Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Ольга МЕЛКОЗЬОРОВА

_____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Аналіз структури фішингових атак та дослідження механізмів їх реалізації в корпоративному й приватному сегментах користувачів сучасних інформаційних систем»

оцінка « »

Голова ЕК

Олександр ЛЕМЕШКО _____

Керівник доцент каф. БІСТ

Малахов С. В.

Рецензент Головний метролог

ХНУ імені Каразіна

Гостєв О. Л.

Виконавець : студентка групи КБ-61

Лєсная Ю. Є.

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 69 сторінок, 16 рисунків, 7 таблиць, 7 додатків, 75 джерел.

Метою дипломної роботи є узагальнення відомостей щодо передумов виникнення фішингових атак та визначення структури і механізмів їх реалізації в умовах використання сучасних інформаційних систем (ІС).

Об’єкт дослідження: - шляхи та методи реалізації інтегрованих фішингових атак, як важливого елементу у спектрі сучасних загроз безпеки.

Предмет дослідження: - цілі, структура і механізми здійснення фішингових атак в корпоративному та приватному сегментах користувачів сучасних ІС.

Основними методами досліджень є аналіз та порівняння.

У роботі досліджені питання вразливостей сучасних інформаційних систем та їх користувачів від впливу складних (інтегрованих) фішингових атак. Запропоновано аналіз структури та змісту фішингових атак, що притаманні різним нішевим сегментам сучасного ІТ-ринку. Систематизовано типові цілі фішингу та визначені основні механізми реалізації інтегрованих атак. Досліджено характерні сценарії сучасного фішингу та сформовані рекомендацій, щодо можливостей комплексного захисту від даного типу загроз інформаційної безпеки (ІБ). Узагальнено подальші тенденцій в еволюції фішингових атак з урахуванням фактору інформатизації основних сфер діяльності сучасного суспільства.

Результати роботи можуть бути використані в освітніх цілях з курсу дисципліни «Управління інформаційною безпекою» та, як довідковий матеріал для розширення рівня професійної обізнаності персоналу підрозділів з ІБ.

Ключові слова: ФІШИНГ, АТАКА, ІНЦИДЕНТ, РЕСУРС, ПІБ, ПЕРСОНІФІКАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, СОЦІАЛЬНА ІНЖЕРЕРІЯ, АВТЕНТИФІКАЦІЯ, ІНТЕРНЕТ РЕЧЕЙ.

ABSTRACT

The explanatory note contains 69 pages, 16 figures, 7 tables, 7 annexes, 75 sources.

The aim of the thesis is to synthesize information regarding the scope and relative proportion of phishing attacks within the broader spectrum of Information Security (IS) threats. It involves analyzing primary directions and components of countermeasures, as well as investigating industry-specific, regional, and user-specific characteristics in the implementation of these attacks.

The subject matter is encompassing the methods and pathways of integrated phishing attacks, recognized as crucial elements within the spectrum of contemporary security threats.

The scope of the study is the analysis the goals, structure, and mechanisms of phishing attacks in both corporate and private user segments of modern IS.

Research methods are analysis and comparison.

The thesis explores vulnerabilities in modern information systems and their users to the influence of complex (integrated) phishing attacks. An analysis of the structure and content of phishing attacks prevalent in various niche segments of the contemporary IT market is presented. The study categorizes typical phishing objectives and identifies key mechanisms for implementing integrated attacks. Furthermore, it investigates characteristic scenarios of modern phishing and formulates recommendations for comprehensive protection against this type of information security threat. The findings are generalized to highlight future trends in the evolution of phishing attacks, considering the factor of informatization across fundamental sectors of contemporary society.

Keywords: PHISHING, ATTACK, INCIDENT, RECOURSE, ISP (INFORMATION SECURITY POLICY), PERSONIFICATION, INFORMATION SECURITY, SOCIAL ENGINEERING, AUTHENTICATION, IoT (INTERNET OF THINGS).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

ІБ	–	Інформаційна безпека
SE	–	Соціальна інженерія
AI	–	Штучний інтелект
ІС	–	Інформаційна система
ІТ	–	Інформаційні технології
ОС	–	Операційна система
ML	–	Машинне навчання
IoT	–	Інтернет речей
URL	–	Уніфікований локатор ресурсів
ПЗ	–	Програмне забезпечення
ПІБ	–	Політика інформаційної безпеки
CRM	–	Система управління взаємодією з клієнтами
ERP	–	Інтегрована система управління підприємством
DLP	–	Захист від витоку даних
DNS	–	Система доменних імен
SPF	–	Система політики відправника
DKIM	–	Електронна пошта із визначеними ключами домену
DMARC	–	Доменна аутентифікація повідомлення, звіти та відповідність
VR	–	Віртуальна реальність

ВСТУП

У розгляді сталого зростання загроз інформаційної безпеки (ІБ) принциповим є те, що будь-який комунікаційний ресурс або онлайн технологія чи сервіс, котрі забезпечують обмін інформацією, виступають у якості технічної платформи для здійснення будь-яких проявів соціального інжинірингу [1], що є однією з головних передумов сучасних фішингових атак, із притаманними для них особливостями моніторингу та можливостями протидії цьому різновиду загроз безпеки. За результатами аналітичного огляду інцидентів безпеки і стану питань з протидії сучасному фішингу, можна стверджувати, що в подальшому цей різновид атак буде тільки поширюватись. Перш за все це обумовлено активним впровадженням технології Інтернету речей (IoT) та стійким збільшенням чисельності користувачів мережі Інтернет і учасників різних соціальних мереж.

У контексті даної проблематики важливим є поетапне дослідження особливостей фішингу, починаючи з історичних етапів еволюції даного явища. За результатами всебічного аналізу різних історичних етапів розвитку фішингу, можливо визначити основні тенденції кожного з них, що зумовлює базове розуміння, стосовно класифікації основних способів реалізації та передумов поширення даного явища. Визначення питомої частки фішингу серед інших загроз ІБ, свідчить про тісний взаємозв'язок між еволюційними періодами у розвитку засобів електронного зв'язку і ІТ-сфери, та безпосередньо етапами в еволюції фішингових атак.

Визначення специфіки сегментації атак на користувальницькі (*корпоративні й приватні*), галузеві та регіональні ресурси, є один із головних чинників для всебічного аналізу цього явища, що висвітлює певні відмінності у структурі, змісті та способах реалізації фішингових атак, та підтверджує ключові тенденції подальшого розвитку цього явища.

Дослідження типових сценаріїв та механізмів реалізації фішингу ґрунтується на попередньому визначенні характерних потенційних цілей (*перш за все інформаційних та апаратних ресурсів жертв*) атак на різні нішеві сегменти сучасних ІС. Визначення відмінностей і класифікація таких ресурсів дає змогу проаналізувати особливості даних, які фігурують в кожному з таких сегментів з точки зору критичності втрати доступу до них та/чи потенційної вигоди атакуючої сторони в разі отримання несанкціонованого доступу до них.

Із метою ефективного захисту користувачів сучасних ІС від впливу сучасних різновидів фішингу, базовою умовою з протидії цим загрозам, повинно бути комплексне впровадження відповідних організаційно-технічних заходів. Всебічне узагальнення можливих напрямів протидії фішингу, із визначенням специфічних рівнів захисту й характеристикою можливостей щодо їх впровадження для корпоративного та приватного сегментів користувачів, являється основним підґрунтям для формування рекомендацій, стосовно організації багатовекторного захисту від даного типу загроз, включаючи усунення основних передумов їх виникнення. В цьому контексті, особлива увага повинна бути надана огляду нормативно-правових особливостей з протидії фішингу, відповідно до їх регіональних відмінностей та відповідності основним аспектам правового регулювання даного типу атак (у тому числі й вітчизняне законодавство).
Логічним закінченням відповідних досліджень є спроба прогнозної оцінки подальшого розвитку методів здійснення фішингових атак з урахуванням:

1) чиннику загальної інформатизації всіх сфер діяльності сучасного суспільства;
2) очікуваних тенденцій, щодо вибору цільових ресурсів для фішерів.

Таким чином, процес прогнозування майбутнього розвитку фішингових загроз, можна попередньо сепарувати за 3-ма головними напрямками: - впровадження технічних інновацій, соціальних аспектів та нових засобів/заходів із забезпечення ІБ.

1 АНАЛІЗ РОЗВИТКУ ТА УЗАГАЛЬНЕННЯ СТРУКТУРИ Й ЗМІСТУ ФІШИНГОВИХ АТАК, ЩО ПРИТАМАННІ РІЗНИМ НІШЕВИМ СЕГМЕНТАМ СУЧАСНОГО ІТ-РИНКУ

1.1 Аналіз інцидентів та визначення основних етапів еволюції фішингових атак

Фішингові атаки – це такий різновид кібератак, що передбачає використання сукупності методів і технік маніпулювання потенційною жертвою. Головною метою фішингу є неправомірне отримання доступу до чутливої інформації жертви шляхом реалізації послідовності специфічних дій. У загальному випадку до чутливого інформаційного ресурсу відносяться: - конфіденційні, корпоративні та персоніфіковані дані. Можна виокремити конкретні типи даних, що цікавлять фішерів, наприклад:

1) конфіденційні дані, що включають до себе: - *особисті ідентифікаційні, фінансові, соціальні, бізнес-дані, медичну інформацію*;

2) корпоративні дані, котрі поєднують: *комерційну інформацію, фінансові, клієнтські та технічні дані, стратегічні плани та персоналізовану інформацію про компанію тощо.*

3) персоніфіковані дані: *це інтегральна інформація, що містить особисті відомості про конкретну особу*.

Класифікація фішингових атак є критично важливою для розуміння ризиків компрометації зазначеної вище інформації та вдосконалення стратегій протидії. Вона охоплює різноманітні аспекти, такі як групи атак, спосіб їх реалізації та інструменти розповсюдження (див. Рисунок 1.1).

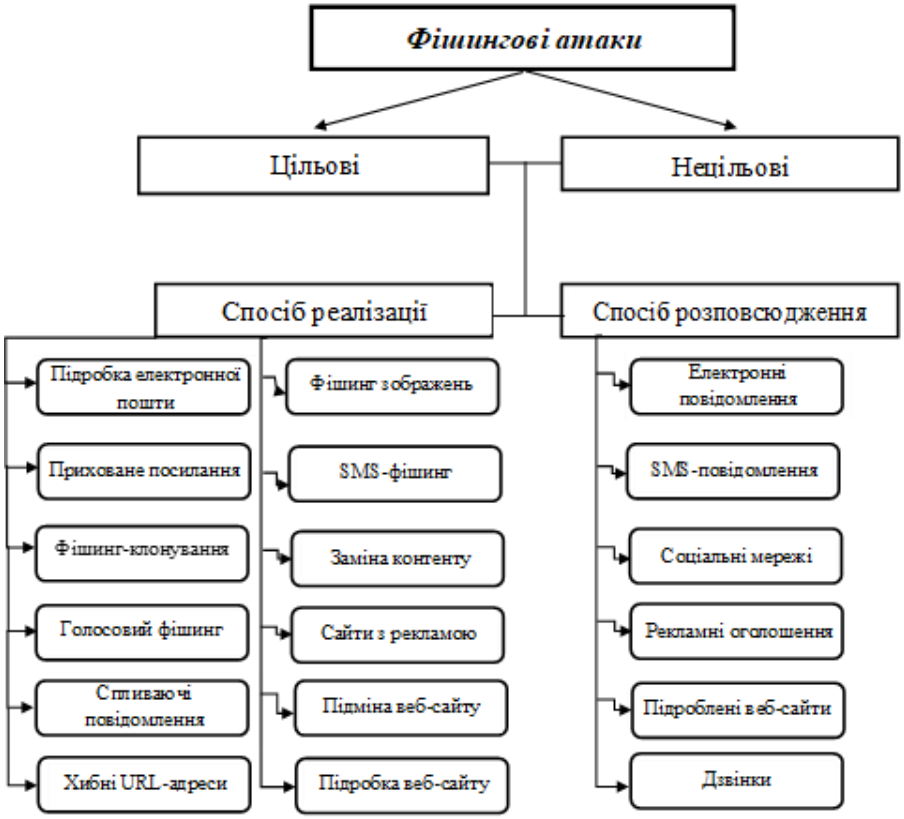

Рисунок 1.1 – Класифікація фішингових атак

За результатами аналізу структури потенційних жертв, усі фішингові атаки можна умовно розділити на дві категорії [1]: - цільові *(таргетовані)*, які спрямовані на окрему конкретну особу/організацію; - нецільові *(класичні, групові, невибіркові)*, тобто ті, що не враховують характеристики й властивості потенційних цілей атаки. Детальний розгляд усіх способів реалізації атак наведено у Додатку А.

Отже, існує безліч способів реалізації фішингу, кожному з яких притаманне використання різних методів та інструментів, що варіюються в залежності від цілей та специфічних сценаріїв розгортання такої атаки.

Зважаючи на стрімкий розвиток інтернет-технологій, фішинг, як вид кібератак, пройшов довгий та складний шлях еволюції. Від його перших виявлень у 1990-х роках до сучасних форм, цей метод кіберманіпуляцій зазнав значних змін та вдосконалень. Дослідження ключових фаз еволюції фішингу дозволяє виокремити основні характеристики кожної з них.

Слід звернути увагу, що еволюція фішингових атак пройшла кілька історичних етапів, кожен з яких відзначався новими методами та підходами до їх здійснення, а саме:

1) *Початковий етап (1990-ті роки)* – характеризується першими спробами реалізації фішингових атак. Цей період відзначився формуванням базових методів, які використовуються фішерами для обману користувачів й отримання конфіденційної інформації. Ключові характеристики даного періоду наведені в Додатку Б.

Отже, етап 1990 років був початковим у формуванні методів фішингових атак. Фішери використовували базові засоби, а їхні атаки нерідко були успішними через недостатню обізнаність користувачів та брак сучасних засобів захисту. Із часом методи фішингу стали більш складними та спеціалізованими, що стало наслідком поширення й розвитку Інтернету та нових засобів і сервісів для здійснення комунікацій.

2) *Ера Інтернету (2000-ті роки)* – характеризується зростанням популярності мережі Інтернет, що стало однією з причин появи фальшивих банківських та фінансових веб-сайтів для збору й викрадання фінансових даних. Цей етап продовжив еволюцію фішингових атак, додаючи нові можливості та методи до арсеналу фішерів. Детальна характеристика основних аспектів даного періоду наведена в Додатку Б.

В цілому, можна стверджувати, що *«Ера Інтернету»* відкрила широкі можливості для фішерів, які стали більш технічно продуманими та цілеспрямованими у своїх атаках. Цей період характеризується появою нових видів фішингу та способів його розповсюдження (див. Додаток Б). При цьому, збільшення кількості інцидентів фішингових атак відбувалось паралельно з розвитком технологій і засобів захисту.

3) *Соціальні мережі (2010-ті роки)* – на виникнення цього історичного етапу розвитку фішингових атак вплинуло розширення використання соціальних мереж. Зловмисники почали використовувати ці комунікаційні платформи для здійснення

атак та отримання конфіденційних даних від користувачів. Характерні особливості даного етапу представлені в Додатку Б. За результатами узагальнення головних відмінностей даного етапу слід відзначити, що він характеризується збільшенням можливостей здійснення атак та маніпуляцій користувачами. Однак потрібно додати, що саме в цей час зростає інформованість користувачів соціальних мереж з питань інформаційної безпеки (ІБ), а власниками відповідних сервісів здійснюється впровадження певних захисних заходів з протидії деяким кібератакам.

4) *Спрямований фішинг (Spear Phishing)* – етап формування більш адресних *(прецизійних або таргетованих)* фішингових атак, який розвинувся у 2010-х роках. На відміну від загальних масових атак, у даному разі зловмисники зосереджувались на конкретних особах чи організаціях, використовуючи додаткову персональну інформацію для збільшення впливу та ефективності атаки. Основні характеристики четвертого етапу розглянуті в Додатку Б.

В цілому, *спрямований фішинг* став більш складним та вдосконаленим методом атаки, який вимагає від атакуючої сторони (може бути й група) більшої підготовки та часового ресурсу для аналізу даних про потенційних жертв. Саме для цього періоду характерне істотне підвищення рівня персоналізації атакуючих дій, що в свою чергу означає використання специфічного інструментарію в рамках фішингової атаки.

5) *Бізнес-Електронна Пошта Компрометації (Business Email Compromise - BEC)* – етап, що розпочинається з середини 2010-х років, коли атаки почали спрямовуватись на більш великі/важливі цілі *(жертви)*, такі як компанії та організації. *BEC* представляє собою злочинну схему, в якій зловмисники намагаються отримати доступ до фінансової чи конфіденційної інформації, використовуючи фальшиві електронні листи, які мають вигляд легітимних. Фішери використовували скомпрометовані акаунти співробітників для фінансовго шахрайства або інших злочинів. Характерні особливості 5-го етапу представлено в Додатку Б.

Резюмуючи розгляд особливостей цього періоду, можна констатувати, що *BEC*-етап став важливим історичним періодом розвитку фішингових атак, характерною рисою якого є спрямованість на корпоративний сегмент потенційних жертв. Очевидно, що в даному разі прослідковується тенденція із адаптації різних методів та використання інноваційних підходів для здійснення фішингу, яка вимагає більшої усвідомленості в сфері використання електронної пошти та здійснення фінансових операцій, а також безперервного оновлення захисту для запобігання реалізації *BEC*-атак.

6) *Мультифакторна автентифікація (Multi-Factor Authentication, MFA)* – замикаючий етап історичного розвитку фішингу, а саме період часткового усунення вразливостей існуючих інформаційно-комунікаційних систем до фішингових атак. *MFA* стала важливим інструментом через те, що вона передбачає використання кількох методів автентифікації для перевірки ідентичності користувача перед наданням йому доступу до облікового запису та/чи делегування певних повноважень управління [2-4]. Таким чином, використання *MFA* допомагає значно ускладнити завдання атакуючій стороні, яка намагається отримати несанкціонований доступ до інформаційного ресурсу. Основні етапи еволюції *MFA* та їх вплив на фішингові атаки наведено в Додатку Б.

Мультифакторна автентифікація [5] відіграє критично важливу роль у зменшенні ризиків фішингових атак, оскільки вона вимагає від користувача надання додаткового фактору для підтвердження своєї ідентичності. При реалізації фішингу шляхом використання електронної пошти зловмисники не можуть здійснити вхід до облікового запису жертви без другого фактору автентифікації, навіть у випадку отримання доступу до пароля. При спробі спрямованого фішингу, зловмисники, котрі використовують соціальну інженерію *(SE)* [6,7] для збору інформації й таргетованих атак, неминуче стикнуться з додатковим бар'єром *MFA*.

Станом на сьогоднішній день, етап впровадження мультифакторної автентифікації є заключним періодом розвитку фішингових атак, що відрізняється від попередніх своєю суттю (*а саме направленістю на захист від даного типу*

атак) та спрямованістю, завдяки вектору щодо усунення ризиків реалізації різних форм фішингу. Можна зробити висновок, що внаслідок зростання рівня обізнаності та поінформованості користувачів/персоналу стосовно питань ІБ, існуючі комунікаційні платформи стали приділяти більше уваги виявленню та блокуванню підозрілих дій, а організації почали користуватися більш ефективними інструментами захисту [8-9].

Із метою всебічного аналізу еволюційних відмінностей для зазначених вище етапів розвитку фішингових атак, проведено ретельний аудит декількох показових прикладів атак [Таблиця В.1], що були реалізовані в різні історичні періоди. Також було порівняно їх характеристики, методи розповсюдження та потенційні наслідки [10-16]. Результати подібної роботи формалізовані у Таблиця В.1, Додатку В.

За результатами проведеного аналізу атак було зроблено ряд висновків, а саме:

- фішингові атаки приймають різні форми та способи реалізації, однак зберігається першість електронної пошти як платформи їх розповсюдження;
- тенденція використання прийомів *SE* зберігається на всіх етапах розвитку фішингу в хронологічному порядку;
- використання тематичних векторів, таких як, соціальні події, фінансові питання тощо, значно збільшує ймовірність успішної реалізації атаки;
- способи реалізації фішингу постійно вдосконалюються, включно з більш точною імітацією легітимних ресурсів, сигналізуючи при цьому про значне зростання складності атак;
- деякі атаки стають більш специфічними, спрямовуючись на конкретні категорії користувачів або організацій, що свідчить про тенденцію збільшення сегментації цільових груп жертв;
- фішинг може виступати способом отримання початкового доступу для іншої вишуканої атаки (наприклад з використанням експлойтів) [17].

Загалом, еволюція фішингу свідчить про постійний розвиток методів та підходів до обману користувачів із метою отримання конфіденційної інформації. Було виявлено закономірність між розвитком інформаційних технологій та

серйозністю наслідків «успішно» реалізованих фішингових атак. Крім того, протягом усіх історичних періодів розвитку фішингу зберігалась актуальність використання прийомів *SE*, що могли функціонувати як самостійні засоби впливу на жертву, так і використовуватись у комплексі з іншими методами й техніками нападу [6, 18].

Основні умовні хронологічні етапи розвитку фішингу можна сформулювати наступним чином:

- *період формування основних методів* (основний акцент на розповсюдження по електронній пошті; зрозумілі та відносно прості способи обману жертви);
- *період технічної еволюції* (виникнення нових видів фішингу внаслідок технологічного прогресу);
- *період спеціалізації та професіоналізації* (підвищення спеціалізації атак через користування прийомами *SE* й глибокою технічною експертизою);
- *період розширення атак на нові цільові групи* (стало можливим через поступове зростання кількості можливих способів розповсюдження);
- *період використання нових технологій* (адаптація до сучасних технологій та використання інноваційних методів, включно з шифруванням, штучним інтелектом (*AI*) тощо).

Однак при цьому слід зазначити істотне зростання ролі засобів захисту та усвідомленості користувачів базових правил користування ІТ-технологіями, свідченням чого є впровадження мультифакторної автентифікації, як інструменту усунення вразливостей інформаційних систем (ІС) від фішингу.

1.2 Визначення місця та частки фішингових атак у загальному спектрі загроз ІБ на різних етапах розвитку ІТ-сфери

У руслі швидкого технологічного прогресу, що спостерігається у XXI столітті, інформаційні технології (ІТ) здобувають все більше визнання, як ключовий каталізатор суспільного та економічного розвитку. Однак слід брати до уваги не тільки безперечні переваги цієї галузі, але й явні недоліки, серед яких значне місце займає розповсюдження кібератак, включно з фішингом. Кожен етап розвитку ІТ-

сфери приніс із собою не тільки нові технологічні можливості, але й суттєво вплинув на спосіб життя суспільства в цілому.

Початковий етап (1940-1960рр.) розвитку ІТ-сфери характеризується виникненням перших електронних обчислювальних машин (в подальшому *комп'ютерів*) та початком розвитку програмування, основними задачами якого була обробка обчислювальних задач та розробка програм для наукових досліджень. Оскільки концепт фішингу, як шахрайська практика для викрадення чутливої інформації, з'явився в значно більш пізній період, доля цих атак на початковому етапі розвитку ІТ-технологій була нульовою.

Етап особистих комп'ютерів (1970-1980рр.) характеризується появою й розповсюдженням персональних комп'ютерів, поширенням операційних систем (ОС), створенням перших текстових та графічних інтерфейсів. Хоча в цей період ІТ-галузь переживала стрімке зростання, однак концепція фішингу ще не була визначеною в тому числі й через відсутність широкосмугового Інтернету та соціальних мереж. Отже, протягом етапу «етапу особистих комп’ютерів», питома частка фішингу була практично нульовою.

Етап Інтернету (1990-2000рр.) характеризується зростанням доступу до глобальної мережі через появу інтернет-спільнот та розширенням її функціоналу. Питома частка фішингових атак на цей період була помірною, хоча їх точність (успішність) була невеликою. Однак загальна кількість фішингу була значно меншою, ніж у подальших етапах розвитку ІТ-сфери.

Бум «доткомів» (2000-2010рр.) характеризується поширенням та активним розвитком веб-технологій, створенням великої кількості дотком-компаній (підприємств, зосереджених на використанні Інтернету та електронної комерції) та інтернет-проектів. Саме з цим періодом асоціюється значне збільшення кількості електронних листів, а також використання соціальних мереж та інших онлайн-платформ для обміну інформацією. Як наслідок, фішингові атаки почали активно набирати обертів. Масова частка фішингу була високою, адже атаки на особисті дані, паролі та фінансову інформацію користувачів ставали дедалі поширенішими.

Етап соціальних медіа і мобільних технологій (2010-2020рр.) характеризується поширенням та зростанням відсотку користування мобільними додатками й сервісами, розвитком хмарних технологій. Підчас цього етапу фішингові атаки набули нових форм та стали більш спеціалізованими. Типовими сценаріями для реалізації такого роду атак було використання соціальних мереж для таргетингу і SMS-повідомлень. Питома частка фішингових атак була дуже високою, оскільки зловмисники адаптували свої методи до нових можливостей, які надали соціальні мережі та мобільні пристрої.

Епоха Штучного інтелекту (AI) та Інтернету речей (IoT) (з 2020р.) характеризується зростанням значущості штучного інтелекту, машинного навчання (*ML*) та інтернету речей (Internet of Things, *IoT*) у різних сферах життя, що створює нові можливості та виклики для ІБ. Оскільки цей історичний період розвитку ІТ-сфери ще триває, то повною мірою оцінити складову частку фішингу у зальному спектрі загроз ІБ складно. Проте, спираючись на статистичні дані (див. Рисунок 1.2), можна зробити висновок, що доля таких атак набуває рекордних по кількості значень впродовж останніх двох років.

