтримка керівництва, підготовлена інфраструктура, увага до етики і приватності, локалізований та доступний контент, збалансований ритм роботи, якісний зворотний зв’язок, зріла аналітика, підготовлена команда і продумана взаємодія разом формують основу для стійкого зниження фішингового ризику. Саме за таких умов метод навчання стає не одразовою кампанією, а невід’ємною частиною і системою операційної культури, яка самопідсилюється і підтримує безпеку електронної пошти та пов’язаних цифрових активів у довгій перспективі.

Висновки до другого розділу МД

У цьому розділі сформовано цілісну модель запобігання вразливості корпоративних клієнтів до фішингових атак із пріоритетом на канал електронної пошти, де вирішальним чинником стає підготовлений навчений користувач, який може розпізнати ознаки фішингу, відмовитися від ризикованої дії та оперативно повідомити про підозріле повідомлення. Насамперед тому навчання персоналу визначено як основний базовий інструмент зменшення ймовірності інцидентів і скорочення часу реагування на фішингові атаки, а його формат має бути практичним, контекстним і безперервним.

Запропонований метод Train–Simulate–Measure надає цій ідеї операційну завершеність та системність. Використання власних SMTP-розсилок для реалістичних симуляцій, телеметрія дій користувача від моменту відкриття листа до введення даних і проходження багатофакторної перевірки, а також автоматичне формування звітів із перерахунком у індивідуальні та командні індекси ризику створюють керований послідовний цикл. На основі ризик профілю система визначає таргетовані мікрокурси й рольові вправи, а згодом надсилає перевірочні листи для фіксації зміни поведінки. Такий контур знімає розрив між теорією і практикою, переводячи «обізнаність» у стійкі навички, що відтворюються під тиском терміновості та авторитету відправника.

Водночас ефективність методу залежить від умов його впровадження. В цьому розділі визначено управлінський мандат і вимірювані цілі, підготовку інфраструктури поштової інтеграції та збору телеметрії, етичні рамки обробки персональних даних, локалізацію контенту під доменну специфіку підрозділів,

доступність матеріалів для різних режимів і пристроїв, а також модульну архітектуру навчання з швидкими оновленнями під нові тактики зловмисників.

Сукупний ефект підходу залежить від зміщення фокусу з разових інформаційних кампаній на керовану поведінкову трансформацію, в якому організація отримує не лише кращі показники за симуляціями, а й відчутні зміни у виробничій практиці: зростає частка коректних користувацьких репортів, скорочується час між отриманням листа і повідомленням, зменшується кількість випадків передачі облікових даних і небезпечних дій у рекламних та адміністративних кабінетах соціальних мереж. Навчання у цьому випадку стає частиною операційної культури, а не додатковим навантаженням, оскільки кожен крок у циклі закінчується вимірюванням і персональним зворотним зв’язком.

Отже, поєднання практико орієнтованого навчання, реалістичних поштових симуляцій та аналітики ризику формує стійкий захисний прошарок, який доповнюється технічними контролями та компенсує людський фактор. Розроблений у розділі підхід придатний до масштабування, забезпечує прозорість для менеджменту й аудитів, а головне — демонструє кероване зниження імовірності успішної компрометації корпоративних облікових записів. У подальших частинах роботи доцільно представити результати впровадження на вибраних підрозділах, порівняти динаміку ключових показників до і після запуску програми та уточнити параметри моделі ризик-скорингу з урахуванням реальних інцидентів і сезонних коливань поштового трафіку. Це закріпить доказовість методу та стане основою для його тиражування на рівні всієї організації.

3 РЕАЛІЗАЦІЯ МЕТОДУ НАВЧАННЯ ПЕРСОНАЛУ ПРОТИДІЇ ФІШИНГУ

3.1 Архітектура системи TSM боротьби з фішингом через навчання персоналу

Система складається з трьох головних сервісів (рисунок 3.1): Simulate для проєктування і доставки симуляційних листів, Train для призначення навчальних дій та перевірок, Measure для збору телеметрії, обчислення ризику й аналітики. Кожен сервіс самостійно масштабується, має власні інтерфейси взаємодії і працює за принципом мінімально необхідних доступів, завдяки цьому рішення легко адаптується під різні організаційні структури та вимоги безпеки.

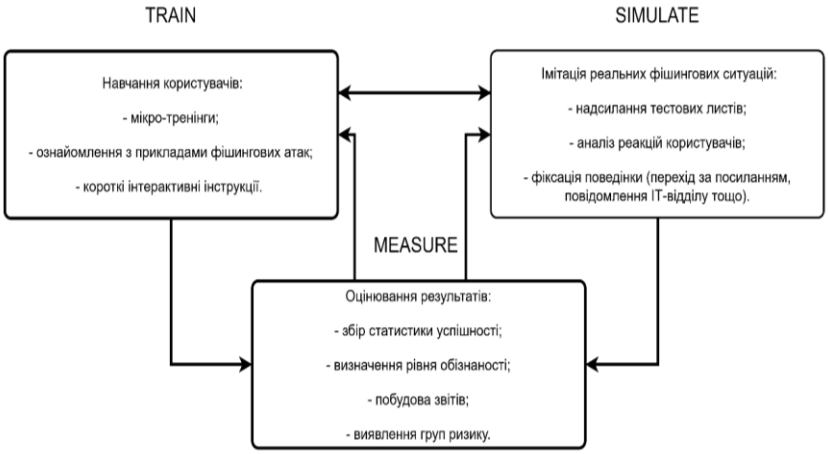

Рисунок 3.1 - Схема взаємодії систем методу TSM

Концепція методу включає в себе взаємодію користувача з симуляційними листами. Будь-який клік, відкриття, спроба введення даних або повідомлення про підозрілий лист перетворюються на автоматизовані дії з часовими мітками і довідковими атрибутами, потім ці події аналізуються та виставляють індекси ризику і формують навчальні призначення. Повернення до Simulate відбувається через планові та перевірочні відправлення, що повинні визначити, чи перетворилося знання на реальну навичку.

Для впровадження обраного методу потрібно використання програмного продукту який буде збирати данні, має можливість інтегруватися з корпоративними системами та у якому є можливість впровадження розробленого методу. Для реалізації методу TSM було обрано саме програму ITS CSAT (CyberSecurity Awareness Tracker) – система обліку активностей в рамках програм з підвищення обізнаності користувачів з питань кібербезпеки.

Застосунок призначений для оптимізації організації і ефективного планування навчань з кібербезпеки, моніторингу ризиків співробітників, зменшення ризиків кіберінцидентів, пов’язаних з людським фактором

На рисунку 3.1 показана загальна схема роботи програми CSAT, у яку імплементовано розроблений метод.

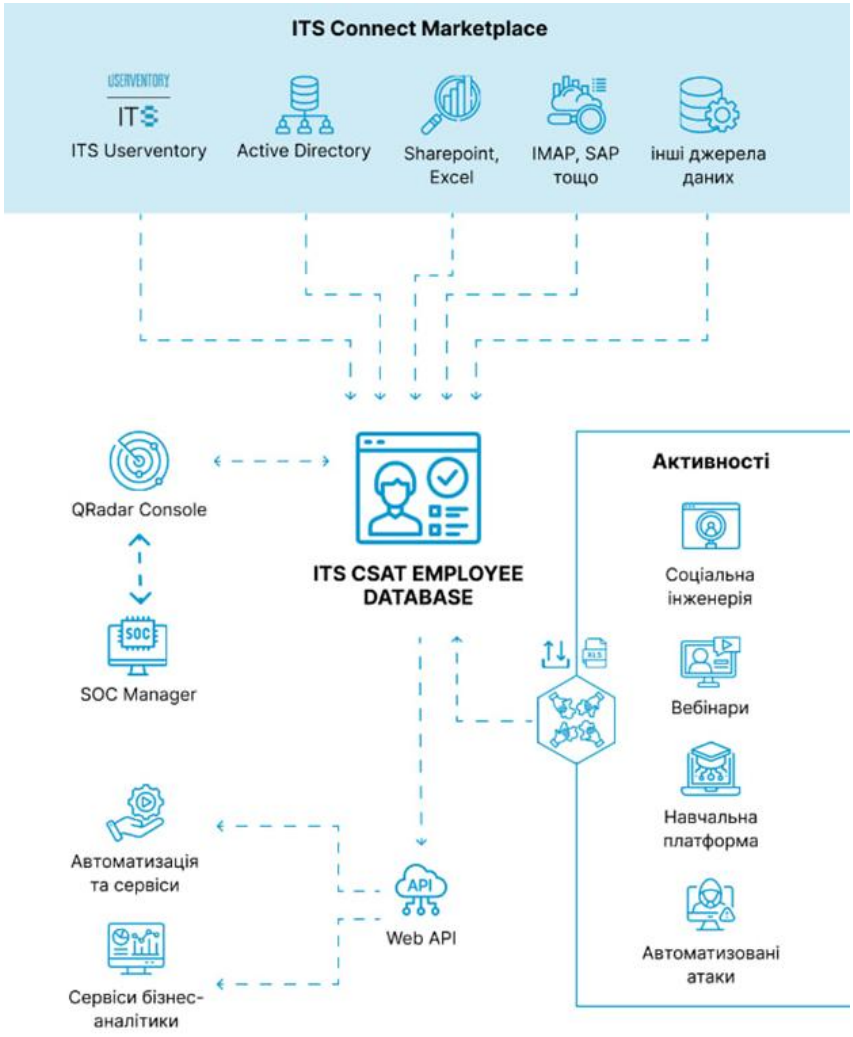

Рисунок 3.1 - Загальна схема роботи додатку ITS CSAT

Після аналізу внутрішньої роботи додатку було сформовано загальну схему роботи методу TSM у вигляді Work Flow впровадженого у програму CSAT і описано на рисунку 3.2.

Рисунок 3.2 - Схема циклу роботи методу Simulate–Train–Measurey

Сервіс Simulate забезпечує правдоподібну і керовану імітацію фішингових атак, він має власні SMTP сервери, виділені домени та піддомени, налаштовані записи SPF DKIM DMARC і окремі списки розсилок. Детальна архітектура роботи сервісу Simulate організованого на базі програми ITS CSAT зображена на рисунку 3.3.

