ISSN 2519-2310

CS&CS Journal

KARAZIN UNIVERSITY
CLASSICS AHEAD OF TIME

1(23)2023

COMPUTER SCIENCE AND CYBERSECURITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

ISSN 2519-2310

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 1(23) 2023

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information-communication systems and information security question based, on advanced mathematical methods, information technologies and technical means.

The journal is published every six months.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (December 25, 2023, Protocol No.23).

The journal has Digital Object Identifier: **10.26565/2519-2310** (Online).

Editorial office:
V.N. Karazin Kharkiv National University
Svobody Sq., 6, office 315a, Kharkiv, 61022, Ukraine *(North building of University, 3th floor)*

E-mail: *cscsjournal@karazin.ua*
Web-page: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

В журналі публікуються наукові статті з теоретичних і науково-технічних проблем, що пов'язані зі створенням ефективних засобів комп'ютерних інформаційно-комунікаційних систем та питань захисту інформації, на основі передових математичних методів, інформаційних технологій і технічних засобів.

Журнал виходить кожні півроку.
Схвалено до розміщення в мережі Інтернет Вченою радою Харківського національного університету імені В.Н. Каразіна (25.12.2023 р., Протокол № 23).

ISSN (Онлайн): **10.26565/2519-2310**.

Редакція:
Харківський національний університет імені В.Н. Каразіна
пл. Свободи, 6, офіс 315а, Харків, 61022, Україна *(Північний корпус університету, 3 поверх)*

Електронна пошта: *cscsjournal@karazin.ua*
Веб-сторінка: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Опубліковані статті пройшли внутрішнє та зовнішнє рецензування.

ЗМІСТ
TABLE OF CONTENTS

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-

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.

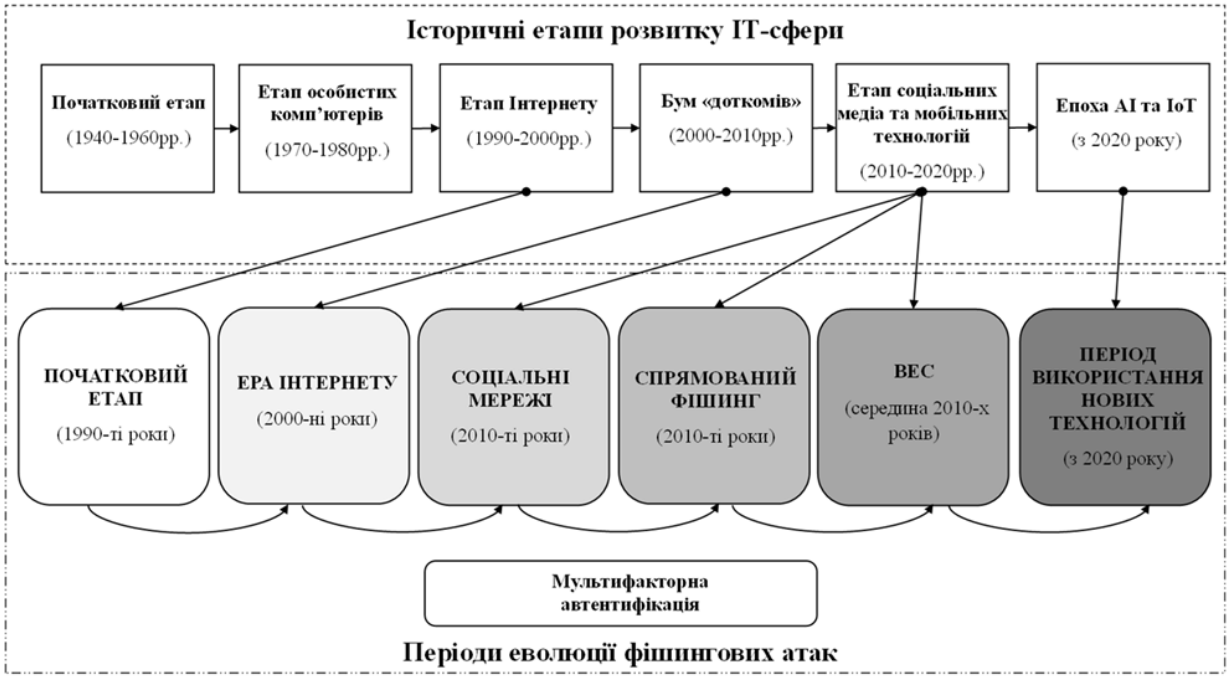


Рис. 1 – Взаємозв'язок між етапами еволюції інформаційних технологій та етапами розвитку фішингових атак

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].

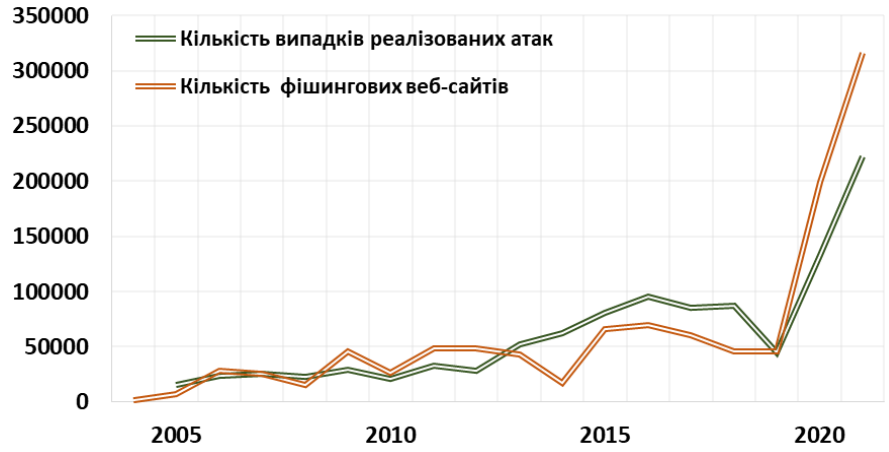


Рис. 2 – Узагальнення щорічних оглядів стосовно частки фішингових атак

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].

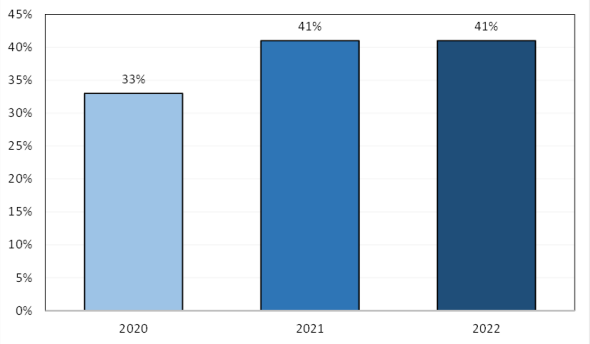


Рис. 3 – Питома частка фішингових атак *(серед інших)* станом на 2022 р

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.