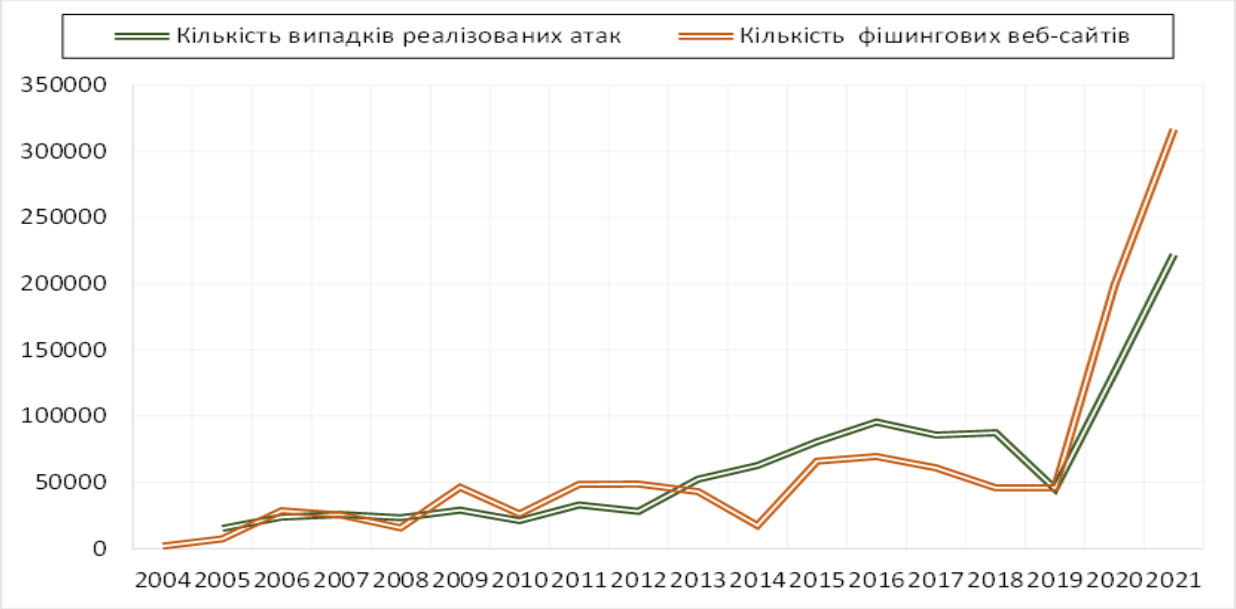

Рисунок 1.2 – Узагальнення щорічних оглядів щодо частки фішингових атак

Отже, динаміка частки фішингових атак у загальному спектрі загроз ІБ суттєво змінюється протягом усіх вище зазначених етапів розвитку ІТ-сфери та визначається різними факторами: - розвиток технологій, поширення Інтернету, поточний рівень обізнаності користувачів й впровадження заходів кібербезпеки та ін. [19, 20].

Для визначення питомої частки фішингу проаналізовано дані [21-38] за період 2004-2021рр. Проведений огляд дозволив прослідкувати тенденцію постійного зростання їх кількості, як для фішингу через електронні листи, так і для створення хижацьких веб-сайтів.

Показники кількості випадків реалізованих *фішингових атак* свідчать про стійкий та істотний ріст цього виду кіберзлочинності. Особливо сприятливим періодом для реалізації атак можна вважати 2020 рік. Це пов’язано з глобальними змінами в способах роботи та комунікації через Інтернет, спричиненими пандемією COVID-19. Крім того, у цей період фішери почали активно користуватись алгоритмами AI, що дозволяють аналізувати та адаптувати контент атаки в реальному часі, враховуючи психологічні особливості кожної потенційної жертви. Варто відзначити зростаючу популярність способу атаки через SMS-повідомлення, що дозволяє зловмисникам обходити захисні бар'єри, які можуть бути встановлені на електронній пошті чи в браузері, направляючи підроблені повідомлення безпосередньо на мобільний пристрій жертви. Ця тенденція свідчить про пошук нових векторів атак та використання різних комунікаційних каналів для досягнення своєї мети [20]. Загалом саме ці ідеї відкрили нові можливості для персоналізації та ускладнення атак, про що свідчать рекордні статистичні показники, наведені на Рисунку 1.2.

При цьому основними характерними рисами використання *фішингових сайтів* є варіативність та адаптивність, адже протягом багатьох років фішери розробляють більш важко розпізнавані ресурси. Крім того, спостерігається поширення мультимедійних компонентів, що дозволяє зловмисникам використовувати візуальні та аудіовізуальні засоби для підвищення автентичності сторінок. Можна

зробити висновок, що збільшення кількості фішингових веб-сайтів на даний період часу, пов’язане з тенденцією підвищення складності їх виявлення, адже з’являються нові технології імітації легітимності веб-сторінок. Саме цими факторами обумовлений рекордний показник кількості фішингових веб-сайтів за вересень 2022 року, що складає 415630 шт [39].

Аналіз схем розгортання фішингових сайтів станом на 2021р. показав, що цей процес не вирізняється простотою реалізації й потребує значного часового ресурсу від атакуючих. Крім того, з’ясувалося, що такі веб-сайти мають короткий термін функціонування, майже третина використовувалась менше доби, а в деяких випадках лише 7-8 годин, перед тим як більшість постачальників хостингу визнавали сайт хижацьким та блокували його. Кожне таке розгортання в середньому має не більше 75-ти потенційних жертв, які відвідали веб-сайт [40]. До того ж, прослідковується характерна закономірність щодо зацікавлення чутливою інформацією, серед якої найбільше збирались дані кредитної картки, що становить 61% від усіх запитів. На другому місці із показником у 40% розташувались дані про електронну адресу користувачів. Найменша масова частка належить даним про номер телефону (22%), дату народження (17%), номер ідентифікаційного документу (15%), відповіді на контрольні запитання (14%) та ПІН-коди банкомату (3%).

За даними 2022 року [41], можна стверджувати, що термін функціонування фішингових веб-сайтів збільшився вдвічі, і медіанний показник цієї характеристики становив 3,7 днів, а кількість потенційних жертв-відвідувачів зросла до 93-х користувачів. Серед видів чутливої інформації, яку збирали фішери є адреси електронної пошти (73%), домашні адреси (66%), паролі (58%). Масова частка інформації про кредитні картки зменшилася з 61% до 29%, що свідчить про значну зацікавленість збору особистих ідентифікаційних даних.

Починаючи з 2021 року, фішинг став найпоширенішим методом отримання первинного доступу для реалізації наступних кібератак із показником у 41%, що на

8% більше у порівнянні з 2020 роком. Станом на 2022 рік, фішингові операції продовжують залишатися в топі та становлять 41% (див. Рисунок 1.3).

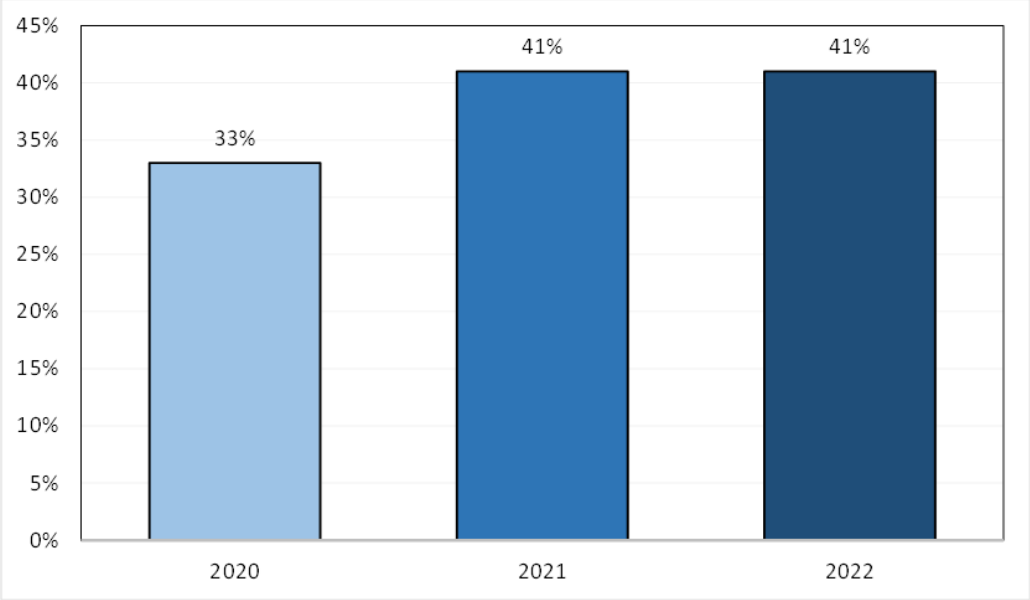

Рисунок 1.3 – Питома частка фішингових атак серед інших станом на 2022р.

Причому із загальної кількості випадків фішингу можна виділити масову частку кожного типу цих атак (див. Рисунок 1.4).

Рисунок 1.4 – Типи фішингу як відсоток від загальної кількості атак станом на 2022р.

Зрозуміло, що найпоширенішим видом фішингу із показником 62% від загальної кількості таких атак є спрямований фішинг із вкладеним додатком [41]. Він характеризується використанням електронного листа з прикріпленим додатком, що містить певний зловмисний код. У випадку, коли користувач ініціює цей файл, його система може бути заражена або скомпрометована, дозволяючи атакуючому здійснити несанкціонований доступ (НСД) або отримати чутливу інформацію.

Другим по популярності серед зловмисників є спрямований фішинг із вкладеним посиланням, що становить 33% загального спектру атак. Цей тип атак передбачає надсилання електронного листа, який містить посилання з хибним URL. Коли користувач переходить за цим посиланням, він може потрапити на сторінку, яка імітує легітимний веб-ресурс, що, у свою чергу, дозволяє зловмисникам заволодіти його конфіденційною інформацією.

Фішинг як сервіс, охоплює 5% від загальної кількості атак та займає третє місце серед найбільш розповсюджених типів фішингу. Являє собою своєрідне поєднання шкідливих додатків та використання фішингового сервісу, що надає атакуючим ефективні інструменти, інфраструктуру та методології для реалізації атак. Прикладом послуг фішинг-сервісу можуть бути шаблони для фішингових листів, вбудовані віруси тощо.

Таким чином, у результаті аналізу та оцінки динаміки питомої частки фішингових атак у загальному спектрі загроз ІБ встановлено, що такі атаки характеризуються адаптивністю та варіативністю, тобто постійно вдосконалювались та пристосовувались до технологічних реалій на різних етапах розвитку ІТ-сфери.

1.3 Узагальнення відомостей стосовно регіональних та галузевих відмінностей реалізації фішингових атак

Регіональні та галузеві відмінності у реалізації фішингових атак є ключовими аспектами аналізу кібербезпеки, оскільки вони визначають унікальні особливості та шаблони, характерні для конкретних географічних областей та галузей діяльності. Так, найважливішим аспектом фішингу на *галузеві ресурси* є здатність

атакуючих адаптувати свої методи до специфіки цільового сектору *(тобто потенційних жертв)*. Послуговуючись вивченням галузевих особливостей, комунікаційних звичаїв, технічних та термінологічних нюансів, фішери мають можливість реалізовувати складні інтегровані атаки. Серед основних галузевих особливостей фішингових атак слід відзначити:

- *рівень обізнаності в галузі* – достатній рівень розуміння сфери, на яку спрямовується атака, включаючи термінологію та загальний ритм комунікацій у даній галузі;
- *врахування географічних аспектів* – розуміння специфіки географічного розташування організацій та їх клієнтів, що дозволяє впроваджувати локалізований контент та робити повідомлення більш звичними для потенційних жертв;
- *експлуатація специфічних подій та новин* – використання нагальних новин, подій або тенденцій у галузі для гнучкої адаптації до актуального становища справ;
- *використання реквізитів галузевих організацій* – використання назв та логотипів відомих в обраній сфері організацій для підвищення ступеню довіри користувачів до фішингового повідомлення;
- *використання фахової термінології й спеціальних технічних аспектів* – імітація технічних або наукових термінів із метою реалізації більш автентичної атаки, яка виглядатиме переконливо навіть для фахівців обраної галузі;
- *експлуатація зв'язків між об'єктами галузі* – інсайдерське та *SE* вивчення структури взаємозв'язків між організаціями, фахівцями та іншими учасниками галузі для підвищення вірогідності «успішності» атаки, що планується.

Таким чином, фішинг на галузеві ресурси вимагає від атакуючого глибокого розуміння конкретної сфери, щоб створити атаки, які максимально наближені до легітимних повідомлень та легко приймаються цільовими об'єктами.

Якщо оцінювати окремі галузі з точки зору потенційної вигоди фішерів, то стане зрозуміло, що для більшості з них вона буде високою [19]. У Таблиці 1.1 наведено загальну оцінку потенційної шкоди від «успішно» реалізованої фішингової атаки для деяких галузей, проте потрібно розуміти, що її показник буде варіюватися в залежності від конкретної ситуації та обставин.

Таблиця 1.1 – Потенційна шкода від фішингових атак для деяких галузей

Сфера діяльності	*Потенційна вигода для атакуючого*
Фінансовий сектор	Висока. Можливість отримання доступу до значних фінансових активів та чутливої інформації.
Медична сфера	Висока. Має високу вартість на «чорному» ринку, можливе її використання для шахрайства, шпигунства та булінгу [19, 20].
IT-індустрія	Висока. Доступ до конфіденційних технічних даних, можливість впливу на розробку та безпеку програмного забезпечення [17, 18].
Електронна комерція та роздрібна торгівля	Висока. У разі отримання доступу до облікових записів та фінансової інформації можливе її використання на «чорному ринку», а також в якості особистої матеріальної вигоди.
Соціальні мережі та медіа	Висока. Викрадені облікові записи та особисті сторінки можуть слугувати не тільки для розповсюдження дезінформації й маніпулювання громадською думкою, але мати серйозні репутаційні й фінансові наслідки [42].
Криптовалюти й блокчейн	Висока. Доступ до крипто гаманців дає можливість для їх використання з ціллю викрадення значних фінансових активів.
Логістика та транспорт	Середня. Доступ до інсайдерської інформації про логістичні процеси може мати суттєве значення для умов конкурентного ринку.

За останній десятирічний період галузеві атаки стали важливим об'єктом дослідження та аналізу в контексті заходів забезпечення кібербезпеки. Цей період відзначився значним розширенням кіберзлочинності, а також появою нових та вдосконаленням уже існуючих методів атак. Зростання використання технологій та цифровізація суспільства призвели до того, що багато галузей стали більш уразливими перед потенційними загрозами. У цьому контексті було проведено дослідження направленості галузевих атак протягом терміну 2008-2022рр. Так, за

даними *Anti-Phishing Working Group* [25-39] сформовано діаграми для цільових галузевих секторів при реалізації фішингових атак (див. Рисунок 1.5).

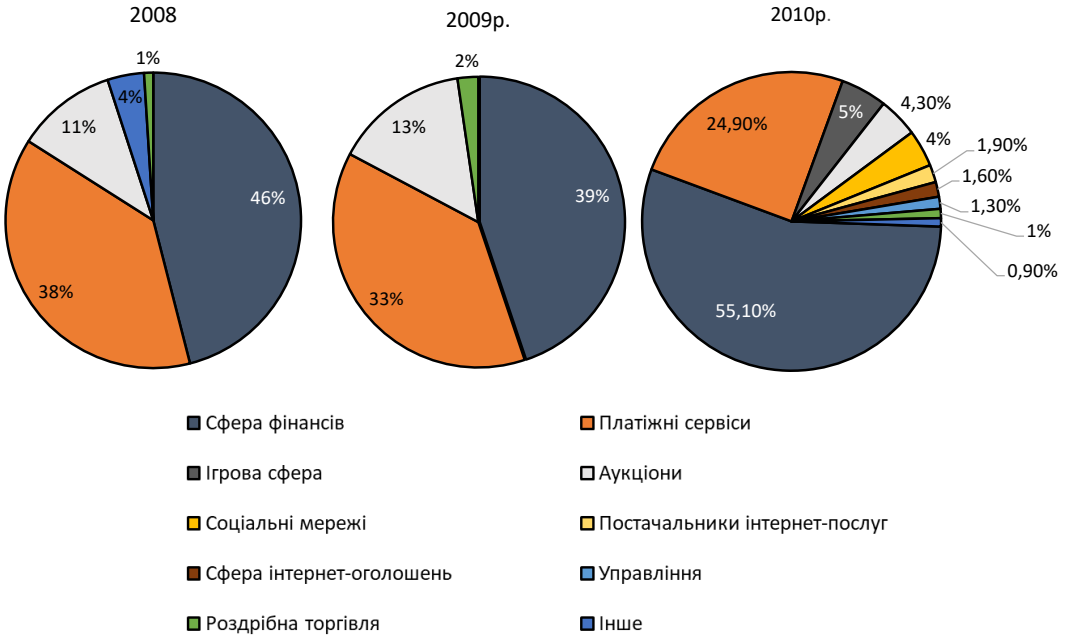

Рисунок 1.5 – Розподіл галузевих секторів при реалізації фішингових атак (станом на 4-й квартал 2008-2010рр.)

Очевидним лідером по кількості фішингових атак є сфера фінансів та платіжних систем. Це пояснюється відносно невисокою цифровізацією інших галузей під час даного історичного проміжку та найбільшою потенційною вигодою для зловмисників. Зрозуміло, що станом на 2010 рік кількість безпечних сфер діяльності людини в цифровому просторі значно зменшилась, що свідчить про збільшення випадків фішингових атак у загальному спектрі загроз ІБ. Більш того, для цього проміжку часу характерний бум соціальних мереж, саме тому починаючи з 2010 року і надалі, ця сфера буде займати значне місце серед галузей, котрі активно використовуються фішерами.

Період наступних 3-х років (2011-2013 рр.) також характеризується лідерством фінансової галузі (див. Рисунок 1.6).

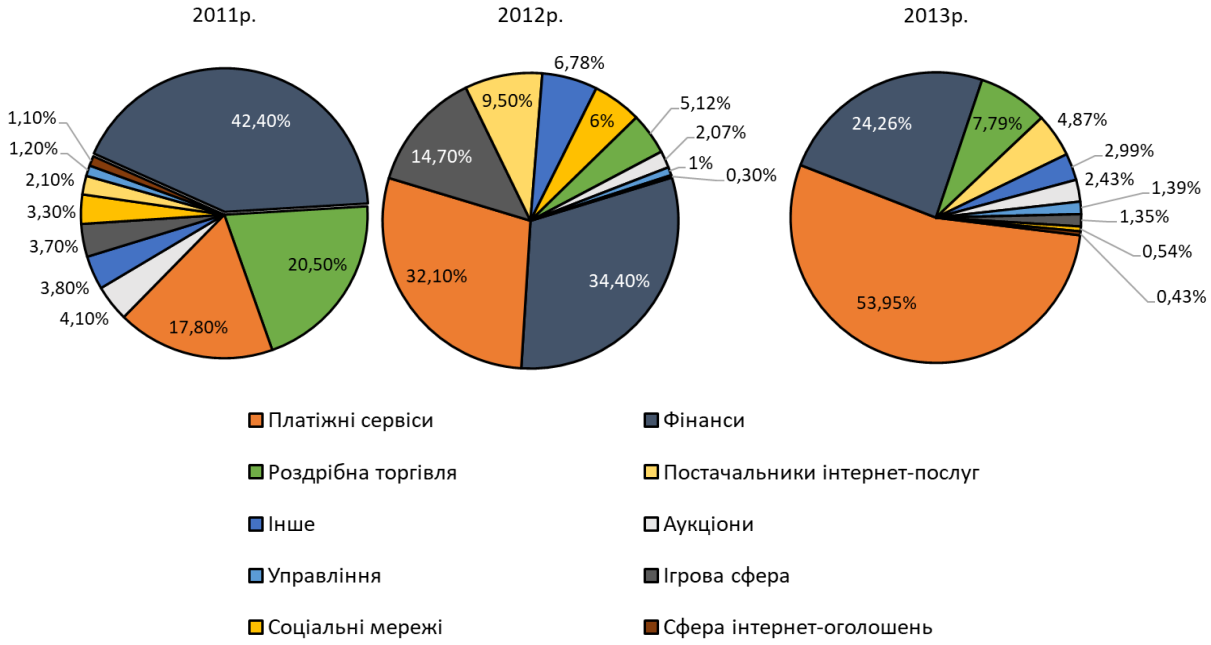

Рисунок 1.6 – Галузеві відмінності при реалізації фішингових атак (станом на 4-й квартал 2011-2013 рр.)

Аналізуючи дані за 4-й квартал наступних 3-х років, можна зробити висновок про продовження тенденції зростання кількості галузей, атакованих фішерами. Однак лідерство серед них все ще займає фінансова сфера.

За період 2014-2017 рр. було отримано дані, які свідчать по виникаючу зацікавленість зловмисників галузями освіти, сферою управління та значним ростом фішингових атак на сферу електронної комерції (*роздрібної торгівлі*) (див. Рисунок 1.7).

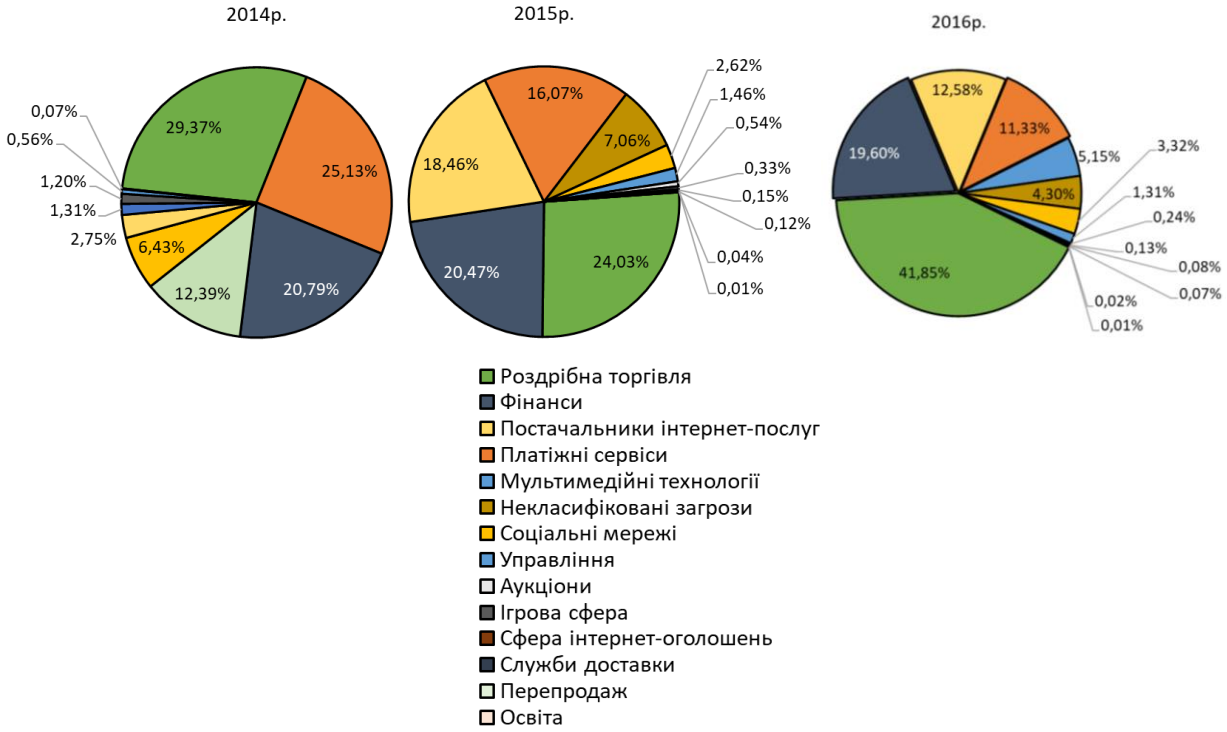

Рисунок 1.7 – Галузеві відмінності при реалізації фішингових атак (станом на 4-й квартал 2014-2017 рр.).

А спираючись на дані 2017-2019 рр. (див Рисунок 1.8), можна зробити висновок, що серед нових сфер діяльності людини, що піддавались фішингу, було виявлено логістику, телекомунікацію та хмарні сховища.

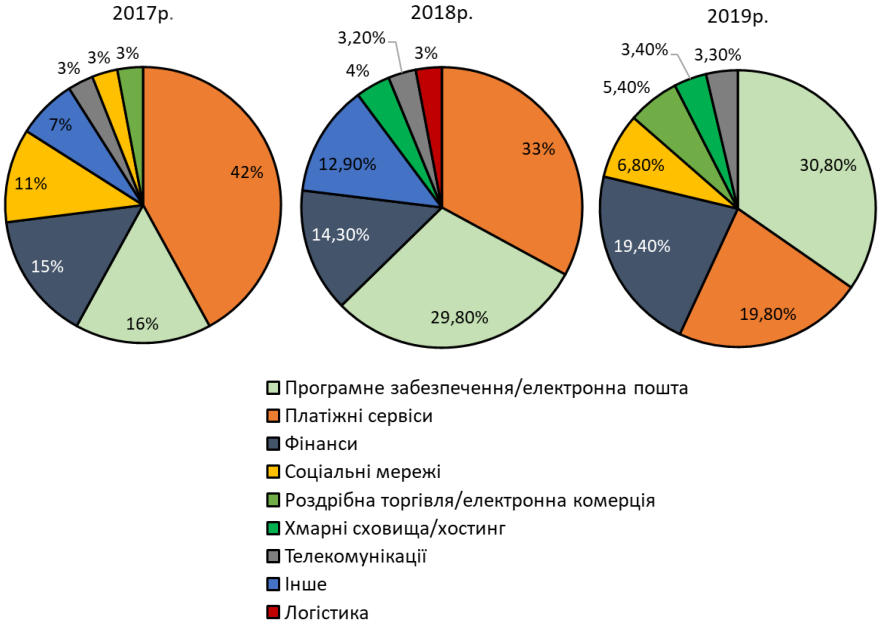

Рисунок 1.8 – Галузеві відмінності при реалізації фішингових атак (станом на 4-й квартал 2017-2019 рр.)

Крім того, 4-й квартал 2017-2019 рр. характеризується поступовим зростанням ролі електронної пошти та програмного забезпечення (ПЗ). Ця сфера займає найбільше відсоткове співвідношення відносно інших галузей у четвертому кварталі 2019 року, та стає лідером серед реалізованих атак. Це пов'язано з початком триваючої ери AI.

Останній досліджений період 2020-2022 рр. (див. Рисунок 1.9) характеризується не тільки збільшенням відсоткової долі соціальних мереж серед інших областей, але й значною роллю ПЗ та електронної пошти.