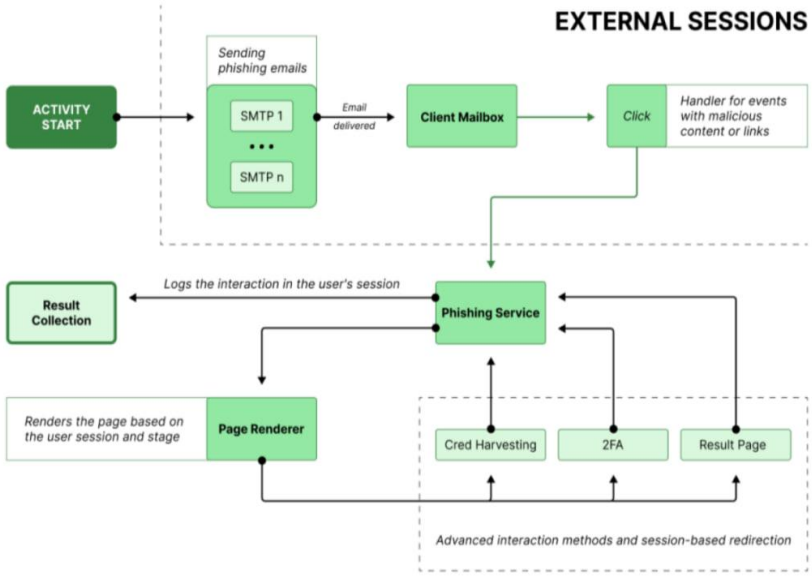

Рисунок 3.3 - Архітектура роботи активності сервісу Simulate

Все це дозволяє мати повний контроль над технічними параметрами і створювати сценарії, які максимально схожі на реальні службові повідомлення або листи від соціальних платформ, рекламних кабінетів, фінансових і кадрових систем.

Зміст електронного повідомлення створюється шаблонізатором із підтримкою персоналізації на основі тегів (міток), замість яких при

пересиланні вставляються персоналізовані посилання або конкретні данні користувача(рисунок 3.4.).

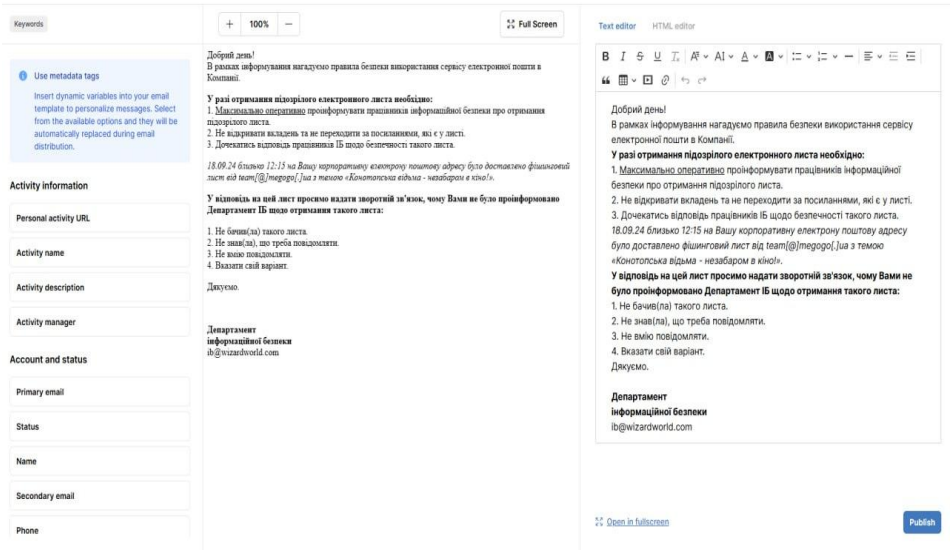

Рисунок 3.4 – Налаштування шаблону повідомлення у програмі ITS CSAT

За зразком створюються родини сценаріїв, візуальний стиль, мова, часові рамки доставки та версії сторінок. Також шаблонізатор підтримує можливість додавання реальних листів які спочатку проходять етап очищення від сторонніх індикаторів компрометації (шкідливих посилань та вкладень у листи вбудованих гіперпосилань на автоматичні скрипти тощо). Кожне посилання зазначається унікальним ідентифікатором адресата, для фіксації його відкриття застосовується сигнальний елемент, а для сценаріїв з введенням даних використовуються тренувальні лендінги у захищеній мережевій зоні. На цих сторінках завжди фіксується факт взаємодії, але реальні паролі або коди не

зберігаються, бо вкладення замінюються безпечними макетами, які дозволяють визначати спроби завантаження та відкриття без ризику.

Планувальник Simulate має гнучке системне налаштування. Сценарії пристосовуються під роль, підрозділ і історію помилок конкретних користувачів, важливо розуміти, що планувальник не просто надсилає листи за певним розкладом, а балансує складність і частоту взаємодій так, щоб підтримувати навички без перевантаження співробітників. Система також має можливість балансування повідомлень по відділам і відкладених посилань(рисунок 3.5).

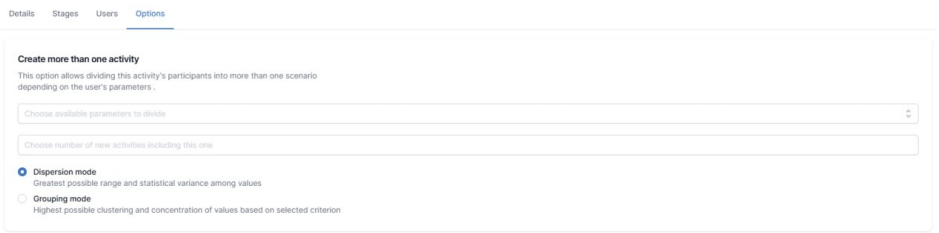

Рисунок 3.5 – Налаштування хвиль повідомлень у програмі ITS CSAT

Функція забезпечує більш реальний досвід симуляції, наприклад, якщо листи будуть надходити одночасно всім користувачам у один і той самий час та день, отримувач просто поверне голову до іншого співробітника і спитає чи надходив такий лист, з’ясувавши, що це фішинг, вони можуть проігнорувати повідомлення, що буде правильно, але втратиться сенс симуляцій через навчання. Всі етапи пройдені співробітником відображаються для адміністратору системи рисунок 3.6-3.7

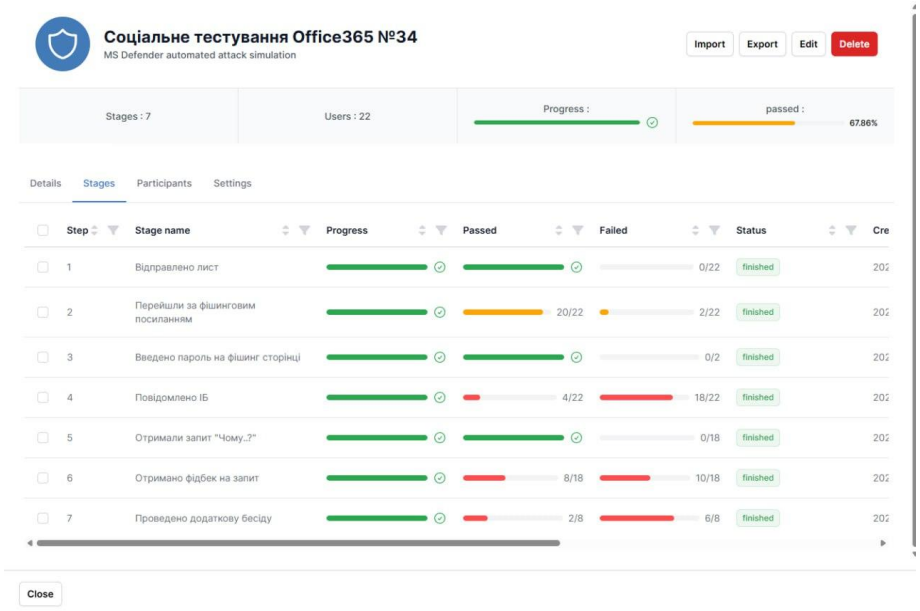

Рисунок 3.6 –Вигляд етапів активності у програмі ITS CSAT.

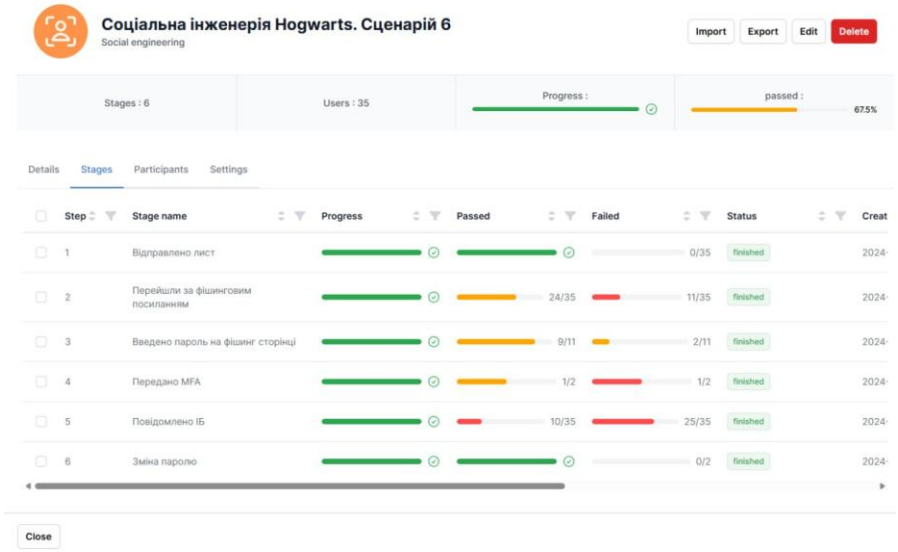

Рисунок 3.7 –Вигляд етапів активності у програмі ITS CSAT

Сервіс Train налагоджує навчальні призначення, рольові траєкторії і перевірочні листи(рисунок 3.8.).

