УДК 004.415.53

АНАЛІЗ РОЗВИТКУ, ТИПОВІ ЦІЛІ ТА МЕХАНІЗМИ ЗДІЙСНЕННЯ ФІШИНГОВИХ АТАК

Юлія Лєсная, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
xa12284109@student.karazin.ua, malakhov@karazin.ua

Надійшла: жовтень 2023. Прийнята: листопад 2023.

Анотація: *У роботі розглянуто проблематику фішингових атак. Підкреслено взаємозв'язок між етапами розвитку інформаційних технологій та періодами еволюції фішингу. Звернено увагу на те, що будь-який новий комунікаційний ресурс або онлайн технологія в значної мірі поширюють спектр можливих прийомів соціального інжинірингу, що є однім із головних елементів сучасного фішингу. За результатами огляду відомих інцидентів стверджується, що в подальшому цей різновид атак буде тільки поширюватись. Основними чинниками для подальшого зростання фішингу є: - активне впровадженням технологій штучного інтелекту та Інтернету речей; - поширення супутникового Інтернет; - стійке збільшення чисельності мережевих користувачів; - технологічне протистояння між основними акторами постіндустріального світу. Зроблено акцент на тому що, підвищення рівня доступності до всесвітньої мережі Інтернет, приведе до зростання кількості користувачів нових комунікаційних сервісів та служб. Однак, масштабна цифровізація сучасного суспільства при збереженні низьких рівнів «цифрової» компетентності окремих соціальних прошарків, зумовить потенційну вразливість для великих груп технологічно непоінформованих користувачів. Одночасне існування цих двох тенденцій зумовить збільшення кількості потенційних жертв фішингових атак у майбутньому. Підкреслено, що інтеграція фішингу з іншими різновидами кібератак, забезпечує підвищення показника кількості фішингу. Звернено увагу, що значне розповсюдження соціальних мереж зумовлює факт їх найчастішого використання, як засобу поширення фішингу. Зроблено висновок, що фішингові атаки в корпоративному та приватному сегментах сучасних інформаційних систем, при всій своїй зовнішній схожості, спрямовані на отримання суттєво різних «бонусів»: 1 - за масштабами їх реалізації й наслідків; 2 - субстантивністю дій. Саме ці - неявні відмінності, визначають різницю у обраних векторах впливу та сценаріях дій атакуючої сторони. Акцентовано увагу на те що, використання багатофакторної автентифікації помітно ускладнює підміну ідентифікаційних даних користувачі послуг та сервісів сучасних інформаційних систем, що суттєво знижує «успішність» фішингу, роблячи його менш ефективним. Зазначено, що впровадження комплексного захисту від фішингових атак, передбачає неперервне удосконалення наявних технологій і засобів безпеки у їх нерозривному взаємозв'язку із організаційними заходами. Організаційна складова повинно чітко регламентувати рівні персональної та колективної відповідальності за поточний рівень безпеки використовуваних систем та інформаційних ресурсів.*

Ключові слова: *фішинг, атака, ресурс, інформаційна безпека, соціальна інженерія, система доменних імен.*

1. 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 (*SE*), що є однією з головних передумов сучасних фішингових атак, із притаманними для них особливостями моніторингу та можливостями протидії цьому різновиду загроз безпеки. За результатами огляду відомих 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 технологій штучного інтелекту (*AI - Artificial Intelligence*) і Інтернету речей (*IoT*) та стійким збільшенням чисельності користувачів мережі Інтернет й учасників різних соціальних мереж.

2. Основні етапи в розвитку фішингових атак та їх питома частка у загальному спектрі загроз ІБ

Фішингові атаки – це такий різновид кібератак, що передбачає використання сукупності методів і технік маніпулювання потенційною жертвою. Головною метою фішингу є непра-

 © Лєсная Ю., Малахов С., 2023

вомірне отримання доступу до «чутливої» інформації та/чи інших цільових ресурсів жертви атаки, шляхом реалізації послідовності специфічних злочинних дій. У загальному випадку до чутливої інформації відносяться: – конфіденційні, корпоративні та персоніфіковані дані, а в якості цільових ресурсів можуть виступати фінансові, репутаційні, технічні та інші відомості. На рис. 1 представлено взаємозв'язок між етапами розвитку IT сфери та періодами еволюції фішингових атак, кожен із яких відзначився новими методами та підходами до їх здійснення. Слід зазначити, що замикаючий етап розвитку даного типу загроз ІБ, а саме період мультифакторної автентифікації, відрізняється від попередніх своєю направленістю на часткове усунення вразливостей існуючих інформаційних систем (ІС) до фішингу.

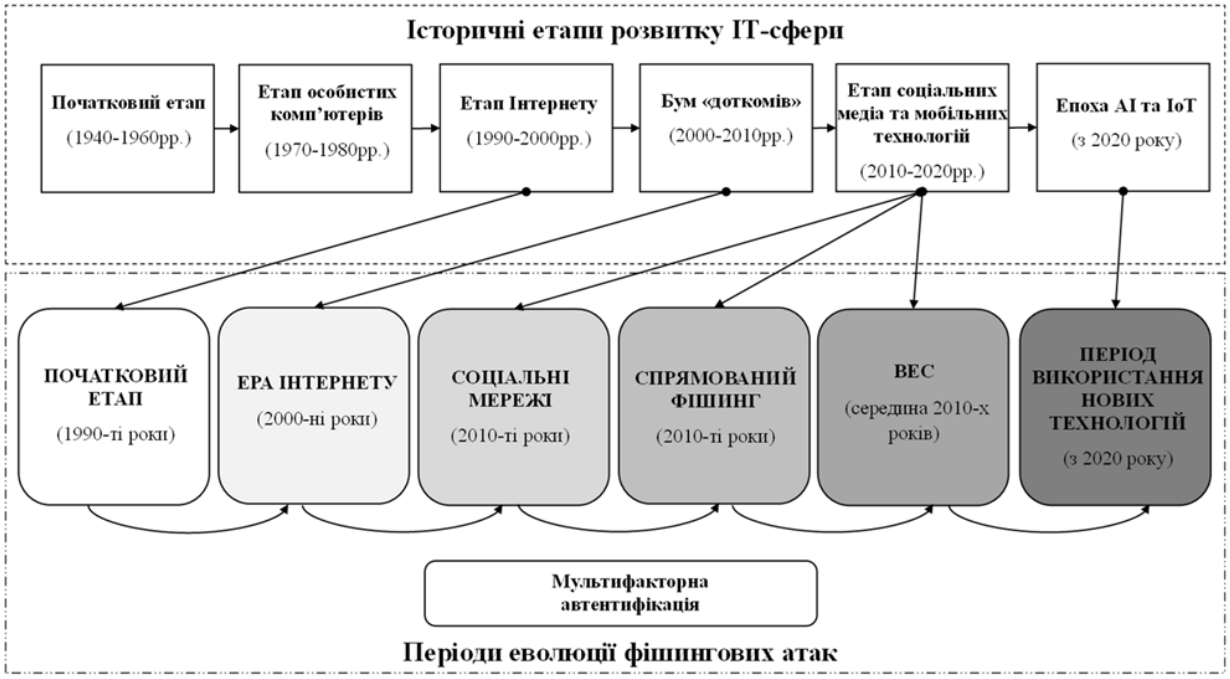

Рис. 1 – Взаємозв'язок між етапами еволюції інформаційних технологій та етапами розвитку фішингових атак

Fig.1 - The relationship between the stages of the evolution of information technologies and the stages of the development of phishing attacks

За результатами проведеного аналізу показових прикладів атак було визначено, що:

- фішингові атаки приймають різні форми та способи реалізації, однак зберігається першість електронної пошти, як головної 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*) [1].