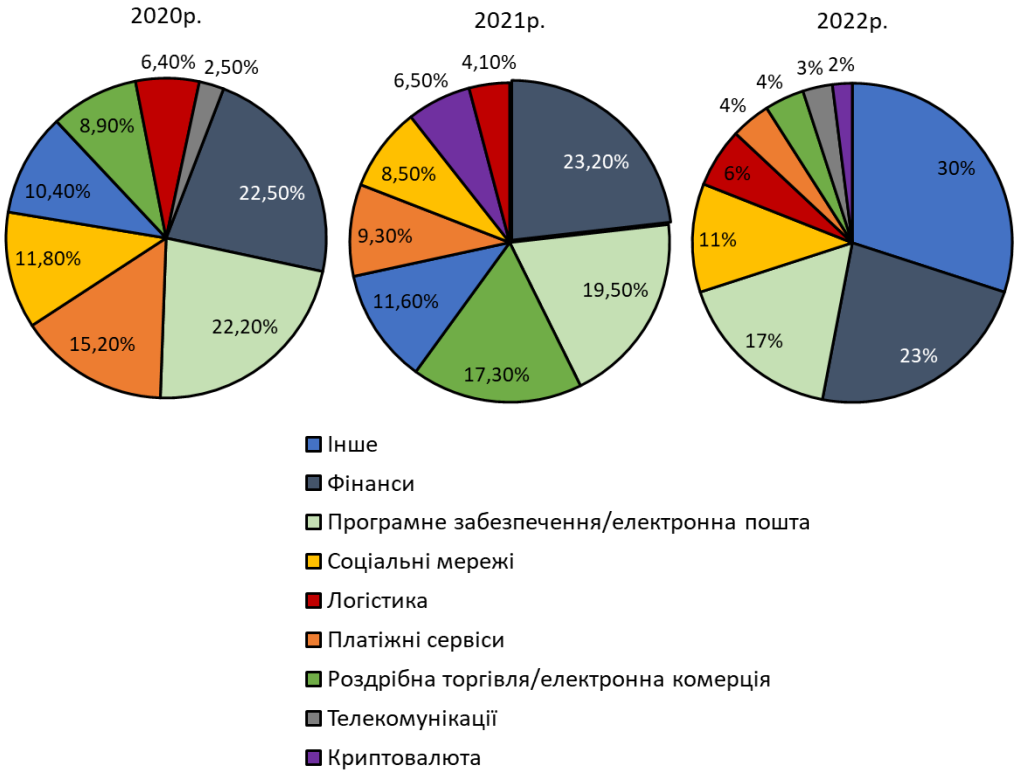

Рисунок 1.9 – Галузеві відмінності при реалізації фішингових атак (станом на 4-й квартал 2020-2022 рр.)

Загалом, дані 4-тих кварталів 2020-2021рр. показали, що більшість атакованих галузей були перенесені в цифровий простір, порівняно з попереднім часовим періодом. Так, станом на 3-тій квартал 2022р [39], основними сферами діяльності, де були успішно реалізовані фішингові атаки, стали фінанси, ПЗ й електронна пошта та соціальні мережі.

Отже, за останні десятиріччя спостерігалася помітна еволюція фішингових атак, яка супроводжувалася зміною пріоритетних цілей для кіберзлочинців. Виявлено, що галузі фінансового сектору та банківської діяльності залишаються основним об'єктом атак, проте спостерігається зниження їх відносної частоти у порівнянні з іншими галузями. Водночас, сектори електронної комерції та поштових сервісів залишаються стійкими до фішингу.

Ці результати свідчать про важливі зрушення в стратегіях кіберзлочинців та підкреслюють необхідність постійного вдосконалення заходів кібербезпеки в усіх галузях економіки. Крім того, важливим виявляється розгляд фішингових атак в контексті конкретних особливостей різних галузей, що дозволяє розробляти більш ефективні та цілеспрямовані стратегії захисту.

Реалізація фішингу на *регіональні ресурси* має свою власну специфіку, оскільки вона спрямована на конкретний географічний сегмент аудиторії:

- *Маскування під місцевий бізнес* – створення вигляду легітимного місцевого підприємства, використовуючи його логотипи, кольорову схему та географічну інформацію.
- *Локалізація контенту* – використання мови, а також інших деталей, *характерних* для конкретного регіону, із метою більшої переконливості потенційних жертв.
- *Використання локальних подій/новин* – адаптивність фішингових повідомлень до актуальних подій, що відбуваються в конкретному регіоні, що спонукає жертв до відкриття фішингових сповіщень.
- *Використання внутрішньорегіональних ланок довіри* – імітація назв легітимних авторитетних організацій регіону для переконливості та виклику довіри потенційної жертви.
- *Специфічні способи контакту* – використання широковживаних контактних даних *(телефонні номери з певним кодом, електронні адреси з конкретної доменної зони тощо)*, притаманних конкретному регіону.

- *Сегментація аудиторії* – збільшення ефективності фішингу при реалізації більш персоналізованих атак.
- *Використання місцевих правописних і граматичних особливостей* – сприяє відтворенню особливостей мовлення та письма, що характерні для певного регіону.

Загалом, кожен регіон можна оцінити з точки зору потенційної «вигоди» для атакуючого, враховуючи специфічні особливості кожного з них (див. Таблиця Г.1, Додатку Г).

В цілому, регіональний фішинг є специфічною варіацією атаки, яка використовує місцеві особливості та контекст для збільшення ймовірності успішного проведення шахрайської схеми. В якості найбільш важливих (для фішингових атак) регіональних відмінностей слід визначити: - *мовні особливості* (використання специфічних мов та діалектів впливає на граматику та орфографію фішингового сповіщення); - *культурні відмінності*; *технічні обмеження* (різний рівень науково-технічного розвитку та засобів захисту); - *правові аспекти* (варіювання норм законодавства, щодо кіберзлочинності та ІБ). Залежно від ефективності впровадження *SE*-атак і використання місцевих аспектів, такий вид атаки може мати значний вплив на регіональних користувачів.

Так, для *Азійських країн* характерний високий рівень мовної специфіки й соціальних і культурних особливостей регіону. Детальний розгляд цих аспектів наведено в Додатку Г. У сукупності таких специфічних аспектів формувались й характерні риси реалізації фішингових атак, серед яких особливе місце займає адаптивність до мов і культур Азії. Тобто можна зробити висновок, що внаслідок особливої лінгвістики регіону, складність фішингу значно підвищується.

Технологічний стек азійського регіону характеризується низкою особливостей, а саме:

- *Високий рівень розвитку IT галузі* є визначальним чинником економічного та соціокультурного прогресу.

- *Мовний аспект* при якому розробники ПЗ повинні приділяти увагу локалізації та адаптації продуктів до різних мовних середовищ. Це включає не лише інтерфейс, але й підтримку введення тексту, переклади сервісна підтримка та інші аспекти.
- *Мобільні Технології та Електронна Комерція* – високий рівень використання мобільних пристроїв та зростання електронної комерції.
- *Швидке впровадження IoT.*
- *Інвестування розвитку AI та ML,* включно з розробкою алгоритмів і створенням систем автоматизації та аналітики контенту що циркулює.
- *Висока увага до галузі блокчейн і криптовалют.*

Загалом, використання ІТ у азійських країнах відзначається високим рівнем розвитку та широким застосуванням технологій у різних галузях економіки й суспільства. Саме завдяки цьому рівень потенційної вигоди для фішерів досить високий. Адже зловмисники, що спрямовуються на цей регіон, можуть мати користь від чисельності потенційних жертв та обсягів призового фонду.

Високий рівень мовної специфіки й соціальних і культурних особливостей *Європейських країн*, знайшло своє продовження у низці аспектів, які представлені в Додатку Г. В цілому, в контексті особливостей європейського регіону, слід відзначити наступні аспекти:

Цифрова трансформація та Індустрія 4.0 – впровадження та використання IoT, AI, ML, блокчейн та інших сучасних технологій для покращення виробництва та послуг.

- *Високий рівень ІБ та кіберзахисту.*
- *Широке використання онлайн-сервісів для взаємодії з урядом.*
- *Високий рівень фінансових технологій (Fintech)* – регіон є одним з центрів розвитку фінансових технологій (онлайн-платежі, блокчейн та криптовалюти).
- *Широке використання хмарних технологій* стало стандартом для багатьох компаній та установ регіону.

- *Високий рівень розвитку мобільних додатків та електронної комерції,* які впливають на багато сфер суспільства та економіки.

Таким чином, показник потенційної вигоди для фішерів дуже високий, адже у цьому регіоні широко представлена вся номенклатура потенційних об'єктів атаки, але в той же час конкуренція та поточний рівень ІБ також є високий, що впливає на успішність подібних атак.

Високий показник мовної специфіки *Північної Америки* обумовлений наявністю білінгвальності та культурної суміші різних етносів. Рівень соціальних та культурних особливостей також досить високий. В цілому, за результатами аналізу специфіки розвитку ІТ сфери та розвитку галузей технологічного стеку, варто виділити наступні аспекти:

- *Лідерство у галузі цифрової трансформації та інновацій.*
- *Активна розробка та вдосконалення систем кіберзахисту.*
- *Високий рівень фінансових технологій (Fintech).*
- *Використання хмарних технологій* є стандартом для багатьох компаній та установ.
- *Високий розвиток медіа сфери.*
- *Високий рівень розвитку електронної комерції та мобільних додатків.*

Саме завдяки високому рівню технологічного базису, ведучі країни Північної Америки можуть розглядатися фішерами, як регіон зі значною потенційний вигодою в разі успішної реалізації атак. Однак слід брати до уваги достатній рівень розвитку сфери ІБ, що ускладнює умови реалізації атак.

Латинська Америка відзначається великим різноманіттям мовних спільнот та культурних особливостей. Аспекти, що сформували високий рівень мовної специфіки та культурних і соціальних особливостей регіону більш докладно викладені в Додатку Г. При цьому, в розвитку технологічного стеку регіону домінують наступні аспекти:

- *ІТ-інфраструктура;*
- *цифрова трансформація та інновації;*

- *фінансові технології (Fintech);*
- *електронна комерція та мобільні додатки;*
- *електронний уряд та E-послуги;*
- *розвиненість стартапів та нових технологічних систем.*

Технологічний рівень розвитку країн Латинської Америки робить цей регіон привабливим для реалізації фішингових атак. У даному випадку, фішери можуть розраховувати на потенційну вигоду за рахунок відносно низького рівня кіберзахисту в деяких країнах, а також в наслідок широкого розповсюдження електронних платежів та онлайн-банкінгу.

Отже, можна зробити висновок, що реалізація фішингу в різних регіонах має унікальні аспекти, котрі обумовлені економічним, культурним, технологічним та освітнім середовищем кожного окремого регіону.

Аналізуючи дані про найбільш постраждали від кібератак регіони [41], було зроблено порівняння кількості відповідних загроз для 5-ти основних регіонів, впродовж 2020-2023рр. (див. Рисунок 1.10).

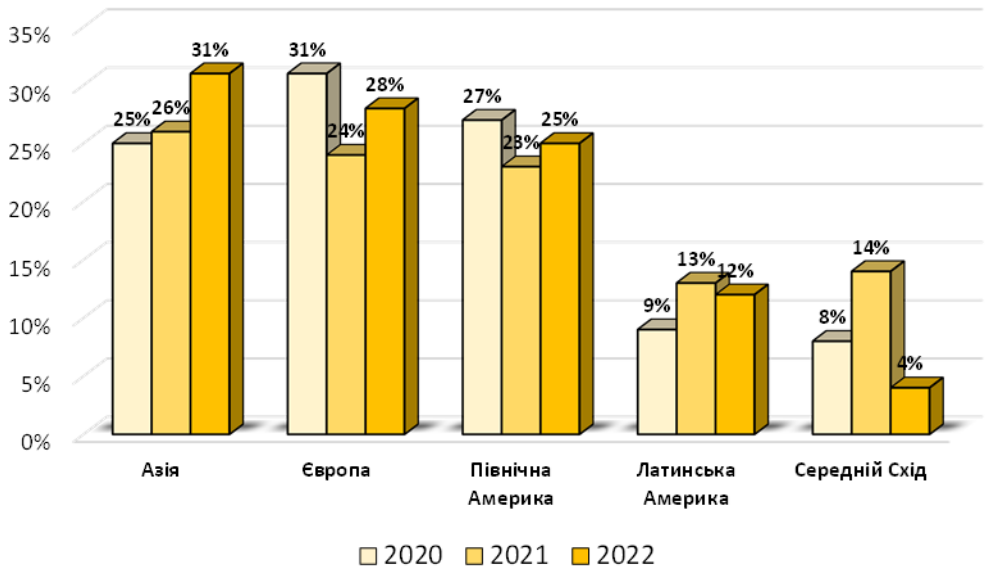

Рисунок 1.10 – Регіональні відмінності в кількості атак (2020-2023 рр.)

В цілому, можна зробити висновок, що найбільшу вигоду для порушників безпеки становлять атаки саме Азійських країн. При цьому цей регіон утримує «лідерство», як найбільш атакованого вже другий рік поспіль. Європа «тісно»

слідувала за ним із показником 28% атак, а Північна Америка зазнала 25% інцидентів ІБ, станом на 2022р. При цьому Азійський регіон та Європа зафіксували вищі показники випадків порушення безпеки, котрі виросли на 5 та 4 відсоткових пункти відповідно, порівняно з 2021 роком, у той час як Середній Схід відзначився значущим зниженням з 14% до 4%.

Найбільш атакованою галуззю *Азійського регіону* станом на 2022р. стала виробнича сфера, що становить 48% від загальної кількості атак , а фінанси та страхування займали другу позицію з показником 18%. При цьому спрямований фішинг із вкладеннями був найпоширенішим вектором зараження у цьому регіоні, становлячи 40% від загальної кількості інцидентів. Випадки використання зовнішніх віддалених сервісів та спрямований фішінг через посилання посіли третю позицію, із показником 12% кожний.

Серед найбільш атакованих галузей *Європейського регіону* станом на 2022р. варто відзначити професійні, бізнес, споживчі послуги, фінанси та страхування, кожна з яких становить 25% від усіх випадків. Виробнича сфера посіла друге місце з показником 12%, а енергетика та охорона здоров'я поділили третє місце, кожна з них складала 10% від загальної кількості атак. Спрямований фішинг через посилання став третім по поширеності методом інфікування з питомою часткою 14% від загальної кількості векторів, що на 28% менше, ніж в 2021 році. Це зменшення показника є результатом зростання обізнаності користувачів, посилення уваги засобам захисту електронної пошти та ефективнішого виявлення зловмисного ПЗ.

Регіон *Північної Америки* характеризується галузевим розподілом загроз ІБ, при якому 20% усіх випадків займала енергетична сфера. Виробнича сфера та сектор роздрібно-оптової торгівлі поділили друге місце з показником 14%, а професійні, бізнес- та споживчі послуги зайняли третє місце у 2022 році, складаючи 12% від загальної кількості випадків. Спрямований фішинг через вкладення займав друге місце серед найважливіших векторів інфікування із показником 20%.

У 2022 році тенденції галузевих атак у країнах *Латинської Америки* відхилилися від глобальних, повернувши роздрібно-оптову торгівлю як найбільш атаковану сферу з 28% випадків. Фінансова та страхова галузь стала другою за кількістю атак – 24% випадків, третьою була енергетика з 20%. При цьому спрямований фішинг через вкладення складав 10% від загальної кількості методів початкового доступу під час реалізації атак.

Фінанси та страхування у 2022 році були найбільш націленою галуззю на *Близькому Сході та в Африці*, становлячи 44% всіх випадків ІБ. Професійні, бізнес- та споживчі послуги відповідали за 22% атак, при цьому виробництво та енергетика ділили третє місце, кожна з них складала 11% від загальної кількості інцидентів. При цьому спрямований фішінг через посилання, як метод отримання початкового доступу, використовувався в двох третинах випадків.

Отже, можна зробити висновок, що регіони світу різняться за характером та обсягами фішинг-атак, адже їх масштаби визначаються не тільки технічними аспектами, але і соціально-політичними та економічними факторами [43]. В цілому, можна стверджувати, що:

- по-перше, галузеві відмінності вказують на те, що фішери активно адаптують свої стратегії в залежності від специфіки конкретного сектору.
- по-друге, наявність яскраво виражених регіональних відмінностей зумовлює те, що кіберзлочинці орієнтуються на конкретні особливості кожного регіону. Наприклад, у регіоні Азійсько-Тихоокеанського басейну активно використовуються атаки, спрямовані на виробничі підприємства, тоді як у Європі набуває популярності використання *«backdoors» та «ransomware»*.

1.4 Визначення структури та змісту здійснення фішингових атак, що притаманні для корпоративного та приватного сегментів користувачів сучасних ІС

Як свідчать результати проведеного аналізу, проблематика фішингу має свої варіації та специфічні особливості у різних сегментах суспільства. Корпоративний сектор, в своїй переважній більшості, потребує індивідуального підходу та

комплексного захисту. Із іншого боку, приватні користувачі, керуючись власним досвідом, зазнають інших ризиків, проте й вони є не менш вразливими перед цією загрозою. Тому в межах роботи було зроблено всебічний аналіз структури і змісту фішингових атак у кожному з цих сегментів з метою визначення ефективних стратегій захисту та протидії даній загрозі.

Корпоративний сегмент користувачів відзначається рядом унікальних характеристик, що впливають на сценарії та наслідки фішингових атак у ньому. Однією з ключових особливостей є наявність великої кількості конфіденційних або «чутливих» даних, що стосуються як самої компанії, так і її клієнтів та партнерів [19].

Ще однією особливістю корпоративного сегменту є велика кількість співробітників, що використовують загальну інфраструктуру. Це створює додаткові «точки входу» для зловмисників, оскільки компанії намагаються створити більш зручні в управлінні системи, які можуть мати певні вразливості. Фішери користуються ними для проведення атак, намагаючись вплинути на працівників та отримати несанкціонований доступ до корпоративних ресурсів. Крім того в корпоративному сегменті існує висока ступінь взаємозалежності між співробітниками, внаслідок чого одна недбалість чи помилка може призвести до ланцюгової реакції, що відкриє нове «вікно можливостей» для зловмисників.

Аналізуючи специфіку фішингових атак для *приватного сегменту* користувачів, можна виявити кілька ключових аспектів. Перш за все, приватні користувачі володіють обмеженими технічними ресурсами та не мають доступу до високотехнологічних заходів безпеки, що робить їх вразливими перед широким спектром загроз, особливо в контексті варіативності *SE*-атак, як одного з найефективніших інструментів фішингу. По-друге, існує проблема підвищення профільної компетентності з питань ІБ. У цьому разі освіченість користувача є ключовою складовою захисту від фішингу, оскільки це є умовою розпізнавання потенційно небезпечних ситуацій та вдалого з них виходу. По-третє, приватні користувачі можуть власноруч зробити акцент на використанні надійних

антивірусних рішень, паролів та двоетапної автентифікації, що є ефективним способом захисту від більшості загроз.

При реалізації фішингу в приватному сегменті користувачів характерне одночасне використання різних комбінацій методів та стратегій, спрямованих на посилення шкоди атаки. Варто зазначити, що зловмисники намагаються адаптувати свої методи відповідно до характеристик та поведінки приватних користувачів. Зокрема, деякі спроби атаки можуть надійти через електронну пошту відомих компаній або інституцій, де хакери вдаються до імітації легітимних повідомлень для отримання конфіденційних даних. Крім того, приватні користувачі можуть стати жертвами фішингу через соціальні мережі, де зловмисники встановлюють підроблені профілі або надсилають шкідливі посилання.

Слід відзначити, що корпоративні та приватні користувачі можуть зазнавати різних форм атак, оскільки вони оперують в неоднакових інформаційних середовищах та мають відмінні апаратні обмеження та характер взаємодії із зовнішнім інформаційним середовищем (див. Таблиця Г.2, Додатку Г).

За результатами узагальнення відомостей Таблиці Г.2, можна зробити висновок, що для корпоративного та приватного сегментів користувачів існують важливі відмінності:

- у корпоративному секторі, важливим є комплексний захист, котрий регламентується шляхом впровадження відповідних політик інформаційної безпеки (ПІБ);
- приватні користувачі мають справу з інакшою динамікою та різнорідністю загроз. Їхні можливості зазвичай більш обмежені, і вони можуть не мати доступу до таких можливостей що притаманні для корпоративного сегменту.

Виходячи з вищесказаного, вочевидь, що стратегії фішингу для цих двох сегментів потенційних жертв атаки відрізняються.

Стратегію типової фішингової атаки на *корпоративний* сегмент користувачів можна представити наступним набором дій (*безвідносно їх взаємної композиції та послідовності застосування*):

1) *Перехоплення доступу до корпоративних облікових записів* шляхом надсилання електронного листа, що імітує офіційне повідомлення IT-служби компанії або партнерської організації. Такий лист може містити посилання на підроблений веб-сайт, де співробітник повинен ввести свої облікові дані.
2) *Імперсоніфікація (уособлення) керівництва* це не тільки спроба впливу на бізнес-процеси, але й метод оволодіння конфіденційною інформацією компанії. Фішер імітує звернення керівництва організації до співробітника через електронний лист, який містить вимоги передачі потрібної для атакуючого інформації. Задля більшої переконливості, зловмисник може підробити ідентифікаційні документи та застосувати прийоми *SE.*
3) *Відправка шкідливих вкладень* притаманна для обох сегментів користувачів IT-ринку, однак має свої особливості у рамках атаки на компанії та організації. Зловмисники намагаються вбудувати шкідливий код або вірус у вкладення листа. Через досить високий показник внутрішньої комунікації в організаціях, це може призвести до інфікування корпоративних мереж.
4) *Використання SE* є одним із спільних підходів фішингу до користувачів як приватного, так і корпоративного сегментів. Проте для останнього з них характерне вибіркове використання інформації із зовнішніх джерел, із метою більшої переконливості.
5) *Створення фальшивих веб-сайтів та форм* (у разі введення співробітником даних на таких сторінках, атакуючий повною мірою отримує доступ над інформацією, що його цікавить [19]).

Структура типової фішингової атаки на корпоративний сегмент користувачів з каналом впливу через електронну пошту, містить наступні етапи:

1) *Створення листа, що має вигляд автентичного,* це початковий етап атаки, де фішер намагається створити максимально правдоподібний лист, що містить сповіщення про необхідність оновлення паролю для забезпечення безпеки облікового запису.

2) *Використання авторитетного джерела,* тобто імітація звернення члена внутрішнього підрозділу компанії, що надає всій процедурі більшої переконливості.
3) *Додавання специфічного повідомлення,* тобто посилення ґрунтовності (є прийомом *SE),* де наприклад вказується, що в системі виявлено підозрілу активність в обліковому записі одержувача тощо.
4) *Створення почуття обмеження часу (часовий пресинг)* задля виклику почуття невідкладності та терміновості. У зверненні фішер наголошує на необхідності негайної дії. Ціллю дій є позбавлення жертви часу на усвідомлення ситуації.
5) *Додавання посилання на імітований веб-сайт компанії*, що виглядає як легітимний ресурс Ціллю подібних дій є посилення аргументованості пропонованих дій, що дезорієнтує жертву атаки.
6) *Збір облікових даних* співробітника, наприклад на сервері зловмисника.
7) *Надсилання сповіщення про успішну зміну паролю* необхідне для створення оманливого почуття повного контролю ситуації з боку атакованого.

Як видно з цього прикладу, структура атаки побудована таким чином, що має вигляд офіційного сповіщення від відомого джерела та спонукає користувача перейти за посиланням, де йому пропонується ввести свої особисті дані. Такий підхід є особливо небезпечним для корпоративних користувачів, а зміст подібної атаки імітує офіційні комунікації від довіреного джерела (установи).

В цілому, фішинг на корпоративні ресурси є досить складним та вимагає від атакуючих високого рівня технічної компетентності. Успішна реалізація таких атак може призвести до серйозних наслідків, включаючи втрату конфіденційної інформації та фінансові збитки для компанії чи приватного користувача.

Структура фішингової атаки на *приватного* користувача буде формуватися в залежності від її мети, обраного способу реалізації та рівня освіченості жертви. Для прикладу було розглянуто типову фішингову атаку *«Електронний лист від банку»*. У цьому випадку стратегія фішера виглядає наступним чином:

- по-перше, звичним для жертви каналом зв’язку користувач отримує лист, що має вигляд повідомлення від довіреної організації;

- по-друге, лист містить твердження, що в користувача присутні невирішені питання, які потребують негайної уваги. Таким чином зловмисник тисне на терміновість, що є елементом *SE*;

- по-третє посилюється ґрунтовність. Для цього прикріплюється посилання на заздалегідь підроблений (або скомпрометований) веб-сайт банку;

- по-четверте, формується сповіщення про успішність процедури, що створює умови для наступних дій та забезпечує виграш часу для атакуючого.

У випадку введення даних, атака вважається реалізованою, адже зловмисник отримує доступ до конфіденційної інформації. У підсумку, атакуючий може або видалити фальшивий сайт, або продовжувати надсилати жертві подібні листи, аби отримати ще більшу кількість додаткової інформації [19].

Зміст цієї атаки можна представити наступним алгоритмом дій фішера:

1) *Підробка заголовка електронного листа*, що повинен виглядати як офіційне повідомлення від банку, а також містить псевдо екстрене повідомлення, яке вимагає від користувача негайних дій.
2) *Підробка логотипу та кольорової схеми* офіційної банківської організації з метою підсилення відчуття автентичності та враження надійності.
3) *Надання схожості адресі відправника* для більшого введення в оману користувача-жертву.
4) *Формування тексту повідомлення* в якому викладається основна проблема, що потребує невідкладного втручання користувача та є заклик відкрити прикріплений файл або перейти за посиланням для вирішення проблеми. Для більшої переконливості користувачу надається підроблена контактна інформація служби підтримки банку.
5) *Прикріплення шкідливих вкладень* таких як посилання на фішинговий сайт, або додавання небезпечного файлу, де останній фігурує в якості такого, що «розблокує» або «захистить» банківський акаунт жертви.