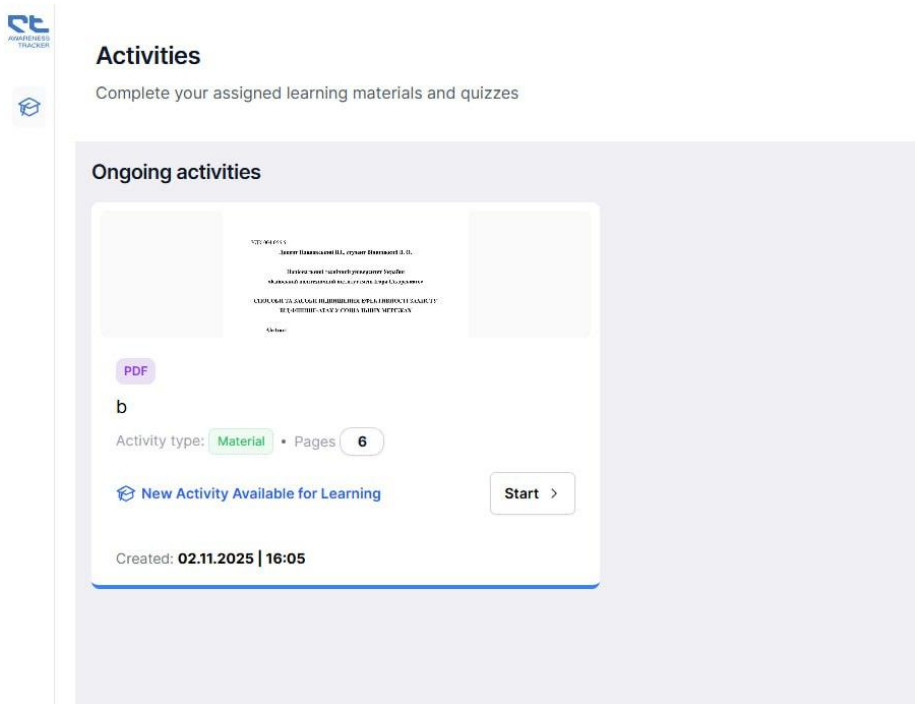

Рисунок 3.8 –Вигляд налаштованого матеріалу зі сторони користувача

Він працює поверх корпоративної LMS (рисунок 3.9.) або як власний мікро LMS для коротких модулів, його завдання - призначити персоналізовані навчальні дії одразу після зафіксованої поведінки у симуляції.

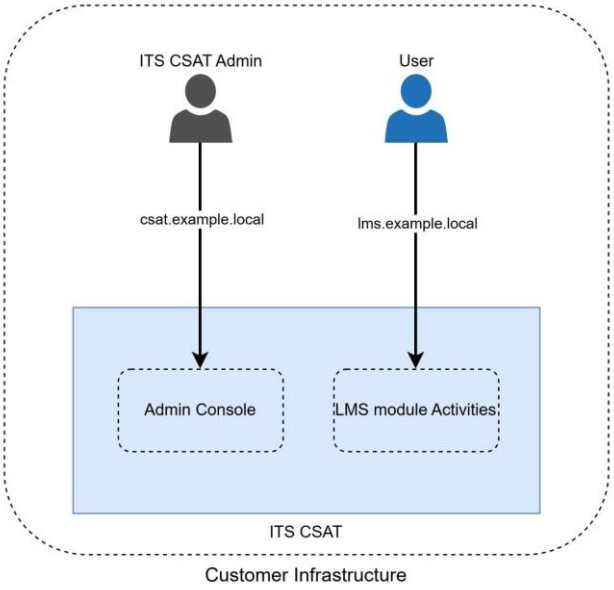

Рисунок 3.9 –Архітектура роботи LMS сервісу

У випадку, коли користувач клікнув за посиланням або ввів дані, йому після симуляцій автоматично призначають короткий розбір із прикладами та мікромодуль на ту саму ознаку ризику. Якщо користувач коректно натиснув кнопку «Повідомити про фішинг», то він отримує підтвердження правильності своїх дій і підсилювальний матеріал для закріплення навички.

Train забезпечує рольові траєкторії: для адміністраторів акаунтів передбачені модулі щодо передачі прав доступу до систем, для фінансистів - модулі щодо підроблених інвойсів і зміни реквізитів, для HR - модулі з теми вкладень у резюме та оновлення політик. Система підраховує повторювані помилки, час реакції, частоту і якість користувацьких репортів, за потреби інтенсивність навчання для конкретної людини або групи зростає, а після постійно правильних реагувань автоматично зменшується.

Дуже важливо враховувати, що Train може ініціювати сервіс Simulate у яких надходять тестові листи. Після завершення модуля користувач отримує новий, або схожий сценарій, який оцінює, чи перетворилася теорія на стійку поведінку. Результати перевірки автоматично потрапляють до підсистеми Measure і визначають ризик-профіль.

LMS модуль дозволяє проходити не лише міні курси, це повноцінний модуль навчання, який має змогу взаємодіяти з Microsoft Teams, планувати зустрічі у календарі для співробітників, організовувати квізи тощо.

Сервіс Measure має модель ризику, забезпечує аналітику, дашборди і зворотній зв'язок у процесах(рисунок 3.10.).

Рисунок 3.10 –Вигляд аналітичного блоку у програмі ITS CSAT

Він отримує потік подій з Simulate і сигнали про прогрес з Train, події нормалізуються, поповнюються атрибутами з каталогу ідентичностей і складаються у сесії взаємодій (рисунок 3.11.).

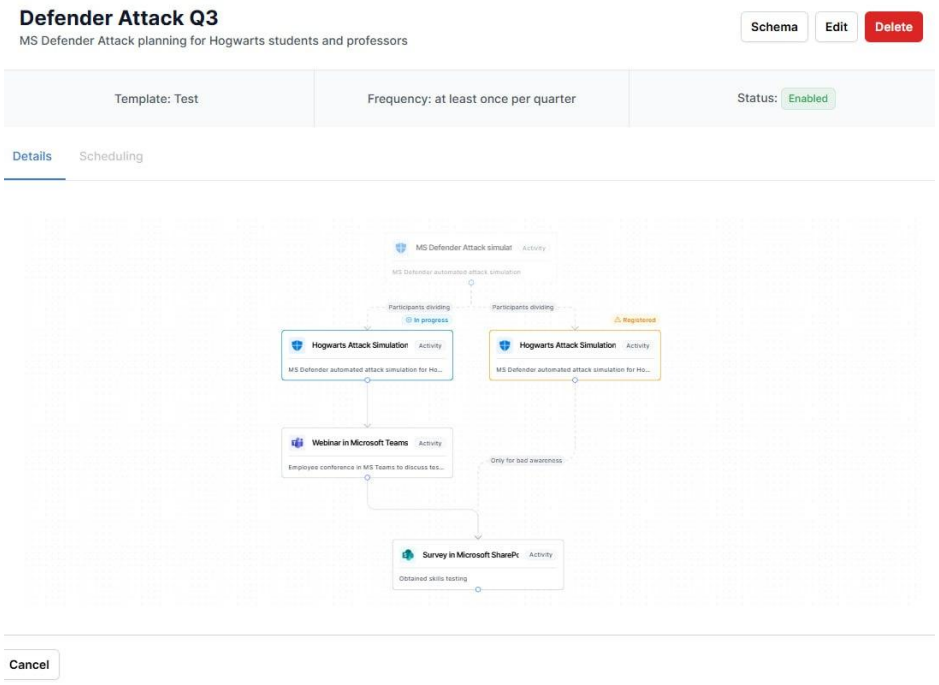

Рисунок 3.11 –Вигляд налаштованого блоку тестування у програмі ITS CSAT

Для методики оцінювання застосовується декларативна модель, де ваги присвоєні типам дій: клік має одну вагу, введення даних іншу, спроба пройти багато факторну перевірку ще більшу. Часові метрики підсилюють або послаблюють ефект події, швидкий та імпульсивний клік підвищує ризик, швидке повідомлення знижує, роль і чутливість доступів впливають на підсумковий індекс, а профілі високого впливу набувають вищих коефіцієнтів.

Аналітика має вигляд дашбордів для різних аудиторій. Керівники бачать динаміку індексів по підрозділах, команда безпеки отримує деталізацію до рівня сценарію і версії листа, та може виявляти слабкі місця в контенті або

в корпоративних процесах, а для узагальнення звітності впроваджена анонімізація персональних даних і накопичення до безпечного рівня.

Measure забезпечує два режими вимірювання: перший - пов’язаний із навчальними хвилями, другий є незалежним і використовується для оцінки довготривалої пам’яті без підказок. Вони обидва працюють на одному форматі подій і тій самій моделі ризику, що спрощує інтерпретацію.

3.2 Сценарії використання рішення

Сценарій 1. Реакція на актуальну фішингову атаку

Розглянемо ситуацію підвищеної чутливості часу: моделюємо отримання попередження від CSIRT-NBU про кампанію, яка маскується під повідомлення від сервісу MEDOC, і спрямована на дії бухгалтерів та фінансистів. Ризики в тому, що саме ця категорія працівників має регулярний контакт із фінансовими документами та сервісами звітності, де одна їх помилка може призвести до компрометації ключових облікових записів і доступу до внутрішніх систем. Необхідно швидко зрозуміти, чи здатні ці користувачі розпізнати обман, чи перейдуть за шкідливим посиланням та нададуть облікові дані, і визначити, де конкретно найслабші ланки. Потрібно координувати усі дії, щоб паралельно з моніторингом запустити навчальну реакцію, і не дати ймовірній загрозі перейти у реальний інцидент.

Розділимо описану ситуацію на етапи (рисунок 3.12) і почнемо вибудовувати сценарій у набір дій які потрібно зробити у застосунку ITS CSAT для впровадження навчання методом TSM.

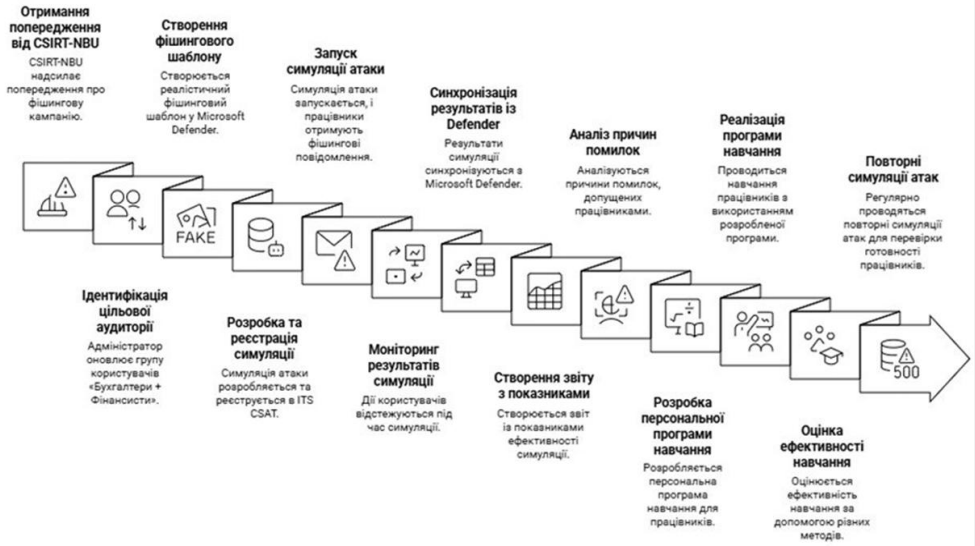

Рисунок 3.12 - Схема реагування на фішингову атаку

Реалізація розпочинається з чіткої ідентифікації цільової аудиторії: адміністратор актуалізує групу «Бухгалтери + Фінансисти», щоб звернення було релевантним саме тим, хто щоденно має справу з MEDOC, а на основі опису атаки з повідомлення CSIRT-NBU в Microsoft Defender створюється правдоподібний фішинговий шаблон, який копіює стилістику сервісу, типову лексику та очікувану поведінку користувачів під час подання звітів. Далі в ITS CSAT розробляється та реєструється симуляція атаки з використанням цього шаблону й визначеної групи. Після завершення симуляції проводиться синхронізація результатів із Defender, створюється звіт із показниками переходів, введенням даних і спробами завантаження вкладень. Здійснюється аналіз причин помилок, потім для користувачів та підрозділів, які потребують пріоритетної уваги, готується персональна програма навчання з короткими практичними модулями, нагадуваннями про ознаки фішингу та прикладами

справжніх і підроблених повідомлень MEDOC. Внаслідок організації такого підходу, компанія постійно перевіряє реальну готовність працівників, виявляє слабкі місця, закриває їх цільовими навчальними заходами і тим самим зменшує ймовірність успішної атаки у фінансовій частині.