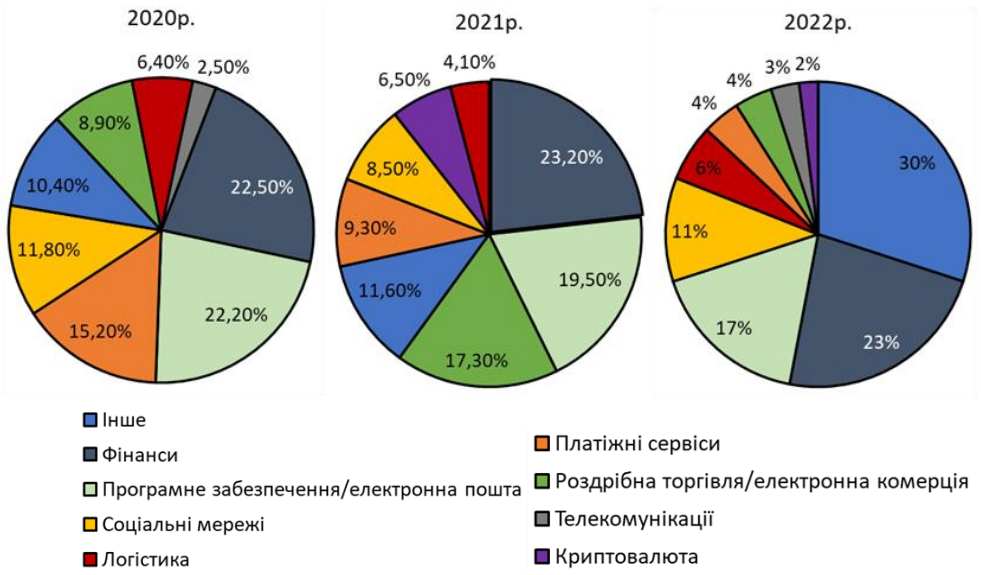


Рис. 5 - Галузеві відмінності при реалізації фішингових атак *(на 4-й квартал 2020-2022 рр.)*
Fig. 5 - Industry differences in the implementation of phishing attacks *(for the 4th quarter of 2020-2022)*

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.

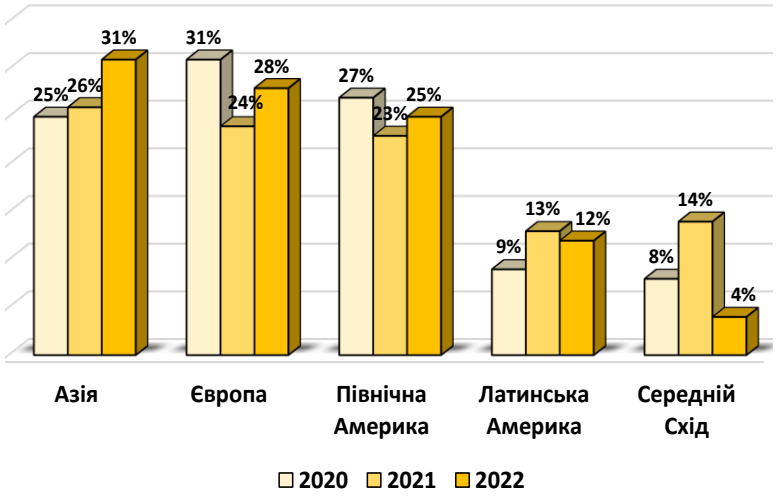


Рис. 6 – Регіональні відмінності кількості фішинг атак *(станом на 2020-2023 рр.)*

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*).

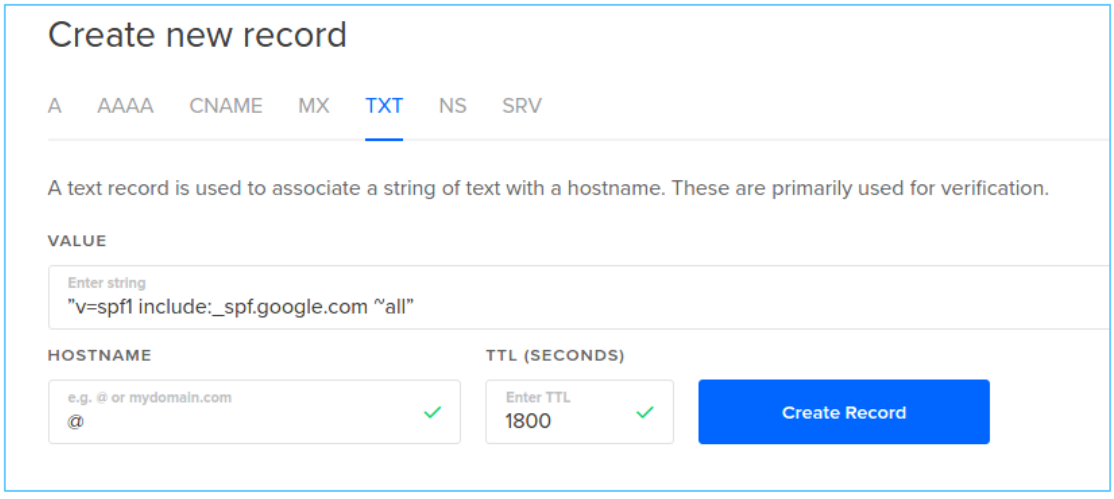


Рис. 8 – Приклад характерного *DNS*-запису «*SPF*»
Fig. 8 – An example of a characteristic DNS record «*SPF*»

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.

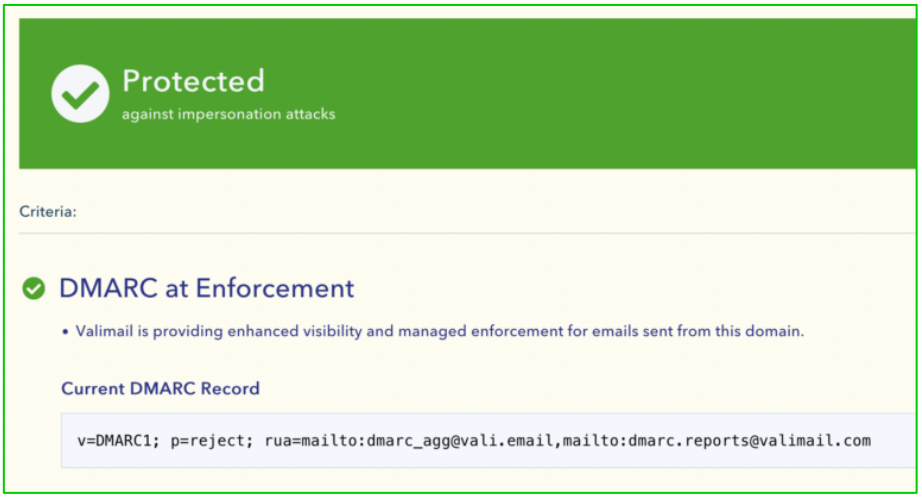


Рис. 10 – Приклад *DMARC*-запису в режимі *«Reject»*
Fig. 10 – An example of *DMARC* entry in *«Reject»* mode

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.