6) *Підписання листа* несправжнім підписом, який створює ілюзію комунікації з повноважним представником банківської організації.
7) *Підробка банківського веб-сайту та форми введення даних*, де жертві пропонується залишити особисту інформацію.

Такий сценарій фішингової атаки враховує психологічні та технічні аспекти, які допомагають атакуючим максимізувати ймовірність її успішної реалізації.

Отже, специфіку атак на різні сегменти потенційних жертв варто вивчати окремо, оскільки ці дві групи мають різні особливості та ризики. Так, у приватному сегменті фішери найчастіше апелюють до особистих емоційних реакцій та індивідуальних слабкостей запланованої жертви. Зловмисники використовують загальнодоступні джерела інформації, такі як соціальні мережі, для персоналізації атак та спроби зробити їх більш переконливими. При цьому, приватні користувачі, як правило, мають меншу кількість обов'язкових заходів безпеки, що робить їх більш вразливими.

У корпоративному сегменті атаки спрямовані на отримання конфіденційної чи комерційної інформації [19]. При цьому фішери використовують більш високий рівень *SE* методів та вивчають специфіку організаційних процесів потенційної жертви для створення адаптованих схем атак, зокрема вони часто вдаються до імітації внутрішніх комунікацій.

Отже, захист від більшості різновидів фішингових атак (див. Додатки А, Г) повинен бути інтегрованою частиною денної практики кожного користувача сучасних електронних комунікацій, незалежно від його функціонального статусу.

2 ВИЗНАЧЕННЯ ТИПОВИХ ЦІЛЕЙ РЕАЛІЗАЦІЇ ФІШИНГОВИХ АТАК І ДОСЛІДЖЕННЯ ОСНОВНИХ МЕХАНІЗМІВ ЇХ ЗДІЙСНЕННЯ

2.1 Визначення й узагальнення найбільш характерних цілей (ресурсів) при здійсненні фішингових атак у корпоративному та приватному сегментах користувачів сучасних інформаційних систем

Корпоративний сегмент відіграє критичну роль у глобальному економічному середовищі, а питання забезпечення потрібного рівня його безпеки є основною проблемою для сучасних підприємств. Фішингові атаки, що спрямовані на корпоративний сектор, мають великий і пролонгований у часі деструктивний потенціал: - втрати конфіденційності та приватності даних можуть призвести до значних фінансових збитків і репутаційної шкоди [19]. Тому в даному контексті важливо визначити найбільш характерні цілі та ресурси, які привертають увагу фішерів у кожному з визначених сегментів користувачів.

У широкому розумінні проблематики фішингу, атакуюча сторона має «інтерес» до різноманітних видів чутливої інформації. Основні категорії таких даних наведено в Додатку Д.

Таким чином, несанкціонований доступ до інформаційних ресурсів може викликати серйозні проблеми, стосовно конфіденційності, приватності та безпеки фізичних осіб, незалежно від нішевого сегмента атакованої інформаційної системи (ІС).

Інформація корпоративного сегменту може бути класифікована відповідно до рівня конфіденційності та чутливості даних:

1) Висока конфіденційність і чутливість:
   - облікові дані користувачів та авторизаційна інформація (логіни та паролі);
   - службові дані доступу до ключових систем персоналу компаній та установ (логіни та паролі до *CRM (Customer Relationship Management – система*

управління взаємодією з клієнтами, яка орієнтована на вдосконалення відносин між компанією та її клієнтами), ERP (Enterprise Resource Planning – це інтегрована система управління підприємством, яка об'єднує в собі різні функціональні області підприємства в єдину інформаційну систему), поштових серверів, *VPN* тощо);

- конфіденційна інформація про компанію (фінансові й технічні дані, стратегічні плани, комерційні угоди).

2) Середня конфіденційність і чутливість:

- дані клієнтів та контрагентів (імена, адреси, контактні дані);
- внутрішні документи та специфікації (проекти, плани, технічні специфікації);
- дані про проекти та дослідження компанії.

3) Низька конфіденційність і чутливість:

- дані персоналу (контактна інформація, соціальні страхування, податкові ідентифікаційні номери);
- інформація про внутрішні процеси та структуру організації (схеми роботи, технологічні процеси).

4) Мінімальна конфіденційність і чутливість:

- інформація про колишні оцінки або результати аудитів стану безпеки та розслідування інцидентів з ІБ (детектовані вразливості, прийняти заходи щодо усунення виявлених проблем тощо).

Ця класифікація надає загальну структуру для оцінки рівня конфіденційності та важливості інформації у корпоративному сегменті. Однак додатково слід зазначити, що конфіденційність деяких даних може бути посилена відповідними регуляторними вимогами або стандартами галузі.

У процесі здійснення фішингових атак, визначення цільового ресурсу жертви і обрання відповідного механізму для її ураження є критичним етапом, у загальному ланцюзі дій, який визначає «успішність» атаки.

У Таблиці 2.1 систематизовано сутність механізмів здійснення фішингових атак та їх наслідки у разі компрометації різних категорій корпоративних ресурсів.

Таблиця 2.1 – Механізми здійснення фішингових атак на ресурси приватного сегменту користувачів

Ресурс	Механізми здійснення атаки	Наслідки для обраної цілі
Корпоративні дані	Використання методів *SE* для отримання доступу до внутрішньої інформації	Загроза витоку стратегічної інформації, бізнес-планів, конфіденційних проєктів
	Експлуатація слабкостей у системах управління доступом	
	Використання фішингових електронних листів для отримання доступу до облікових даних співробітників організації	
Корпоративні облікові записи	Спуфінг електронних листів (*e-mail spoofing*) із метою отримання облікових даних користувачів	Ризик НСД до конфіденційних корпоративних ресурсів, можливість виведення з ладу бізнес-процесів
	Використання «маніпуляції з введенням» (*input manipulation*) для отримання доступу до облікових записів	
	Формування фішингових веб-сайтів для видачі інформації	
Інтелектуальна власність	Атаки на внутрішню мережу з метою оволодіння інтелектуальною власністю та конфіденційною інформацією	Загроза репутаційних ризиків та втрати інноваційного потенціалу й конкурентної переваги
	Використання прийомів *SE* для залучення співробітників до витоку чутливої інформації	

Продовження Таблиці 2.1 – Механізми здійснення фішингових атак на ресурси приватного сегменту користувачів

Ресурс	Механізми здійснення атаки	Наслідки для обраної цілі
Системи управління доступом	Експлуатація слабкостей в автентифікації та авторизації	Ризик НСД, можливість зміни прав доступу та порушення конфіденційності даних
	Реалізація атак типу *«men-in-the-middle»* для отримання доступу до систем управління доступом	

Отже, зв'язок між вибором цільового ресурсу та здійснюваним механізмом атаки підкреслює адаптивність методів впливу порушника на потенційну жертву, а також варіативність обраних способів та інструментів реалізації фішингу, відповідно до контексту та конкретних цілей атаки.

Приватний сегмент користувачів, також є предметом зростаючого інтересу для кіберзлочинців. Здійснення фішингових атак у цьому сегменті ІС може мати серйозні наслідки для особистої безпеки, фінансового стану та приватності користувачів.

Інформація корпоративного сегменту може бути класифікована відповідно до рівня її конфіденційності та чутливості (*тобто ступеню тяжкості можливих наслідків у разі її протиправного використання*) таким чином:

1) Висока конфіденційність і чутливість:
   - облікові дані для фінансових акаунтів (номери банківських карт, банківські реквізити);
   - паролі до фінансових та електронних акаунтів;
   - медична інформація, включаючи діагнози та лікування.
2) Середня конфіденційність та чутливість:
   - особиста інформація (імена, прізвища, адреси, контактні дані);
   - дані доступу до електронних платіжних систем (PayPal, Skrill тощо);

- інформація про соціальні мережі та інтернет-платформи.

3) Низька конфіденційність та чутливість:

- інформація про онлайн-сервіси та додатки (логіни та паролі);
- дані геолокації та переміщення особи;
- особисті фото та відеоматеріали.

4) Мінімальна конфіденційність та чутливість:

- сімейна інформація та дані про сімейний стан.

Дана класифікація є загальною та може варіюватися залежно від конкретних обставин, контексту та законодавчого фону для кожного конкретного випадку.

Наслідки від реалізації типових механізмів здійснення фішингу на ресурси жертв приватного сегменту ІС, формалізовані в Таблиці 2.2.

Таблиця 2.2 – Механізми й наслідки здійснення фішингових атак на інформаційні ресурси приватного сегменту

Ресурс	Механізми здійснення атаки	Наслідки для обраної цілі
Особисті дані	Фішингові атаки через електронну пошту *(phishing e-mails)*	Можливість ідентифікації та викрадення особистості, крадіжка особистої інформації для шахрайських цілей, можливість фінансових втрат та порушення конфіденційності.
	Використання методів *SE* для отримання паролів та особистої інформації	

Продовження Таблиці 2.2 – Механізми й наслідки здійснення фішингових атак на інформаційні ресурси приватного сегменту

Ресурс	Механізми здійснення атаки	Наслідки для обраної цілі
Банківські реквізити та картки	Фішингові атаки на банківські облікові записи та картки	Загроза НСД до конфіденційних банківських даних, фінансові втрати
	Використання підроблених веб-сайтів для отримання банківської інформації та конфіденційних даних	
	Спроби використання кредитних карток через прийоми *SE*	
Електронні облікові записи	Спроби отримання доступу до особистих облікових записів	Ризик втрати особистих даних, можливість НСД до особистої інформації та електронних облікових записів
	Реалізація атак через соціальні мережі та інші онлайн сервіси	
	Використання фішингових посилань для отримання паролів та інших особистих даних	
Особиста інформація в мережі	Витіснення особистої інформації через соціальні мережі	Потенційне порушення конфіденційності, можливість втрати контролю над особистою інформацією та репутаційні ризики
	Фішингові атаки через електронні повідомлення та месенджери	
	Використання методів *SE* для стимуляції витоку конфіденційної інформації через онлайн-форуми та спільноти	
Особистий комп'ютер та пристрої	Фішингові атаки через шкідливе ПЗ	Ризик втрати контролю над особистими даними, можливість крадіжки конфіденційних даних та можливість пошкодження особистих файлів та інформації.
	Спроби отримання доступу до особистої інформації через вразливості в ОС та програмах	
	Використання методів *SE* для отримання паролів	

Продовження Таблиці 2.2 – Механізми й наслідки здійснення фішингових атак на інформаційні ресурси приватного сегменту

Ресурс	Механізми здійснення атаки	Наслідки для обраної цілі
Особиста безпека	Атаки на особисті файли та паролі через недостатній рівень безпеки	Загроза безпеці особистих даних, можливість втрати конфіденційності та ризик використання даних для злочинних цілей
	Використання слабких паролів та повторне використання паролів	
	Спроби атак на вищеназвані ресурси через слабкість безпеки в особистих пристроях та програмах	

Зрозуміло, що спектр цільових ресурсів жертв приватного сегменту значно ширший, у порівнянні з корпоративним сегментом, що пов’язано з більш детальним розумінням з боку атакуючої сторони, психології користувачів, вивчення їхньої мережевої поведінки та формуванням ключових факторів, які впливають на вразливість до *SE* атак [1]. Отже, за результатами аналізу можна констатувати, що фішингові атаки в корпоративному й приватному сегментах ІС спрямовані на отримання різних видів інформації та використовують для цього різні вектори та сценарії.

Так, у корпоративному сегменті основною ціллю атак є отримання доступу до важливих функцій цільових систем та/чи конфіденційних (чутливих) даних. В якості цільових даних найчастіше виступають дані автентифікації, фінансова інформація та дані клієнтів. У приватному сегменті, фішери націлені на особисті дані, такі як імена, контактні дані та фінансова інформація. В обох випадках загальна стратегія та реалізовані механізми проведення атак на інформаційні ресурси жертви, варіюють в залежності від: - обсягів наявної інформації про жертву

та/чи цільову нішу [43]; - особливості використовуваних ними програмно-апаратних платформ (у тому числі засобів ІБ); - очікуваного "призового" фонду (тобто, монетизуючого еквіваленту).

2.2 Дослідження основних і типових сценаріїв та механізмів при реалізації фішингових атак на цільові ресурси жертви

Під терміном «сценарій фішингової атаки», будемо розуміти змістовну частину загального плану відповідної атаки, що визначає: – терміни заходів; – етапність (послідовність) дій; – залучені ресурси (фінансові, апаратні та людські); – механізми реалізації заходів на кожному з етапів; – параметри локалізації *(тобто, масштаби реалізації)* зусиль, які здійснюються для оволодіння бажаним (цільовим) інформаційним ресурсом потенційних жертв атаки. Цей план може включати в себе створення фішингових повідомлень, встановлення фішингових веб-сайтів, використання соціальної інженерії та інші маніпуляції, у залежності від умов реалізації атаки, з метою залучення жертв до виконання небезпечних дій [1].

Як правило, типовий сценарій фішингової атаки передбачає наступну послідовності етапів (процесів):

1) *Процес підготовки:*
- вибір цілі (цільової групи або конкретної організації) для атаки;
- збір інформації (здійснення досліджень про обрану ціль та/або користувачів).

2) *Створення фішингового засобу:*
- створення фішингового листа або повідомлення (імітація легітимності довіреної організації);
- використання методів *SE* з метою виклику емоційної реакції у жертви та підвищення ймовірності виконання вимог атакуючого.

3) *Розсилка фішингового засобу:*
- застосування масової розсилки (відправка фішингових листів або повідомлень через обраний спосіб розповсюдження).

4) *Виведення на фішинговий ресурс:*

- додавання фішингового посилання чи вкладення (лист може містити посилання на фішинговий сайт або вкладення з шкідливим вмістом);
- спонукання до дій (спроби переконати жертву виконати певні дії).

5) *Збір фінансової інформації й інших даних:*

- розробка фішингової форми (спосіб отримання доступу до інформаційного ресурсу жертви у разі введення нею даних);
- використання інших типів збору інформації (використання атаки для встановлення шкідливого ПЗ або спроби оволодіння іншими конфіденційними даними користувача-жертви).

6) *Використання Даних:*

- використання фінансової інформації (отримана в результаті атаки конфіденційна інформація може бути використана для отримання НСД до різних ресурсів);
- поширення шкідливого вмісту (використання здобутих даних для подальшого розповсюдження шкідливих елементів або атак на інших користувачів).

Під *механізмом здійснення* фішингової атаки розуміється сукупність технічних, соціальних та інформаційних засобів і методів, які використовуються для успішного виконання загального сценарію атакуючих дій. Ці механізми включають в себе технічні прийоми, такі як створення фішингових веб-сайтів, використання шкідливого ПЗ для збору інформації, а також соціально-інженерні (*SE*) методи для маніпулювання поведінкою об'єктів атаки та підтримки потрібного зовнішнього інформаційного фону запланованих заходів [44].

Механізми фішингових атак можуть варіюватися від використання застосовуваних програмних інструментів для автоматизації атак, до влучного вибору методів їх масштабування, адаптуючись до конкретної ситуації чи цільової аудиторії. Огляд основних сценаріїв атак, механізмів їх реалізації та інструментів здійснення, наведені в Таблиці 2.3.

Таблиця 2.3 – Узагальнення сценаріїв і механізмів при реалізації фішингу

Сценарій, притаманний конкретному виду фішингу	Тактичні дії атакуючого	Інструментарій
Електронна пошта	Створення фішингового повідомлення	Phishing kits
	Масова розсилка	Email spoofing tools
	Використання методів соціальної інженерії	Social engineering tactics
Веб-сайти	Створення фішингового веб-сайту	Phishing frameworks
	Розсилка фішингових посилань	URL shortening services
	Використання HTTPS	SSL certificates
Соціальні мережі	Створення фішингового профілю	Fake account creation tools
	Розповсюдження фішингових посилань	URL shortening services
	Використання актуальних тем	Trend analysis tools
Телефонія *(Vishing)*	Спам-дзвінки	Caller ID spoofing tools
	Використання голосових повідомлень	Pre-recorded voice messages
	Використання психологічного тиску	Social engineering tactics
SMS-фішинг *(Smishing)*	Відправка фішингових SMS	SMS spoofing services
	Використання мессенджерів	Messaging platforms
	Спілкування через чат	Social engineering tactics
Фішинг-клонування (Pharming)	Створення фішингового сайту	Phishing frameworks
		Fake domain registration services
		DNS spoofing tools
	Розсилка фішингових посилань	Email campaigns
		URL shortening services
		Social engineering tactics
	Використання HTTPS	SSL certificates
		Fake SSL certificates
	Використання маскировки домену	Domain name registrar manipulation
		Typosquatting techniques
	Використання соціальної інженерії	Social engineering tactics
		Gathering information from public sources

Отже, фішингові атаки використовують різноманітні сценарії та механізми, здебільшого поєднуючи технічні та соціальні аспекти для досягнення своїх цілей. При цьому *SE* атаки відіграють ключову роль, використовуючи психологічні та соціальні методи для ефективного маніпулювання свідомістю потенційних жертв. Переконливі фішингові листи, підроблені веб-сайти, багатоетапність заходів, моніторинг мережевої поведінки та інші методи стають все більш вдосконаленими та важко визначуваними.

Технічні аспекти фішингу включають у себе: - мультиплатформність комунікаційних платформ, що використовуються; - використання розподілених бот-систем; - гібридизація застосовуваного контенту; - експлуатація вразливостей ПЗ та/чи устаткування; - активація експлойтів; - впровадження шкідливого коду на апаратні платформи жертв та/чи використовуваних ними хмарних сервісів й онлайн служб (*тобто атака через скомпрометовану інстанцію*). А враховуючи активне залучення можливостей сучасних технологій, таких як AI та ML, фішингові атаки будуть ставати все більш автоматизованими та складними для виявлення.

3 УЗАГАЛЬНЕННЯ ОСНОВНИХ НАПРЯМІВ ТА СКЛАДОВИХ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ І ФОРМУВАННЯ РЕКОМЕНДАЦІЙ СТОСОВНО КОМПЛЕКСНОГО ЗАХИСТУ ВІД ДАНОГО ТИПУ ЗАГРОЗ

3.1 Узагальнення основних напрямів та складових (організаційних і технічних) протидії фішинговим атакам, включно з інтегрованими

Зважаючи на постійний ріст кількості і складності фішингових атак [43], захист від них стає важливим завданням у сфері ІБ. У цьому контексті слід приділити особливу увагу узагальненню основних напрямків протидії фішинговим атакам, включаючи специфіку їх організаційно-технічних складових.

Організаційна складова протидії фішинговим атакам передбачає комплекс організаційних заходів і політик безпеки, спрямованих на запобігання, виявлення та ефективну реакцію на спроби протиправного отримання чутливої інформації шляхом маніпулювання та використання методів *SE*. Вони включають у себе розробку і впровадження політик безпеки, навчання персоналу, моніторинг та аналіз вразливостей, а також впровадження контрольних механізмів для мінімізації ризиків фішингу.

Впровадження політики інформаційної безпеки (ПІБ) є однією з ключових складових протидії фішинговим атакам. Це включає в себе:

- розробку та впровадження документів, що регулюють правила та стандарти безпеки в організації;
- визначення відповідальності співробітників за дотримання ПІБ, а також механізмів контролю та аудиту її виконання;
- встановлення процедур реагування на інциденти та події, пов'язані з можливими фішинговими атаками.

Освітні програми з безпеки дозволяють підвищити обізнаність персоналу щодо потенційних загроз та навчити їх розпізнавати спроби здійснення фішингу. Освітні програми включають у себе:

- регулярні навчальні курси і тренінги персоналу, які надають інформацію щодо методів реалізації фішингу та способів захисту;
- проведення тестувань навичок персоналу щодо розпізнавання атак;
- розробка інформаційних матеріалів щодо правил ІБ;
- регулярні навчальні курси та тренінги для співробітників, які надають інформацію щодо методів реалізації фішингу та способів захисту від них;
- проведення тестувань навичок співробітників щодо розпізнавання атак;
- розробка інформаційних матеріалів щодо правил ІБ.

Процес *безперервного моніторингу та аналізу* потенційних загроз є важливим компонентом захисту від фішингових атак. Він включає в себе:

- виявлення потенційно небезпечних ситуацій та аналіз їх характеристик;
- використання спеціалізованих програм та інструментів для виявлення незвичайних або підозрілих активностей;
- системний аналіз звітів і лог-файлів щодо можливих інцидентів та подій.

Впровадження *систем виявлення та попередження* атак включає в себе:

- встановлення спеціалізованих програм та засобів для виявлення фішингових атак та недопущення витоку даних;
- моніторинг електронної пошти та веб-ресурсів на наявність підозрілих листів та сторінок;
- використання аналітичних систем для аналізу трафіку та виявлення аномалій.

Технічна складова протидії фішинговим атакам включає у себе використання спеціалізованих технологій, ПЗ та апаратних засобів для виявлення, блокування та мінімізації ризиків реалізації відповідних загроз ІБ. Технічні заходи охоплюють розробку та впровадження систем автоматизованого виявлення аномальних активностей, впровадження захисних механізмів, включаючи антивірусне та антиспамове ПЗ, а також встановлення та конфігурування брандмауерів й інших засобів мережевої безпеки (наприклад, мережевих пасток) з метою превентивного захисту організаційних систем і мереж від даного типу загроз.

Оскільки фішинг є специфічним типом *SE* атаки, він не базується тільки на апаратному чи ПЗ, а використовує комплексний підхід до реалізації маніпуляцій жертвами відповідної атаки. Саме тому пріоритетним напрямом протидії даному типу загроз є мінімізація залежності від впливу людського фактору. Зважаючи на це, умовно виділяють 3 рівні захисту від даного типу атак (див. Рисунок 3.1).

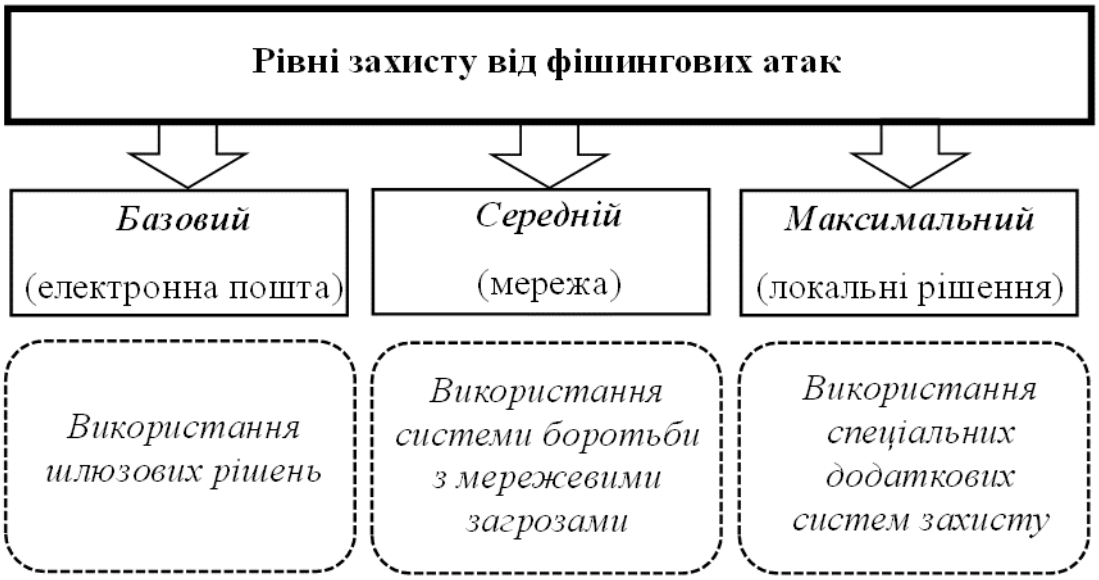

Рисунок 3.1 – Класифікація рівнів протидії фішингу

Базовий рівень розуміє собою захист електронної пошти користувача за допомогою відповідного шлюзу безпеки. Спочатку встановлюється фільтруючий шлюз для перевірки поштових листів із метою блокування фішингових повідомлень, перед їх надходженням безпосередньо до поштової скриньки. Сучасні шлюзові рішення здатні реалізовувати фільтрацію контенту на таких рівнях:

- *рівень доступу* – передбачає URL-фільтрацію, що дозволяє відрізняти посилання на легітимні сайти від фішингових та їх блокування;
- *рівень активного контенту* – розуміє собою застосування фільтрації HTML-коду з метою виявлення наявності шкідливого коду чи його частин;
- *комунікаційний рівень* – використовується у випадку, коли основною метою атакуючої сторони є залучення жертви на фішинговий сайт для інфікування його апаратного засобу. Незважаючи на велику кількість зловмисного ПЗ,

інтенсивність його взаємодії з центром керування досить незначна, тому на даному рівні фільтрації контенту здійснюється його блокування;

- *рівень передачі даних* – передбачається використання *Data Leak Prevention* (*DLP*) рішень, тобто засобів додаткового захисту, що передбачає контроль та блокування потенційних каналів витоку інформації.

Отже, базовий рівень розуміє собою використання тільки засобів захисту електронної пошти.

Середній етап направлений на здійснення додаткового захисту від фішингових атак на мережевому рівні. До мережевих засобів захисту належать: антивірусне ПЗ, мережеві брандмауери, *DNS*-фільтрація, корпоративні proxy (*наприклад, User Gate*), мережеві пастки (*Honeypot*) та вбудовані механізми виявлення фішингу електронних поштових сервісів тощо.

Максимальний рівень захисту передбачає одночасне застосування двох попередніх етапів, а також створення спеціальних платформ для навчання користувачів (характерний для корпоративного сегменту). Дозволяє створити ізольоване віртуальне середовище для перевірки потенційно шкідливих файлів.

Апаратно-програмні рішення щодо організаційної протидії фішингу повинні втілювати комплексний підхід до захисту від таких атак.

Серед *апаратних засобів* прийнято виділяти:

1) *Фільтри мережевого трафіку* – аналізують трафік, що проходить через мережу організації, та виявляють підозрілі або шкідливі пакети, крім того, фільтри можуть блокувати небажану або потенційно небезпечну активність. Найбільш поширеними серед них є *Cisco ASA Firewall, Palo Alto Networks* та *Fortinet FortiGate* [45-47].