Сценарій 2. Оцінка та зниження ризиків перед аудитом

Підготовка до аудиту з інформаційної безпеки завжди підіймає питання про те, де саме організація може бути вразлива, які групи користувачів є критичними, і наскільки вони схильні до випадкових або умисних дій, що призводять до витоків даних. Керівництво бажає не загальних фраз, а розуміння фактичної картини з конкретними іменами, рівнями ризику та зрозумілими кроками на зниження цих ризиків до прийнятного рівня до моменту перевірки. Це може створювати брак часу і потребує прозорої методики, яка дозволяє пояснити аудиторам, чому саме такі заходи були обрані, та як вони вплинули на показники безпеки.

Рішення починається з застосування можливостей CSAT для аналізу користувачів за релевантними критеріями. Адміністратор забезпечує формування вибіркт за рівнем ризику, приналежністю до груп ризику та інтегральним показником обізнаності, отримуючи перелік працівників, які статистично частіше помиляються, виявляють фішинг гірше або порушують політики поводження з даними. На основі цієї вибірки менеджер з інформаційної безпеки готує план персональних активностей, який відрізняється для різних підгруп залежно від причин ризику, наприклад, додаткове навчання для користувачів із низьким балом обізнаності або технічні обмеження доступу для груп із підвищеним ризиком витоку. Далі в ITS CSAT створюються відповідні сценарії навчання, симуляції, вебінари та перевірки

знань, які запускаються у стислих циклах і швидко дають зворотний зв’язок, а результати кожної активності відображаються у звітах, що дозволяє показати прогрес у динаміці та зниження ризиковості до аудиту. Завдяки такій послідовності компанія демонструє аудиторам не лише обізнаність про власні слабкі місця, а й керованість процесу з вимірюваним ефектом, де кожен крок має мету, метрику і підтверджений результат у графіках і підсумкових таблицях. На рисунку 3.13 графічно показано реалізація конкретно цієї ситуації.

Рисунок 3.13 - Процес оцінки ризиків інформаційної безпеки

Сценарій 3. Регулярна оцінка обізнаності співробітників через симуляції

Довгострокова стратегія інформаційної безпеки компанії впроваджує системність, а не разові кампанії. Якщо визначено, що щоквартально певна кількість працівників повинна проходити симуляції соціальної інженерії, то стає зрозуміло, що організація переходить від реактивних заходів до прозорого циклу вимірювання, навчання і повторної перевірки. Така системність дозволяє уникати пікових навантажень, вирівнювати рівень обізнаності між підрозділами та прогнозувати ризики з опорою на статистику, а не на припущення. Важливим фактором є справедливий і рівномірний розподіл активностей, щоб один департамент не отримував однотипні завдання, а інший залишався поза увагою, що спотворює загальну картину. Графічний опис вирішення ситуації продемонстровано на рисунку 3.14.

Рисунок 3.14 - Процес оцінки обізнаності співробітників

Рішення починається з часового розподілу та планування між менеджерами з безпеки та пентестерами, які узгоджують типи сценаріїв, кількість симуляцій, критерії оцінювання та пул користувачів. В ITS CSAT створюються та налаштовуються активності з правилами автоматичного розподілу учасників, які не допускають повторюваності однотипних сценаріїв в одному підрозділі. Одразу після проведення симуляції адміністратор отримує результати у форматі CSV, імпортує їх у систему, й аналізує показники переходів, введення даних, часові проміжки та повторювані помилки. Ті

користувачі, які не пройшли перевірку, автоматично запрошуються на короткий вебінар, що пояснює типові ознаки атаки, та формує правильні дії в подібних ситуаціях. Для спрощення повторення процесу створюється шаблон активності, який зберігає налаштування сценаріїв, правила відбору та параметри звітності, та дозволяє запускати новий часовий цикл у кілька кліків без втрати послідовності й якості. Внаслідок цього, компанія має масштабований і стійкий механізм підвищення обізнаності, який створює передбачувану динаміку покращень, прозорі метрики для керівництва і можливість швидко коригувати програму відповідно до нових загроз.

Сценарій 4. Симуляція обробки підозрілого листа з адаптивним реагуванням залежно від дій користувача

Моделюємо ситуацію реалістичного надходження листа на корпоративну пошту від нібито знайомого контрагента з темою про надтерміновий рахунок. Лист створюється як навчальна симуляція та надсилається лише вибраним користувачам фінансового профілю без попередження. Вміст складається з правдоподібного тексту, підпису відповідальної особи, схожого домену відправника, посилання на файл у хмарному сховищі та варіант вкладення. Поштова інфраструктура і навчальна платформа фіксують кожен крок взаємодії користувача включно з відкриттям листа, попереднім переглядом, переходом за посиланням, введенням облікових даних на фішинговій сторінці, завантаженням і запуском вкладення, а також натисканням кнопки щодо повідомлення про фішинг. На основі цієї ситуації будується розгалужена схема реагування, яка підлаштовує навчальні та технічні дії до фактичної глибини ризикованих кроків. Описаний сценарій є типовим прикладом методу TSM його етапи зображені на рисунку 3.15.

Рисунок 3.15 – Сценарій базового методу TSM реалізованого у CSAT.

У випадку, якщо користувач не відкрив листа, система фіксує це як відсутність експозиції і надає мікронавчання через коротке повідомлення з ключовими ознаками підробок для підвищення усвідомленості без додаткових втручань. Якщо ж лист було відкрито, але не виконано жодних дій, то користувач отримує подяку та стислу консультацію із поясненням, які елементи виявляли ознаки підробки, зокрема, відмінність у домені відправника, емоційний тиск у тоні звернення та невідповідності у підписі. У випадку переходу за посиланням без введення даних активується навчальна сторінка з миттєвим зворотним зв’язком, де демонструються маркери фішингу саме в цьому макеті сторінки, а для користувача планується короткий вебінар

протягом тижня з акцентом на перевірку адрес сайту, сертифіката і способів самоперевірки перед введенням облікових даних.

Коли користувач ввів логін або пароль на фішинговій сторінці, симуляція сигналізує про серйозний індикатор ризику і ініціює технічні кроки разом із навчанням: обліковий запис користувача одразу позначається як потребуючий уваги, виконується примусова зміна пароля та перевіряється впровадження багатоетапної автентифікації. Проводиться аналіз активних сесій в хмарних сервісах і вони завершуються, а журнали подій переглядаються на предмет підозрілих входів. Користувач автоматично отримує персоналізований модуль, де ретельно аналізується саме його шлях помилки від моменту відкриття листа до введення даних, та проходить короткий тест для закріплення навичок розпізнавання підміни сторінок авторизації. Для керівників формується окремий звіт із рекомендаціями щодо зменшенняабо припинення доступів цього користувача до критичних систем до повторного підтвердження компетенції.

Якщо користувач завантажив і запустив вкладення з макросами або виконуваним вмістом, сценарій набуває ступеня підвищеної небезпеки. Вхідна точка тимчасово ізолюється від мережі через засоби захисту від загроз, запускається цільове сканування, а профілі автостарту і нові процеси проходять перевірку на наявність сторонніх компонентів. Не зважаючи на те, що інцидент навчальний, усі технічні дії виконуються достовірно для відпрацювання процедури і перевірки готовності інфраструктури. Користувачеві організовується розбір ризиків, пояснюється, чому навіть легітимно надісланий документ може бути небезпечним, та обов’язково призначається додаткове практичне заняття щодо безпечної поведінки з надісланими вкладеннями.

Окремого розгляду заслуговує поведінка, коли користувач натискає кнопку «повідомити про фішинг» або пересилає отриманий перевірочний лист до спеціальної скриньки служби безпеки. У такому випадку він отримує миттєве підкріплення своєї правильної дії та короткий мікрокейс з показом, які індикатори саме він виявив, а також бейдж внутрішнього визнання. Ця модель ситуації підсилює правильність поведінки і допомагає створити позитивну культуру повідомлення про інциденти. Для інших користувачів, які проігнорували лист без повідомлення, запроваджується попереджувальне нагадування про важливість інформування служби безпеки, тому що навіть відсутність реакції не допомагає виявити масштаб можливої розсилки.

Усі методи симуляції поєднуються у фазі підсумкового аналізу, де вимальовується персональний профіль результатів і рекомендацій для кожного учасника. Система сама аналізує та розраховує ключові показники включно з часом до першої дії, кількістю переходів за посиланнями, кількістю введення облікових даних, кількістю запуску вкладень, рівнем використання кнопки повідомлення і середнім показником обізнаності за групами. На підставі цих даних автоматично призначаються наступні навчальні кроки, наприклад, короткий курс для тих, хто перейшов за посиланням, інтенсивна програма для тих, хто ввів дані, поглиблене практичне заняття для тих, хто запускав вкладення, а також сертифікація або спрощений повторний тест для тих, хто одразу розрізнив та повідомив про загрозу.

У підсумку формується рішення про впровадження циклу безперервного покращення на рівні як користувачів, так і технологій. Для користувачів розробляється персоналізована траєкторія навчання, пов’язана з фактичною глибиною ризикованості дій у симуляції. Для інфраструктури - це впровадження перевірених на практиці механізмів ізоляції пристроїв, примусового виходу із сесій, блокування підозрілих доменів і центрованого

збору доказів. Організація отримує підсумковий звіт для керівництва з аналізом змін і списком практичних кроків, що вже вплинули на зниження ризику. Впровадження такого системного підходу трансформує звичайну симуляцію листа на керований навчальний та технічний експеримент, що точно вимірює поведінку користувачів, гнучко підлаштовує їх реакцію та відчутно підвищує стійкість компанії до реальних фішингових атак.