Таким чином, 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).

Кожен етап еволюції в сфері IT призводив до виникнення не лише нових технологічних можливостей, але й суттєво впливав на соціокультурні та соціоекономічні аспекти суспільства. Одночасно цей процес породив технічні виклики, зокрема фішингові атаки, як загрозу ІБ.

Динаміка частки фішингових атак у загальному спектрі загроз ІБ суттєво змінюється протягом усіх етапів розвитку IT сфери (Рис. 2) та визначається різними факторами: - розвиток технологій, поширення Інтернету, поточний рівень обізнаності користувачів, впровадження заходів кібербезпеки та ін. [2,3].

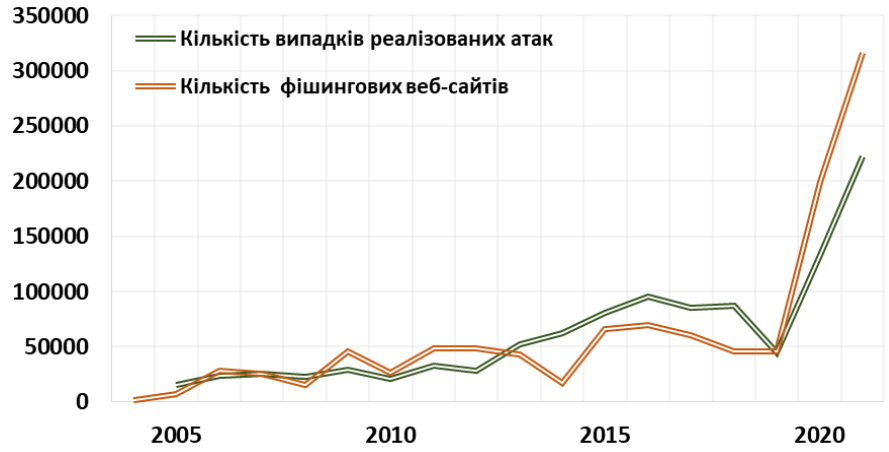

Рис. 2 – Узагальнення щорічних оглядів стосовно частки фішингових атак

Fig. 2 - Summary of annual reviews regarding the share of phishing attacks

Показники кількості випадків реалізованих *фішингових атак* свідчать про стійкий та істотний ріст цього виду кіберзлочинності. Очевидно, що особливо сприятливим періодом для реалізації фішингу був період пандемії *COVID-19*, що зумовило глобальні зміни у способах роботи та комунікації через інтернет. 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 даними 2022 року [4], 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 інших різновидів кібератак (Рис. 3-4), а цей вид атак продовжує залишатися в «топі» та станом на 2022 рік складає 41% [4].

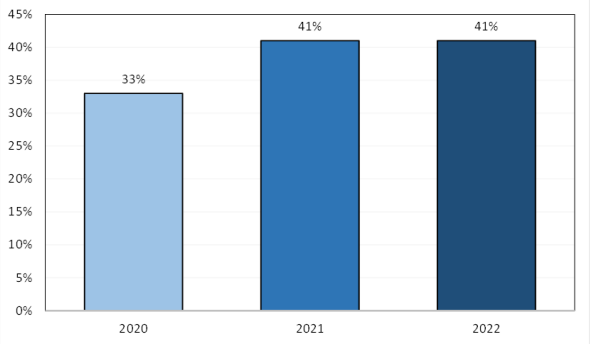

Рис. 3 – Питома частка фішингових атак *(серед інших)* станом на 2022 р

Fig. 3 - Specific share of phishing attacks *(among others)* as of 2022

Рис. 4 – Різновиди фішингу від загальної кількості атак на 2022 р

Fig. 4 – Types of phishing from the total number of attacks in 2022

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.

3. Особливості 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)*.

Серед основних *галузевих* особливостей фішингових атак слід відзначити: - рівень обізнаності в галузі; - врахування географічних аспектів; - експлуатація специфічних подій та новин; - використання реквізитів галузевих організацій; - використання фахової термінології й спеціальних технічних аспектів; - експлуатація зв'язків між об'єктами галузі.

Якщо оцінювати окремі галузі з точки зору потенційної вигоди фішерів, то стане зрозуміло, що для більшості з них вона буде високою [2]. У табл. 1 наведено загальну оцінку потенційної шкоди від «успішно» реалізованої атаки для деяких галузей, проте потрібно розуміти, що її показник буде варіюватися в залежності від конкретної ситуації та обставин.

За результатами аналізу векторів направленості галузевих атак протягом останніх 3-х років очевидно, що еволюція фішингових атак супроводжувалася зміною пріоритетних цілей атакуючих (Рис. 5). Так встановлено, що галузі фінансового сектору та банківської діяльності залишаються основними об'єктами атак. Водночас, сектори електронної комерції та поштових сервісів залишаються стійкими до фішингу.

Реалізація фішингу на *регіональні ресурси* має свою власну специфіку, оскільки вона спрямована на конкретний географічний сегмент аудиторії: - маскування під місцевий бізнес; - локалізація контенту; - використання локальних подій/новин; - використання внутрішньо - регіональних ланок довіри; - специфічні способи контакту; - сегментація аудиторії; - використання місцевих правописних і граматичних особливостей.

Таблиця 1 – Потенційна шкода від фішингових атак для деяких галузей
Table 1 - Potential harm from phishing attacks for selected industries

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 злочинному ринку, можливе її використання для шахрайства, шпигунства, шантажу та кібербулінгу [3].
IT-індустрія	Висока. Доступ до конфіденційних технічних даних, можливість впливу на розробку та безпеку діючого програмного забезпечення (ПЗ).
Електронна комерція та роздрібна торгівля	Висока. У разі отримання доступу до облікових записів та фінансової інформації можливе її використання на злочинному ринку *(в т.ч. Dark Net)* [5], 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.
Криптовалюти та 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.