2) *Захист хосту (або кінцевих точок)*, розуміє використання апаратних пристроїв, що можуть бути встановлені на самому комп'ютері або сервері та контролювати системні ресурси й процеси, щоб виявити незвичайну активність, яка може вказувати на спробу здійснення фішингу. Прикладом таких рішень є *Microsoft Defender* та *Symantec Endpoint Protection* [48,49].

Найпоширенішими *програмними компонентами* протидії фішингу є:

1) Антивірусне та антифішингове ПЗ – це продукти, призначені для виявлення й блокування шкідливого коду, включаючи той, який може бути вбудований у фішингові листи чи веб-сторінки. Прикладами таких засобів є *Norton AntiVirus, Extreme Security NextGen від* ZoneAlarm*, ESET Cyber Security, McAfee* [50] та *Trend Micro*.

2) Системи двофакторної автентифікації являють собою програмні рішення, які вимагають введення додаткового ідентифікатора. Прикладами найуспішніших реалізацій є такі системи, як *Google Authenticator, RSA SecurID* [51] та *Duo Security.*

3*) Системи виявлення та попередження вторгнень* – це програмні засоби, що аналізують та виявляють незвичайну або підозрілу активність у системі, а також надають можливість реагувати на потенційні загрози. Наприклад, *Splunk, IBM QRadar* [52], *ArcSight* тощо.

У контексті аналізу функціональних особливостей ПЗ слід звернути увагу на стандарти *SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail)* та *DMARC (Domain-based Message Authentication, Reporting and Conformance),* що являються критичними інструментами для ефективної боротьби саме з фішингом. Кожен із них пропонує свій оригінальний підхід до автентифікації та перевірки поштових листів, дозволяючи забезпечити найвищий рівень впевненості в автентичності та недоторканості електронної переписки.

Sender Policy Framework (SPF) – механізм автентифікації в електронній пошті, призначений для перевірки автентичності відправника листа, основною метою якого є запобігання відправленню листів, що підробляють доменні адреси [53]. *SPF* використовує *DNS*-записи для вказівки тих серверів, які мають право надсилати пошту від імені конкретного домену.

Основними особливостями та принципами *SPF* є:

- *DNS-записи SPF* – розуміє собою процес, при якому адміністратори домену можуть додавати спеціальні *DNS*-записи *SPF* до свого домену. Вони містять

інформацію про те, які поштові сервери мають право надсилати листи від імені цього домену (див. Рисунок 3.2).

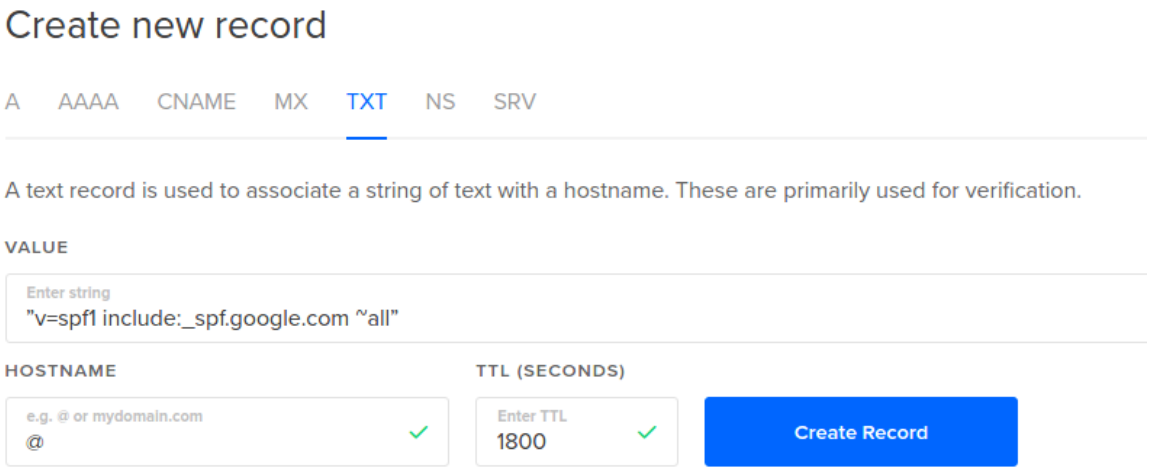

Рисунок 3.2 – Приклад типового *DNS*-запису *SPF*

У цьому прикладі *«v=spf1»* свідчить про те, що це *SPF*-запис, *«include:_spf.google.com»* вказує на те, що включається *SPF*-запис для домену *_spf.google.com*, а *«~all»* показує, що для всіх інших серверів дозволяється виконувати просту перевірку *(«soft fail»).*

- *Механізми SPF* використовуються для вказівки того, які сервери мають право надсилати пошту від імені домену. До основних механізмів слід віднести:
  1) *«include»:* вказує на включення *SPF*-запису іншого домену у поточний запис;
  2) *«a»:* перевірка того, чи відправник знаходиться в діапазоні IP-адрес, що відповідає домену;
  3) *«mx»:* перевірка того, чи відправник є *MX*-записом для домену;
  4) *«ip4 і ip6»:* вказує конкретний IPv4 або IPv6 адресу сервера.
- *Модифікатори SPF* – додаткові правила, які можуть застосовуватись до *SPF*-записів. Наприклад, *«all»* вказує, як поводитися з листами, які не пройшли перевірку *(hard fail),* або *«~all»* для простішого підходу *(soft fail).*

- *Механізми «ptr» і «exists»* – деякі додаткові механізми, які дозволяють використовувати *PTR-запити* (резервні *DNS*-запити) та перевіряти існування *DNS*-записів для підтвердження відправника.

SPF-перевірка виконується одержувачем при надходженні нового листа на його електронну пошту. Якщо сервер відправника не відповідає вимогам *SPF*, одержувач може прийняти рішення про обробку повідомлення (наприклад, відхилити або помістити в спам). Загалом, SPF є важливим інструментом для боротьби з фішинговими атаками, так як він дозволяє перевіряти правомірність відправників електронних листів і захищає від різновидів спаму, що має на меті імітацію відомих доменів (тобто підміну). Загалом, *SPF* є важливим інструментом для боротьби з фішинговими атаками, так як він дозволяє перевіряти правомірність відправників електронних листів і захищає від спаму, що має на меті імітацію відомих доменів.

DomainKeys Identified Mail (DKIM) – це стандарт автентифікації електронної пошти, що дозволяє здійснити перевірку листів, надісланих від певного домену, на легітимність. *DKIM* використовує криптографічний підхід для забезпечення автентичності та цілісності листів, що надсилаються від вказаних доменів [53].

Основними компонентами та принципами стандарту є:

- *Наявність приватного та публічного ключів*: для встановлення *DKIM*, власник домену створює пару ключів – приватний і публічний. Приватний ключ зберігається на сервері власника домену, а публічний розповсюджується через *DNS* записи домену.
- *Підписування повідомлення:* перед відправленням листа, поштовий сервер власника домену використовує приватний ключ для створення цифрового підпису, який додається до заголовка листа.
- *DNS-запис DKIM*: власник домену повинен додати спеціальний *DNS*-запис, який містить публічний ключ *DKIM*. Цей запис дозволяє одержувачам перевіряти цифровий підпис (див. Рисунок 3.3).

```
k1._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIGfMAOGCSqGSIb3DQE..."
```

Рисунок 3.3 – Приклад *DNS*-запису *DKIM*

У цьому прикладі *«k1._domainkey.example.com»* – це субдомен, який вказує на перший ключ *DKIM*, *«v=DKIM1»* – версія *DKIM*, *«k=rsa»* – тип криптографічного алгоритму (*RSA*), а *«p=»* – публічний ключ.

Для перевірки *DKIM-підпису* одержувач електронного повідомлення може використовувати публічний ключ з *DNS-запису.* У разі успішності перевірки вважається, що повідомлення не було підроблене після його підписання.

Загалом, *DKIM* дозволяє одержувачам впевнитися в автентичності листів, відправлених від імені конкретного домену. Це допомагає у боротьбі з фішингом, спамом та іншими видами атак, які використовують підроблені адреси електронної пошти.

Domain-based Message Authentication, Reporting and Conformance (DMARC) – є стандартом, що дозволяє власникам доменів встановлювати політики автентифікації для своєї електронної пошти та отримувати звіти про спроби надсилання листів від їхнього домену [53]. Головною метою *DMARC* є захист від спаму, фішингу та інших видів атак, що використовують підроблені адреси електронної пошти. Основні компоненти *DMARC* підтримують:

- *Політики автентифікації:* власник домену встановлює політику *DMARC*, яка описує, які заходи слід вживати для листів, що намагаються виглядати, як надіслані від імені його домену, але можуть бути підроблені. Існують 3 види політик аутентифікації:

  «None» – листи, що не проходять аутентифікацію й не блокуються, але отримувачі генерують звіти.

  «Quarantine» – листи, що не проходять аутентифікацію та помічаються як спам, але не блокуються.

«Reject» – листи, що не проходять аутентифікацію й блокуються.

Приклад *DMARC*-запису, що використовує політику блокування листів представлено на Рисунку 3.4.

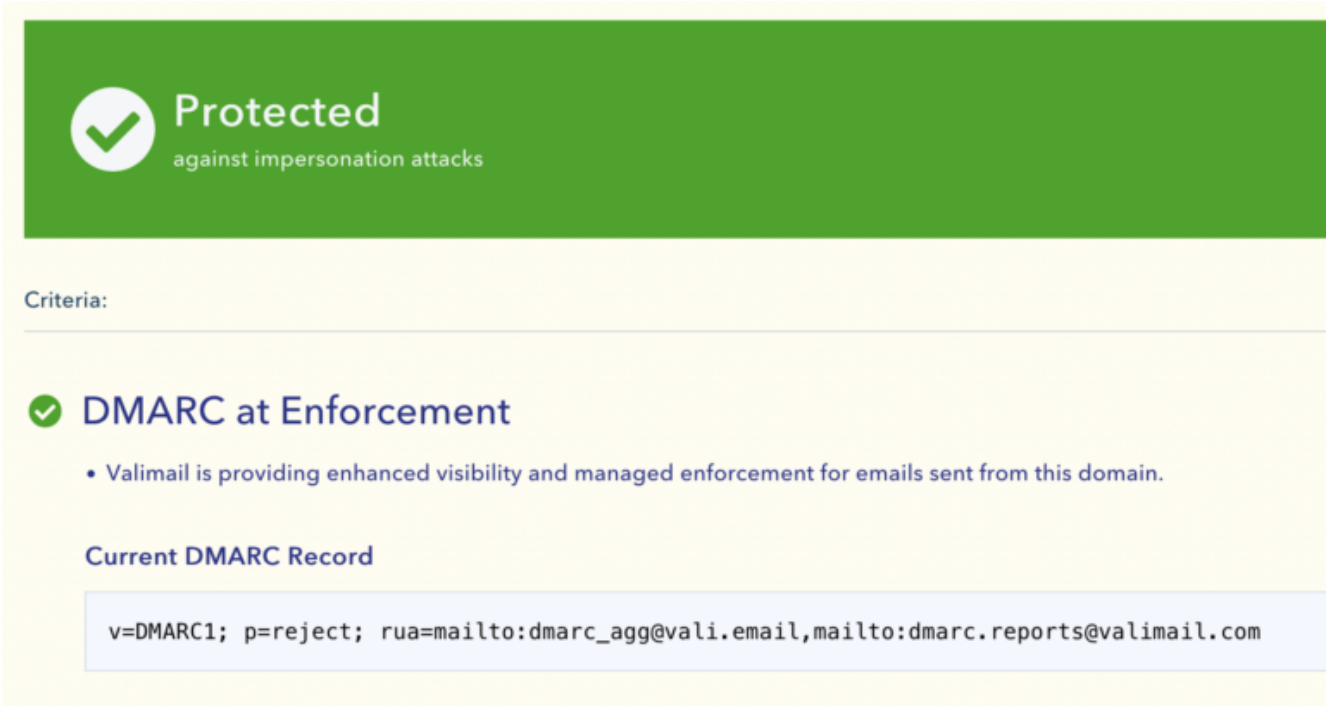

Рисунок 3.4 – Приклад *DMARC*-запису політики аутентифікації *«Reject»*

У цьому прикладі *«v=DMARC1»* вказує на версію *DMARC*, *«p=reject»* – на те, що небажані листи мають бути блоковані, а *«rua»* та *«ruf»* вказують на адреси для надсилання звітів.

- *SPF та DKIM аутентифікація*: стандарт передбачає використання інструментів *SPF* та *DKIM* для перевірки листів. Ті з них, що проходять автентифікацію, відповідають політиці *DMARC* вказаній у *DNS*.
- *Звіти DMARC*: *DMARC* дозволяє отримувачам надсилати звіти власникам домену, які містять інформацію про спроби надсилання листів від їхнього домену та результати автентифікації.

Отже, DMARC являється потужним інструментом для захисту від фішингу та інших атак, що використовують підроблені адреси електронної пошти. Робота DMARC у поєднанні з SPF та DKIM надає високий рівень захисту від шкідливих

листів, що виглядають як надіслані від власного домену. Порівняльна характеристика зазначених технологій наведена в Таблиці Е.1, Додатку Е.

Таким чином, сумісне використання *SPF*, *DKIM* та *DMARC* дозволяє досягти найвищого рівня захисту від фішингу та інших атак через електронну пошту, однак слід враховувати, що їх використання залежить від конкретних потреб та можливостей власника домену. Також, для уникнення випадків не доставлення листів, слід забезпечити правильне налаштування кожного з цих рішень.

Загалом ці технічні засоби спільно з організаційними дозволяють створити інтегрований підхід, який забезпечить максимально ефективний захист від фішингових атак. Це означає впровадження та оптимізацію технічних рішень у поєднанні з організаційними політиками та навчанням персоналу.

3.2 Огляд нормативно-правових особливостей щодо протидії фішингу

Однією з ключових стратегій у протидії фішинговим атакам є розробка та впровадження спеціалізованих нормативно-правових актів, які мають на меті встановити правові основи функціонування кіберпростору та гарантувати його безпеку (*в сенсі декларування правових норм*), а також надати механізми виявлення, блокування та розслідування фішингових атак.

Нормативно-правові особливості протидії фішинговим атакам відзначаються комплексністю та мультидисциплінарністю. Вони охоплюють такі сфери, як захист особистих даних, електронна комунікація, кібербезпека, інформаційні технології та правові аспекти електронної комерції. Важливим елементом у цьому випадку є визначення відповідальності за порушення цих норм та встановлення механізмів судового переслідування осіб, що реалізували атаку.

Серед основних аспектів правового регулювання фішингу слід виокремити такі:

1) *визначення та класифікація* (чітке формулювання того, що саме вважається фішинговою атакою та які її різновиди існують);
2) *встановлення відповідальності* (покарань і санкцій для осіб, винних у здійсненні фішингу);

3) *захист особистих даних* (регулювання щодо збору, зберігання та обробки особистих даних із метою запобігання їх неправомірному використанню);
4) *встановлення обов'язкової процедури відписки від фішингових повідомлень;*
5) *кібербезпека та превенція* (регулювання обов'язків організацій щодо захисту від фішингових атак та вживання активних заходів);
6) *міжнародне співробітництво* (визначення процедур та механізмів міжнародного співробітництва з метою виявлення, розкриття правопорушень, викликаних реалізацією фішингу, а також притягнення до відповідальності винних осіб).

Отже, можна зробити висновок — чим вищий рівень IT-розвитку країни, тим більш важливим та складнішим має бути законодавче регулювання протидії фішингу для забезпечення ефективної боротьби з цим видом кіберзлочинності.

В якості прикладу було розглянуто 5 нормативно-правових документів різних регіонів. Основними критеріями порівняння стали направленість протидії фішингу та відповідні процедури відписки від зловмисних повідомлень, а також притягнення до відповідальності за скоєне (див. Таблиця 3.1).

Таблиця 3.1 – Особливості нормативно-правових документів протидії фішингу

Назва закону	Країна/Регіон	Рік прийняття	Визначення фішингу	Покарання	Вимоги до відправників	Захист даних
CAN-SPAM Act	США	2003	Частково	Грошові штрафи	Так	Ні
GDPR	Європейський Союз	2018	Ні	Грошові штрафи	Так	Так
CASL	Канада	2010	Ні	Грошові штрафи	Так	Ні
Spam Act 2003	Австралія	2003	Ні	Грошові штрафи	Так	Ні
APPI	Японія	2005	Частково	Грошові штрафи	Так	Так

CAN-SPAM Act (*Controlling the Assault of Non-Solicited Pornography And Marketing Act)* [54], прийнятий в США 2003 року, встановлює обов'язкові вимоги

для комерційних електронних повідомлень, зокрема обов'язок надавати можливість відписатися від їх надсилання. Передбачає заборону використання оманливих заголовків та адрес електронної пошти, а також надає правовий статус вимогам до комерційних електронних повідомлень. Закон не має чіткого визначення фішингу та не включає конкретні положення щодо захисту особистих даних. Порушення *CAN-SPAM Act* може призвести до накладення адміністративних санкцій, грошових штрафів та цивільної відповідальності. Частковий захист від фішингу забезпечується тим, що даний закон фокусується на регулюванні комерційних електронних повідомлень та наданні можливості відписатися.

GDPR *(General Data Protection Regulation)* – закон прийнятий 2018 року Євросоюзом (ЄС), що регулює збір, обробку та збереження персональних даних громадян ЄС [55]. Встановлює вимоги до захисту особистих даних та обов'язок повідомляти про можливі порушення безпеки [56]. Порушення *GDPR* може призвести до накладення значних грошових штрафів, які можуть сягати до 20 млн євро або 4% річного обороту компанії-порушника (залежно від того, яке значення більше).

Закон не специфікує вимог до відправки комерційних електронних повідомлень, а також не має конкретних положень щодо процедур відписки від них, але встановлює важливі вимоги до захисту та обробки особистих даних.

CASL *(Canada's Anti-Spam Legislation)*, прийнятий у Канаді 2010 року, регулює надсилання комерційних електронних повідомлень, включаючи електронні листи, SMS та інші форми електронного спілкування. Закон визначає фішинг як відправку електронних повідомлень, що мають намір обману або надання оманливої інформації для отримання особистих даних або фінансових відомостей. *CASL* встановлює вимоги до одержування згоди перед надсиланням комерційних повідомлень. У Канаді за порушення *CASL* можуть бути накладені грошові штрафи, які можуть складати до 1 мільйона канадських доларів для

фізичних осіб та до 10 мільйонів канадських доларів для організацій. Закон передбачає процедуру відписки від надсилання комерційних повідомлень [57].

Spam Act 2003, прийнятий 2003 року в Австралії регулює надсилання небажаних електронних повідомлень, включаючи електронні листи та SMS і встановлює вимоги до надання чіткої інформації відправника [58]. Закон забезпечує можливість відписатися від надсилання небажаних електронних повідомлень, але не має конкретних положень щодо захисту особистих даних. У *Spam Act 2003* термін "фішинг" не має окремого визначення. У випадку порушення *Spam Act 2003* в Австралії будуть накладені грошові штрафи, які можуть складати до 2,2 мільйонів австралійських доларів для фізичних осіб та до 11 мільйонів австралійських доларів для організацій.

APPI (*Act on the Protection of Personal Information*) – закон, прийнятий 2005 року в Японії для регулювання збору, обробки та збереження персональних даних. Він встановлює вимоги до захисту особистих даних та передбачає адміністративні та цивільні санкції за порушення правил їх обробки [59]. Закон не специфікує вимоги до надсилання комерційних Е-повідомлень і не має конкретних положень щодо процедур відписки від них, але встановлює важливі вимоги, стосовно процедур захисту та обробки особистих даних.

Отже, нормативно-правові особливості протидії фішинговим атакам становлять складну та важливу частину у загальній стратегії забезпечення кібербезпеки в сучасному інформаційному суспільстві. Вони спрямовані на створення правових механізмів для виявлення, запобігання та припинення розгортання фішингових атак, а також надання санкцій за їх вчинення.

Необхідним є розуміння, що конкретного та всебічного законодавства, яке б регулювало всі правові норми з протидії фішингу, не існує. Однак притягнення до відповідальності за даний вид кіберзлочину стає можливим у випадку комплексного поєднання різних законів конкретної держави, де ступінь відповідальності варіюється в залежності від серйозності скоєного та специфіки

законодавства. В якості прикладу були розглянуті випадки притягнення до відповідальності за реалізацію фішингу, що притаманні для різних регіонів. Враховуючи особливості кожного законодавства, виконано аналіз видів порушень, передбачені санкції та ступінь важливості боротьби з даним типом атак у правовому просторі кожної з розглянутих країн. Таким чином, було виявлено спільні та відмінні аспекти притягнення до відповідальності за здійснення фішингових атак у різних правових системах. Аналізуючи ці аспекти, можна визначити потенційні напрямки удосконалення правових механізмів для більш ефективної протидії фішингу та забезпечення кібербезпеки в цілому (див. Таблиця 3.2).

Таблиця 3.2 – Приклади законодавчих норм покарання за реалізацію фішингу

Регіон	Рік	Випадок	Законодавство
Північна Америка, США	2011	Петеріс Сахуровс	Кримінальний кодекс США [60]
Європа	2017	Евальдас Рімасаускас	18 USC § 1343 (США) [61]
Азія, Республіка Корея	2019	Ким	Кримінальний кодекс Республіки Корея [62]
Південна Америка, Бразилія	2019	Ігор Єгорушкін	Закон про цифрову культуру (Бразилія) [63]
Австралія	2021	Allergy Pathway Pty Ltd & Anor	Закон про споживчий захист та конкуренцію (Австралія) [64]

Детальний розгляд кожного з випадків наведено в Таблиці Ж.1, Додатку Ж.

Отже, за результатами суміщення відомостей, щодо розглянутих випадків та застосовності існуючих правових норм, зроблено ряд висновків:

- приклади притягнення до відповідальності за реалізацію фішингових атак охоплюють різні регіони світу, що свідчить про глобальний характер цього кіберзлочину;

- кожному регіону притаманна наявність власного законодавства, за яким можуть бути притягнуті до відповідальності особи (або угруповання), які реалізували фішингову атаку;
- високий рівень кількості судових вироків свідчить про серйозність намірів з протидії фішингу у різних країнах;
- гарантування кібербезпеки та захисту від фішингу є важливим завданням для всіх країн незалежно від географічного розташування;
- існує прямий взаємозв'язок між рівнем розвитку ІТ-сфери в країні та комплексністю законодавчого регулювання боротьби з фішингом. Причинами цього є: технічний потенціал країн (розвинута ІТ-інфраструктура передбачає використання більш складних методів реалізації фішингу), великі обсяги Е-комунікацій, широкі сфери діяльності компаній та користувачів, високий показник інформаційної грамотності населення, накопичення досвіду боротьби з кіберзлочинністю.

В Україні нормативно-правове регулювання фішингу базується на комплексі законодавчих актів, які охоплюють правові, технічні та організаційні аспекти протидії цьому виду кіберзлочинності. Основні принципи нормативного регулювання фішингу в Україні включають визначення правового статусу фішингових атак, встановлення відповідальності за їх скоєння, а також розробку та впровадження заходів із профілактики та реагування на інциденти фішингу. Крім того, українське законодавство передбачає механізми міжнародного співробітництва та видачі осіб, замішаних у фішингових атаках, за межі країни.

Правове регулювання фішингу в Україні визначено рядом нормативно-правових актів, спрямованих на запобігання та протидію шахрайським діям в електронному середовищі. Основні норми включають [65-68]:

1) *Кримінальний кодекс України. Стаття 361. «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»* (визначається

кримінальна відповідальність за несанкціонований доступ, зміну, знищення або блокування роботи таких систем, комп'ютерів або мереж).

2) *Закон України "Про електронну комерцію"* (містить норми, що регулюють електронні транзакції та надання послуг в електронному середовищі, а також передбачає обов'язковість надання відомостей користувачам та захист їх персональних даних).
3) *Закон України "Про захист персональних даних"* (норми цього закону встановлюють правила обробки та захисту персональних даних громадян).
4) *Закон «Про основні засади забезпечення кібербезпеки України»* (визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки).

Останнім часом вітчизняне законодавство у сфері протидії фішингу зазнало декількох суттєвих нововведень. Наприклад, розпорядження Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв’язку (НКЕК) “Про впровадження системи фільтрації фішингових доменів” від 30.01.23 р. № 67/850, стало актом [69], що схвалив регламент роботи системи фільтрації фішингових доменів. Таким чином, була створена централізована система автоматичного блокування інтернет ресурсів на державному рівні.

Крім того, законопроект “Про внесення змін до Закону України “Про електронні комунікації” (*щодо протидії фішингу*) від 28.04.23 р. № 9250 [70] передбачає створення центрального органу виконавчої влади у сферах електронних комунікацій та радіочастотного спектру, який буде зобов’язаний не тільки розробити та затвердити правила протидії фішингу, але й встановити права та обов’язки постачальників служб *DNS*.

Загалом, нормативно-правова база свідчить про високий рівень усвідомлення важливості кібербезпеки та захисту інформаційних ресурсів в Україні. Проте, враховуючи стійке зростання кіберзлочинності, подальше вдосконалення законодавчого регулювання та впровадження сучасних технологічних рішень є невід'ємним етапом для забезпечення ефективної кібербезпеки в державі.

Отже, за результатами аналізу виділено такі нормативно-правові особливості протидії фішинговим атакам:

- *Специфічність законодавства* (кожна країна має власні особливості у правовому регулюванні боротьби з фішингом, адаптовані до специфічних потреб і технологічного розвитку).
- *Термінологія та визначення* (визначення та термінологія, які використовуються в законодавстві, можуть відрізнятися в різних країнах, що може впливати на сприйняття та застосування норм).
- *Ступінь важливості протидії фішингу* (у деяких країнах фішинг розглядається як значне правопорушення, що може мати серйозні правові наслідки, включаючи кримінальну відповідальність).
- *Захист конфіденційності та особистих даних* (багато країн приділяють велику увагу захисту особистих даних та конфіденційності).
- *Штрафи та покарання* (у різних країнах можуть бути встановлені різні рівні штрафів та покарань за фішинг).
- *Міжнародне співробітництво* (деякі країни активно співпрацюють з іншими в боротьбі з фішингом, в той час як інші можуть бути менш активними в цьому напрямі).
- *Шляхи протидії фішингу* (крім законодавчого регулювання, країни можуть вживати інші заходи для протидії фішингу, такі як освіта та популяризація безпеки в мережі Інтернет).