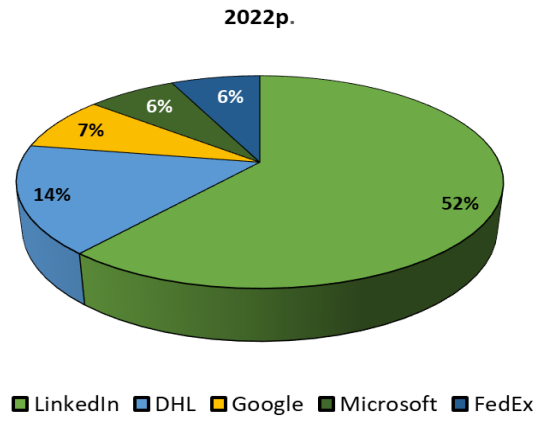


Рис. 11 – Найбільш імітовані бренди у фішингових атаках *(станом на 2022р.)*

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.*

UDC 004.056.5

A SHORT SURVEY OF THE CAPABILITIES OF NEXT GENERATION FIREWALLS

Sichkar Mykhailo, Pavlova Larysa

V.N. Karazin National University, Kharkiv, 61022, Ukraine
sichkar2020kb13@student.karazin.ua, l.v.pavlova@karazin.ua

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

Abstract: *This article examines the history, types, capabilities, and advantages of next-generation firewall (NGFW) technology. Firewalls are an important tool for protecting network resources from various information security threats. With the development of technology and the changing nature of attacks, especially those involving artificial intelligence, firewalls have also evolved, acquiring new functions and capabilities. This work provides a short survey of the main types, capabilities and benefits of next-generation firewall (NGFW) technology, which is a modern solution for comprehensive network protection against complex and sophisticated security threats. The work also analyzes the distinct features of NGFW and differences between NGFW and previous generations of firewalls, as well as examples of NGFW from well-known vendors that dominate the market, such as Palo Alto Networks, Fortinet and Cisco. The article highlights the main trends, prospects for the development and implementation of NGFW, including the impact of artificial intelligence, machine learning, cloud technologies and the Internet of Things, advantages and disadvantages, capabilities, important aspects, purpose and sphere of application. The article also addresses the significant impact this technology will have on network security. It is emphasized that the introduction of NGFW does not replace other security technologies and tools, but effectively expands the existing arsenal of countering new security threats (primarily as an instrument of proactive countermeasures and rapid response to complex network incidents). The article may be useful for students, researchers, and information security professionals who seek to expand their competencies related to the development of modern firewall technologies and their capabilities.*

Keywords*: NGFW, Firewalls, Information Security, Cybersecurity, Malware.*

1. Introduction

Ensuring the security of modern computer networks is one of the most important aspects of information security (IS), as both the number and complexity of computer threats are increasing every day. Amidst the measures and activities used to counteract the modern cyber attacks, firewalls are undoubtedly one of the most powerful tools for protecting network resources from a number of different threats [1-6]. They provide the ability to administer network access, effectively filter network traffic, and timely detect and block potentially dangerous network activity [7-8, 5].

2. Main part

A firewall is a network security tool that controls and administers incoming and outgoing network traffic and determines whether to allow or block specific traffic based on a set of security rules. Firewalls have been acting as a conditional "first line of defense" in the field of network security for more than 25 years. They establish a kind of barrier between secure and controlled internal networks and untrusted, i.e. "external" to the controlled resources, networks and/or their users. In general, a firewall can be: - hardware, software, software as a service (*SaaS*), public-cloud or private-cloud (*virtual*) [9]. To understand the principles of functioning of different types of firewalls, it is important to realize their place and role at the appropriate levels of the OSI model [10].

The evolution of firewall filtering technologies. 1988 - the first generation, packet filtering firewalls; 1989 - the second generation, the so-called "Stateful Firewall"; 1991 - the third generation, the appliance-level firewall; 2004 - IDC (International Data Corporation) introduces the term "Unified Threat Management" (UTM); 2009 - Gartner defines the next-generation firewall (NGFW) [11].

In 1988, the Digital Equipment Corporation (*DEC*) introduced the first generation of internetwork traffic filtering technology called the Packet-Filter Firewall [12]. These firewalls analyzed

packets of information that circulated between computers on the network. If a packet did not meet the rules of the packet filtering firewall, it was rejected. Packets that met the filtering criteria were allowed to be transmitted. The filtering rules were based on various parameters, such as: source and destination addresses, protocols used, and port numbers on both of the communicating computers. It is important to note that this type of firewall did not take into account the connection state of the packet and did not store its state. Because of this, it was called *«Stateless Firewalls»*. They functioned at the network layer of the OSI model and were also known as *«Network Layer Firewalls»* [10].

In 1989, AT&T Bell Labs first developed a second-generation firewall technology called Circuit Level Gateway, which was the first to introduce firewall, known as *Stateful Firewall*. *Stateful Firewall* keeps track of active network sessions and connection states. These firewalls use information about the state of the connection to control the packet filtering process. If a packet that is to be transmitted does not match an active connection, it is evaluated against a set of filtering rules that are set up for creating new connections. *Stateful Firewalls*, once a connection is established, transmit only packets that are associated with the connections specified in the dynamic state tables. Sessions stored in these tables are automatically closed if there has been no data transmission for a certain time interval to prevent state tables from overflowing. *Stateful Firewalls* are the second type of network-level firewalls, but they also function at a transport layer [10].

In 1991, Digital Equipment Corporation introduced the 3rd generation of firewall technology (*SEAL - Secure External Access Link*), which was called the *«Application Layer Firewall»*. These firewalls operate at the *OSI* application layer [10], and their main goal is to protect computers from malicious software. Thus, application-level firewalls (*Gauntlet by Trusted Information Systems and FireWall-1 by Check Point in 1994*) control the traffic of applications, such as web browsers and others, that connect to the Internet and/or other "external networks" and transmit or receive data from them. It also regulates traffic on the FTP, Telnet, and HTTP protocols [7,10].

In 2004, IDC introduced a new term - Unified Threat Management (*UTM*). Under the new terminology, the evolution of traditional (*i.e., previous models*) firewalls should be viewed as an attempt to create a new integrated solution for network security. UTM involves the simultaneous use of technologies such as a network firewall, web page filtering, gateway antivirus, intrusion prevention system (*IPS*), anti-spam, VPN, etc. [7,10].

In 2009, Gartner introduced the concept of «Next-Generation FireWall» (*NGFW*). The *NG* firewall simultaneously uses the concepts of a traditional firewall and some new technologies: – IPS, Deep Packet Inspection (*DPI*), sandboxing, application control, URL filtering, protection against complex/integrated malware, network profiling, identity policy, VPN, etc. At the same time, the most distinctive feature of NGFW is the *DPI* function at the application level, not only within the framework of port and protocol inspection, which was typical for previous solutions [10,13].

In this way, software and hardware NGFWs combine the functions of a traditional firewall and an intrusion prevention system. The use of such software and hardware NGFWs helps to increase the level of security of network traffic.

Let us briefly consider the key features and benefits of NGFW solutions (Fig. 1).

Capabilities.

1. Analyzing and filtering traffic not just by port, but at the application level.

2. Implementing IPS, which allows blocking unwanted traffic in a timely manner or disconnect part of the network to prevent the spread of the threat.