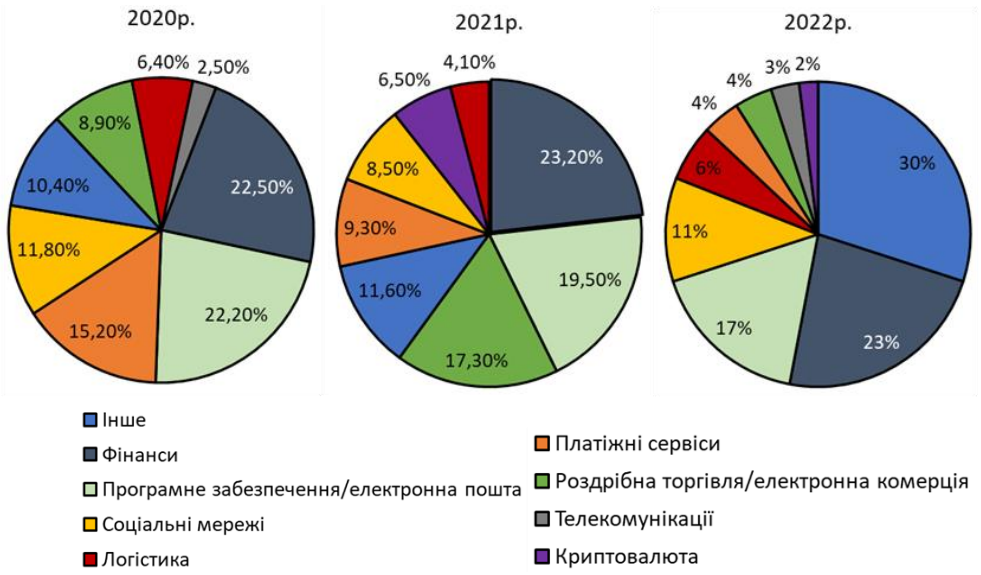

Рис. 5 - Галузеві відмінності при реалізації фішингових атак *(на 4-й квартал 2020-2022 рр.)*
Fig. 5 - Industry differences in the implementation of phishing attacks *(for the 4th quarter of 2020-2022)*

Узагальнюючи дані про найбільш постраждалі від кібератак регіони [4], було зроблено порівняння *(див. Рис. 6)* кількості відповідних загроз для 5-ти основних регіонів впродовж 2020-2023рр.. 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.

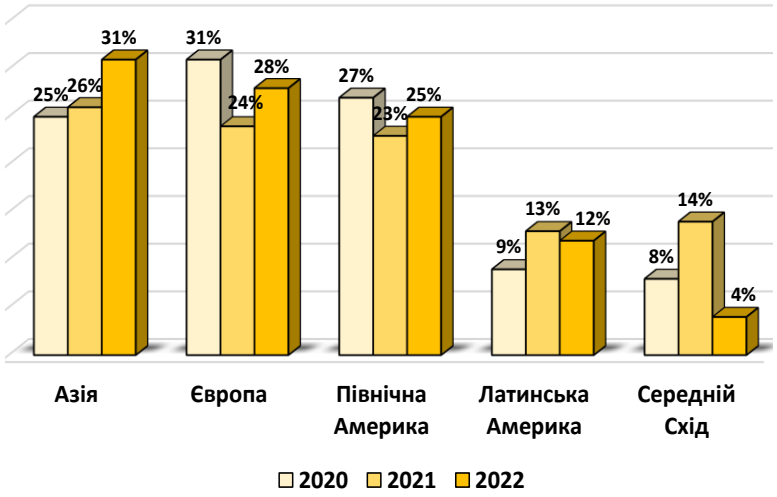

Рис. 6 – Регіональні відмінності кількості фішинг атак *(станом на 2020-2023 рр.)*

Fig. 6 – Regional differences in the number of phishing attacks *(as of 2020-2023)*

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 3-м 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 і страхування у 2022 році були найбільш націленою галуззю на *Близькому Сході і Африці*, становлячи 44% всіх випадків. Професійні, бізнес та споживчі послуги відповідали за 22% атак, при цьому виробництво й енергетика ділили 3 місце, кожна з них складала 11% від загальної кількості інцидентів. При цьому спрямований фішинг через посилання, як метод отримання початкового доступу, використовувався в двох третинах випадків ІБ.

Отже, регіони світу різняться за характером та обсягами фішингових атак, адже їх масштаби визначаються не тільки технічними аспектами, але і соціально-політичними та економічними факторами [5]. 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»*.

4. Узагальнення основних цілей і механізмів здійснення фішингових атак, притаманних корпоративному та приватному сегментам користувачів сучасних ІС

Проблематика фішингу має свої варіації та специфічні особливості у різних сегментах сучасного суспільства. Так, *корпоративний сектор*, в своїй переважній більшості, потребує індивідуального підходу і комплексного захисту. Із іншого боку, *приватні користувачі*, керуючись власним досвідом, зазнають помітно інших ризиків, проте й вони є не менш вразливими перед цією загрозою безпеки.

Корпоративний сегмент користувачів відзначається рядом унікальних характеристик, що впливають на сценарії та наслідки фішингових атак, а саме: - наявність великої кількості конфіденційних або «чутливих» даних, що стосуються як самої компанії, так і її клієнтів й партнерів; - велика кількість співробітників, що використовують загальну інфраструктуру; - висока ступінь взаємозалежності між співробітниками, внаслідок чого одна недбаліть чи помилка може призвести до ланцюгової реакції, що відкриє нове «вікно можливостей» для потенційних зловмисників [6]. У табл. 2 систематизовано сутність механізмів здійснення фішингових атак і їх наслідки для різних категорій корпоративних ресурсів.

Таблиця 2 – Особливості здійснення фішингових атак на корпоративні ресурси
Table 2 – Features of phishing attacks on corporate resources

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 проектів
	Експлуатація вразливостей 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 несанкціонованого доступу (НСД) до конфіденційних корпоративних ресурсів, можливість порушення технологічних та/чи 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	
Системи управління доступом	Експлуатація вразливостей в автентифікації та авторизації	Ризик НСД, можливість неправомірної зміни прав доступу та порушення конфіденційності даних
	Реалізація атак типу *«men-in-the-middle»* для отримання доступу до систем управління доступом	

Аналізуючи специфіку фішингових атак для *приватного сегменту* користувачів, можна виявити кілька ключових аспектів: - приватні користувачі володіють обмеженими технічними ресурсами та не мають доступу до високотехнологічних засобів ІБ, що робить їх вразливими перед широким спектром загроз, особливо в контексті варіативності *SE* атак; - існує проблема підвищення профільної компетентності з питань ІБ; - приватні користувачі можуть власноруч зробити акцент на використанні надійних антивірусних рішень, паролів та двоетапної автентифікації, що є ефективним способом захисту від більшості загроз безпеки. Можливі механізми й наслідки від реалізації типових реалізацій фішингу на інформаційні ресурси потенційних жертв в приватному сегменті сучасних ІС, формалізовані в табл. 3.