Висновки до третього розділу МД

У третьому розділі представлено практичну реалізацію навчального підходу протидії фішингу побудовану на основі програми ITS CSAT. Детально розглянуто архітектурні рішення у сервісі Simulate, практичні сценарії застосування методу та особливості впровадження програми у закриті корпоративні мережі. Кожен крок мимтеми взаємо пов'язаний за забезпечує цілісне навчання та підвищення обізнаності працівників. Симуляції формують та надсилають правдоподібні учбові листи, навчальні сервіси мають змогу створювати персональні мікромодулі, квізи та інтегруються з компаративними месенджерами по типу Teams, аналітичні сервіси проводять аналіз ризивів та розробляють план навчання для кожного користувача індивідуально. У підсумку знання не залишаються теорією, а відразу перевіряються на практиці і переходять у стійкі робочі звички.

Архітектура TSM довела здатність працювати з реалістичними обмеженнями Ентерпрайз організацій. Сервіси Simulate, Train і Measure взаємодіють через універсальні точки з’єднання, не порушують корпоративні політики організацій та дотримуються принципу мінімально необхідних прав.

Ризик модель є декларативною, завдяки чому спрощується керування показниками ризиків та рольовими коефіцієнтами без зміни коду.

Представлені сценарії використання рішення охоплюють базові тактики на кшталт листів із терміновими вимогами або виграшами, при розширенні ліцензії є можливість налаштування складної багатокрокової схеми з підміною офіційних сповіщень соціальних платформ, зловмисними вкладеннями, consent phishing та атаками на багато факторну перевірку. Персоналізація за допомогою тегів та ролів робить симуляції та модулі навчання релевантними для конкретних підрозділів та має змогу всебічно навчити користувачів боротьбі з фішингом.

Дослідження пропонує обґрунтований та перевірений підхід до інтеграції у закриті корпоративні мережі. Програма CSAT включає в себе конектори, які працюють через REST API із сервісними обліковими записами, короткочасними токенами та взаємним шифруванням трафіку. Пілот, який пропонує компанія ITS, на обмеженій аудиторії підтверджує працездатність ланцюжка від доставки листа до призначення курсу і відображення метрик у дашбордах, після чого проводиться повноцінне провадження системи і масштабування на підрозділи.

Отриманий результат демонструє кероване зниження ризику завдяки замиканню циклу навчання на практичних діях користувачів. Менеджмент отримує прозору видимість у динаміку індексів ризику та вплив конкретних навчальних інтервенцій.

4 ВПРОВАДЖЕННЯ СИСТЕМИ TSM У КОРПОРАТИВНУ МЕРЕЖУ

4.1 Проблеми впровадження системи TSM на базі програмного продукту

У всіх сучасних компаній мережеве середовище є ізольованим від публічної мережі і багатошаровим. Чим більше компанія зосереджена на кібербезпеці тим більш заплутаним і сегментованим становиться мережа. У випадку впровадження методу TSM на базі програми CSAT потрібно врахувати момент поділу мережі, яка включає в себе багаторівневі міжмережеві екрани, проксі з інспекцією трафіку, внутрішні DNS з окремими зонами, вимоги до шифрування трафіку та управління секретами. Перше початковим корком для роботи системи знадобиться налаштування доступів, яке зазвичай проходить через формальні вимоги та політики компанії та повинно мати узгодження з інформаційною безпекою, мережею, експлуатацією пошти та ризик менеджментом. Досвід впровадження рішення ITS CSAT вказує, що успіх впровадження залежить не стільки від самої технології, скільки від правильного маршруту отримання дозволів на інтеграції та розуміння чітких меж системи замовника.

4.2 Інфраструктурні вимоги та мережеві параметри системи

ITS CSAT – контейнеризований застосунок, що може розгортатись в IT-інфраструктурі за наступними сценаріями(рисунок 4.1.):

1. Застосунок-розширення (Application) для IBM QRadar SIEM. У цьому випадку інтерфейс ITS CSAT вбудовується у вебконсоль IBM QRadar.

2. Застосунок-розширення (Add-On) на виділеному сервері. На окремому виділеному сервері на базі Linux розгортається платформа для автоматизації – ITS Engine Platform. ITS CSAT розгортається як застосунок розширення до платформи.

3.

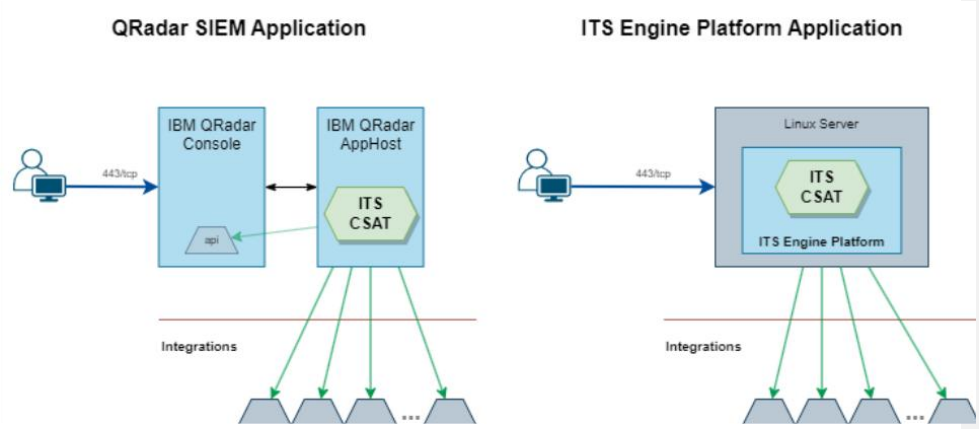

Рисунок 4.1 – Варіації налаштування програми ITS CSAT

Для сценарію розгортання QRadar SIEM Application застосунок встановлюється на сервері типу QRadar SIEM AppHost. Для сценарію розгортання ITS Engine Platform Application використовується виділений сервер, це може бути фізична машина або віртуальний екземпляр з гарантованими ресурсами. Подобні характеристики системи зазначені у таблиці 4.1.

Таблиця 4.1 Вимоги до сервера розгортання

Сценарій розгортання	QRadar SIEM Application	ITS Engine Platform Application
Хост для застосунку	Сервер QRadar SIEM AppHost	Виділений сервер (фізичний або віртуальна машина)
CPU	12 Cores	4 Cores
RAM	2 GB (вільного обєму)	12 GB or more (recomended 16 GB)
HDD	20 GB	100 GB
Операційна система	-	64-bit Linux (Ubuntu, Debian, Oracle, RHEL)

При розгортанні треба також зважити що операційна система має бути 64-бітовою версією Linux з підтримуваних родин, зокрема Ubuntu, Debian, Oracle Linux або Red Hat Enterprise Linux. На окремому сервері під розгортання застосунку необхідно завчасно встановити Docker Engine та Docker Compose відповідно до офіційної інструкції, доступної на сторінці документації Docker за адресою https://docs.docker.com/engine/install/.

Стандартні вимоги до мережевого доступу зазначено в таблиці 4.2.

Таблиця 4.2 Вимоги до мережевого доступу

DNS Name	Protocol/Port	Description
vm.my-itspecialist.com	443\tcp	Сервіс перевірки ліцензій та оновлення
gitlabregistry.service-team.biz	443\tcp	Онлайн репозиторій дистрибутивів програмного забезпечення від "IT Specialist"
active-directory server	389\tcp (або 636\tcp в разі використання LDAPS)	Авторизація через AD та вивантаження даних з конектора AD

DNS Name	Protocol/Port	Description
graph.microsoft.com	443\tcp	Проведення активностей з використанням інтеграцій з MS Teams та MS Defender
login.microsoftonline.com	443\tcp	Проведення активностей з використанням інтеграцій з MS Teams та MS Defender

Обов'язкові вимоги до мережевих комунікацій на сервері ITS Engine Platform зазначено в таблиці 4.3.

Таблиця 4.3 Вимоги до мережевих комунікацій

Port	Protocol	Description
22\tcp	SSH	адміністрування серверу та встановленого програмного забезпечення, діагностика інцидентів у роботі
80\tcp	HTTP	підключення до вебконсолі ITS Engine Platform та модулів, що розгорнуті на базі платформи
443\tcp	HTTPS	підключення до вебконсолі ITS Engine Platform з підтримкою шифрування TLS

Система TSM налаштована за допомогою CSAT працює через чітко налаштовані конектори, які отримують і віддають дані з різних систем та сервісів через REST API. Під час впровадження рішення потрібно врахувати також цей момент, бо кожен конектор має визначений технічний конфігурацію доступів і прогнозовані мережеві потоки. Весь обмін інформацією з поштовими шлюзами, клієнтами, SIEM, IDM, HR системою, LMS, трекером інцидентів, корпоративними месенджерами та звітними сховищами відбувається через REST API встановлених конекторів. Використання обраної моделі чудово вписується в політики мінімально необхідних прав і полегшує

аудит, оскільки кожен виклик залишає трасу у журналах, які завжди можна відстежити та продивитися через логування систем.

Розгортання початкових компонентів починається з розміщення сервісів. В залежності від архітектури замовника сервіси можуть змінювати своє розташування, для прикладу розберемо стандартне налаштування у закритій мережі.

У типових умовах Simulate і лендінги розташовуються зовнішньому середовищі мережи для правдоподібності надсилань повідомлень. Замовнику потрібно налаштувати SMTP трафік з зовні до внутрішньої мережі. Алгоритм впровадження конфігурації SMTP трафіку продемонстровано на рисунку 4.2.