3. DPI, which analyzes the smallest details of data packets, including the data sender and receiver.

4. Supporting application traffic control lists.

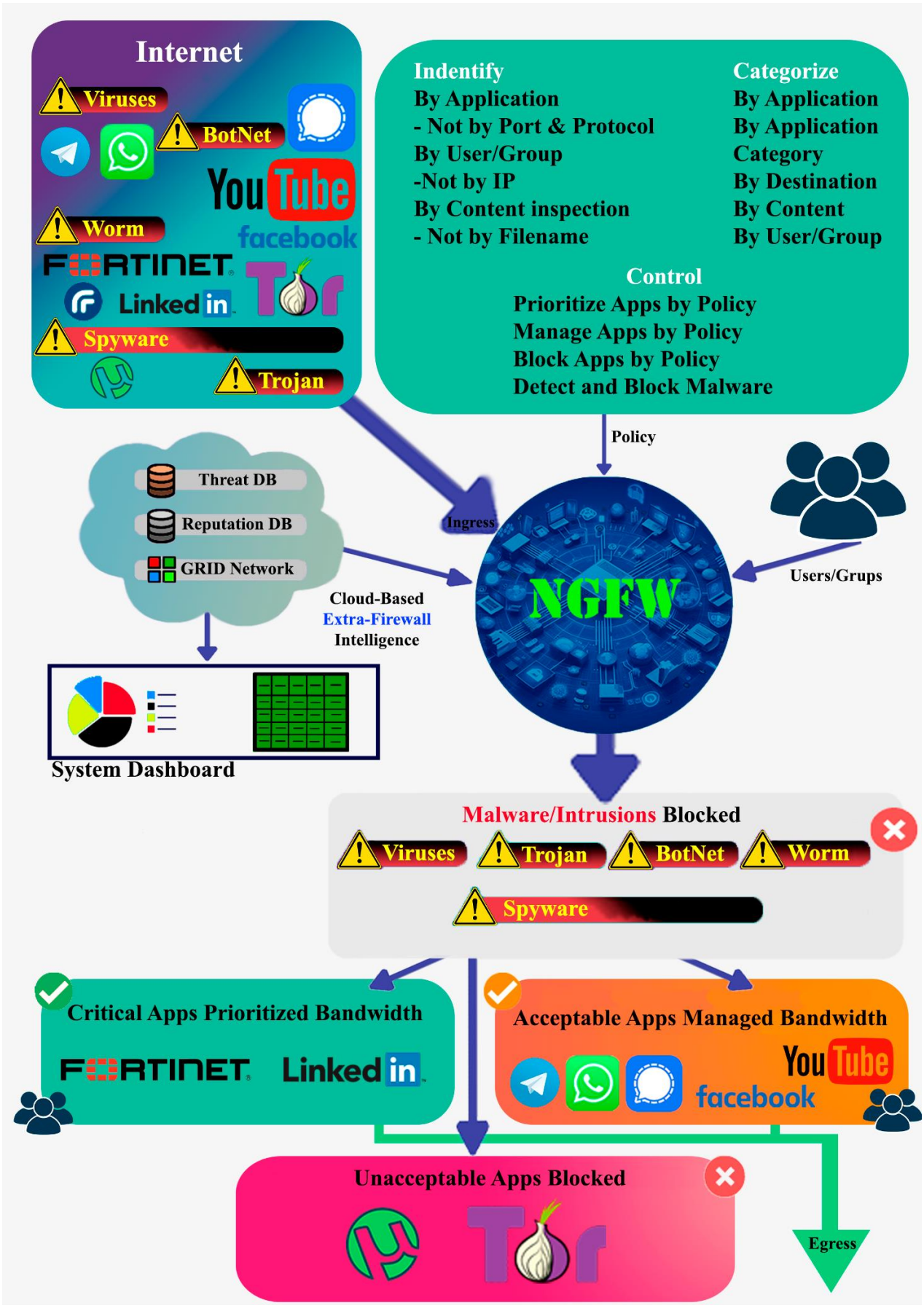


Fig. 1 - Generalized interpretation of the NGFW concept

5. Implementing a centralized network management console that simplifies network configuration and monitoring.

Benefits.

1. Increased performance: - is achieved through the use of DPI, which allows identifying and managing applications regardless of their IP port.

2. Multifunctionality: - as the result of integrating IDS and IPS systems that detect attacks based on network behavior analysis (*NBA*), threat signatures, and anomalous activity, while retaining all the functions of traditional firewalls. That provides for in-depth inspection of network traffic and improves filtering of the packet content at the application level.

3. Content filtering: - the ability to filter content is very useful for preventing unauthorized data leakage in real time.

4. Visibility and manageability makes it possible for security administrators to control the network and to identify users. Integration with third-party user directories makes it easier to control and identify users and groups.

5. Prevention and mitigation of the effects of security threats: - antivirus and anti-malware software that is automatically updated whenever new security threats appear [14]. Also, it is possible to restrict the running applications by checking them for potential vulnerabilities [2,6].

6. Advanced security policy control provides a detailed level of control over applications, blocking negative aspects of their operation (*for example, excessive traffic during peak times*).

7. Low cost: as the result of deep integration of several solutions under the control of a single management console [15].

Solutions based on NGFW technology are offered by most large companies, such as: Palo Alto Networks Fortinet, Cisco and others [6,13], where each of them offers a wide range of functions and capabilities to protect against various threats (network security gateways). Common security features are: *firewall protection; IPS; URL filtering; malware protection; DLP; identity matching (IDP); role-based access control (RBAC); content control. In general, such solutions are used in the following areas: large organizations and government agencies; small and medium-sized enterprises; banks and financial institutions; ordinary organizations and businesses* [5-8,13].

For example, Palo Alto Networks offers NGFWs for different enterprise environments and in several variants: physical, virtual, and containerized. Physical firewalls are hardware devices that are directly installed in a data center or office. Virtual solutions are software products that can run on virtual machines, and container solutions are specially designed products for protecting container environments. For enhanced performance, Panorama is a configuration and policy management solution that allows network security administrators to centrally manage all Palo Alto firewalls, regardless of type and/or location. That allows network security administrators to create and edit security policies easily [16].

Fortinet's solutions are available in several variants, including physical, virtual, and containerized. The proprietary FortiOS operating system supports unified policy configuration, enabling network administrators to manage all policies, including access to Zero Trust Networks (*ZTNA*). FortiGuard security services are available to Fortigate users, providing such features as IP geotracking and IoT device detection. The cloud sandbox feature addresses potential security threats (*e.g., the so-called "zero-day"* [2]).

FortiGuard's capabilities allow monitoring specific device and network policies, including operational technology policies, and its *IPS* accesses threat signature libraries and uses artificial intelligence and machine learning (*AI/LM*) capabilities to block these threats based on existing IPS rules. Fortigate is a versatile NGFW solution that is suitable for businesses with multiple data centers as well as single branch offices.

Thus, NGFW Fortigate has the following key differences: a wide range of deployment options and firewall bandwidth; a cloud-based sandbox; its own operating system that allows administering network security policies [15].

Cisco Secure Firewall focuses on extending policy enforcement to all distributed applications on your network, making the network infrastructure a part of the firewall security.

Cisco has several hardware firewalls (*e.g., Firepower and Meraki MX series*), and Cisco Secure Firewall (*CSF*) is available as a virtualized private cloud solution that provides protection in VMware ESXi, Microsoft Hyper-V, and KVM (*Kernel-based Virtual Machine*) environments [15]. It also exists as a public cloud solution for data and application security on Azure and AWS (*Amazon Web Services*).