Таблиця 3 – Особливості здійснення фішингових атак на ресурси приватного сегменту
Table 3 – Peculiarities of phishing attacks on private segment resources

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
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 персоніфікованої інформації та електронних облікових записів
	Реалізація атак через соціальні мережі та інші онлайн сервіси	
	Фішингові посилання для отримання паролів та ін. особистих даних	
Особиста інформація в мережі	Витіснення особистої інформації через соціальні мережі	Потенційне порушення конфіденційності, можливість втрати контролю над особистою інформацією, репутаційні ризики, шантаж та булінг
	Фішингові атаки через *E-mail* та месенджери	
	Використання методів *SE* для стимуляції витоку конфіденційної інформації через онлайн форуми і спільноти	
Особистий комп'ютер та інші пристрої	Фішингові атаки через шкідливе ПЗ	Ризик втрати контролю над особистими даними, можливість крадіжки конфіденційних даних, пошкодження особистих файлів і інформації та/або порушення штатних режимів роботи устаткування та/чи захисного ПЗ
Особиста безпека	Атаки на особисті файли та паролі через недостатній рівень загальної (базової) безпеки пристроїв Використання слабких паролів та їх повторне використання	Загроза безпеці особистих даних, можливість втрати конфіденційності та ризик використання даних для злочинних цілей (доксінг) [2]
	Атаки через не усунені вразливості (*Exploits ma Zero day*) пристроїв і ПЗ	

Отже, для корпоративного та приватного сегментів користувачів існують 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.

5. Узагальнення сценаріїв і механізмів реалізації фішингу

Під терміном *«сценарій»* фішингової атаки розуміється змістовна частина загального плану відповідної атаки, що визначає: – терміни заходів; – етапність дій; – залучені ресурси *(фінансові, апаратні та людські)*; – механізми реалізації заходів на кожному з етапів; – параметри локалізації *(тобто, масштаби реалізації)* зусиль, які здійснюються для оволодіння 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 [7].

Під терміном *«механізм»* 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 *SE* методи для маніпулювання поведінкою об'єктів атаки та підтримки потрібного зовнішнього інформаційного фону запланованих заходів [3,6].

Узагальнення основних сценаріїв фішингових атак, механізмів їх реалізації та інструментів здійснення, представлено в табл.4. З аналізу відомостей табл. 4 слід, що 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.

6. Основні напрями та нормативно-правові особливості, щодо комплексної протидії фішингу

Зважаючи на постійний ріст кількості та складності фішингових атак [6], захист від них є важливим завданням у сфері забезпечення ІБ. У цьому контексті слід приділити особливу увагу узагальненню основних напрямів з протидії відповідним атакам, включаючи всебічне врахування специфіки її організаційної та технічної 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 ПІБ, навчання персоналу, моніторинг та аналіз вразливостей, а також впровадження контрольних механізмів для мінімізації ризиків фішингу.

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 аномальної поведінкової активності, впровадження захисних механізмів, включаючи антивірусне та антиспамове ПЗ, а також встановлення та

конфігурування брандмауерів й інших засобів мережевої безпеки *(наприклад, мережевих пастоk)* з метою превентивного захисту організаційних систем і мереж від даного типу загроз.

Таблиця 4 – Узагальнення сценаріїв і механізмів реалізації фішингу
Table 4 – Summarization of scenarios and mechanisms of phishing implementation

Сценарій, що притаманний до конкретному виду фішингу	**Тактика дій атакуючого**	**Використовуваний інструментарій**
Електронна пошта	Створення фішинг повідомлень	Phishing kits
	Масова розсилка	Email spoofing tools
	Використання SE методів	Social engineering (SE) 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 фішинг посилань	URL shortening services
	Використання актуальних тем	Trend analysis tools
Телефонія *(Vishing)*	Спам-дзвінки	Caller ID spoofing tools
	Голосові повідомлення	Pre-recorded voice messages
	Використання психологічного тиску	SE tactics
SMS-фішинг *(Smishing)*	Відправка фішингових SMS	SMS spoofing services
	Використання месенджерів	Messaging platforms
	Спілкування через чат	SE tactics
Фішинг клонування *(Pharming)*	Створення фішингового сайту	Phishing frameworks
		Fake domain registration services
		DNS spoofing tools
	Розсилка фішингових посилань	E-mail campaigns
		URL shortening services
		SE tactics
	Використання HTTPS	SSL certificates
		Fake SSL certificates
	Використання маскування домену	Domain name registrar manipulation
		Typosquatting techniques
	Використання SE	SE tactics
		Gathering information from public sources

Оскільки фішинг, в цілому, є специфічним типом *SE* атаки, то він не базується тільки на експлуатації вразливостей апаратного чи ПЗ, а використовує комплексний підхід до реалізації маніпуляцій жертвами відповідної атаки. Саме тому пріоритетним напрямом з протидії даному типу загроз, є мінімізація залежності від впливу людського фактору. Зважаючи на це, можливо умовно виділити 3 основні рівні захисту від даного типу атак *(див. Рис. 7)*.

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.

Рис. 7 – Класифікація рівнів протидії фішингу
Fig. 7 - Classification of levels of counter-phishing

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, 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* [7-9].

2. *Захист хосту (кінцевих точок)*, розуміє використання програмно-апаратних засобів, що можуть бути встановлені на самому комп'ютері або сервері та контролювати системні ресурси й процеси, щоб виявити незвичайну мережеву активність, котра може вказувати на

спроби здійснення фішингу. Прикладом таких програмних рішень є *Symantec Endpoint Protection* або *ESET Endpoint Security* та ін. [10-11].

Найпоширенішими *програмними компонентами* для 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 Check Point, ESET Cyber Security, McAfee* [12] 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* [13] 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* [14], *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, котрі підробляють доменні адреси [15]. *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 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 цього домену (*див. Рис. 8*).

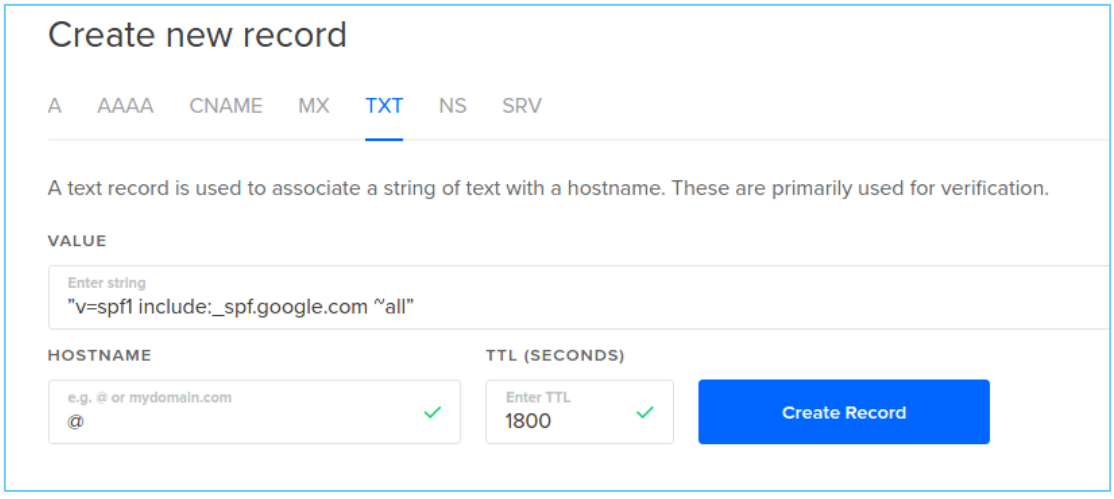

Рис. 8 – Приклад характерного *DNS*-запису «*SPF*»
Fig. 8 – An example of a characteristic DNS record «*SPF*»

У цьому прикладі *«v=spf1»,* свідчить про те, що цей *SPF* запис *(include:_spf.google.com)* включається для домену *_spf.google.com. Відповідно,* запис *«~all»* означає, 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»* та *«exists»* – деякі додаткові механізми, які дозволяють використовувати *PTR-запити* (*резервні DNS-запити*) і 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.