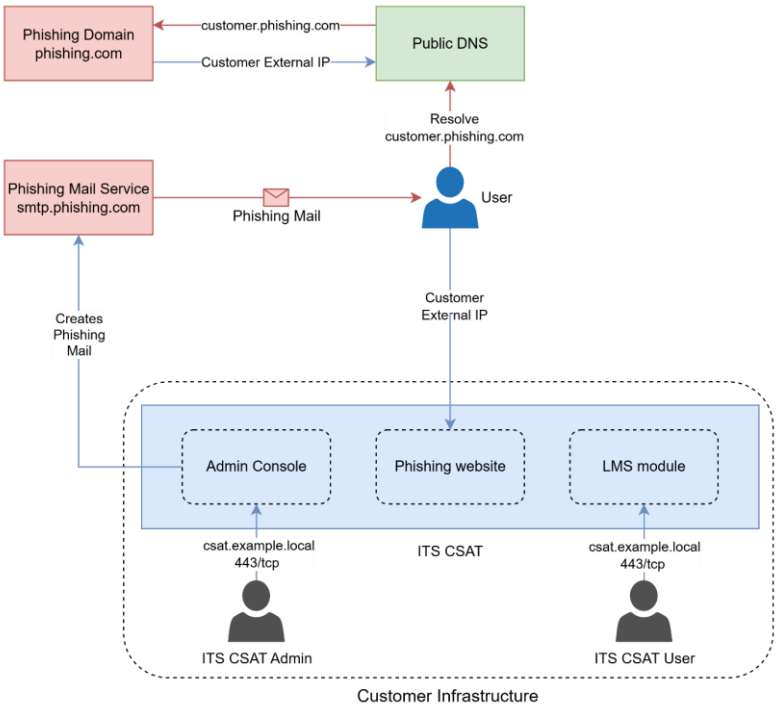

Рисунок 4.2 - Конфігурації SMTP трафіку

Measure і сховище подій розміщуються у DMZ зоні, відокремленої від продуктивних систем даних. Train працює в тісній інтеграції з LMS, тому логічно розміщувати його в тому самому сегменті або з мінімальною кількістю перетинів між екранами. На етапі планування бажано одразу описати замовнику які підмережі відкривають доступ до яких REST кінцевих точок і які сертифікати використовуються Якщо інтернет з корпоративної мережі недоступний або строго проксійований, потрібні додаткові налаштування Nginx для просіювання SMTP серверів, попереднього завантаження ліцензійних даних та докер образів.

Конфігураційні налаштування електроної пошти зазвичай вимагає окремі домени і розділені DNS записи SPF і DKIM, щоб не змішувати тренувальний і продуктивний трафік. При розгортанні компанія ITS надає вже готові поштові сервера з налаштованими конфігураційними параметрами та зареєстрованими DKIM, якому вже більше пів року(рисунок 4.3.).

Рисунок 4.3 – Шаблонне посилання на сайт фішингу.

Для вимірювання взаємодій потрібне дозволити мережеве вікно на веб доступ до LMS із робочих станцій співробітників, і це вікно має проходити через корпоративний проксі з TLS інспекцією, якщо така політика діє.

Для Measure знадобиться дозвіл на приймання подієвого трафіку з конекторів і право писати агрегати в аналітичне сховище. Для Train знадобиться API доступ до LMS і канали для надсилання сервісних повідомлень у корпоративні месенджери та календарі. Під час налаштування конекторів система CSAT має опис який набір правил (конкретних REST маршрутів, необхідних HTTP методів, обмежень за частотою, розмірів відповідей, політики ідентифікації і тривалості токенів) вона потребує.

Таким чином, у закритій корпоративній мережі TSM працює не всупереч обмеженням, а завдяки продуманій моделі конекторів на REST API і поетапній побудові доступів. Завдяки продуманій архітектурі CSAT кожен модуль системи може бути гнучко налаштований під потреби замовника. Саме така інтеграційна варіативність дозволяє перетворити симуляції, навчання і вимірювання на стійкий виробничий процес, який не руйнує політики безпеки і водночас дає керований ефект зниження фішингового ризику.

4.3 Етапи та часовий план реалізації методу TSM у мережі замовника

У таблиці 4.4 Описано деталі робот та план графік впровадження методу TSM на базі програми CSAT у мережу замовника.

Таблиця 4.4 План-графік виконання етапів для впровадження програми CSAT

Етап	Назва	Опис робіт	Тривалість, робочі дні*
1	Забезпечення початкових умов і деталізація архітектури	Формування команди, запуск комунікацій і доступів. Уточнення джерел даних та інтеграцій. Підготовка інфраструктури і базових політик безпеки. Підготовка тестового дистрибутиву ITS CSAT з документацією та ліцензіями.	8
1.1	Формування проєктної команди та відкриття доступів	Призначення менеджера проєкту і складу команди. Створення робочих просторів і каналів взаємодії. Надання облікових записів і прав доступу спеціалістам Виконавця.	2
1.2	Уточнення джерел даних та інтеграцій	Аналіз наявних систем AD, HR, SIEM. Визначення переліку конекторів. Підготовка доступів і технічних параметрів підключення.	2
1.3	Підготовка інфраструктури для впровадження ITS CSAT	Виділення серверів і сховищ із резервуванням. Налаштування мережевих доступів, VPN і правил фільтрації. Підготовка інтеграційних точок до AD, HR, SIEM та інших джерел. Установлення рольової моделі доступів, аудиту та антивірусного контролю.	3
1.4	Підготовка тестового дистрибутиву ITS CSAT	Передача інсталяційного пакета і матеріалів. Підготовка ліцензій і ключів. Розгортання тестового середовища для пробної інсталяції.	1
2	Встановлення та налаштування ITS CSAT	Розгортання базової платформи, інсталяція компонентів і первинна перевірка працездатності на підготовленій інфраструктурі.	1

Етап	Назва	Опис робіт	Тривалість, робочі дні*
2.1	Розгортання та налаштування ITS Engine Platform	Інсталяція ITS Engine. Конфігурація бази даних і серверних служб. Перевірка роботи середовища та мережевих з'єднань.	0,5
2.2	Інсталяція, конфігурація та демодані ITS CSAT	Встановлення ITS CSAT на платформу. Налаштування модулів і конфігурацій. Перевірка доступів, журналювання та старт системи.	0,5
3	Демонстрація роботи з ITS CSAT	Проведення показу для учасників проєкту. Огляд ключових можливостей і сценаріїв. Надання методичних матеріалів і рекомендацій.	3
4	Активності на даних і системах Замовника	Конфігурація конекторів до корпоративних джерел. Запуск пілотних навчальних активностей. Перевірка коректності обміну даними.	3,5
4.1	Конектори для вивантаження даних про користувачів	Розробка, налаштування і тестування підключень до AD, HR, SIEM та інших систем. Валідація передачі даних у CSAT.	1
4.2	Webinar in MS Teams	Створення активності у CSAT. Розсилка запрошень тестовій групі. Проведення пілотного вебінару й фіксація результатів.	0,5
4.3	MS Defender automated attack simulation	Створення та запуск симуляції для тестової групи. Автоматичне завантаження результатів з MS Defender у систему.	0,5
4.4	Obtained skills testing	Підготовка перевірки набутих компетенцій. Імпорт результатів у відповідну активність CSAT для аналізу.	0,5
4.5	Skills testing with LMS Collaborator	Створення пов'язаної активності. Завантаження результатів з LMS	0,5

Етап	Назва	Опис робіт	Тривалість, робочі дні*
		Collaborator та перевірка коректності інтеграції.	
4.6	Quiz	Підготовка квізу з тестовим завданням. Призначення тестовій групі з унікальними посиланнями. Проведення пілотного тестування і перевірка підсумків.	0,5
5	Тестова експлуатація	Запуск CSAT для обмеженої аудиторії. Моніторинг стабільності, збір відгуків і оперативне усунення недоліків. Підготовка до промислового запуску.	30
6	Оцінка результатів пілота та підбиття підсумків	Перенесення у продуктивне середовище. Супровід і підтримка користувачів перші тижні. Передача в постійну експлуатацію і фінальне оформлення документів.	1

Висновки до четвертого розділу

У розділі проведено технічний аналіз процесу впровадження системи Train–Simulate–Measure у корпоративну інфраструктуру, визначено ключові залежності між її компонентами та проблеми сучасного впровадження. Особливу увагу приділено архітектурі інтеграції стимуляційного сервісу а також налаштуванню взаємодії системи CSAT з корпоративними сервісами електронної пошти. Розгортання рішення вимагає налаштування конекторів та налаштування їх доступів, перевірки каналів обробки подій, узгодження політик доступу та визначення порядку обміну даними між компонентами TSM й мережкою замовника.

Важливою та детальною частиною роботи стало реалізація графіку пілотного проєкту, його розділ на етапи, які включали підготовчі конфігурації,

тестове розгортання, перевірку коректності телеметрії та інтеграцій, а також запуск пробної симуляції на обмеженій групі користувачів. У ході пілоту є також ряд внутрішніх оцінок стабільність системи, точність фіксації подій, швидкість обробки результатів та якість зворотного зв’язку, які потребують комунікації з замовником.

ВИСНОВКИ

Фішинг залишається одним із наймасштабніший та динамічніших загроз у корпоративному середовищі. Різноманітність тактик та методів з поєднанням технічної правдоподібності та психологічного тиску призводить до невиправних наслідки, які варіюються від компрометації облікових записів до зупинки критичних бізнес-процесів. Ефективна протидія вимагає не лише технічних бар'єрів, а й сформованих навичок безпечної поведінки користувачів, регулярної практики розпізнавання підмін і здатності приймати правильні рішення під час взаємодії з електронною поштою та суміжними каналами. Саме поєднання навчання, симуляцій реальних атак і вимірювання результатів створює керований цикл зменшення ризиків, який узгоджується з наявною інфраструктурою безпеки та підсилює її.

У магістерській роботі проведено комплексне дослідження проблеми протидії фішинговим атакам у корпоративному середовищі, розглянуто програмні реалізації навчання персоналу та розроблено унікальний метод навчання персоналу Train–Simulate–Measure (TSM).Основною метою методу є системне підвищення кіберобізнаності співробітників компаній і зменшення ризиків компрометації інформаційних ресурсів організації. Дослідження, яке проведено у роботі, підтвердило, що саме людський фактор на сьогодні лишається критичною ланкою у багатошаровій безпеці організації, і жодні технічні засоби не можуть забезпечити достатній рівень захисту без належної підготовки користувачів. У роботі обґрунтовано, практично змодельована та експериментально перевірено методологію TSM, що дозволяє інтегрувати

навчання, симуляції фішингу та вимірювання результатів у єдину керовану систему безпеки.

У першому розділі здійснено огляд сучасного стану загрози фішингу в електронному листуванні та оцінено еволюцію методів його виявлення і протидії. Проаналізовано сигнатурні підходи, методи поведінкового аналізу та комбіновані системи захисту дали конкретні приклади вразливостей у безпеці. Доведено, що хоча сучасні системи виявлення суттєво підвищують рівень безпеки, вони не здатні гарантувати повного блокування фішингових атак. Особливою проблемою є таргетовані атаки на окремі підрозділи компаній, що використовують соціальну інженерію, копіювання легітимних сервісів і контекстні повідомлення. Саме через це наголошується на впроваджені навчання користувачів, бо у момент атаки лише вони приймають ключове рішення про взаємодію чи ні зі шкідливим повідомленням.