Cisco's NGFW solutions use behavioral analytics to respond to threats faster, and for the log management data from all CSF firewalls in the enterprise network (*even geographically disrtibuted*) are used. Cisco Transport Layer Security (*TLS*) Server Identity and Discovery allows supporting OSI Layer 7 security policies for the encrypted traffic (TLS 1.3). In this case, network administrators have an opportunity to monitor the traffic, even if it is not decrypted, and Layer 7 security policies remaining unchanged.

Thus, Cisco's NGFW has the following key differences: - firewall log management with behavioral analytics; immutable OSI Layer 7 policies for encrypted traffic; virtual firewall with support for multiple virtual environments.

3. Conclusions

1. *NGFW* solutions have a good potential: They offer a broader range of security features than previous iterations, and they can be deployed in the cloud to detect and block malicious traffic, phishing attacks [3], denial-of-service attacks, and other security threats [2,6-8].

2. *NGFWs* use *AI* and *LM* technologies to detect both new and evolving threats [2,14], which greatly facilitates the task of countering them when they cannot be detected by traditional methods *(e.g., signature scanning).*

3. The main trends that will directly influence the development and implementation of *NGFW* include the following

- growing influence of *AI* and *LM* technologies. That is, *NGFWs* will increasingly rely on *AI* and *LM* capabilities to identify new and evolving types of security threats [2,5];
- increasing adoption of cloud technologies. *NGFWs* will increasingly gravitate towards cloud deployment, which may make them more affordable and easier to maintain and use;
- the increased scale of application and integration of modern *IS* threats. Obviously, *NGFWs* have greater potential against network bot systems that generate complex polymorphic and/or targeted malware.

References

[1] Азаров, С., Нємцев, М., & Малахов, С. Огляд аналогій та обгрунтування принципів створення демон юнітів відстеження мережевої активності користувачів. Proceedings of the XX International Scientific and Practical Conference. Graz, Austria. 2023. Pp. 447-453. https://isg-konf.com/technologies-innovative-and-modern-theories-of-scientists/

[2] Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека,* (2), 35-40. https://periodicals.karazin.ua/cscs/article/view/21039/19745

[3] 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. https://isg-konf.com/system-analysis-and-intelligent-systems-for-management/

[4] Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості інтеграції систем захисту від несанкціонованих дій в сучасних інформаційних системах. *Комп'ютерні науки та кібербезпека,* (1), 39-44. https://periodicals.karazin.ua/cscs/article/view/20912/19616

[5] Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. Proceedings of the XXI International Scientific and Practical Conference. Melbourne, Australia. 2023. Pp. 483-487. https://isg-konf.com/scientists-and-methods-of-using-modern-technologies/
[6] Погоріла К.В., Богданова Є.С., Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 07.10.2022 р. / МЦНД. – Вінниця: Європейська наукова платформа, 2022. - 142 с. DOI 10.36074/mcnd-07.10.2022
[7] Джон Маллери, & Джейсон Занн (2007). Безопасная сеть вашей компании. (Е. Линдеманн, пер. с англ.). – М.: НТ Пресс
[8] Рондалєв, Д., Мелкозьорова, О., & Нарєжній, О. (2019). Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS. *Комп'ютерні науки та кібербезпека,* (3), 11-21. https://periodicals.karazin.ua/cscs/article/view/15614/14707
[9] Next-Generation Firewalls. Вилучено з https://www.paloaltonetworks.com/network-security/next-generation-firewall
[10] Who Invented the Firewall? History, Types, and Generations of Firewall. (2023). Вилучено з https://www.thepcinsider.com/who-invented-firewall-history-evolution-types-generations/
[11] What Is a Firewall? Вилучено з https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
[12] 8 Types of Firewalls: Know Which One Is Best for Your Network By John Villanueva. (2022). Вилучено з https://techgenix.com/types-of-firewalls
[13] Information Technology Gartner Glossary. Вилучено з https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws
[14] Яремчук, К., Воскобойников, Д., & Мелкозьорова , О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та кібербезпека,* (2), 28-34. https://periodicals.karazin.ua/cscs/article/view/21038/19744
[15] What is a Next-Generation Firewall (NGFW)? Вилучено з https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall
[16] Top Next Next-Generation Firewall (NGFW) Software (2022). Вилучено з https://www.cioinsight.com/security/ngfw-software/#What-is-a-next-generation-firewall.

Надійшла: Жовтень 2023. **Прийнята**: Листопад 2023.

Автори:
Михайло Січкар, студент факультету комп'ютерних наук (бакалавріат), Харківський національний університет імені В.Н. Каразіна, Україна.
E-mail: sichkar2020kb13@student.karazin.ua

Лариса Павлова, ст. викладач кафедри іноземних мов професійного спрямування, факультет іноземних мов, Харківський національний університет імені В.Н. Каразіна, Україна.
ORCID ID https://orcid.org/0000-0002-5854-4209
E-mail: l.v.pavlova@karazin.ua

Бліц-огляд можливостей міжмережевих екранів покоління NG (*Next-Generation*).

Анотація. У рамках цієї роботи коротко розглядається історія, типи, можливості та переваги технології брандмауерів наступного покоління (*NGFW*). Брандмауери є важливим засобом захисту мережевих ресурсів від різноманітних загроз інформаційній безпеці. З розвитком технологій і зміною характеру атак, особливо тих, що включають штучний інтелект, брандмауери також еволюціонували, набуваючи нових функцій і можливостей. У межах цієї роботи представлений короткий огляд основних типів, можливостей та переваг технології брандмауерів наступного покоління *NGFW*, яка є сучасним рішенням для комплексного захисту мережі від складних і комплексних загроз безпеки. У статті, також, аналізуються особливості та відмінності *NGFW* від брандмауерів попередніх поколінь, а також приклади *NGFW* від відомих вендорів, які займають основну частину ринку, таких як *Palo Alto Networks, Fortinet* та *Cisco*. У статті висвітлено основні тенденції, перспективи розвитку та впровадження *NGFW*, зокрема вплив штучного інтелекту, машинного навчання, хмарних технологій та Інтернету речей, переваги та недоліки можливості, важливі аспекти, призначення та галузь використання. У роботі також йдеться про те, який значний слід залишить ця технологія у проблематиці мережевої безпеки. Підкреслено, що впровадження *NGFW* не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (насамперед як інструмент проактивної протидії та швидкого реагування на складні мережеві інциденти). Стаття може бути корисною для студентів, науковців та фахівців з інформаційної безпеки, які прагнуть розширити рівень своїх компетенцій, пов'язаних із розробкою сучасних технологій міжмережевого захисту та їх можливостей.

Ключові слова: *NGFW, брандмауер, інформаційна безпека, кібербезпека, зловмисне програмне забезпечення.*

УДК 004.056.5

ПОРІВНЯЛЬНА ОЦІНКА СИСТЕМ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

Олександр Пелюх[1], Марина Єсіна[1,2], Дмитро Голубничий[2]

[1]Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
oleksandrpelyukh@gmail.com, m.v.yesina@karazin.ua
[2]АТ «ІІТ», вулиця Коломенська, 15, Харків, 61166, Україна
goldim1971@gmail.com

Надійшла: жовтень 2023. Прийнята: листопад 2023.