Domain Keys 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 [15].

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 електронного листа, поштовий сервер власника домену використовує приватний ключ для створення цифрового підпису, який додається до заголовка цього листа.
- *DNS-запис DKIM*: власник домену повинен додати спеціальний *DNS*-запис, який містить публічний ключ *DKIM*. Цей запис дозволяє всім одержувачам перевіряти цифровий підпис у заголовку цього листа (*див. Рис. 9*).

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

Рис. 9 – Приклад *DNS*-запису в *«DKIM»*
Fig. 9 – An example of a DNS entry in *«DKIM»*

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

Для перевірки *DKIM-підпису* одержувач *e-mail* 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, що використовують механізм підроблення *e-mail* адресів.

Domain-based Message Authentication, Reporting and Conformance (DMARC) – є стандартом, що дозволяє власникам доменів встановлювати політики автентифікації для своєї елект-

ронної пошти та отримувати звіти про спроби надсилання листів від їхнього домену. Головною метою *DMARC* є захист від спаму, фішингу та інших видів атак, що використовують підроблені адреси електронної пошти. Основні компоненти *DMARC* підтримують [15]:

- *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. Для цього використовують 3 види політик:
  - *«None»* – листи, що не проходять автентифікацію й не блокуються, але їх отримувачі генерують Звіти.
  - *«Quarantine»* – листи, що не проходять автентифікацію та помічаються, як спам, але не блокуються.
  - *«Reject»* – листи, що не проходять автентифікацію та блокуються.

Приклад *DMARC* запису, котра використовує політику блокування листів представлено нижче, на Рис. 10.

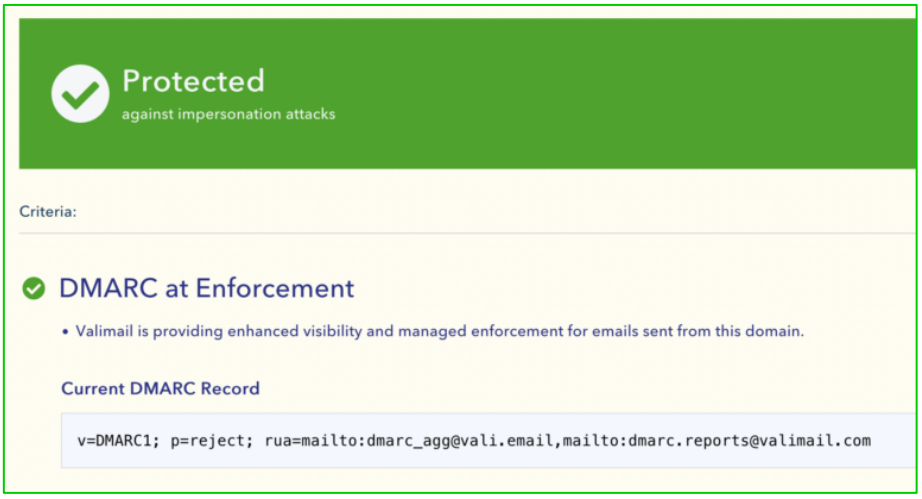

Рис. 10 – Приклад *DMARC*-запису в режимі *«Reject»*
Fig. 10 – An example of *DMARC* entry in *«Reject»* mode

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

- *SPF та DKIM автентифікація*: стандарт передбачає використання інструментів *SPF* та *DKIM* для перевірки ел. листів. Ті з них, що проходять автентифікацію, відповідають політиці *DMARC* що вказана у *DNS (Domain Name System)*.
- *Звіти DMARC*: *DMARC* дозволяє їх отримувачам надсилати Звіти власникам домену, які містять відомості про спроби надсилання листів від їхнього домену та, відповідно, результати автентифікації.

Отже, *DMARC* являється потужним інструментом для захисту від фішингу та інших різновидів атак, що використовують підроблені адреси електронної пошти. Робота *DMARC* у поєднанні з *SPF* та *DKIM* надає високий рівень захисту від шкідливих *E-mail*, що виглядають як такі, що надіслані від власного (легітимного) домену.

Таким чином, сумісне використання *SPF*, *DKIM* та *DMARC* дозволяє досягти високого рівня захисту від фішингу та інших атак через канал електронної пошти, однак при цьому слід враховувати, що їх використання залежить від конкретних потреб та можливостей власника домену. Також, для уникнення випадків не доставки *E-mail*, слід забезпечити коректне налаштування кожного з цих рішень.

Поряд з використання відповідних захисних рішень, ключовою стратегією у заходах з протидії фішинговим атакам, є постійне вдосконалення й імплементація у практичну діяль-

ність спеціалізованих нормативно-правових актів, які мають на меті: 1 - впровадити правові основи безпечного функціонування кіберпростору [16] та його основних акторів (*в сенсі декларування профільних правових норм*); 2 - надати механізми виявлення, блокування та розслідування випадків реалізації фішингових атак.

Нормативно-правові особливості протидії фішинговим атакам відзначаються комплексністю та мультидисциплінарністю. Вони охоплюють такі сфери, як захист особистих даних, електронна комунікація, кібербезпека [16], інформаційні технології (ІТ) 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 відповідні злочинні дії (тобто, фішингову 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).

Важливим є розуміння того, що конкретного та всебічного законодавства, яке б регулювало всі правові аспекти з протидії фішингу, не існує. Однак притягнення до відповідальності за даний вид кіберзлочину стає можливим у випадку комплексного поєднання різних законів та норм кожної конкретної держави, де ступінь відповідальності варіюється в залежності від серйозності (*наслідків*) скоєного інциденту та специфіки існуючих законодавчих норм за даної проблематики.