У другому розділі представлено аналіз засобів навчання протидії фішингу, що використовуються у провідних корпоративних рішеннях: Terranova, KnowBe4, Cofense, Proofpoint, ITS CSAT та інших. Вивчення технічних можливостей та функціоналу додатків показало, що найефективніші платформи мають лише обмежене поєднання освітніх матеріалів, симуляції та гнучкої системи оцінювання обізнаності та мають суттєві проблеми у впроваджені для сучасних компаній на території України. На основі порівняння існуючих систем сформульовано концептуальну основу методу Train–Simulate–Measure. У роботі визначено ключові складові TSM та обґрунтовано важливість циклічного підходу, який передбачає: навчання персоналу, симуляцію реальних фішингових атак та вимірювання результатів із подальшим удосконаленням процесів навчання. Розроблено системну модель TSM, яка дозволяє застосовувати метод у корпоративному середовищі різного масштабу. Підкреслено, що ефективність TSM визначається низкою

умов: актуальність контенту, адаптивність до ролей працівників, інтеграція з технічними засобами захисту, регулярність симуляцій, застосування персоналізованого навчання та використання багаторівневих метрик.

У третьому розділі запропоновано архітектуру програмно-організаційної системи реалізації методу TSM. Розроблена архітектура включає модулі навчання, стимуляційного інструментарію, телеметрії активностей користувачів, модуль звітування та аналітики, а також механізми інтеграції з системами електронної пошти, SIEM, EDR/XDR та платформами управління ідентичністю. Створено детальні сценарії використання системи для практичних ситуацій корпоративної безпеки. Зокрема, розглянуто чотири ключові сценарії: реакція на актуальну фішингову атаку; оцінка й зниження ризиків перед аудитом; регулярна оцінка обізнаності; моделювання взаємодії з підозрілим листом із адаптивним реагуванням. Для кожного сценарію визначено учасників, очікувані події, точні технічні дії, зв’язки між модулями системи та результати впливу на безпеку організації. Розділ описує як можна імплементувати розроблений методу у вже існуючу програму ITS CSAT та як програма буде взаємодіяти з методом TSM.

У четвертому розділі представлено результати практичного впровадження системи TSM у корпоративному середовищі на основі реалізації CSAT. Описано процес інтеграції системи з корпоративною інфраструктурою, налаштування компонентів та модулів. Порівняння результатів до й після навчання довело, що метод TSM забезпечує вимірюваний позитивний ефект, а його регулярне застосування призводить до сталого зниження ризику успішних фішингових атак. Важливо, що метод дозволяє виявляти групи підвищеного ризику, формувати персоналізовані програми навчання та автоматично запускати повторні симуляції для відстеження прогресу.

Таким чином у магістерській роботі доведено, що запропонований метод Train–Simulate–Measure є не лише ефективним інструментом зменшення вразливості корпоративних клієнтів до фішингових атак, а і легко впроваджується та не потребує значних коштів для підтримки. Одною з головних переваг методу є його циклічність та гнучкість: він дозволяє безперервно вдосконалювати навчання співробітників, перевіряти їхню готовність до реальних атак, вести детальну аналітику та приймати обґрунтовані рішення щодо інформаційної безпеки. Розроблена архітектура TSM підтвердила можливість масштабування методу TSM та його використання у корпоративних середовищах різного рівня складності. Застосування методу не лише підвищує загальну безпеку, а й сприяє формуванню культури кібергігієни, яка є фундаментальною умовою стійкості організації до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Keepnet Labs. Top Phishing Statistics and Trends You Must Know.CSO Online, 2025. URL: https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

2. Бєрковський В.В., Безсонов О.С. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему. Системи управління, навігації та зв'язку, №3(43), 2017.

3. Proofpoint. State of the Phish 2024. Proofpoint, 2024. URL: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

4. Reshetova E., Karhunen J., Nyman T. Security of Email Authentication Protocols: A Formal Analysis. IFIP SEC 2018, pp. 219–232.

5. Hong J. The State of Phishing Attacks. Communications of the ACM, 55(1), 2012, pp. 74–81.

6. Microsoft. Microsoft Digital Defense Report 2025 — Overview. Microsoft Security Insider, 2025. URL: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

7. Anti-Phishing Working Group (APWG). Phishing Activity Trends Reports (Quarterly Series, 2008–2025). APWG, 2025. URL: https://apwg.org/trendsreports

8. Hong J. The State of Phishing Attacks. Communications of the ACM, 55(1), 2012, pp. 74–81. DOI: 10.1145/2063176.2063197

Додаток А

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
Навчальний контент та формати	Персоналізоване навчання з кібербезпеки; курси й тести знань для співробітників.	Різноманітний контент: повний каталог із курсами різної тривалості, nano- та micro-уроки, рольові сценарії, ігри, вікторини, just-in-time навчання тощо. Контент доступний понад 40 мовами та відповідає вимогам доступності WCAG 2.1.	Найбільша бібліотека контенту на ринку: інтерактивні курси, відеоролики, постери, розсилки та інший матеріал для різних стилів навчання. Підтримує 35+ мов локалізації контенту і консолі, регулярно додаються оновлення.	Основний фокус – навчання розпізнаванню фішингу та email-загроз. Містить бібліотеку відео та навчальних роликів (спільно з Ninjio) з акцентом на тематику фішингу й електронної пошти. Контент доступний 36 мовами (HTML5-шаблони листів, відео, навчальні ігри тощо). Може включати короткі інтерактивні модулі, інфографіку, головоломки тощо, але тематичне покриття вужче (переважно	Широкий набір тем кібербезпеки і форматів: інтерактивні модулі, micro-навчання, відео, тести, опитування культури безпеки тощо. Контент доступний 40+ мовами (заявлено до 41). Присутні елементи гейміфікації, навчання з урахуванням ролей користувачів та їхніх навичок.

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
				соціальна інженерія).	
Симуляції кібератак	Симуляції фішингових розсилок з персоналізованими сценаріями (наприклад, імітації фішингу електронною поштою на основі ролей чи рівня знань співробітника). Підтримуються різні типи атак (фішинг, шкідливі вкладення тощо).	Phishing-симуляції реальних загроз: повністю настроювані розсилки із сучасними тактиками фішингу; можна проводити багатомовні кампанії (кілька мов одночасно). Є симуляції різних видів фішингу (посилання, атаки типу BEC, шкідливі вкладення, smishing/vishing – останні висвітлюються у навчальних матеріалах) та інтерактивні кібервчення (наприклад, кібер-ігри) для практики.	Фішингові тести з великою бібліотекою шаблонів – понад 25 000 шаблонів фішинг-листів, що постійно оновлюються під актуальні загрози. Платформа дозволяє проводити таргетовані кампанії (email-фішинг) з адаптацією під користувача за допомогою AI (автодобір складності шаблонів залежно від успішності користувача). Підтримуються розсилки з вкладеннями, посиланнями, а також callback	PhishMe фокусується на імітації реальних фішингових атак, особливо тих, що обходять захист електронної пошти (SEG). Надає сценарії фішингу, побудовані на реальних загрозах (сперфішинг, соціальна інженерія, BEC, шкідливі вкладення, drive-by атаки тощо). Особливість – усі шаблони базуються на актуальних атаках, які не були відфільтровані захистом (SEG misses), завдяки розвідці загроз від глобальної мережі Cofense (35+ млн користувачів).	ThreatSim® – модуль Proofpoint для симуляції атак – дозволяє моделювати фішинг електронною поштою, а також SMS-фішинг (смішинг). Є сценарії атак через підкинуті USB-носії та інші методи соціальної інженерії. Фішингові кампанії можуть таргетуватися на конкретні групи або користувачів на основі ризику. Після “провалу” симуляції користувачам демонструються навчальні сторінки (Teachable Moments) з

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
			phishing – комбінована атака (листи + телефонний дзвінок) для імітації телефонного соціального інженерингу.	Основний канал – email; платформа неявно підтримує навчальні симуляції й в інших формах (наприклад, навчальні ігри, логічні задачі для розпізнавання атак), але не акцентується на смішингу/вішингу.	поясненнями. Також надається кнопка для повідомлення про підозрілі листи (PhishAlarm) і тісна інтеграція з реальними даними про атаки (TAP Threat Intelligence).
Аналітика та звітність	Аналітичні панелі для відстеження рівня обізнаності співробітників: показники успішності навчання, статистика фішинг-тестів (хто проходить, хто натискає на фішингові посилання), індекс ризику по кожному працівнику. Автоматичні дашборди для керівництва та	Security Culture Index – інтегрований індекс культури безпеки, що на основі десятків параметрів оцінює ризик поведінки співробітників та показує покращення ситуації з часом. Адмін-консоль пропонує гнучку звітність: налаштовувані дашборди, віджети для моніторингу прогресу навчання в реальному часі. Є	Потужна система звітності: понад 60+ вбудованих звітів для оцінки прогресу по всій організації, включно з C-level звітами для керівництва. Платформа обчислює показник Phish-prone (схильність до фішингу) та індекси обізнаності, дозволяє порівнювати їх з	Детальні метрики “кількісної стійкості”: платформа надає показники Employee Engagement Index (EEI) – індивідуальні оцінки залученості та стійкості кожного працівника. Звіти містять аналіз результатів симуляцій (хто відкрив, хто повідомив),	CISO Dashboard – спеціальна панель для інформаційної безпеки, яка відстежує поведінкові зміни, вразливість користувачів та дозволяє порівнювати результати із середніми показниками по галузі. People Risk Explorer – аналітичний інструмент, що збирає дані про

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
	детальна статистика по підрозділах.	можливість галузевого бенчмаркінгу (наприклад, участь у глобальному «Gone Phishing Tournament» для порівняння показників).	середніми по індустрії. Smart Risk оцінює ризик кожного користувача, враховуючи до 37 факторів поведінки, і відображає “червоних” користувачів з високим ризиком. Є мобільний додаток для навчання та відстеження прогресу.	динаміку покращення, частоту звітування про фішинг тощо. Є функція бенчмаркінгу і порівняння ефективності навчання між підрозділами. Дані можуть сегментуватися для таргетування додаткового навчання (наприклад, визначення груп підвищеного ризику).	кожного користувача (роль, привілеї, історія атак, поведінка) і відображає “групу ризику” співробітників. Платформа вимірює зміни ризику з часом і ефективність навчання, підтримує бенчмаркінг по індустрії. Звіти гнучко налаштовуються, є повна історія успішності тестів кожного співробітника та функція відстеження змін у культурі безпеки (опитування, індекси тощо).
Інтеграція та сумісність	Active Directory/SSO: підтримується імпорт та	SaaS-платформа, сумісна зі SCORM. Надає розвинені інтеграції із	Директорії та доступ: інтеграція з AD та провайдерами SSO	E-mail Security EcoSystem: сильна сторона Cofense – інтеграція з	E-mail та SOC: тісно інтегрується з рішеннями Proofpoint з email-