Анотація: *В умовах сучасного світу кіберзагрози стають серйозною проблемою для компаній у всіх професійних галузях. Для всіх організацій незалежно від сфери діяльності, кіберзагрози в сучасному світі є, безперечно, вагомим викликом. Безсумнівно, сучасні організації повинні ставити перед собою завдання ефективної протидії кіберзагрозам незалежно від їхньої професійної галузі. Задля ефективного протистояння цим загрозам, організації повинні мати ефективні системи з реагування на інциденти, зокрема у кіберпросторі. У США існує безліч фреймворків з реагування на інциденти, кожен з яких має свої переваги та недоліки. Ця стаття пропонує порівняльний аналіз чотирьох провідних фреймворків з реагування на кіберінциденти в США: NIST Cybersecurity Framework (CSF), CISA Cyber Incident Response Guide, ISO/IEC 27001 та NIST Special Publication 800-61. Мета дослідження полягає в тому, щоб надати організаціям огляд чотирьох провідних фреймворків реагування на інциденти в США, аби вони могли обрати найбільш відповідний фреймворк для власних конкретних потреб. Задля проведення дослідження було використано якісний підхід, що складався з ретельного вивчення офіційних документів, перегляду релевантної сучасної літератури та консультування із фахівцями з кібербезпеки. Ця стаття є додатковим інформаційним ресурсом для організацій і компаній, які шукають дієвий та оптимальний метод реагування на інциденти, включаючи кіберпростір. Вона надає огляд чотирьох провідних фреймворків в США, що дозволяє організаціям порівняти їх переваги й недоліки, та у результаті обрати найбільш відповідний фреймворк для своїх чітких цілей.*

Ключові слова: *реагування на кіберінциденти, NIST CSF, CISA, ISO/IEC 27001, NIST SP 800-61, управління ризиками, системи безпеки.*

1. Вступ

У сучасному світі кіберзагрози є серйозною проблемою для всіх організацій, незалежно від їхньої галузі. Згідно з оцінкою *Cybersecurity Ventures*, у 2023 році глобальні щорічні витрати на кіберзлочинність сягнуть 8 трильйонів доларів США. Крім того, очікується зростання вартості збитків від кіберзлочинів, обсяг яких до 2025 року сягне 10,5 трильйонів доларів США [1]. Ця тенденція продовжуватиме зростати в міру того, як кіберзлочинці будуть розробляти все більш складні методи атак.

Щоб ефективно протистояти цим загрозам, організації повинні мати ефективні системи реагування на інциденти, зокрема у кіберпросторі. Система реагування на інциденти – це комплекс заходів, спрямованих на виявлення, реагування та усунення кіберінцидентів. Вона включає в себе наступні компоненти [2]:

- детектування – виявлення ознак кіберінциденту;
- локалізація – реагування на кіберінцидент у спосіб, що мінімізує його вплив;
- ліквідація – усунення наслідків кіберінциденту;
- відновлення – прийняття заходів для виключення повторної ймовірності виникнення кіберінциденту.

У США існує безліч фреймворків реагування на інциденти, кожен з яких має свої переваги та недоліки. Ця стаття пропонує порівняльний аналіз чотирьох провідних фреймворків реагування на інциденти в США [3-6]:

- NIST Cybersecurity Framework (CSF);

- CISA Cyber Incident Response Guide;
- ISO/IEC 27001;
- NIST Special Publication 800-61.

Мета дослідження полягає в тому, щоб надати організаціям огляд чотирьох провідних фреймворків реагування на інциденти в США, щоб вони могли обрати найбільш відповідне джерело для своїх конкретних потреб.

2. Огляд основних аспектів фреймворків

Задля проведення всебічної оцінки, необхідно ознайомитися з кожним із фреймворків більш детально й визначити їх основні аспекти.

- NIST Cybersecurity Framework (CSF)

NIST – Національний інститут стандартів і технологій при Міністерстві торгівлі США. Така концепція кібербезпеки NIST допомагає компаніям будь-якого розміру краще розуміти, управляти та зменшувати ризики кібербезпеки, а також захищати свої мережі та дані. Вона надає компанії перелік найкращих практик, які допоможуть визначити, на чому зосередити свій час і гроші для захисту кібербезпеки.

NIST CSF може бути застосована у роботі підприємства в наступних п'яти напрямках: ідентифікація, захист, виявлення, реагування та відновлення. Вона базується на загальновідомих стандартах і практиках та представляє найкращі сучасні підходи у сфері кібербезпеки [3,7]. Однак кожна організація і галузь повинні будуть визначити свої особливі теми і питання, на які слід звернути увагу. Проте більшість тем є спільними для всіх секторів.

Концепція визначає рівні, які описують міру, до якої впроваджуються вимоги (табл. 1). Ці категорії іноді називають рівнями зрілості, але, згідно з NIST, вони є скоріше інструментом для внутрішньої комунікації між управлінням ризиками кібербезпеки та управлінням операційними ризиками, і не повинні розглядатися як рівні зрілості. Проте, вищі рівні представляють вищий ступінь досконалості та зрілості в управлінні ризиками кібербезпеки та реагування на них [7].

Таблиця 1 – Рівні «зрілості» у *NIST Cybersecurity Framework*
Table 1 – «Maturity» levels in *NIST Cybersecurity Framework*

Рівень	Назва	Пояснення
1	Частковий	Неформальні практики; обмежена обізнаність; відсутність координації у сфері кібербезпеки
2	З урахуванням ризиків	Затверджені процеси та визначені пріоритети, але не впроваджені в масштабах всієї організації; існує високий рівень обізнаності, надані адекватні ресурси; неформальний обмін інформацією та координація дій.
3	Постійно оновлюваний	Офіційна політика визначає процеси управління ризиками з регулярним переглядом та оновленням; загально організаційний підхід до управління ризиками кібербезпеки з впровадженими процесами; регулярна формалізована координація.
4	Адаптивний	Практики активно адаптуються на основі отриманих уроків та прогнозних показників; кібербезпека впроваджена і є частиною культури всієї організації; активне управління ризиками та обмін інформацією.

Загалом, процес впровадження рамкової концепції від NIST можна звести до вигляду у форматі спрощеного циклу дій (рис. 1).

Рис. 1 – Схема впровадження «*NIST Cybersecurity Framework*»
Fig. 1 – «*NIST Cybersecurity Framework*» implementation scheme

- CISA Cyber Incident Response Guide

У 2021 році Агентство з кібербезпеки та безпеки інфраструктури (*CISA*) опублікувало документ з двома окремими інструкціями, спеціально призначеними для інцидентів та вразливостей. Інструкція щодо інцидентів дуже схожа на систему реагування NIST, але розбиває процес на менші частини. Інструкції щодо вразливостей також дуже схожі, але переосмислені, щоб зосередитися на проблемах, які ще не призвели до інцидентів.

Документ містить комбінацію інструментів і програмного забезпечення (ПЗ) з відкритим кодом, послуг, що пропонуються державними та приватними організаціями з кібербезпеки, а також ресурсів, які безкоштовно надає саме *CISA* [5].

Агентство спочатку рекомендує компаніям вжити базових заходів для підвищення рівня власної безпеки, включаючи впровадження циклів виправлень для усунення відомих вразливостей ПЗ, впровадження двофакторної або багатофакторної автентифікації (*2FA/MFA*), оновлення застарілого та/чи непідтримуваного ПЗ, а також оновлення стандартних або «старих» паролів. Після виконання вищезазначених кроків *CISA* рекомендує організаціям ознайомитися з додатковими категоріями.