За результатами узагальнення відомостей, стосовно відомих інцидентів з фішингу та застосовності існуючих правових норм, можна зробити 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 кожної конкретної країні та комплексністю законодавчого регулювання боротьби з фішингом. Причинами цього є: - технічний потенціал країн *(розвинута ІТ інфраструктура передбачає використання більш складних методів реалізації фі-*

шингу); - великі обсяги ел. комунікацій; - широкі сфери діяльності компаній та користувачів; - високий показник інформаційної грамотності населення; - поступове 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 включають визначення правового статусу фішингових атак, встановлення відповідальності за їх скоєння, а також розробку та впровадження заходів із профілактики й реагування на інциденти фішингу. Крім того, вітчизняне законодавство передбачає механізми міжнародного співробітництва та видачі осіб, що причетні до здійснення фішингових атак, за межі країни. Правове регулювання фішингу визначено рядом нормативно-правових актів, що спрямовані на запобігання та протидію шахрайським діям в електронному середовищі. Основні норми включають:

1) *Кримінальний кодекс України. Ст. 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 України «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, 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 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,наявна нормативно-правова база свідчить про високий рівень усвідомлення важливості кібербезпеки та захисту вітчизняних інформаційних ресурсів. Проте, враховуючи стійке зростання кіберзлочинності (*див. рис. 2,6*), подальше вдосконалення законодавчого регулювання та впровадження сучасних технологічних рішень є невід'ємними умовами для забезпечення ефективної протидії сучасним фішинговим атакам.

В цілому, узагальнюючи специфіку нормативно-правового регулювання протидії фішингу, слід виділити наступні особливості:

- *Специфічність законодавства* (кожна окрема країна чи їх союз має власні особливості у правовому регулюванні боротьби з фішингом, котрі адаптовані до специфічних потреб і рівню їх поточного технологічного розвитку).
- *Термінологія та визначення* (визначення та термінологія, які використовуються в законодавстві, можуть помітно відрізнятися в різних країнах, що може впливати на сприйняття та застосування відповідних 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 протидії, такі як освіта та популяризація безпеки в мережі Інтернет).

Узагальнюючи розглянуті вище організаційно-технічні напрями з протидії сучасним фішинговим атакам, можна сформувати деякі рекомендації, щодо комплексного захисту від даного типу загроз безпеки та завчасного виключення передумов їх реалізації для користувачів сучасних ІС, у вигляді послідовного алгоритму відповідних дій (*див. табл. 5*).

В цілому, обидва сегменти користувачів мають спільну потребу в постійному контролі (*в т.ч. аудиті*) і вдосконаленні чинних заходів безпеки, оновленні стратегій захисту (*ПІБ для умов корпоративного сегменту*) відповідно до нових загроз та сприянні у вдосконаленні загальної «культури» кібербезпеки. Реалізація цих заходів сприятиме створенню безпечного інформаційного простору, з одного боку, та формування необхідних умов відповідності діючих стандартів кібербезпеки, з іншої сторони, одночасно для обох сегментів користувачів.

У контексті аналізу взаємопов'язаної генези розвитку ІТ технологій та збільшення масштабів й кількості фішингових атак [6], проведено прогнозний огляд подальшої еволюції методів їх здійснення. В цілому, цій процес передбачає врахування цілої сукупності взаємозалежних аспектів, включаючи: - технологічні інновації, соціокультурні тренди, медійний пресинг (*тобто неявне, свідоме нав'язування «нової» парадигми суспільних взаємовідносин у кіберпросторі*) та впровадження нових заходів безпеки та/чи нових норм безпекових рефлексій з боку пересічних користувачів.

Серед основних чинників збільшення фішингових атак слід виділити наступні:

1) *Стрімкий розвиток AI та машинного навчання (ML)* – є 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 [5-6] 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 (*Monero* або *Zcash*).

Таблиця 5 – Інтегровані рекомендації, щодо комплексної протидії фішингу
Table 5 – Recommendations on comprehensive countermeasures against phishing

Умовні кроки	**Сегменти IT-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, тести на проникнення (*penetration testing*))	*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 виявлення аномальної мережевої активності)	*Активна перевірка автентичності електронних листів*
4	*Використання систем фільтрації електронної пошти* (для блокування фішингових повідомлень)	*Активне управління паролями* (використання унікальних/різних 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 протидії прийомам *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)
8	*Співпраця та обмін інформацією* (участь у міжнародних ініціативах щодо обміну досвідом боротьби з фішингом)	*Регулярна перевірка фінансових операцій (відповідних log- файлів)* на предмет підозрілої фінансової активності
9	*Розробка кризового плану* (тобто дій, що регламентують перелік кроків для реагування на фішингові інциденти)	*Активне дотримання рекомендацій та заходів ІБ, щодо протидії останнім (новим) загрозам безпеки*
10	*Неперервне вдосконалення* діючих правил та заходів безпеки у відповідності до актуальних векторів здійснення фішингу. Удосконалення корпоративної ПІБ.	*Вдосконалення* моделі особистої мережевої поведінки та оновлення діючих параметрів засобів безпеки на основі постійного самонавчання і розширення досвіду

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 (*т. званих фішингових послуг*). Тобто, атакуючі можуть використовувати вразливості в системах *IoT* для отримання доступу до особистої інформації 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 ресурси.

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 криптографічно захищених даних, що робить фішингові атаки більш ефективними та збільшує рівень їх складності (тобто, комбінаторику можливих сценаріїв атак).

8) *Підвищення рівня доступності Інтернету* – безумовно приведе до зростання кількості користувачів мережі, що аж ніяк не буде пов'язано з посиленням рівня їх фахових компетенцій і комп'ютерної грамотності. Навпаки, ця тенденція зумовить збільшення кількість жертв для широкомасштабних фішингових атак. До прикладу, компанія «*Starlink*» надає послуги понад 1 млн. активних клієнтів у 60-ти країнах та забезпечує неконтрольований з боку національних телекомунікаційних інтеграторів, доступ до відповідного контенту, одночасно в багатьох регіонах світу [17].

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 чи доповненої реальності для охоплення нових цільових груп*) відповідно до зростання новітніх технічних інновацій.

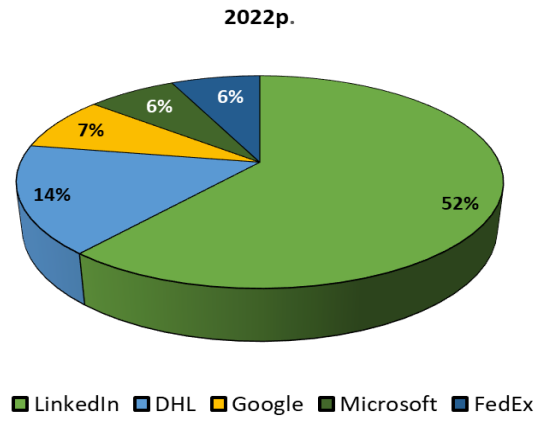

Рис. 11 – Найбільш імітовані бренди у фішингових атаках *(станом на 2022р.)*

Fig. 11 – The most imitated brands in phishing attacks *(as of 2022)*

Серед соціальних передумов прогнозованого зростання кількості фішингових атак, слід виділити наступні:

1) Масштабна цифровізація основних сфер сучасного суспільства при низьких рівнях «цифрової» компетентності – зумовлює потенційну вразливість великих груп технологічно непоінформованих користувачів *(наприклад, підлітків та осіб старшого віку)* при постійному збільшенні кількості доступних цифрових сервісів й додатків. Дана тенденція стала особливо явною з початком пандемії *COVID-19*, коли відбулось посилення дистанційних комунікацій й поширення масштабів віддаленої роботи для корпоративного сегменту користувачів. Свідченням цих процесів є відомості, стосовно розповсюдження імітованих (*тобто, навмисно емульованих*) брендів і послуг під час реалізації фішингових атак (*Рис.11*) [18].