3.3 Рекомендації, стосовно комплексного захисту від фішингових атак та виключення передумов їх реалізації в корпоративному і приватному сегментах користувачів

Виходячи з вищеописаних організаційно-технічних напрямів протидії фішинговим атакам, сформовано рекомендації, щодо комплексного захисту від даного типу атак та виключення передумов їх реалізації для користувачів сучасних ІС у вигляді послідовного алгоритму дій (див. Таблиця 3.3).

Таблиця 3.3 – Інтегровані рекомендації щодо комплексної протидії фішингу

Кроки	Сегменти ІТ-ринку	
	Корпоративний	*Приватний*
1	*Розробка політики безпеки* (створення чіткої ПІБ, включно з правилами користування електронною поштою та доступом до корпоративних ресурсів)	*Освіта та навчання* (участь у тренінгах із ІБ та освітніх програмах, щодо виявлення та уникнення фішингу)
2	*Технічні заходи* (вдосконалення антивірусного і антифішингового ПЗ, включно з системами виявлення та виправлення вразливостей)	*Використання антивірусного ПЗ та засобів мережевого захисту* (встановлення й регулярне оновлення антивірусного ПЗ та параметрів їх налаштувань у відповідності до поточного стану загроз)
3	*Моніторинг та аналіз діяльності користувачів* (впровадження систем моніторингу для виявлення аномальної активності)	*Активна перевірка автентичності електронних листів*
4	*Використання систем фільтрації електронної пошти* (для блокування фішингових повідомлень)	*Активне управління паролями* (використання унікальних та «сильних» паролів для різних облікових записів)
5	*Захист інформації* (шифрування чутливого інформаційного ресурсу та обмеження доступу до нього, впровадження систем захисту від НСД)	*Регулярне оновлення ПЗ* (автоматичне оновлення ОС та ПЗ для усунення відомих вразливостей)
6	*Захист від SE* (навчання персоналу щодо виявлення та уникнення прийомів *SE*)	*Безпечне підключення до мережі* (використання надійних мереж та уникання непідтверджених Wi-Fi точок доступу)
7	*Проведення регулярних аудитів ІБ* (виявлення і усунення вразливостей ІС)	*Захист особистих даних* (уникання розголошення особистої інформації у відкритих джерелах і соціальних мережах)

Продовження Таблиці 3.3 – Інтегровані рекомендації щодо комплексної протидії фішингу

Кроки	Сегменти ІТ-ринку	
	Корпоративний	*Приватний*
8	*Співпраця та обмін інформацією* (участь у міжнародних ініціативах щодо обміну досвідом боротьби з фішингом)	*Регулярна перевірка фінансових операцій* на предмет підозрілої активності
9	*Розробка кризового плану* (регламентує перелік дій для реагування на фішингові інциденти)	*Активне дотримання рекомендацій і заходів ІБ*
10	*Постійне вдосконалення* діючих стратегій та заходів безпеки у відповідності до актуальних загроз реалізації фішингу	*Постійне вдосконалення* моделі мережевої поведінки та діючих заходів ІБ на основі навчання і досвіду

За результатами аналізу відомостей Таблиці 3.3 можна стверджувати, що у корпоративному сегменті користувачів, важливо акцентувати увагу на створенні та впровадженні ефективної ПІБ, вдосконаленні технічних засобів, моніторингу активності користувачів та сприянні міжнародному обміну інформацією. При цьому, регулярні аудити, кризові плани та навчання персоналу щодо виявлення *SE* атак, стають ключовими елементами гарантування безпеки організації.

У приватному сегменті, зокрема серед індивідуальних користувачів, самоосвіта та активна участь у процесі захисту є вирішальними чинниками. Використання антивірусного ПЗ, засобів міжмережевого екранування, уважне ставлення до електронних листів та практика особистих безпечних звичок у мережі, можуть стати головними чинниками ефективного захисту чутливих даних.

В цілому, обидва сегменти користувачів мають спільну потребу в постійному контролі (аудиті) і вдосконаленні чинних заходів безпеки, оновленні стратегій захисту (*ПІБ для умов корпоративного сегменту*) відповідно до нових загроз та сприянні культурі кібербезпеки. Реалізація цих заходів сприятиме створенню безпечного інформаційного простору та відповідності високим стандартам кібербезпеки в обох сегментах користувачів.

4 ПРОГНОЗНА ОЦІНКА ТЕНДЕНЦІЙ ПОДАЛЬШОГО РОЗВИТКУ МЕТОДІВ ЗДІЙСНЕННЯ ТА ЦІЛЕЙ ФІШИНГОВИХ АТАК

4.1 Прогнозний огляд подальшого розвитку методів здійснення фішингових атак

У контексті стрімкого технологічного прогресу та сталого збільшення кількості фішингових атак [43], проведено прогнозний огляд подальшого розвитку методів їх здійснення, спрямований на спробу розуміння можливих процесів подальшої еволюції фішингу. Він передбачає розгляд різних аспектів, включаючи *технічні інновації*, *соціальні тенденції* та *впровадження нових заходів безпеки*.

Аналіз сутності попередніх етапів еволюції фішингу (Розділ 1) та триваючих процесів сучасного інформаційного суспільства [1] з великою часткою впевненості дозволяє стверджувати, що розвиток технічних інновацій буде зумовлювати значне збільшення кількості фішингу. Серед основних чинників такої тенденції варто виділити такі:

1) Стрімкий розвиток AI та ML – використання методів машинного навчання й штучного інтелекту буде каталізатором вдосконалення способів аналізу впливу фішерів на цільову аудиторію. Самонавчальні алгоритми можуть аналізувати великі обсяги даних про потенційних жертв для створення більш ефективних схем фішингу, тому використання нейронних мереж для аналізу психологічних особливостей різних груп [43] користувачів, може сприяти більш ефективному емоційному маніпулюванню та підвищити ймовірність «успішності» атак.

2) Використання блокчейн технологій – розуміє собою збільшення способів ускладнення виявлення та відслідковування фінансових операцій, що пов'язані з фішингом, через можливість використання анонімних криптовалют *(*наприклад*, Monero* або *Zcash)*.

3) *Поширення Інтернету речей (IoT)* – зі збільшенням кількості пристроїв, підключених до Інтернет, включаючи розумні побутові прилади та інші IoT-

продукти, значно зростає кількість умовних «точок входу» для фішингових атак (*так званих фішингових послуг*). Тобто, атакуючі можуть використовувати вразливості в системах IoT для отримання доступу до особистої інформації користувачів та розширення масштабів атак.

4) Зростання масштабів використання хмарних сервісів – зумовлює збільшення випадків імітації платформ хмарних сервісів (найбільш популярними серед яких є Google Drive, Dropbox та Microsoft Azure) для створення фішингових веб-сайтів із метою розповсюдження шкідливих файлів через спільні теки.

5) Зростання масового аутсорсінгу – тенденція сучасності, яка розуміє собою збільшення кількості «зовнішніх» користувачів із правом доступу до чутливої інформації та/чи процесів, що в свою чергу є передумовою до значного розширення поля цільових жертв фішингу.

6) *Розвиток віртуальної реальності (VR)* – впровадження цих технологій може призвести до появи нових способів розповсюдження й методів реалізації фішингових атак. Наприклад, атакуючі зможуть застосовувати прийоми *SE* в середовищі віртуальної реальності з метою отримання НСД до конфіденційної інформації користувачів та/чи масштабування своїх дій до потрібного рівня впливу на різні цільові групи.

7) *Розвиток квантових обчислень* – відкриває можливість розшифрування криптографічних даних, що робить фішингові атаки більш ефективними та збільшує рівень їх складності.

8) Підвищення рівня доступності Інтернету – однозначно приведе до зростання кількості користувачів мережі, що аж ніяк не пов’язано з рівнем їх фахових компетенцій та комп’ютерної грамотності. Це зумовить збільшення кількість жертв широкомасштабних фішингових атак. До прикладу, компанія «Starlink» надає послуги понад 1 млн активних клієнтів у 60-ти країнах та забезпечує неконтрольований з боку національних інформаційних інтеграторів, доступ до відповідного контенту, одночасно в багатьох регіонах світу [71].

9) Об'єднання фішингу з іншими кібератаками – забезпечує підвищення показника кількості фішингу, як способу для отримання початкового доступу в інших різновидах атак. Більше того, можлива комбінація фішингу з принципово новими способами атак *(наприклад, використання технологій VR та/чи доповненої реальності для охоплення нових цільових груп*) відповідно до зростання новітніх технічних інновацій.

Серед соціальних аспектів прогнозованого зростання кількості фішингу слід виділити наступні:

1) Масова цифровізація та зниження показника загальної компетентності – сценарій, при якому збільшується кількість цифрових сервісів і додатків, але прослідковується зростання показника «цифрової» некомпетентності серед користувачів. Дана тенденція стала особливо актуальною з початком пандемії COVID-19, коли відбулось посилення дистанційної взаємодії й розвиток інфраструктури віддаленої роботи для корпоративного сегменту користувачів. Свідченням чого є статистика найбільш розповсюджених імітованих брендів під час реалізації фішингових атак (див. Рисунок 4.1) [72].

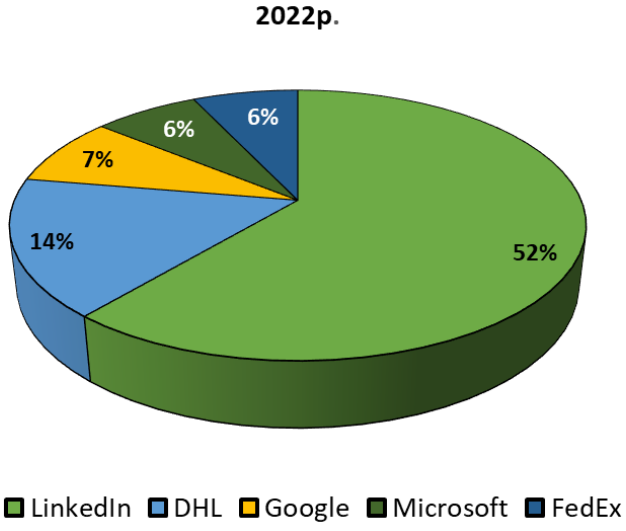

Рисунок 4.1 – Найбільш імітовані бренди у фішингових атаках (станом на 2022р.)

2) Значне розповсюдження соціальних мереж – зумовлює факт найчастішого використання цих мереж, як засобу поширення фішингу. Так, кількість

користувачів соціальних мереж становила 4,59 мільярдів станом на 2022р., а за прогнозними оцінками їх чисельність зросте до 5,85 мільярдів до 2027 року [73]. Атакуючі можуть використовувати інформацію з профілів більшої кількості користувачів для персоналізації атак та збільшення вірогідності їх успіху.

3) Підвищення ролі освіти у взаємодії з цифровим середовищем – важливий аспект прогнозування зміни методів та сценаріїв фішингу, адже увага користувача сучасних ІТ-систем все більше зосереджена на захисті від загроз ІБ, включно з фішингом, у порівнянні з попередніми історичними етапами його розвитку. Свідченням чого є регулярне проведення тренінгів, курсів, розповсюдження статей тощо, які мають на меті інформування користувача ІТ-технологій щодо розпізнавання й уникнення фішингу.

4) Впровадження нових нормативно-правових актів і законів щодо запобіганню фішингу – один із ключових аспектів боротьби з даними атаками, що дозволяє на державному та міждержавному рівнях регламентувати правила функціонування сучасних ІТ-систем. Саме завдяки таким рішенням ефективність атак (як превентивного засобу) значною мірою знижується.

Наступний вагомий аспект в прогнозуванні еволюції фішингових атак, це впровадження нових заходів безпеки, серед яких слід виділити:

1) Автоматизація систем захисту – впровадження методів AI та ML для швидкого виявлення й блокування механізмів поширення фішингу. Завдяки алгоритмам аналізу поведінки користувачів та виявлення аномалій, можливе ефективне реагування на нові загрози [74].

2) Інтеграція біометричних технологій – впровадження біометрії в системи автентифікації, а також їх більша розповсюдженість, може суттєво підвищити рівень безпеки та ускладнити можливість НСД через фішингові атаки.

4.2 Узагальнення тенденцій у виборі цілей (ресурсів) фішингових атак

Узагальнюючи останні тенденції у виборі бажаних цілей (*ресурсів*) для здійснення фішингових атак з урахуванням регіональних, галузевих та

користувальницьких особливостей потенційних жертв, слід розглядати водночас кілька ключових аспектів. При цьому слід враховувати широкий спектр факторів, які впливають на стратегії фішерів, від геополітичних та культурних особливостей до їх можливостей, стосовно використання сучасних технологій.

Серед загальних тенденцій слід визначити:

1) Використання методів *SE* (збільшення застосування соціальної інженерії для отримання доступу до конфіденційної інформації через маніпулювання).

2) Застосування розширених технологій (*таких як, AI та ML для створення більш складних та персоналізованих, наприклад, за групами, атак*).

3) Атаки з використанням вірусів та розширень (*збільшення кількості атак, спрямованих на застосування шкідливого ПЗ для зараження систем та отримання НСД до чутливих даних й процесів*).

Серед регіональних особливостей варто виділити такі:

1) *Геополітична спрямованість атак:* - прослідковується зростання фішингу, спрямованого на певні регіони через геополітичні аспекти або регіональні конфлікти. Так, станом на 2022 р. НБУ звітував про виявлення більше 4500 фішингових доменів, однак уже в першому кварталі 2023р. було викрито більше 11000 таких ресурсів [75].

2) *Правові середовища:* - прослідковується адаптивність до регулятивних умов конкретного регіону/країни для визначення цілей і способів обходу заходів безпеки, встановлених на державному рівні.

3) *Культурна відмінності:* - адаптація атак до конкретних культурних особливостей регіону для збільшення їх ефективності (див. Додаток Г).

Поміж основних галузевих особливостей, що зумовлюють характер вибору цілей для фішингу, слід зазначити тенденцію з*більшення фокусу атак на конкретні сектори*, такі як: критична інфраструктура, енергетика й інші стратегічно важливі

напрями. Так, найбільш атакованою галуззю станом на 2022р. стала виробнича із показником 58%, хоча її питома частка зменшилась із 61% в порівнянні з 2021р. (див. Рисунок 4.2) [41].

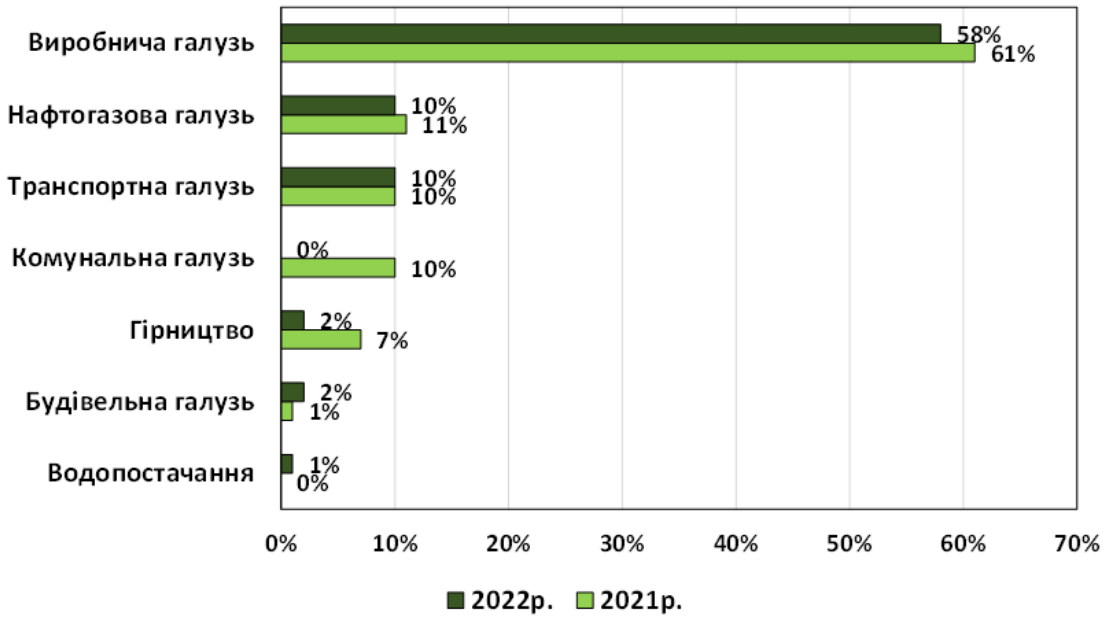

Рисунок 4.2 – Галузі з найбільшою кількістю порушень ІБ (2021-2022рр.)

Причому, аналізуючи вектори початкового доступу в індустріях, спрямований фішінг становив 38% випадків, зокрема фішинг через вкладення – 22%, фішинг через посилання – 14%, а фішинг як сервіс у 2% інцидентів.

До користувальницьких *(корпоративних і приватних)* особливостей вибору ресурсів для атак слід віднесено такі тенденції:

1) *Персоналізація фішингу* – розуміє собою застосування глибокого вивчення та аналітики для персоналізованих фішингових атак враховуючи індивідуальні особливості потенційних жертв (у тому числі через розвиток AI та ML).

2) *Залучення спільнот та соцмереж* – тенденція використання інформації, отриманої з відкритих джерел на цих платформах, з метою легітимації та оптимізації атак.

3) *Зростання кількості атак платформ дистанційної взаємодії* – розуміє собою фішингові атаки на користувачів, що дистанційно працюють/навчаються.

Таким чином, можна зробити висновок, що в контексті останніх тенденцій у виборі цілей для фішингових атак присутня тенденція персоналізації, тобто вони забезпечують композитний облік географічних, галузевих та індивідуальних аспектів. Залучення методів *SE*, технологій штучного інтелекту та аналітики робить їх все більш ефективними та складними для своєчасного виявлення. Крім того, високий рівень геополітичної спрямованості і фокусування атак на певні (критичні) галузі, свідчить про ретельне попереднє планування майбутніх заходів та перманентне вдосконалення використовуваних методів здійснення фішингових атак. Таким чином, ефективні заходи протидії майбутнім фішинговим атакам, повинні бути орієнтовані на всебічне врахування особливостей різних сфер діяльності, регіональних відмінностей та індивідуальності привабливих для атакуючого цільових груп.

ВИСНОВКИ

1) Існує безліч способів реалізації фішингу, кожному з яких притаманне використання різних методів, інструментів й умов здійснення, що варіюються в залежності від цілей та специфічних сценаріїв розгортання таких атак.

2) Використання технологій мультифакторної автентифікації [5] є головним чинником поточного історичного розвитку фішингу. Використання різних автентифікаційних факторів ускладнює підміну ідентифікаційних даних та знижує успішність фішингу, роблячи його менш ефективним.

3) Способи здійснення фішингових атак постійно розвиваються та адаптуються, але першість електронної пошти, як платформи для їх розповсюдження зберігається на всіх етапах розвитку фішингу. Крім того існують тенденції до збільшення сегментації цільових груп потенційних жертв та використання прийомів *SE* протягом усіх етапів розвитку фішингу.

4) На перших двох етапах розвитку IT-сфери (Розділ 1) питома частка фішингу була практично нульовою, однак починаючи з так званого *«Emany Інтернету»* (1990-2000 рр.) досліджуваний тип атак починає активно розвиватися. Внаслідок еволюційних змін, доля фішингу набуває рекордних значень протягом останніх двох років [41]. Перш за все ця тенденція обумовлена активним впровадженням технологій AI та IoT [19,20]. Крім того, в цей період фіксувались рекордні показники кількості фішингових веб-сайтів, що пов’язано з підвищенням складності їх виявлення через появу нових технологій імітації легітимності веб-сторінок на цьому часовому проміжку [40, 41].

5) Протягом останніх десятиріч спостерігалася помітна еволюція фішингу, яка супроводжувалася зміною пріоритетних цілей для кіберзлочинців. Так, галузі фінансового сектору та банківської діяльності залишаються основним об'єктом атак, проте станом на 2020-2022рр. спостерігається зниження їх відносної частоти у порівнянні з іншими галузями [37-39]. Водночас, сектори електронної комерції та

поштових сервісів залишаються стійкими до фішингу впродовж усього історичного розвитку фішингу.

6) Специфіка реалізації фішингу на регіональні ресурси й потенційна вигода атакуючого залежать від локальних особливостей кожного регіону, де виняткове місце посідає технологічний стек кожного з них. Прослідковується збільшення кількості фішингу в регіонах, свідченням чого є ріст показника випадків порушення безпеки в Азії та Європі на 5 та 4 відсоткових пункти відповідно, порівняно з 2021 роком [41].

7) Зважаючи на специфіку фішингових атак для приватного й корпоративного сегментів користувачів, слід зазначити важливі відмінності: - у корпоративному секторі ключовим є комплексний захист, котрий регламентується шляхом впровадження відповідних ПІБ; - приватні користувачі мають справу з інакшою динамікою та різнорідністю загроз, а їхні можливості захисту зазвичай більш обмежені в порівнянні з корпоративним сегментом. Таким чином, специфіку атак на різні сегменти потенційних жертв варто вивчати окремо, оскільки ці дві групи мають суттєво різні особливості та ризики.

8) Зв'язок між вибором цільового ресурсу та здійснюваним механізмом атаки підкреслює адаптивність методів впливу порушника на потенційну жертву, а також варіативність обраних способів та інструментів реалізації фішингу, відповідно до контексту та конкретних цілей атаки. При чому, атаки в корпоративному й приватному сегментах ІС спрямовані на отримання різних видів інформації та використовують різні вектори впливу і сценарії. Хоча в обох випадках загальна стратегія та реалізовані механізми проведення фішингу на інформаційні ресурси жертви варіюються в залежності від: - обсягів наявної інформації про жертву та/чи цільову нішу [43]; - особливості використовуваних ними програмно-апаратних платформ (у тому числі засобів ІБ); - очікуваного "призового" фонду (тобто, монетизуючого еквіваленту).

9) Використання комплексного підходу щодо захисту від фішингових атак, передбачає впровадження та оптимізацію технічних рішень (апаратно-програмних

компонентів), які поділяються за рівнем захисту (базовий, середній, максимальний), у поєднанні з організаційними (ПІБ, освітні програми, системи виявлення та попередження, процес безперервного моніторингу та аналізу).

10) У процесі порівняння субстантивної частини стандартів *SPF*, *DKIM* та *DMARC* (Розділ 3) встановлено, що їх сумісне використання дозволяє досягти найвищого рівня захисту від фішингу та інших атак через електронну пошту, однак слід враховувати, що існує можливість не доставлення листів, тому слід забезпечити правильне налаштування кожного з використовуваних захисних рішень (див. Додаток Е або Розділ 3.1).

11) Складність законодавчого регулювання протидії фішингу (спрямованого на створення правових механізмів для виявлення, запобігання та припинення розгортання фішингових атак, а також надання санкцій за їх вчинення) прямо пропорційна рівню ІТ-розвитку країни. Притягнення до відповідальності за даний вид кіберзлочину стає можливим у випадку комплексного поєднання різних законів конкретної держави, де ступінь відповідальності варіюється в залежності від серйозності скоєного та специфіки законодавства. Вітчизняне законодавство передбачає механізми міжнародного співробітництва та видачі осіб, задіяних у фішингових атаках, за межі країни та постійно оновлюється й адаптується під історичні реалії сьогодення [69,70].

12) В якості основних рекомендацій із захисту від фішингу в корпоративному сегменті користувачів ІС є: - створення та впровадження ефективної ПІБ, вдосконаленні технічних засобів, моніторингу активності користувачів та сприянні міжнародному обміну інформацією. У приватному сегменті вирішальними чинниками є самоосвіта та активна участь у процесі захисту. В цілому, обидва сегменти користувачів мають спільну потребу в постійному контролі (аудиті) і вдосконаленні чинних заходів безпеки, оновленні стратегій захисту (*ПІБ для умов корпоративного сегменту*) відповідно до нових загроз.

13) Основними чинниками прогнозного *збільшення* кількості фішингу є такі аспекти:

- технічні інновації (*зростання масштабів використання хмарних сервісів, стрімкий розвиток AI та ML, використання блокчейн технологій, поширення IoT, зростання масового аутсорсінгу, розвиток технологій віртуальної реальності (VR), розвиток квантових обчислень, підвищення рівня доступності Інтернету, об'єднання фішингу з іншими кібератаками*);

- соціальні тенденції *(масова цифровізація та зниження показника загальної компетентності, значне розповсюдження соціальних мереж, підвищення ролі освіти у взаємодії з цифровим середовищем, впровадження нових нормативно-правових актів і законів щодо запобіганню фішингу)*;

- впровадження нових технологій й заходів безпеки *(автоматизація систем захисту, інтеграція біометричних технологій)*.