Серед ресурсів є посилання на служби оцінки фішингу, віддалені тести на проникнення, розподілений захист від атак типу «відмова в обслуговуванні» (*DDoS*), *Project Shield*, сховища даних про загрози, антивірусні інструменти, ПЗ для аудиту випадків та служби резервного копіювання. Слід зазначити, що передбачені різні рівні кваліфікації для кожного сервісу або інструменту, які розділені на базові та більш професійні. Список CISA буде постійно оновлюватися,тому в майбутньому агентство має намір створити процес для організацій, які зможуть подавати безкоштовні інструменти та послуги на їх розгляд.

- ISO/IEC 27001

ISO/IEC 27001 – це міжнародний стандарт інформаційної безпеки (ІБ). Він встановлює специфікацію для ефективної СУІБ (*системи управління інформаційною безпекою*). Підхід ISO 27001, заснований на найкращих практиках, допомагає організаціям управляти своєю інформаційною безпекою, звертаючи увагу на людей, процеси та технології [6].

Сертифікація за стандартом ISO 27001 визнана в усьому світі і свідчить про відповідність СУІБ найкращим практикам у сфері інформаційної безпеки. Рішення про сертифікацію

приймається акредитованим органом сертифікації після успішного аудиту СУІБ організації. Стандарт ISO 27001, який є частиною серії ISO 27000, встановлює основу для створення, впровадження, функціонування, моніторингу, аналізу, підтримки та постійного вдосконалення СУІБ в організаціях.

Згідно із визначенням ISO 27001, основною метою СУІБ є захист трьох аспектів інформації [6, 8]:

- конфіденційність: тільки уповноважені особи мають право доступу до інформації;
- цілісність: тільки уповноважені особи можуть змінювати інформацію;
- доступність: інформація має бути доступною для уповноважених осіб у будь-який час, коли вона їм потрібна.

Це досягається шляхом з'ясування того, які потенційні інциденти можуть статися з інформацією (тобто, оцінки ризиків), а потім визначення того, що необхідно зробити, щоб запобігти таким інцидентам (*тобто, зменшення ризиків або їх обробки*). Таким чином, основна концепція ISO 27001 ґрунтується на процесі управління ризиками: з'ясуванні, де знаходяться ризики, а потім систематичної обробки їх шляхом впровадження засобів контролю безпеки.

- NIST Special Publication 800-61

NIST SP 800-61 – це документ, який містить керівні принципи та найкращі методи роботи з інцидентами. Він охоплює весь життєвий цикл реагування на інциденти, від підготовки та виявлення до дій після інциденту та узагальнення отриманих уроків. Він також містить рекомендації щодо політик, процедур, ролей та обов'язків, а також інструментів і методів аналізу для пом'якшення наслідків інцидентів. Стандарт ґрунтується на принципах гнучкості, масштабованості, координації та комунікації [4].

Варто зауважити, що NIST SP 800-61 надає ключові рекомендації для боротьби з кіберінцидентами (табл. 2), зокрема деталізовану схему координування дій під час інциденту ІБ.

Таблиця 2 – Ключові рекомендації *NIST Special Publication 800-61*

Table 2 – The main recommendations *NIST SP 800-61*

Рекомендація	**Пояснення**
Плануйте координацію інцидентів із зовнішніми сторонами до їх виникнення	Зовнішні сторони, такі як групи реагування на інциденти, правоохоронні органи та Інтернет провайдери, відіграють вирішальну роль у скоординованому плануванні для забезпечення ефективної комунікації та чітких обов'язків.
Проконсультуйтеся з юридичним відділом, перш ніж розпочинати будь-які зусилля з координації	Можуть існувати контракти або інші домовленості, які необхідно укласти до початку обговорення.
Здійснюйте обмін інформацією про інцидент протягом усього життєвого циклу реагування на інцидент	Обмін інформацією є життєво важливим для координації між організаціями. Не варто відкладати обмін деталями інциденту до його повного вирішення.
Намагайтеся автоматизувати якомога більшу частину процесу обміну інформацією	Ефективна міжорганізаційна координація є економічно вигідною. Слід прагнути до балансу між автоматизованим обміном інформацією та процесами управління потоками, орієнтованими на людину.
Збалансуйте переваги обміну інформацією з недоліками обміну конфіденційною інформацією	Тільки важлива інформація має бути надана потрібним сторонам. Деталі впливу на бізнес у командах, технічна інформація в цілому та зосередження на технічних деталях з організаціями-партнерами.
Діліться якомога більшою кількістю відповідної інформації про інцидент з іншими організаціями	Організації повинні вирішити, якою технічною інформацією ділитися. Зовнішні показники, такі як характеристики атак, зазвичай безпечні, але деталі використаних вразливостей можуть бути приховані з міркувань безпеки та відповідальності.

У цілому, чотири розглянуті фреймворки пропонують широкий спектр рекомендацій, які можуть допомогти організаціям розробити ефективну систему реагування на інциденти.

3. Порівняльний аналіз розглянутих документів

У цьому розділі ми проведемо детальний порівняльний аналіз чотирьох розглянутих фреймворків реагування на інциденти. Розглянемо наступні аспекти:

- Цільова аудиторія

NIST CSF та NIST Special Publication 800-61 призначені для широкого загалу організацій, незалежно від їхнього розміру, галузі або рівня кібербезпеки. CISA *Cyber Incident Response Guide* призначений для організацій, які підпадають під юрисдикцію CISA. ISO/IEC 27001 призначений для організацій, які хочуть отримати сертифікацію за цим стандартом.

- Сфера застосування

NIST CSF та NIST *Special Publication 800-61* мають широку сферу застосування, яка включає в себе всі аспекти реагування на інциденти. Порівняно з ним CISA *Cyber Incident Response Guide* має більш вузьку сферу застосування, яка фокусується на практичних аспектах реагування на інциденти. А сфера застосування ISO/IEC 27001 в більшої мірі сконцентрована на управлінні ризиками та запобіганні інцидентів безпеки.

- Рівень деталізації

NIST CSF та NIST Special Publication 800-61 є високорівневими фреймворками, які пропонують загальні рекомендації щодо реагування на інциденти. CISA *Cyber Incident Response Guide* є більш детальним фреймворком, який пропонує конкретні кроки та процедури для реагування на інциденти. ISO/IEC 27001 є найдетальнішим з розглянутих документів, що пропонує детальні вимоги та рекомендації, щодо управління ризиками та запобігання інцидентам ІБ.

- Переваги та недоліки

Кожен з розглянутих фреймворків має свої сильні та слабкі сторони. NIST CSF є хорошим вибором для організацій, які шукають гнучкий і адаптивний фреймворк, який охоплює весь цикл реагування на інциденти. ISO/IEC 27001 є хорошим вибором для компаній, які шукають всеосяжну і визнану міжнародну систему управління інформаційною безпекою. CISA *Cyber Incident Response Guide* є доволі прийнятним вибором для організацій, які шукають практичні і конкретні рекомендації щодо реагування на інциденти. NIST *Special Publication 800-61* є хорошим вибором для компаній і структур, які шукають докладні і всеосяжні рекомендації щодо виявлення та реагування на інциденти. Узагальнені переваги та недоліки розглянутих документів наведені у табл. 3.