2) Значне розповсюдження соціальних мереж – зумовлює факт найчастішого використання цих мереж, як засобу поширення фішингу. Так, кількість користувачів соціальних мереж становила 4,59 млрд. станом на 2022р., а за прогнозними оцінками їх чисельність зросте до 5,85 млрд. до 2027 року [19]. Атакуючі можуть використовувати інформацію з профілів більшої кількості користувачів для персоналізації атак та збільшення вірогідності їх успіху.

3) Підвищення ролі освіти і самоосвіти у взаємодії з цифровим середовищем – важливий аспект прогнозування сутності змін в методах і сценаріях здійснення фішингу, адже незважаючи на стале впровадження технологій *AI* та *ML (Machine Learning)*, увага користувачів послуг сучасних ІС, у порівнянні з попередніми історичними етапами розвитку фішингу (рис.1), все більше зосереджується на важливості захисту кінцевих пристроїв, як умовних «точок входу» до різноманітних хмарних сервісів й формування обачливої моделі мережевої поведінки. Свідченням цього тренду є поширення різноманітних тренінгів, курсів та онлайн семінарів, які мають на меті посилення інформування спільноти, щодо базових навиків для завчасного розпізнавання й уникнення фішингу.

4) Впровадження нових нормативно-правових актів і законів щодо запобігання фішингу – один із ключових аспектів протидії цій загрозі, що дозволяє на державному й міждержавному рівнях регламентувати правила функціонування сучасних ІС. Саме завдяки таким рішенням ефективність атак *(як превентивного засобу)* значною мірою знижується.

Наступний вагомий аспект в прогнозуванні еволюції фішингових атак, це впровадження нових технологій безпеки, серед яких насамперед слід виділити [20-21]:

1) Масштабну автоматизацію систем ІБ – впровадження методів *AI* та *ML* для оперативного виявлення й випереджального блокування найбільш ймовірних механізмів поширення фішингу. Завдяки алгоритмам аналізу поведінки користувачів та виявлення мережевих аномалій, можливе ефективне реагування на нові загрози безпеки.

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

5. Висновки

1. Протягом останніх десятиріч спостерігалася помітна еволюція фішингу, яка супроводжувалася зміною пріоритетних цілей для кіберзлочинців. Так, галузі фінансового сектору та банківської діяльності досі залишаються основним об'єктом атак, проте станом на 2020-2022рр. спостерігається зниження їх відносної частоти (інцидентів) у порівнянні з іншими галузями. Водночас, сектори електронної комерції та поштових сервісів залишаються відносно стійкими до цих атак впродовж усього історичного розвитку фішингу [21].

2. Використання технологій багатофакторної автентифікації є головним чинником поточного історичного розвитку фішингу. Використання різних автентифікаційних ознак (факторів) помітно ускладнює підміну ідентифікаційних даних користувачі послуг та сервісів сучасних ІС, що суттєво знижує «успішність» фішингу, роблячи його менш ефективним.

3. Зважаючи на специфіку фішингових атак для приватного й корпоративного сегментів користувачів, слід зазначити наступні важливі відмінності: - у корпоративному секторі ключовим є комплексний захист, що реалізується шляхом впровадження та неперервного вдосконалення діючих норм корпоративної ПІБ; - приватні користувачі мають справу з інакшою динамікою та різнорідністю загроз, а їх можливості захисту набагато більш обмежені в порівнянні з корпоративним сегментом. Таким чином, специфіку атак на різні цільові групи (сегменти) потенційних жертв варто вивчати окремо, оскільки ці групи мають суттєво різні властивості, особливості мережевої взаємодії та, відповідно, різні ризики безпеки [21-22].

4. Зв'язок між вибором цільового ресурсу і здійснюваним механізмом атаки підкреслює адаптивність застосовуваних методів впливу порушника на потенційну жертву [3], а також широку варіативність обраних способів та інструментів реалізації фішингу, відповідно до контексту й фактичних цілей (*можливо неявних на перших етапах*) атаки [22].

5. Атаки в корпоративному і приватному сегментах ІС, за всієї своєї зовнішньої схожості, спрямовані на отримання суттєво різних «бонусів», як за масштабами, так і їх субстантивністю, та використовують для цього різні вектори впливу й сценарії дій.

6. Використання комплексного підходу, щодо захисту від фішингових атак, передбачає впровадження і неперервну оптимізацію використовуваних програмно-технічних рішень безпеки у їх нерозривному взаємозв'язку із сукупністю організаційних заходів, що регламентують рівні персональної та колективної відповідальності за поточний рівень ІБ сучасних ІС.

7. Вітчизняне законодавство передбачає процедури міжнародного співробітництва, в тому числі, в частині видачі осіб, котрі були задіяні у фішингових атаках, за межі країни, а також постійно оновлюється й адаптується під соціальні і технологічні реалії сьогодення.

Список літератури

[1] Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social engineering attacks during the COVID-19 pandemic. *SN computer science*, *2*, 1-9. Retrieved from: https://link.springer.com/article/10.1007/s42979-020-00443-1

[2] Колованова, Є. П., Малахов, С. В., & Чорна, Т. Е. (2023, July). Передумови та основні складові з протидії доксінгу персональних даних. In *The 27th International scientific and practical conference "Trends of young scientists regarding the development of science"(July 11–14, 2023) Edmonton, Canada. International Science Group. 2023. 225 p.* (p. 194). Вилучено з: http://surl.li/otbbx

[3] Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*, (1), 50-59. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/17435/16040

[4] IBM. (2023). Security X-Force Threat Intelligence Index 2023 Full Report. https://www.ibm.com/downloads/cas/DB4GL8YM

[5] Даркнет (теневой интернет, DarkNet). (2023). TADVISER. Вилучено з http://surl.li/owlss

[6] Лєсная, Ю. Є., Малахов, С. В., & Мелкозьорова, О. М. (2023, November). АНАЛІЗ РЕГІОНАЛЬНИХ ТА ГАЛУЗЕВИХ ВІДМІННОСТЕЙ ПРИ РЕАЛІЗАЦІЇ ФІШИНГОВИХ АТАК. In *The 8th International scientific and practical conference "Distance learning in universities and modern problems"(November 07-10, 2023) Budapest, Hungary. International Science Group. 2023. 314 p.* (p. 289). Вилучено з: https://isg-konf.com/wp-content/uploads/2023/11/DISTANCE-LEARNING-IN-UNIVERSITIES-AND-MODERN-PROBLEMS.pdf