14) У контексті останніх тенденцій у виборі цілей для фішингових атак [43, 44], присутня тенденція персоналізації, тобто атакуюча сторона намагається забезпечити комплексне врахування географічних, галузевих і індивідуальних аспектів потенційних цілей. Високий рівень геополітичної спрямованості і фокусування атак на критичні сектори і галузі суспільства, свідчить про ретельне попереднє планування майбутніх заходів та перманентне вдосконалення використовуваних методів здійснення фішингових атак [44]. Отже, ефективні заходи з протидії майбутнім фішинговим атакам повинні бути орієнтовані на всебічне врахування: - особливостей різних сфер діяльності, регіональних відмінностей та ступеню потенційної привабливості *(інакше, пролонгованості одержуваного призового фонду)* виділених цільових груп.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лєсная Ю. Є., Малахов С. В. Узагальнення основних передумов реалізації фішингових атак. *System analysis and intelligent systems for management: The 17th International scientific and practical conference*, м. Анкара, 3–5 трав. 2023 р. Анкара, 2023. С. 453–482. URL: http://surl.li/nqwkf.
2. Сербін В., Лєсная Ю., Малахов С. Особливості інтеграції систем захисту від НСД у склад інформаційних систем різного призначення. *Scientific goals and purposes is XXI century*, м. Сієтл, 19–20 січ. 2022 р. Сієтл, 2022. С. 796–803. URL: https://doi.org/10.51582/interconf.19-20.01.2022.088.
3. Мелкозьорова О., Лєсная Ю., Малахов С. Особливості забезпечення захисту від НСД в сучасних інформаційних системах. *InterConf (97)*, м. Мельбурн, 6–8 січ. 2022 р. Мельбурн, 2022. С. 506–511. URL: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18428.
4. Лєсная Ю., Малахов С. Бліц-огляд проблематики захисту від несанкціонованих дій на прикладах характерних реалізацій. *Problems of the development of modern science. Proceedings of the XXXIV International Scientific and Practical Conference*, м. Мадрид, 30 серп. 2020 р. – 2 верес. 2022 р. Мадрид, 2022. С. 326–329. URL: https://isg-konf.com/problems-of-the-development-of-modern-science/
5. Давиденко А., Висоцька О., Потенко О. Захист інформаційних систем на основі аналізу графічних зображень. *Науково-практична конференція «кібербезпека енергетики»*, м. Київ, 31 трав. 2023 р. Київ, 2023. С. 74–77. URL: http://surl.li/nizlt
6. Соціальний інжиніринг, як фактор реалізації інсайдерських загроз / К. Погоріла та ін. *Scientific Collection «InterConf», (111)*, м. Бостон, 6–8 черв. 2022 р. Бостон, 2022. С. 494–501. URL:

https://archive.interconf.center/index.php/conference-proceeding/issue/view/6-8.06.2022

7. Лєсная Ю., Погоріла К., Малахов С. Аналіз структури інсайдерських загроз в IT-сфері та основні складові з протидії цим загрозам. *Діджиталізація науки як виклик сьогодення* : матеріали II Міжнар. наук. конф., м. Одеса, 17 груд. 2021 р. Вінниця, 2021. С. 56–59. URL: https://ojs.ukrlogos.in.ua/index.php/liga/article/view/17555
8. Колованова Є., Малахов С., Чорна Т. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. *The 27th International scientific and practical conference "Trends of young scientists regarding the development of science"*, м. Едмонтон, 11–14 лип. 2023 р. Едмонтон, 2023. С. 194–201. URL: http://surl.li/njpsw
9. 10 Best XDR Solutions: Extended Detection & Response Service. *Software Testing Help*. URL: https://www.softwaretestinghelp.com/xdr-security-solutions/ (дата звернення: 15.08.2023).
10. Rekouche K. Early phishing. 2011. 9 p. (Preprint. arXiv:1106.4692). URL: https://arxiv.org/ftp/arxiv/papers/1106/1106.4692.pdf
11. Dunham K. Mydoom miseries. *Information security journal*. 2004. V. 13 (4). URL: https://www.tandfonline.com/doi/abs/10.1201/1086/44640.13.4.20040901/83726.1
12. Badra M., El-Sawda S., Hajjeh I. Phishing attacks and solutions. *3rd international ICST conference on mobile multimedia communications.*, 1 May 2010. URL: https://eudl.eu/pdf/10.4108/ICST.MOBIMEDIA2007.1899
13. Wong J. C. Snapchat leaks employee data after CEO falls for phishing scam. *The guardian*. 2016. URL: https://www.theguardian.com/technology/2016/feb/29/snapchat-leaks-employee-data-ceo-scam-email

14. A mitigation and prevention model for social engineering based phishing attacks on facebook / A. Jamil et al. *2018 IEEE international conference on big data*. 2018. P. 5040–5048. URL: http://surl.li/nsjiu
15. Mahanta K., Maringanti H. B. Social engineering attacks and countermeasures. *Perspectives on ethical hacking and penetration testing.igi global*. 2023. C. 307–337. URL: https://www.igi-global.com/chapter/social-engineering-attacks-and-countermeasures/330270
16. Social engineering attacks during the COVID-19 pandemic - SN computer science. *SpringerLink*. URL: https://link.springer.com/article/10.1007/s42979-020-00443-1 (дата звернення: 11.08.2023).
17. Богданова Є., Чорна Т., Малахов С. Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека*, м. Харків. Харків, 2022. С. 35–40. URL: https://periodicals.karazin.ua/cscs/article/view/21039/19745
18. Лєсная Ю., Малахов С. Узагальнення основних передумов реалізації фішингових атак. *Proceedings of the XVII International Scientific and Practical Conference*, м. Анкара, 2–5 трав. 2023 р. Анкара, 2023. С. 453–457. URL: https://isg-konf.com/system-analysis-and-intelligent-systems-for-management/
19. Чорна Т., Лєсная Ю., Малахов С. Інсайд, фішинг та SE-атаки як складові проблематики доксінгу. *Proceedings of the XXII International Scientific and Practical Conference*, м. Хельсінки, 6–9 черв. 2023 р. Хельсінки, 2023. С. 506–510. URL: https://isg-konf.com/modern-theories-and-improvement-of-world-methods
20. Гайкова В., Малахов С. Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*. 2021. Т. 1, № 1. С. 50–59. URL: https://doi.org/10.26565/2519-2310-2021-1-04

21. APWG. APWG Phishing Activity Report: December 2004. APWG, 2004. URL: http://surl.li/mjfsm
22. APWG. APWG Phishing Activity Report: December 2005. APWG, 2005. URL: http://surl.li/mjfto
23. APWG. APWG Phishing Activity Report: December 2006. APWG, 2006. URL: http://surl.li/mjftz
24. APWG. APWG Phishing Activity Report: December 2007. APWG, 2007. URL: http://surl.li/mjful
25. APWG. APWG Phishing Activity Report: December 2008. APWG, 2008. URL: http://surl.li/mhbib
26. APWG. APWG eCrime Research Report: Q4 2009. APWG, 2009. URL: http://surl.li/mhdux
27. APWG. APWG eCrime Research Report: H2 2010. APWG, 2010. URL: http://surl.li/mhdww
28. APWG. APWG eCrime Research Report: H2 2011. APWG, 2011. URL: http://surl.li/mhdyf
29. APWG. APWG eCrime Research Report: Q4 2012. APWG, 2012. URL: http://surl.li/mhdzf
30. APWG. APWG eCrime Research Report: Q4 2013. APWG, 2013. URL: http://surl.li/mhdzz
31. APWG. APWG eCrime Research Report: Q4 2014. APWG, 2014. URL: http://surl.li/mheal
32. APWG. APWG eCrime Research Report: Q4 2015. APWG, 2015. URL: http://surl.li/mhebp
33. APWG. APWG eCrime Research Report: Q4 2016. APWG, 2016. URL: http://surl.li/mhecj
34. APWG. APWG eCrime Research Report: Q4 2017. APWG, 2017. URL: http://surl.li/mhedm

35. APWG. APWG eCrime Research Report: Q4 2018. APWG, 2018. URL: http://surl.li/mheeh
36. APWG. APWG eCrime Research Report: Q4 2019. APWG, 2019. URL: http://surl.li/mhegl
37. APWG. APWG eCrime Research Report: Q4 2020. APWG, 2020. URL: http://surl.li/mhegy
38. APWG. APWG eCrime Research Report: Q4 2021. APWG, 2021. URL: http://surl.li/mhehu
39. APWG. APWG eCrime Research Report: Q4 2022. APWG, 2022. URL: http://surl.li/mheir
40. IBM. Security X-Force Threat Intelligence Index 2022 Full Report. IBM, 2022. URL: http://surl.li/gpjrv
41. IBM. Security X-Force Threat Intelligence Index 2023 Full Report. IBM, 2023. URL: https://www.ibm.com/downloads/cas/DB4GL8YM
42. Гайкова В., Малахов С. Суть аналогий кибербуллинга и эксперимента Милгрэма. *Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realta domestiche: збірник наукових праць «ΛΌГОΣ»* : матеріали I Міжнар. наук.-практ. конф., м. Болонья, 14 трав. 2021 р. Болонья, 2021. С. 123–128. URL: https://ojs.ukrlogos.in.ua/index.php/logos/article/view/12571
43. Лєсная Ю., Малахов С., Мелкозьорова О. Аналіз регіональних та галузевих відмінностей при реалізації фішингових атак. *Proceedings of the VIII international scientific and practical conference*, м. Будапешт, 7–10 листоп. 2023 р. Будапешт, 2023. С. 289–297. URL: https://isg-konf.com/wp-content/uploads/2023/11/DISTANCE-LEARNING-IN-UNIVERSITIES-AND-MODERN-PROBLEMS.pdf
44. Лєсная Ю., Малахов С., Гальцева І. Визначення основних цілей фішингових атак та узагальнення механізмів їх здійснення. *Proceedings of the XI International Scientific and Practical Conference*, м. Хельсінки, 28 листоп. – 1 груд. 2023 р. Хельсінки, 2023. С. 440–446. URL: https://isg-konf.com/wp-

content/uploads/2023/11/INTEGRATION-OF-SCIENCE-AS-A-MECHANISM-OF-EFFECTIVE-DEVELOPMENT.pdf

45. Saqib I. Comparison of different firewalls performance in a virtual for cloud data center. *Journal of advancement in computing*. 2023. Vol. 1. P. 21–28. URL: https://journalsriuf.com/index.php/JAC/article/view/49/59
46. Putri H. A., Djibran N., Tulloh R. Implementation of next-generation firewalls to protect applications from malware attacks. *Jurnal indonesia sosial teknologi*. 2023. Vol. 4, no. 11. P. 1961–1970. URL: https://jist.publikasiindonesia.id/index.php/jist/article/view/797/1393
47. Analisa herangkat fortinet sebagai firewall untuk memblokir aplikasi sosial media dan platform streaming saat jam kerja. / B. A. Prasetia et al. *Jurnal Ilmu Komputer, Teknik dan Multimedia*. 2023. Vol. 1, no. 3. P. 496–504. URL: https://www.journal.mediapublikasi.id/index.php/Biner/article/view/3062/1667
48. Dieterich A. Evaluation of persistence methods used by malware on microsoft windows systems. *Proceedings of the 9th international conference on information systems security and privacy (ICISSP 2023)*. 2023. P. 552–559. URL: https://www.scitepress.org/Papers/2023/117102/117102.pdf
49. IC-SECURE: intelligent system for assisting security experts in generating playbooks for automated incident response / R. Kremer et al. 2023. 15 p. (Preprint. arXiv:2311.03825). URL: https://arxiv.org/pdf/2311.03825.pdf
50. Nachaat M. Current trends in AI and ML for cybersecurity: a state-of-the-art survey. *Cogent engineering*. 2023. URL: https://doi.org/10.1080/23311916.2023.2272358
51. ZITA: zero-interaction two-factor authentication using contact traces and in-band proximity verification / N. Ghose et al. *IEEE transactions on mobile computing*. 2023. URL: https://cse.unl.edu/~nghose/pubs/journal/GHOSE_TMC_2023-main.pdf

52. Comparative analysis of IBM Qradar and wazuh for security information and event management / D. Šuškalo et al. *34th DAAAM international symposium on intelligent manufacturing and* automation, Vienna, 2023. URL: https://www.daaam.info/Downloads/Pdfs/proceedings/proceedings_2023/working_papers/dpn34056_a_3_Moric.pdf
53. Ashiq M. I. Measurement and security implications of {DMARC} reporting. *The 32nd USENIX security symposium*, Anaheim, 9–11 August 2023. Anaheim, 2023. P. 4123–4137. URL: https://www.usenix.org/system/files/usenixsecurity23-ashiq.pdf
54. United States Congress. S.877 - 108th Congress (2003-2004): CAN-SPAM Act of 2003. [Електронний ресурс]. – Вашингтон, D.C.: Конгрес США. URL: https://www.congress.gov/bill/108th-congress/senate-bill/877 (дата звернення: 09.09.2023).
55. Колованова Є., Малахов С., Чорна Т. Передумови та основні складови з протидії доксінгу персональних даних. *The 27th International scientific and practical conference "Trends of young scientists regarding the development of science"*, м. Едмонтон, 11–14 лип. 2023 р. Едмонтон, 2023. С. 194. URL: https://isg-konf.com/wp-content/uploads/2023/07/TRENDS-OF-YOUNG-SCIENTISTS-REGARDING-THE-DEVELOPMENT-OF-SCIENCE.pdf
56. General data protection regulation (GDPR) – official legal text. *General Data Protection Regulation (GDPR)*. URL: https://gdpr-info.eu (дата звернення: 24.10.2023).
57. Electronic Commerce Protection Act (CASL) : Канадський уряд. Закон про електронні документи [9]. – Оттава: Парламент Канади, 2014. – 32 с. URL: https://laws-lois.justice.gc.ca/PDF/E-1.6.pdf (дата звернення: 24.10.2023).
58. Electronic Transactions Amendment (2016 Measures No. 1) Act 2016 : Австралійський уряд. Закон про захист персональної інформації [129]. – Кентербері: Парламент Австралії, 203. – 45 с. URL:

https://www.legislation.gov.au/Details/C2016C00614 (дата звернення: 24.10.2023).

59. Act on the Protection of Personal Information (Japan) : Кабінет міністрів Японії. Закон про захист персональних інформаційних даних [57]. – Токіо: Кабінет міністрів Японії, 2003. – 20 с. URL: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (дата звернення: 24.10.2023).
60. United States Code. Title 18 - Crimes and Criminal Procedure. – Вашингтон, D.C.: Правова інформаційна служба США. URL: http://surl.li/mvhqq (дата звернення: 24.10.2023).
61. Правова інформаційна служба Республіки Корея. Закон про персональні дані. – Сеул: Правова інформаційна служба Республіки Корея, 2018. URL: https://www.law.go.kr/LSW/lsInfoP.do?efYd=20181016&lsiSeq=204772#0000 (дата звернення: 24.10.2023).
62. Lei nº 13.709 de 14/08/2018 : Lei від 14.08.2018 р. № 13709 : станом на 26 жовт. 2022 р. *Diário oficial da união*. 2018. 15 серп. URL: https://legis.senado.leg.br/norma/27457334 (дата звернення: 24.10.2023).
63. Balanço trimestral individual a 31 de Março de 2010 : Balanço (extracto) № 10/2010. *Diário da república II série*. 2010. 6 трав. URL: https://dre.pt/application/conteudo/3326377 (дата звернення: 24.10.2023).
64. Competition and Consumer Act 2010: Парламент Австралії. Закон про споживчий захист та конкуренцію Австралії. – Кентербері: Парламент Австралії, 2010. URL: https://www.legislation.gov.au/Details/C2016C00900 (дата звернення: 28.09.2023).
65. Кримінальний кодекс України: Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. URL:

https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-361.htm (дата звернення: 01.11.2023).

66. Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII : станом на 19 листоп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 01.11.2023).
67. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.11.2023).
68. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.11.2023).
69. Про впровадження системи фільтрації фішингових доменів: Розпорядження НЦУ від 30.01.23 р. № 67/850. URL: https://nkrzi.gov.ua/images/news/11/2580/67_30012023.pdf (дата звернення: 05.11.2023).
70. Про внесення змін до Закону України “Про електронні комунікації” (щодо протидії фішингу): проект закону України від 28.04.23 р. № 9250. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1779936 (дата звернення: 06.11.2023).
71. Starlink internet: coverage & availability map | broadbandnow. *BroadbandNow*. URL: https://broadbandnow.com/starlink (дата звернення: 06.11.2023).
72. The latest phishing statistics (updated october 2023) | AAG IT support. *AAG IT Services*. URL: https://aag-it.com/the-latest-phishing-statistics/ (дата звернення: 06.11.2023).
73. Statista - the statistics portal. *Statista*. URL: https://www.statista.com/markets/424/topic/540/social-media-user-generated-content/#statistic1 (дата звернення: 06.11.2023).

74. Михайленко Д., Чорна Т., Малахов С. Використання можливостей AI при реалізації Static та Dynamic Honeypot для покращення параметрів захисту інформаційних ресурсів. *Використання можливостей AI при реалізації Static та Dynamic Honeypot для покращення параметрів захисту інформаційних ресурсів*: матеріали IV Міжнар. наук. конф., м. Суми, 7 жовт. 2022 р. Суми, 2022. С. 54–57.
75. Ukrinform. В Україні запустили проєкт із протидії кібершахрайству у фінансовому секторі. *Укрінформ - актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-economy/3670375-v-ukraini-zapustili-proekt-iz-protidii-kibersahrajstvu-u-finansovomu-sektori.html (дата звернення: 11.11.2023).

ДОДАТОК А

Огляд специфіки відомих способів реалізації фішингових атак

Вважається, що існує велика кількість способів реалізації фішингу, найпоширенішим із яких є *електронна пошта* – у цьому виді фішингу, зловмисник намагається виглядати, як надійне джерело, надсилаючи листи (електронні повідомлення), що імітують легітимні комунікації від відомих компаній, установ чи осіб. Ціллю таких листів може бути отримання доступу до конфіденційних даних або введення шкідливого програмного забезпечення (ПЗ). Крім того, такі повідомлення можуть бути налаштовані для конкретної жертви й слугувати інструментом спрямованого фішингу (тобто, таргетованої атаки).

Спосіб реалізації атаки через *приховане (підроблене) посилання* має кілька цілей, серед яких: обхід фільтрів та виявлення, маскування справжнього призначення, збільшення ймовірності кліків. Зловмисники можуть користуватися прийомами маскування посилання *(використання адреси, схожої на легітимну)*, застосовувати скорочувачі посилань (Bitly, TinyURL тощо), використовувати HTML теги та редіректи, а також приховувати гіперпосилання за іншими об’єктами.

Фішинг-клонування використовується для оманливого здійснення аутентифікації та отримання конфіденційних даних, таких як імена користувачів, паролі, банківські дані тощо. У цьому методі атакуючий створює точну копію легітимного веб-сайту або веб-сторінки, копіюючи її URL посилання та функціонал, із метою збору та використання даних жертви. Окрім вищеописаного, існують фішинг-клони, які намагаються перехопити сесійні файли або дані авторизації, щоб мати доступ до облікового запису користувача.

Голосовий фішинг (Voice Phishing) являється методом атаки, при якому інструментом отримання чутливої інформації виступають телефонні дзвінки. Цей спосіб характеризується імітацією легітимних джерел, коли фішер видає себе за працівника відомої організації, використовуючи при цьому симуляцію голосу або

аутентичні аудіо-записи. Для голосового фішингу характерне використання багатьох прийомів соціального інжинірингу, таких як маніпуляції, створення почуття невідкладності та важливості для жертви, вимагання, шантаж тощо. Особливістю цього способу розповсюдження атак є раптовість, адже пильність обраної жертви значно знижується в порівнянні, наприклад, з фішингом електронною поштою.

Фішинг за допомогою спливаючих повідомлень (Pop-up Phishing) – це метод, при якому атакуючий використовує спливаючі вікна на веб-сторінках для виведення оманливого повідомлення з метою шахрайства чи отримання конфіденційних даних. Для успішної реалізації методу повідомленням надається легітимний вигляд за допомогою імітації логотипів і графіки офіційних організацій. Фішери мають на меті спровокувати почуття невідкладності, вимагаючи при цьому швидкої взаємодії з попередньо розробленими посиланнями.

Фішинг за допомогою хибних URL-адрес (Misleading URLs) реалізується введенням потенційної жертви в оману шляхом використання маніпулятивних веб-адрес. Характерним для цього способу є маскування адреси URL, використання доменної схожості на легітимну, створення підробленого піддомену, використання подібних до справжніх параметрів й анкорних текстів, а також користування скорочувачами посилань.

Фішинг з використанням зображень (Image Phishing) – це метод атаки, при якому атакуючий використовує зображення замість тексту, щоб виглядати менш підозріло та обійти фільтри спаму. Для цього способу характерне використання оманливих імітаційних графічних елементів чи підписів, подібних до автентичної символіки офіційних організацій, внаслідок чого для жертви створюється ілюзія надійності. Зображення можуть приховувати вміст шкідливого тексту чи посилань задля уникнення їх виявлення антивірусними програмами. Особливість фішингу з використанням зображень полягає у складності його візуального виявлення.

SMS фішинг (SMS Phishing або Smishing) – це метод атаки, в якому атакуючий використовує текстові повідомлення (SMS) для обману та отримання

конфіденційної інформації від потенційних жертв. Основними характеристиками цього способу розповсюдження фішингових атак є: імітація легітимності відправника (наприклад, банку, поштового оператора чи іншої довіреної особи), використання підроблених номерів, виклик у жертви відчуття невідкладності через опис критичних ситуацій, вимагання даних. Зазвичай такі SMS-повідомлення змушують користувача-жертву діяти швидко, бо опираються на факт терміновості й важливості. Ефективність такого способу розповсюдження фішингу зумовлена тим, що із розвитком цифрових технологій істотно зріс попит на користування мобільними девайсами.

Фішинг заміною контенту (Content Spoofing) – це метод атаки, при якому атакуючий намагається підробити або змінити вміст веб-сторінки, щоб видати його за автентичний та обманути користувача. Для цього способу характерне не тільки використання імітованих елементів сайту й заміна її вмісту, але й маскування ідентичності, тобто атакуючий робить зміни в HTML-коді сторінки, аби вона виглядала як оригінальна. Більше того, для цього методу фішингу характерне використання захищеного з'єднання HTTPS, що значно підвищує довіру жертви.

Фішинг через сайти з рекламою (Advertise-Based Phishing) – спосіб реалізації атаки, при якому атакуючий використовує рекламу, щоб привернути увагу потенційних жертв та ввести їх у оману. Характерний сценарій методу передбачає створення зловмисником фальшивого рекламного сайту, при цьому використовуючи рекламні мережі в якості платформи його розповсюдження. Характерним для цього способу є використання *SE* методів.

Фішинг з підміною веб-сайту (Website Spoofing) – це метод атаки, при якому атакуючий створює фальшивий сайт, який імітує оригінальний, із метою отримання чутливої інформації. Зазвичай зловмисник створює вигляд аутентичного веб-сайту, який може бути ідентичний оригіналу або мати схожий вигляд, використовуючи для цього відповідні елементи дизайну (логотипи, кольорову схему, шрифти тощо). Отже, такий спосіб фішингу може бути особливо небезпечним через фактор

переконливості, оскільки він ґрунтується на поєднанні багатьох прийомів та великої кількості інструментів.

ДОДАТОК Б

Відмінності основних етапів розвитку фішингових атак та особливості еволюції MFA

Ключовими характеристиками «початкового етапу» еволюції фішингу є:

1) *Підробка електронних листів* – в основі початкового етапу розвитку фішингових атак було використання електронної пошти. Фішери відправляли листи, які містили фальшиві повідомлення від імені відомих організацій, таких як банки, електронні платіжні системи чи поштові служби.
2) *Підробка символіки легітимних організацій* – зловмисники прагнули підробити офіційний вигляд імейлів відомих організацій. Для цього імітувались легітимні деталі листів, такі як структура, логотипи тощо.
3) *Вимоги до інформації* – характерним сценарієм для здійснення початкових фішингових атак був запит особистих даних користувача, тобто паролів, номерів кредитних карток, адреси та інших конфіденційних відомостей.
4) *Використання заголовків із загрозами* – фішери використовували характерні заголовки листів, що створювали враження важливості та терміновості, наприклад, «*Ваш обліковий запис заблоковано. Оновіть пароль негайно».*
5) *Відсутність відповідних заходів захисту* – для початкового етапу 1990-х років, на початку інтернет-ери, характерною рисою був брак налагоджених сучасних систем захисту від кіберзагроз, що спричинило успішну реалізацію фішингових атак через недостатню обізнаність користувачів.
6) *Використання масових розсилок* із метою отримання великої кількості потенційних жертв. Успішність таких атак була невеликою, адже вона залежала від кількості відкритих зловмисних повідомлень користувачами.

Головними характеристиками 2-го етапу, 2000-х років є:

1) *Використання фальшивих веб-сайтів* – підробка легітимних ресурсів, а саме, створення фішерами фальшивих веб-сайтів, із метою збору більшої

кількості інформації про потенційних жертв майбутніх атак. Використовувались нелегітимні веб-сторінки банківських організацій, онлайн-магазинів, соціальних мереж тощо.

2) *Підвищення реалістичності фальшивих веб-сайтів* – зловмисники почали приділяти більше уваги деталям фальшивих веб-сайтів для більшої схожості з легітимними, таким як логотипи, шрифти, кольори тощо.
3) *Використання імітаційних логін-сторінок* – фішери створювали сторінки, які виглядали як логін-сторінки популярних сервісів, наприклад, електронної пошти або соціальних мереж. Жертвам пропонували ввести свої облікові дані, які потім використовувалися для злочинних цілей.
4) *Використання SE* – зловмисники почали використовувати прийоми соціальної інженерії для появи у жертви почуттів важливості й терміновості, такими як емоційні маніпуляції, вигадування переконливих історій тощо.
5) *Розповсюдження через сповіщення* – хоча розсилка фішингових повідомлень по електронній пошті продовжила залишатися популярним методом реалізації атак, проте для цього періоду був характерним початок активного використання інших способів сповіщення, таких як сповіщення в браузерах або повідомлення в месенджерах.
6) *Збільшення видів фішингу* – розвиток інших видів фішингу, включно з фішингом через: електронну пошту, SMS, веб-сайти-підробки, фішинг через соціальні мережі та інші платформи.
7) *Поява антивірусів та заходів захисту* – поява та розвиток заходів захисту від кібератак. Наприклад, поява антивірусних програм, файрволів та інших інструментів для виявлення та блокування фішингових атак.

Основними характеристиками 3-го етапу (соціальних мереж) є:

1) *Зловживання довірою в соціальних мережах* – так як комунікації між користувачами в соціальних мережах базуються на довірі, фішери почали використовувати для підроблення профілі реальних користувачів та

створювати фальшиві облікові записи, щоб виглядати як друзі або колеги потенційної жертви. Таким чином, зловмисники могли заволодіти конфіденційною інформацією жертви, втягнувши її у свою схему.