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
	синхронізація користувачів з AD та іншими каталогами (для автоматичного оновлення списку співробітників). HR-системи: передбачена інтеграція з HR-платформами для отримання даних про структуру компанії (підтримка API). API: відкритий API для інтеграції з зовнішніми системами (можна підключити індикатори ризику або отримувати дані прогресу).	популярними системами: Azure AD/SSO, Okta, OneLogin для єдиного входу та синхронізації користувачів, Active Directory конектор. Інтегрується з корпоративною поштою: є кнопка в Outlook та Gmail для повідомлення про фішинг (Phishing Alert Button), яка може пересилати повідомлення у сервіс аналізу (Fortra) або у внутрішню скриньку реагування. Партнерство з Microsoft забезпечує тісну інтеграцію з Defender/O365: Terranova постачає контент для модуля Attack Simulation Training в Microsoft 365. Також підтримується	(SCIM підтримка Azure AD, Okta, OneLogin) для автоматичного керування користувачами. Електронна пошта: пропонується плагін Phish Alert Button для Outlook/Google – кнопка, що дозволяє користувачам повідомляти про підозрілі листи одним кліком, інтегрується з системою аналізу PhishER. API: надаються API для обміну даними – можна, наприклад, надсилати події безпеки з інших систем (SIEM, поштових шлюзів) у консоль KnowBe4 для врахування в	існуючими засобами захисту пошти. Cofense Reporter – плагін-кнопка в пошті для повідомлення про фішинг (дані одразу надходять до SOC/аналізатора). Cofense Triage & Vision – платформа для автоматизації обробки цих повідомлень та автоматичного вилучення з поштових скриньок небезпечних листів (працює з Microsoft 365 та іншими шлюзами). Таким чином, навчання PhishMe щільно пов’язане із реальним потоком загроз: повідомлені користувачами листи аналізуються централізовано, що замкнено в цикл “тренування–	безпеки (Targeted Attack Protection, TAP). Наприклад, дані про реальні атаки (фішингові URL/вкладення) з email-шлюзу TAP використовуються для адаптації навчання під актуальні загрози. Кнопка “Report Phishing” доступна як аддин для Outlook/Office 365 (іменується CLEAR або PhishAlarm) і працює навіть на мобільних пристроях; повідомлені користувачами листи можуть автоматично аналізуватися та корелюватися з навчанням. SSO/AD: підтримуються інтеграції з AD,

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
		експорт курсів у SAP SuccessFactors (LMS) та інші інтеграції (Power BI, Google Workspace тощо).	ризик-профілі користувача. Інші інтеграції: платформа KnowBe4 зв'язується з власними додатковими модулями (PhishER для автоматизації обробки підозрілих листів, SecurityCoach для інтеграції з SOC-алертами тощо), а також має бібліотеки для взаємодії із сторонніми рішеннями (наприклад, Mimecast, Splunk).	виявлення–реагування". Директорії: підтримується синхронізація користувачів (AD та ін.), SSO. API менш акцентований у публічних джерелах, але можливий у рамках сервісів Cofense для інтеграції з SIEM/SOAR.	SSO (як правило, через SAML/OAuth). ЛМС: можливий експорт/імпорт SCORM-модулів для сторонніх систем (Proofpoint раніше надавав свої курси для імпорту в інші LMS при потребі). Також є API для отримання даних (наприклад, автоматизація через Adaptive API в деяких пакетах).
Адаптивність та автоматизація	Вбудований планувальник навчання: платформа надає інструмент формування плану навчальних заходів	Висока гнучкість налаштування кампаній: Campaign Manager дозволяє адміністратору за кілька кліків створювати складні	AI-режими та Smart Groups: KnowBe4 має функцію Automated Security Awareness Program (ASAP) – майстер,	Ризик-орієнтоване навчання: Cofense дозволяє сегментувати користувачів за показниками EEI та автоматично	Risk-based automation: Proofpoint активно використовує дані про ризик для автоматизації. Через модуль

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
	(розсилок, курсів) для різних груп співробітників.	багатоетапні кампанії (наприклад, серію тренінгів та фішинг-розсилок) і автоматично керувати їхнім виконанням (розсилання нагадувань, збирання результатів тощо). Є готові шаблони кампаній та навчальні “шляхи” для типових сценаріїв. Платформа підтримує повну кастомізацію – від контенту до зовнішнього вигляду (можна змінювати навіть CSS оформлення під бренд компанії). Адаптивність більше залежить від дій адміністратора (цільових розсилок за результатами індексу ризику). Terranova відома персоналізованим	що будує індивідуальний план тренінгів і тестів для організації з набором завдань і календарем. Також реалізовано Smart Groups – динамічні групи, які автоматично змінюються на основі правил (наприклад, всі, хто провалив останній тест, або нові співробітники) і до них автоматично застосовуються відповідні кампанії. Система використовує штучний інтелект для рекомендації як навчального контенту, так і фішингових шаблонів під кожного користувача на	визначати, кому потрібна додаткова освіта. Наприклад, якщо EEI або частота клацань на фішинг у деякого співробітника гірші – адміністратор (або система за рекомендацією) може націлити на нього додатковий тренінг або іншу взаємодію. Крім того, Cofense запровадила функцію Smart Suggest – рекомендації шаблонів фішингу для нових кампаній з урахуванням галузі, рівня зрілості програми та навіть поточних активних загроз. Автоматизація також реалізується через інтеграції: наприклад, Auto-Quarantine	Adaptive Groups адміни можуть визначати правила, за якими користувачі автоматично потрапляють у ті чи інші навчальні потоки (напр. “користувач X з високими привілеями і низьким балом знань” – в групу високого ризику). Pathways – механізм створення навчальних траєкторій: адміністратор задає послідовність активностей (курс -> фішинг-тест -> опитування тощо) з умовами, а система автоматично проводить користувача через цей шлях

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
		підходом, але автоматизовані рекомендації реалізовані переважно через інтеграцію з Microsoft (Defender ATP може автоматично призначати навчання Terranova на основі зафіксованих спроб атак).	основі його поведінки. Таким чином, навчання підлаштовується під прогрес користувача: уразливі отримують більше уваги, обізнані – складніші завдання. В цілому KnowBe4 відома підходом “включив і забув” – після налаштування більшість процесів автоматизовані.	автоматично реагує на реальні інциденти (видаляючи листи) – навчальна платформа може враховувати ці події. Загалом підхід Cofense більш керований (ручне налаштування кампаній), але підкріплений інтелектуальними підказками та зовнішньою автоматизацією через інші продукти.	відповідно до результатів. Високоризикові працівники можуть автоматично отримувати інтенсивніші курси. Навчання адаптується під актуальні загрози: платформа враховує, які атаки зараз поширені, та коригує зміст симуляцій і курсів. Інструмент ZenGuide від Proofpoint фактично діє як “цифровий наставник”, персоналізуючи досвід навчання для кожного (з урахуванням ролі, навичок, навіть ставлення користувача до безпеки, виміряного опитуванням).

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
Масштабованість та ринки	Продукт розроблений командою IT Specialist LLC (Україна) для бізнес-клієнтів різного масштабу. Підходить як малим та середнім компаніям на локальному ринку (з потребою в україномовному контенті), так і більшим підприємствам, яким потрібна кастомізація програм кібернавчання під себе.	Основна аудиторія – середній та великий бізнес, у тому числі глобальні корпорації. Terranova історично сильна в підприємницькому сегменті (enterprise) та має клієнтів у різних галузях: фінансовий сектор, державні установи, ритейл тощо. Платформа витримує навчання десятків тисяч користувачів одночасно по всьому світу. Завдяки 40+ мовам і гнучкому налаштуванню під корпоративний бренд її обирають компанії з розгалуженою міжнародною присутністю. Terranova також підходить для клієнтів, яким потрібна підтримка експертів: вона пропонує	Найбільша частка ринку – KnowBe4 працює з більш ніж 50 тисячами організацій по всьому світу (в т.ч. 47 з топ-50 компаній індустрії кібербезпеки). Підходить для будь-якого розміру: від малих фірм (є навіть безкоштовні інструменти та гнучкі тарифи для SMB) до гігантів з сотнями тисяч співробітників. Особливо популярна серед середнього бізнесу та MSP, оскільки має просте розгортання і багатотенантність (для керування навчанням на багатьох дочірніх компаніях). Галузевий	Cofense PhishMe здебільшого орієнтована на великий бізнес і корпоративний сектор, особливо на організації з підвищеними вимогами до безпеки (фінанси, критична інфраструктура, уряд). Часто використовується там, де вже розгорнуті рішення Cofense для захисту пошти – щоб побудувати цілісний процес. Масштабованість: SaaS-архітектура, що підтримує багатотисячні аудиторії (в кейсах – ~20 000 співробітників по всьому світу). Для дуже великих клієнтів Cofense пропонує	Proofpoint SAT найбільш поширений серед середніх та великих підприємств, часто тих, що вже користуються продуктами Proofpoint (email security, DLP тощо). Проте існує окрема лінійка Proofpoint Essentials для малого бізнесу й керованих сервіс-провайдерів – вона включає спрощену версію навчання (менший контент-кінець, базові фішинг-тести). Завдяки гнучкості пакетів (Standard, Enterprise) компанія може обслуговувати і 100-користувацькі фірми, і міжнародні

Категорія	ITS CSAT (UA)	Terranova Security (Fortra)	KnowBe4	Cofense (PhishMe)	Proofpoint
		консультації своїх CISO та експертної команди на кожному етапі впровадження.	діапазон – універсальний (IT, фінанси, охорона здоров'я, виробництво, держсектор тощо).	розширені преміум-послуги та мульти-організаційні розгортання (для холдингів тощо). Меншим компаніям рішення Cofense може бути затратним і дещо надлишковим, тому більшість клієнтів – середні та великі підприємства.	корпорації. Сфери застосування – всі галузі, особливо ті, де важлива людино-орієнтована безпека: фінанси, технології, охорона здоров'я. Proofpoint як постачальник комплексних рішень "People-Centric Security" часто вибирають компанії, що прагнуть об'єднати навчання з іншими засобами кіберзахисту людей (email, cloud).