[7] Saqib, I. (2023). Comparison Of Different Firewalls Performance In A Virtual For Cloud Data Center. *Journal of Advancement in Computing*, *1*(1), 21-28. Retrieved from: https://journalsriuf.com/index.php/JAC/article/view/49/59

[8] Putri, H. A., Djibran, N., & Tulloh, R. (2023). Implementation Of Next-Generation Firewalls To Protect Applications From Malware Attacks. *Jurnal Indonesia Sosial Teknologi*, *4*(11), 1961-1970. Retrieved from: https://jist.publikasiindonesia.id/index.php/jist/article/view/797/1393

[9] Prasetia, B. A., Ramadhany, D. A., Guniawan, G., & Waluyo, I. G. (2023). Analisa Perangkat Fortinet Sebagai Firewall Untuk Memblokir Aplikasi Sosial Media Dan Platform Streaming Saat Jam Kerja (Studi Kasus: PT. Aplikanusa Lintasarta). *BINER: Jurnal Ilmu Komputer, Teknik dan Multimedia*, *1*(3), 496-504. Retrieved from: https://www.journal.mediapublikasi.id/index.php/Biner/article/view/3062/1667

[10] Dieterich, A., Schopp, M., Stiemert, L., Steininger, C., & Pöhn, D. (2023). Evaluation of Persistence Methods Used by Malware on Microsoft Windows Systems. Retrieved from: https://www.scitepress.org/Papers/2023/117102/117102.pdf

[11] Kremer, R., Wudali, P. N., Momiyama, S., Araki, T., Furukawa, J., Elovici, Y., & Shabtai, A. (2023). IC-SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response. *arXiv preprint arXiv:2311.03825*. Retrieved from: https://arxiv.org/pdf/2311.03825.pdf

[12] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2), 2272358. Retrieved from: https://doi.org/10.1080/23311916.2023.2272358

[13] Ghose, N., Gupta, K., Lazos, L., Li, M., Xu, Z., & Li, J. (2023). ZITA: Zero-Interaction Two-Factor Authentication using Contact Traces and In-band Proximity Verification. *IEEE Transactions on Mobile Computing*. Retrieved from: https://cse.unl.edu/~nghose/pubs/journal/GHOSE_TMC_2023-main.pdf

[14] Šuškalo, D., Morić, Z., Redžepagić, J., & Regvart, D. (2023). COMPARATIVE ANALYSIS OF IBM QRADAR AND WAZUH FOR SECURITY INFORMATION AND EVENT MANAGEMENT. *Annals of DAAAM & Proceedings*, *34*. Retrieved from: http://surl.li/ozagr

[15] Ashiq, M. I., Li, W., Fiebig, T., & Chung, T. (2023). You've Got Report: Measurement and Security Implications of {DMARC} Reporting. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4123-4137). Retrieved from: https://www.usenix.org/system/files/usenixsecurity23-ashiq.pdf

[16] Вдовенко, С., Даник, Ю., & Фараон, С. (2019). Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*, (1), 18-30. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/13080/12378

[17] *Starlink internet: Coverage & availability map | broadbandnow*. (б. д.). BroadbandNow. https://broadbandnow.com/starlink

[18] *The latest phishing statistics (updated december 2023) | AAG IT support*. (б. д.). AAG IT Services. https://aag-it.com/the-latest-phishing-statistics/

[19] *Statista - the statistics portal*. (б. д.-а). Statista. https://www.statista.com/markets/424/topic/540/social-media-user-generated-content/#statistic1

[20] Михайленко, Д. Д., & Нємцев, М. О. (2023, May). ОСОБЛИВОСТІ ТЕХНОЛОГІЇ МЕРЕЖЕВИХ ПАСТОК ЯК ІНСТРУМЕНТУ АКТИВНОГО ЗАХИСТУ ТА АНАЛІЗУ ДІЙ АТАКУЮЧОЇ СТОРОНИ. In *The 21th International scientific and practical conference "Scientists and methods of using modern technologies"(May 30–June 02, 2023) Melbourne, Australia. International Science Group. 2023. 522 p.* (p. 483). Вилучено з: http://surl.li/otbvt

[21] Лєсная Ю. Є. Аналіз структури фішингових атак та дослідження механізмів їх реалізації в корпоративному й приватному сегментах користувачів сучасних інформаційних систем. Пояснювальна записка до дипломної роботи магістра: напрям підготовки 125 – Кібербезпека / Ю. Є. Лєсная; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2023. – 69 с.

[22] Лєсная, Ю., Малахов, С. Узагальнення основних передумов реалізації фішингових атак. Proceedings of the XVII International Scientific and Practical Conference. Ankara, Turkey. 2023. Pp.453-457. Вилучено з: URL: https://isg-konf.com/wp-content/uploads/2023/05/SYSTEM-ANALYSIS-AND-INTELLIGENT-SYSTEMS-FOR-MANAGEMENT.pdf

Received: on October 2023. **Accepted**: on November 2023.

Authors:
Yuliia Liesnaia, CSD Student (magistrate), Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Ukraine.
E-mail: xa12284109@student.karazin.ua

Serhii Malakhov, Ph.D., Senior Researcher, Computer Science Department, V. N. Karazin Kharkiv National University, Ukraine.
ORCID ID https://orcid.org/0000-0001-8826-1616
E-mail: malakhov@karazin.ua

The analysis of development, typical objectives, and mechanisms of phishing attacks.

Abstract. The work discusses the issues of phishing attacks, emphasizing the interconnection between the stages of information technology development and the periods of phishing evolution. Attention is drawn to the fact that any new communication resource or online technology significantly expands the range of possible social engineering techniques, a key element of modern phishing. Based on a review of known incidents, it is asserted that this type of attack will continue to proliferate. The main factors contributing to the further growth of phishing include: -active implementation of artificial intelligence and Internet of Things technologies; -proliferation of satellite Internet; -persistent increase in the number of network users; -technological rivalry among major actors in the post-industrial world. It is emphasized that the increased accessibility of the global Internet will lead to a rise in the number of users of new communication services and platforms. However, the widespread digitization of modern society, coupled with low levels of digital literacy in certain social strata, will result in potential vulnerabilities for large groups of technologically uninformed users. The simultaneous existence of these two trends will increase the number of potential phishing attack victims in the future. It is highlighted that integrating phishing with other types of cyberattacks increases the overall incidence of phishing. The significant prevalence of social networks is noted as a major means of phishing dissemination. The conclusion is drawn that phishing attacks in corporate and private segments of modern information systems, despite their external similarities, aim to obtain substantially different "bonuses" in terms of scale, consequences, and substantive actions. These implicit differences determine the variations in impact vectors and attacking scenarios. Special attention is given to the use of multi-factor authentication, which significantly complicates the impersonation of user identification data, making phishing less effective. It is noted that implementing comprehensive protection against phishing attacks involves continuous improvement of existing security technologies in conjunction with organizational measures. The organizational component should clearly regulate the levels of personal and collective responsibility for the current security status of the utilized systems and information resources.

Keywords*: Phishing, Attack, Resource, Information Security, Social Engineering, DNS.*