2) *Розповсюдження фішингу через приватні повідомлення* – фішери почали відправляти фальшиві повідомлення через особисті або приватні чати, виглядаючи при цьому як реальні друзі чи колеги. Наприклад, запит на відправку грошей або на отримання конфіденційної інформації користувача-жертви.
3) *Розповсюдження фейкових розіграшів та акцій* – фішери використовували відомі назви брендів, компаній або відомості про акції, щоб залучити користувачів до підроблених конкурсів або розіграшів, які вимагали введення особистої інформації.
4) *Розповсюдження фішингових посилань* – зловмисники почали залишати фішингові посилання в коментарях, повідомленнях, сповіщеннях або інших публікаціях в соціальних мережах, що вводило в оману користувачів. Таким чином, жертви могли бути перенаправлені на фальшиві веб-сторінки, що виглядали, як легітимні ресурси.
5) *Використання інших видів соціальної інженерії* – вдосконалення методів соціальної інженерії призвело до збільшення випадків фішингу. Зловмисники використовували методи маніпулювання емоціями та почуттями користувачів, аби залучити їх до вигідних для фішерів дій.
6) *Використання груп і спільнот* – фішери активно використовували групи та спільноти соціальних мережах, де користувачі діляться інформацією та спілкуються. Це дозволяло їм знаходити більше потенційних жертв і в подальшому впливати на них.
7) *Збільшення кількості таргетованих атак* – під час цього історичного етапу розвитку фішингових атак вбачається тенденція популяризації таргетованих атак, що використовують персональні дані користувачів, наприклад,

інформацію з їх профілів у соціальних мережах, із метою більшої переконливості з боку жертви.

Ключовими характеристиками 4-го етапу, «спрямованого фішингу» є:

1) *Підвищення персоналізації* – характеризується використанням спрямованих фішингових атак. Зловмисники здійснювали попередній аналіз жертв, збираючи персональну інформацію з відкритих джерел, таких як соціальні мережі, професійні профілі, блоги тощо.
2) *Точність вибору жертв(и)* – фішери обирали конкретних осіб чи групи осіб як цільову аудиторію, при цьому могли знати імена, посади чи інші деталі про потенційних жертв, отже, атака вдосконалювалась та ставала більш переконливою.
3) *Використання персоналізованих повідомлень* – фішери створювали повідомлення з персональними елементами, які виглядали як такі, що адресовані конкретному користувачу.
4) *Використання методів соціальної інженерії* – етап спрямованого фішингу також характеризується широким використанням методів соціальної інженерії для маніпулювання жертвами шляхом створення переконливих сценаріїв.
5) *Використання імітаційних джерел* – спрямовані атаки могли включати використання імен або адрес електронної пошти, які схожі на офіційні. Фішери могли підробити імена керівників компаній, колег або партнерів для збільшення довіри.
6) *Використання таргетованих тем* – характеризує вибір тем атак фішерів, що співпадали з інтересами та діяльністю жертви, наприклад, використання актуальних новин, або тем, що стосуються конкретної галузі діяльності.
7) *Цілі спрямованих фішингових атак* – такі атаки можуть мати різні цілі, включаючи крадіжку конфіденційної інформації, фінансові шахрайства, розповсюдження шкідливого програмного забезпечення або отримання доступу до облікових записів.

8) *Важливість захисту* – внаслідок зростання спрямованих атак, компанії та організації почали приділяти більше уваги освіті співробітників щодо виявлення підозрілих повідомлень, розширювати заходи захисту та використовувати більш сильні методи аутентифікації.

Ключовими характеристиками 5-го етапу «*BEC*» є:

1) *Зростання складності BEC атак* – перші прояви BEC припадають на середину 2000-х років. На той час атаки полягали в тому, що зловмисники видавали себе керівниками компаній та вимагали від фінансового відділу провести фінансові транзакції або перекази коштів. У 2010-ті роки BEC-атаки стали більш складними та цілеспрямованими. Фішери детальніше вивчали цільові компанії, збираючи інформацію про керівників та фінансовий персонал, а також використовували соціальну інженерію для підвищення успішності атак.
2) *Маніпулювання партнерами та постачальниками* – фішери розширили спектр атак, виходячи з вимог до партнерів та постачальників організацій. Виступаючи в ролі керівників або інших осіб у ланцюгу постачання, зловмисники вимагали платежі або надсилали оманливі платіжні доручення.
3) *Використання компрометованих облікових записів* – зловмисники використовували скомпрометовані облікові записи для того, щоб виглядати як легітимні співробітники або керівники компаній. Для цього могли бути використані підроблені електронні адреси чи зламані електронні скриньки.
4) *Розповсюдження фроду з використанням електронної пошти компанії* – BEC атаки також можуть включати здійснення змін в рахунках, інвойсах або документах компанії, щоб перенаправити платежі на банківські рахунки, контрольовані зловмисниками.
5) *Зловживання важливими подіями* – зловмисники можуть використовувати важливі події, такі як фінансові транзакції, злиття і поглинання, щоб отримати довіру і натякнути на терміновість вимог.

6) *Міжнародний характер BEC* – BEC-атаки характеризуються міжнародністю, адже зловмисники можуть діяти з будь-якої точки світу і направляти атаки на компанії у різних країнах.
7) *Важливість захисту від BEC атак* – компанії та організації активно вдосконалюють свої заходи захисту, включаючи навчання персоналу виявляти підозрілі повідомлення, використання аутентифікації з двома факторами та інші технології захисту, які допомагають виявляти та блокувати спрямовані фішингові атаки. Разом із цим, правоохоронні органи розробляють строгі правила та стандарти для бізнесів, які мають доступ до фінансових операцій та конфіденційної інформації, з метою зменшення ризику BEC атак.

Еволюція *MFA* та їх вплив на фішингові атаки:

1) *«Something You Know + Something You Have»* – перший етап розвитку MFA включав у себе використання пароля, яким володіє користувач, разом із фізичним об'єктом, який він має, наприклад, токеном, смарт-картою або USB-ключем. Це ускладнило завдання фішерам, оскільки вони повинні були не лише дізнатися пароль, але і отримати доступ до фізичного пристрою.
2) *«Something You Know + Something You Are»* – другий етап, де до MFA додались біометричні дані. Тепер користувачі мали вводити свій пароль та підтверджувати свою ідентичність, використовуючи сканування відбитків пальців, розпізнавання обличчя або інші біометричні дані. Це ускладнило спроби атакуючих використовувати лише паролі.
3) *Багатофакторна аутентифікація* – третій етап розвитку Мультифакторної аутентифікації, що передбачає використання багатьох факторів аутентифікації. Наприклад, «Something You Are» + «Something You Have» + «Something You Do», тобто користувач може сканувати відбиток пальця, ввести пароль і отримати одноразовий код на свій мобільний пристрій. Цей

надійний спосіб перевірки ідентичності максимально ускладнює завдання фішерам.

4) *Аналітика та інтелектуальна MFA* – останній етап еволюції *MFA*, на якому почали використовуватись інтелектуальні та аналітичні системи. Основою їх функціонування став штучний інтелект і машинне навчання для аналізу поведінки користувачів та визначення аномалій. Внаслідок цього, стало можливим виявлення вдосконалених фішингових атак, що використовують легітимні дані користувача.

ДОДАТОК В

Порівняльна характеристика фішингових атак

Таблиця В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
America Online (AOL)	1990р., США	Заволодіння конфіденційною інформацією користувачів та їх обліковими записами	Електронна пошта	Після відкриття вкладеного у електронне повідомлення фалу, вірус переписував, видаляв, шифрував файли, та надсилав копії себе самого іншим користувачам через електронну книгу [10].	Втрата облікових записів користувачами	Атака стала однією з перших фішингових у світі та встановила основу для подібних стратегій у майбутньому, показавши, що використання методів соціального інжинірінгу є ефективним способом досягнення бажаної мети.

Продовження Таблиці В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
MyDoom (Novarg)	2004 р.	Достовірно невідомо, однак вважається спроба уникнення конкуренції	Електронна пошта	Після відкриття вкладеного у електронне повідомлення фалу, MyDoom створював копію себе на зараженому комп'ютері та намагався відкрити відомий багатократний атакуючий "backdoor" для дозволу атакуючому отримати дистанційний доступ до системи. Крім того, вірус намагався перевантажити пошукові системи, відправляючи запити до них, та спричиняючи перевантаження мережі й зниження працездатності.	Унаслідок атаки MyDoom багато компаній втратили доступ до електронної пошти та інтернет-ресурсів, що спричинило серйозні перебої в роботі. Велика частина бізнес-процесів була порушена [11].	Атака стала прикладом вдалого використання елементів соціального інжинірингу. MyDoom є явним свідченням того, як тривалість атаки прямо пропорційна вартості виправлення завданої шкоди. Атака показує вразливості не тільки приватного, але й корпоративного сегменту користувачів, що дало поштовх до розширення сегменту вибору цільових жертв фішерів у майбутньому.
Атака на RSA	Березень 2011 р.	Отримання конфіденційної інформації, пов'язаної з SecurID, продуктом RSA, який надає двофакторну аутентифікацію для користувачів.	Електронна пошта	Атака була вирішальним етапом багатоланцюгової схеми. Вона почалася зі спам-пошти, що містила вкладення зі шкідливим кодом. Цей код використовувався для створення спеціального зловмисного програмного забезпечення, яке було розроблене для отримання доступу до систем RSA.	Зловмисники змогли отримати інформацію, пов'язану з технологією аутентифікації SecurID. Це призвело до підвищення загрози для користувачів, які використовують цю технологію для захисту своїх даних [12].	Хоча RSA негайно повідомила про інцидент та почала розслідування, співпрацюючи з правоохоронними органами, атака показала вразливість провідних IT-компаній, що спеціалізуються на кібербезпеці, до фішингу.

Продовження Таблиці В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
Атака на Snapchat	2016р.	Отримання доступу до конфіденційної фінансової інформації компанії	Електронна пошта	Зловмисники надіслали фішинговий лист, в якому було використано прийоми соціального інженірінгу, директору з фінансів (CFO) компанії [13].	Фішери змогли отримати доступ до чутливих фінансових даних компанії. Це включало в себе інформацію, яка могла б мати серйозний вплив на бізнес.	Атака на Snapchat демонструє тенденцію підвищення персоналізації та більш точного використання імітаційних джерел. Більше того, очевидним є те, що роль втраченої репутації починає відігравати одне з найбільш значущих місць серед збитків для IT-компаній.
Атака на Facebook	Квітень 2016 р.	Отримання доступу до облікових записів користувачів із можливістю їх використання для розміщення шкідливого вмісту, розсилання спаму або здійснення фінансових шахрайств.	Електронна пошта	Зловмисники надсилали фішингові листи, які виглядали як офіційні повідомлення від Facebook або інших довірених джерел, з метою переконати користувачів надати свої облікові дані (логін та пароль) або перейти за посиланням, яке вело на підроблену сторінку входу в Facebook [14].	Унаслідок атаки користувачі-жертви втратили конфіденційну інформацію, що дала можливість отримати повний контроль над їх обліковими записами. Крім того, зловмисники могли використовувати втрачений обліковий запис для поширення шкідливого контенту, фінансового шахрайства тощо.	Атака на Facebook у 2016 році відобразила той факт, що соціальні мережі стали однією з основних цілей для фішингу. Зловмисники продовжили використовувати соціальний інжиніринг для більшої переконливості жертви.

Продовження Таблиці В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
Атака на Facebook	Квітень 2016 р.	Отримання доступу до облікових записів користувачів з можливістю використання цих облікових записів для розміщення шкідливого вмісту, розсилання спаму або навіть здійснення фінансових шахрайств.	Електронна пошта	Зловмисники надсилали фішингові листи, які виглядали як офіційні повідомлення від Facebook або інших довірених джерел, з метою переконати користувачів надати свої облікові дані (логін та пароль) або перейти за посиланням, яке вело на підроблену сторінку входу в Facebook [14].	Унаслідок атаки користувачі-жертви втратили конфіденційну інформацію, що дала можливість отримати повний контроль над їх обліковими записами. Крім того, зловмисники могли використовувати втрачений обліковий запис для поширення шкідливого контенту, фінансового шахрайства тощо.	Атака на Facebook у 2016 році відобразила той факт, що соціальні мережі стали однією з основних цілей для фішингу. Зловмисники продовжили використовувати соціальний інжиніринг для більшої переконливості жертви.

Продовження Таблиці В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
Атака на Equifax	Серпень 2017 р.	Крадіжка конфіденційної фінансової інформації споживачів	Електронна пошта	Зловмисники відправили підроблений лист від одного з партнерів компанії Equifax, у якому просили про поновлення доступу до облікового запису [15].	Фішери отримали доступ до внутрішніх систем компанії Equifax та використовували викрадені облікові дані для здійснення несанкціонованих дій. За оцінками, близько 143 мільйони осіб стали жертвами цієї атаки. Компрометована інформація включала ім'я, соціальний номер, адреси, номери кредитних карток та інші конфіденційні дані.	Ця атака мала серйозні наслідки для Equifax, включаючи втрату довіри споживачів та значні фінансові збитки. Компанія втратила репутацію та стала предметом численних судових позовів. Загалом, цей інцидент став показовим щодо серйозності та масовості збитків і наслідків вдалої реалізації фішингу.
Атака по темі COVID-19	2021	Отримання особистої та фінансової вигоди за допомогою маніпулювання пандемічною ситуацією та панікою	Електронна пошта	Зловмисники надсилали фішингові листи, видаючи себе офіційними медичними чи урядовими установами, і пропонували отримати вакцинацію проти COVID-19 за допомогою посилання у листі. При переході за яким жертва потрапляла на підроблений сайт, де їй пропонували ввести конфіденційні дані.	Втрата чутливої інформації користувачами, в тому числі й фінансової. Більше того, компаніям та організаціям, які були скомпрометовані, була завдана репутаційна шкода [16].	Аналіз атаки показав, що цілі та наміри фішингу гнучко підлаштовуються під світові тенденції, а саме епідеміологічні небезпеки. Зберігається тенденція використання прийомів соціального інжинірингу та маніпулювання шляхом вибірковості найбільш вразливої групи користувачів.

Продовження Таблиці В.1 – Порівняльна характеристика показових фішингових атак

Назва атаки	Час і місце	Мета	Спосіб розповсюдження	Спосіб ураження	Шкода від реалізації	Висновок
Атака по темі COVID -19	2021	Отримання особистої та фінансової вигоди за допомогою маніпулювання пандемічною ситуацією та панікою	Електронна пошта	Зловмисники надсилали фішингові листи, видаючи себе офіційними медичними організаціями чи урядовими установами, і пропонували отримати вакцинацію проти COVID-19 за допомогою посилання у листі. При переході за яким жертва потрапляла на підроблений сайт, де їй пропонували ввести конфіденційну інформацію.	Втрата чутливої інформації користувачами, в тому числі й фінансової. Більше того, компаніям та організаціям, які були скомпрометовані, була завдана репутаційна шкода [16].	Аналіз атаки показав, що цілі та наміри фішингу гнучко підлаштовуються під світові тенденції, а саме епідеміологічні небезпеки. Зберігається тенденція використання прийомів соціального інжинірингу та маніпулювання шляхом вибірковості найбільш вразливої групи користувачів.

ДОДАТОК Г

Відомості, щодо регіональних та галузевих відмінностей реалізації фішингових атак

Таблиця Г.1 – Специфічні особливості регіонів з точки зору умов фішингових атак

Регіон	Рівень мовної специфіки	Рівень соціальних та культурних особливостей	Технологічний стек	Потенційна вигода для атакуючого
Азія	Високий. *Показник обумовлений комплексним характером лінгвістичного спілкування*	Високий	Розширене використання символів та ідеограм, специфічні соціальні платформи	Висока
Європа	Висока *(специфічна різноманітність)*	Високий *(специфічна різноманітність)*	Адаптація до різноманіття культур та мов, використання культурних подій	Висока
Північна Америка	Високий	Високий	Використання загальнопоширених платформ, специфічні технологічні рішення	Висока
Латинська Америка	Високий	Високий	Адаптація до локальних культур та соціальних контекстів, врахування місцевої проблематики	Висока

Високий рівень мовної специфіки *Азійського регіону* обумовлений *мовним розмаїттям регіону* (налічує значну кількість мовних груп та діалектів, що мають власні граматичні, фонетичні та семантичні нюанси), *використанням ідеографічних мовних систем* (ідеограми – це символи, що позначають слова, а не звуки та відображають особливості писемності деяких країн), *культурною важливістю точності* (велика увага приділяється відображенню глибокого

розуміння в сказаному), *формалізованим мовним етикетом* (наявність різних формалізованих мовних виразів, які використовуються в залежності від статусу, віку, соціального стану співрозмовника тощо), *літературними традиціями* (багаті літературні традиції та велика кількість класичних текстів в китайській, японській та інших азійських культурах вимагають високого рівня мовної культури та глибокого розуміння сенсу).

Високий рівень соціальних та культурних особливостей регіону обумовлений *історичним контекстом, засадами сімейних відносин, важливістю ієрархічності та поваги, формалізованістю та специфічним етикетом*, а також *релігійним впливом.*

Високий рівень мовної специфіки для *Європейських країн* відображається в ряді аспектів, що визначають унікальність мовного спілкування в цьому регіоні: *великим різноманіттям мовних груп, особливими мовними стандартами та літературними традиціями, історичними та культурними впливами, багатим лексичним запасом, мовним пластичним стилем,* а також *формальностями й етикетом.*

На високий рівень культурних та соціальних особливостей даного регіону вплинули такі фактори: *мультикультурність, історичні культурні впливи, демократичні традиції, міжкультурна толерантність,* а також *соціальна підтримка.*

Серед аспектів, що сформували високий рівень мовної специфіки країн *Латинської Америки* слід виділити: *наявність іспанської, португальської й індігенних мов, культурну синкретизацію, існування мовних впливових середовищ*, а також *наявність діалектів і різних варіантів мов.*

Важливими елементами культурних та соціальних особливостей регіону: *культурний плюралізм та різноманіття; релігійна, міжетична та мовна різноманітність; соціальний активізм.*

Таблиця Г.2 – Співставлення фішингових атак для умов корпоративного та приватного сегменту користувачів

Критерії порівняння	Сегменти користувачів	
	Корпоративний	Приватний
Мета атаки	Оволодіння конфіденційною інформацію з цілю її використання для отримання фінансової вигоди та завдання репутаційної шкоди компанії.	Оволодіння особистими даними користувача з ціллю фінансової вигоди.
Методи атак	Використання комплексу складних методів впливу на жертву, таких як соціальна інженерія, а також імітації корпоративних комунікацій для отримання доступу до облікових записів великих компаній.	Використання відносно простіших методів впливу на жертву, наприклад, відправка електронного листа з шкідливим посиланням, підробка веб-сайту, тощо.
Обсяг потенційних жертв	Фішингові атаки у цьому сегменті можуть потенційно зачіпати сотні, а інколи навіть і тисячі співробітників компанії, що може мати серйозні фінансові та репутаційні наслідки.	Кількість потенційних жертв значно менша, проте втрати в особистій сфері можуть бути так само важливими для кожного окремого користувача.
Рівень захисту	Компанії мають можливість вкласти значні зусилля в розробку та впровадження високотехнологічних засобів захисту та навчання персоналу. Питання захисту покладається на окремих співробітників компанії.	Значно нижчий рівень захисту, адже приватні користувачі не мають тих же ресурсів та можливостей. Зазвичай, вони покладаються на базові антивіруси та файрволи, а також на особисті сили щодо розпізнавання потенційно шкідливих повідомлень.

Продовження Таблиці Г.2 – Співставлення фішингових атак для умов корпоративного та приватного сегменту користувачів

Критерії порівняння	Сегменти користувачів	
	Корпоративний	Приватний
Потенційні наслідки	Втрата конфіденційних даних співробітників і користувачів, репутаційна шкода для компанії, значні фінансові збитки.	Втрата особистих даних, що призводить до фінансових збитків.

ДОДАТОК Д

Класифікація цільової інформації для атакуючої сторони

Основними категоріями даних, що цікавлять фішерів, є:

1) *особиста інформація:*
   - ПІБ;
   - дата народження;
   - адреси проживання;
   - контактні дані;
2) *фінансові дані:*
   - номери банківських карт;
   - банківські реквізити;
   - паролі до банківських акаунтів;
3) *інформація про доступ до електронних платіжних систем:*
   - облікові дані для платіжних систем (наприклад, *PayPal, Skrill, Payoneer* тощо);
4) *дані соціальних мереж та інтернет-платформ:*
   - логіни та паролі до акаунтів у соціальних мережах, електронних поштових скриньок, форумах, онлайн-іграх тощо.
5) *інформація про онлайн-сервіси та додатки:*
   - логіни та паролі для онлайн-сервісів, таких як онлайн-магазини, медіа-платформи, стрімінгові сервіси тощо;
6) *медична інформація:*
   - дані про стан здоров’я;
   - медичні історії;
   - рецепти, тощо;
7) *дані геолокації:*
   - інформація про місце знаходження;

- інформація про переміщення;

8) *особисті фото- та відеоматеріали:*
   - зображення та відеозаписи особистого характеру;
9) *сімейна інформація:*
   - дані про сімейний стан;
   - дані про членів сім'ї;
   - контактні дані родичів тощо.

ДОДАТОК Е

Порівняльна характеристика технологій *SPF, DKIM* та *DMARC*

Таблиця Е.1 – Порівняльна характеристика стандартів *SPF, DKIM* та *DMARC*

Характеристика	*SPF*	*DKIM*	*DMARC*
Опис	Використовує *DNS*-записи для вказівки дозволених серверів, що можуть надсилати листи від імені домену.	Використовує криптографічний підхід для створення та перевірки цифрового підпису листів.	Встановлює політики аутентифікації для електронної пошти та надає звіти про спроби надсилання листів від імені домену.
Головна мета	Попередження від підроблення серверів, які намагаються надсилати листи від імені домену.	Попередження від підроблення листів, які надходять від певного домену.	Контроль над тим, як сервери відправників повинні автентифікувати листи від імені домену та як обробляти неправильно автентифіковані листи.
Використання	Вказівка дозволених IP-адрес або серверів для надсилання листів в DNS-записах домену.	Створення та перевірка цифрового підпису для кожного листа.	Встановлення політики DMARC в DNS-записах, яка вказує, як поводитися з недостовірними листами.
Видимість для користувачів	Невидимий для користувачів, але може призвести до не доставлення листів, якщо не налаштований правильно.	Невидимий для користувачів, але може призвести до не доставлення листів, якщо не налаштований правильно.	Може призвести до не доставлення листів, якщо не налаштований правильно, або вказано політику *"reject"*. Можлива відправка звітів про аутентифікацію.

Продовження Таблиці Е.1 – Порівняльна характеристика стандартів *SPF, DKIM* та *DMARC*

Характеристика	*SPF*	*DKIM*	*DMARC*
Вимоги до налаштування	Правильно вказати дозволені IP-адреси в *SPF*-записах.	Генерація та збереження ключів, а також налаштування *DNS*-записів для них.	Вказати політику та адреси для звітів в *DMARC*-записах, а також налаштувати обробку неправильно автентифікованих листів на сервері.
Ефективність протидії фішингу	Висока	Висока	Дуже висока, особливо в поєднанні з SPF та DKIM
Переваги	Простий для встановлення та налаштування.	Надає високий рівень впевненості в автентичності листів.	Забезпечує найвищий рівень захисту, оскільки комбінує SPF та DKIM та надає додаткову контрольну панель.
Недоліки	Може призвести до не доставлення листів, якщо не налаштований правильно.	Вимагає додаткових витрат на генерацію та зберігання ключів.	Вимагає обслуговування та аналізу звітів для налаштування оптимальних політик. Може потребувати певного рівня експертизи для коректного налаштування.

ДОДАТОК Ж

Розгляд показових випадків порушення ІБ внаслідок здійснення фішингових атак

Притягнення до відповідальності Петеріса Сахуровса, громадянина Латвії, що був визнаний винним у здісненні фішингових атак та спамінгу, які призвели до нанесення значних збитків, типовий приклад використання шахрайських методів для вимагання доступу до фінансових активів жертви. Петеріс Сахуровс був засуджений згідно з Кримінальним кодексом Сполучених Штатів Америки [60], зокрема за статтями 18 USC § 1349 (спроба шахрайства) та 18 USC § 1037 (шахрайство через електронну пошту). У наслідок отримав покарання у вигляді засудження до 33 місяців ув'язнення та відшкодування потерпілим понад 100,000 доларів.

Евальдас Рімасаускас, громадянин Литви, був визнаний винним у схемі фішингу, де він використовував підроблені документи та електронні листи, щоб вимагати гроші у великих корпорацій. Він був притягнутий до відповідальності за статтею 18 USC § 1343 [61], яка стосується махінацій із використанням дроту, радіо, або інших засобів комунікації для шахрайства. У наслідок чого був засуджений до 50 місяців ув'язнення за свою роль у фішинговій схемі та зобов’язаний до відшкодування більше 50 мільйонів доларів.

Причина притягнення до відповідальності Кима, громадянина Південної Кореї, полягає у здійсненні фішингу та шахрайства, у результаті чого були завдані значні фінансові збитки. Він був засуджений згідно з Кримінальним кодексом Республіки Корея [62], а саме за статтею 347 (шахрайство та афери). У наслідок чого отримав покарання у вигляді 4-х років ув'язнення та штрафу близько 2,7 мільйонів доларів.

Ігор Єгорушкін був притягнутий до відповідальності за організацію фішинг-кампанії, яка цілилася на бразильські банки та фінансові установи. Конкретні статті бразильського законодавства не наведені, проте фішинг атаки можуть бути притягнуті до відповідальності відповідно до Закону про кіберзлочини Бразилії [63]. У наслідок чого Ігор Єгорушкін був арештований, але конкретні покарання у цьому випадку не надані.

У випадку притягнення до відповідальності компанії Allergy Pathway був застосований Закон про споживчий захист та конкуренцію Австралії [64]. Ця компанія була притягнута до відповідальності за недостовірні обіцянки та обманну рекламу, що можна розглядати як фішинг. У цьому випадку компанія була змушена сплатити штраф у розмірі 75,000 доларів.