Таблиця 3 – Переваги та недоліки розглянутих документів

Table 3 – Advantages and disadvantages of the documents under consideration

Документ	Переваги	Недоліки
NIST Cybersecurity Framework	Гнучкість, індивідуалізація	Недостатня деталізація процесів
CISA Cyber Incident Response Guide	Практичні рекомендації, вільний доступ	Менш комплексний, ніж інші розглянуті фреймворки
ISO/IEC 27001	Встановлений стандарт, спрямованість на управління ризиками	Не є спеціалізованим для реагування на інциденти
NIST Special Publication 800-61	Є конкретні рекомендації і методи з реагування на інциденти	Можлива складність розуміння та реалізації деяких з процесів

Таким чином, можна стверджувати, що кожен із розглянутих фреймворків може бути корисним для організацій, які шукають ефективні системи реагування на інциденти.

Однак компанії повинні вибрати фреймворк, який відповідає їхнім конкретним потребам і цілям.

4. Висновки

У роботі надано порівняльний огляд 4-х провідних фреймворків реагування на інциденти ІБ в США. Вибір фреймворку залежить від конкретних потреб і цілей організації.

NIST Cybersecurity Framework є хорошим вибором для організацій, які шукають гнучкий і адаптивний фреймворк, який охоплює весь цикл реагування на інциденти. Він пропонує загальні рекомендації, які можуть бути адаптовані до потреб будь-якої організації.

ISO/IEC 27001 слід обирати організаціям, які шукають всеосяжну і визнану міжнародну систему управління ІБ. Він пропонує детальні вимоги та рекомендації щодо управління ризиками та запобігання інцидентам.

CISA Cyber Incident Response Guide є доволі прийнятним для компаній, які шукають практичні і конкретні рекомендації, щодо реагування на інциденти. Пропонує конкретні кроки та процедури, які можуть бути використані для реагування на кіберінциденти.

NIST Special Publication 800-61 є хорошим вибором для організацій і структур, які шукають докладні і всеосяжні рекомендації щодо виявлення та реагування на інциденти. Містить детальні рекомендації та передові методи, які можуть бути використані для підвищення ефективності реагування на інциденти.

Організації, які шукають фреймворк реагування на інциденти, повинні враховувати такі фактори:

- цільова аудиторія: фреймворк повинен відповідати потребам і цілям організації;
- сфера застосування: фреймворк повинен охоплювати всі аспекти реагування на інциденти, які є важливими для організації;
- рівень деталізації: фреймворк має бути достатньо детальним, щоб бути корисним, але не надто, аби запобігти складнощам у розуміння та реалізації.

Організації також можуть розглянути можливість використання комбінації двох або більше фреймворків. Наприклад, організація може використовувати *NIST Cybersecurity Framework* для розробки загальної стратегії реагування на інциденти, а потім використовувати *CISA Cyber Incident Response Guide* для розробки більш конкретних процедур реагування на інциденти, зокрема у кіберпросторі.

Список літератури

[1] eSentire, Inc. (2023). “2022 Official Cybercrime Report.” Retrieved (https://www.esentire.com/resources/library/2022-official-cybercrime-report).

[2] American Public Power Association. (2021). “Public Power Cyber Incident Response Playbook” Retrieved (https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook).

[3] Nist, Gaithersburg Md. (2023). The NIST Cybersecurity Framework 2.0. https://doi.org/10.6028/NIST.CSWP.29.ipd.

[4] NIST. (2021). “NIST SP 800-61 | NIST.” Retrieved (https://www.nist.gov/privacy-framework/nist-sp-800-61).

[5] Cybersecurity and Infrastructure Security Agency CISA. (2021). “CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies | CISA.” Retrieved (https://www.cisa.gov/news-events/news/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen).

[6] Information security, cybersecurity and privacy protection. Information security management systems. Requirements. ISO/IEC 27001. (2022). https://www.iso.org/standard/27001.

[7] NIST. (2023). “Cybersecurity Framework Components | NIST.” Retrieved (https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components).

[8] Kosutic, Dejan. (2023). “What Is ISO 27001? A Detailed and Straightforward Guide.”. Retrieved (https://advisera.com/27001academy/what-is-iso-27001/).

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

Authors:
Oleksandr Peliukh, student of the Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Ukraine.
E-mail: oleksandrpelyukh@gmail.com
ORCID: https://orcid.org/0000-0003-0507-0262
Maryna Yesina, Ph.D., Associate Professor, Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: m.v.yesina@karazin.ua
ORCID: https://orcid.org/0000-0002-1252-7606
Dmytro Holubnychyi, Ph.D., Associate Professor, Head of the scientific department of JSC "IIT", Kharkiv, Ukraine.
E-mail: goldim1971@gmail.com
ORCID: https://orcid.org/0000-0002-1252-7606

Comparative Assessment of US Cyber Incident Response Systems.

Abstract. In today's world, cyber threats are becoming a serious issue for companies in all professional sectors. For all organisations, regardless of their field of activity, cyber threats in today's world are undoubtedly a significant challenge. Undoubtedly, modern organisations should set themselves the task of effectively countering cyber threats regardless of their professional industry. To effectively counter these threats, organisations must have effective incident response systems in place, including in cyberspace. There are many incident response frameworks in the US, each with its own advantages and disadvantages. This article offers a comparative analysis of the four leading US cyber incident response frameworks: NIST Cybersecurity Framework (*CSF*), *CISA Cyber Incident Response Guide*, *ISO/IEC 27001* and *NIST Special Publication 800-61*. The purpose of the study is to provide organisations with an overview of the four leading incident response frameworks in the US so that they can choose the most appropriate framework for their specific needs. The research was conducted using a qualitative approach that included a thorough review of official documents, a review of relevant current literature, and consultation with cybersecurity professionals. This article is an additional informational resource for organizations and companies looking for an effective and efficient method of responding to incidents, including cyber incidents. It provides an overview of the four leading frameworks in the US, allowing organisations to compare their advantages and disadvantages and ultimately choose the most appropriate framework for their specific objectives.

Keywords: *Cyber incident response, NIST CSF, CISA, ISO/IEC 27001, NIST SP 800-61, Risk management, Security frameworks.*

UDC 621.327:621.391

IMPLEMENTATION OF THE METHOD OF ENCODING SERIES LENGTHS TO PROVIDE PROCEDURES STEGANOGRAPHIC IMAGE INSERTION

Honcharov Mykyta, Melkozerova Olha

V. N. Karazin Kharkiv National University, St. Svobody Square, 4, Kharkiv, 61022, Ukraine
m.honcharov@student.karazin.ua, olha.melkozerova@karazin.ua

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

Abstract: *The purpose of this article is to introduce the principle of encoding series lengths to provide inter-block data multiplexing of a hybrid steganoalgorithm. As part of the modeling, it is made the assumption that the attacker has successfully determined one of the two parameters of content processing: the size of the basic blocks (BB) and the implemented principle of series scanning. The modeling was performed on the example of one test halftone image of the «city» type. Samples of the attacked test image obtained for a short sample stack (length in 4 series) are presented. An analysis of the results of attack content when using different ways of smoothing the source images is carried out. The implementation of different smoothing ways allows to improve in the combinatorics of multiplexing series and the number of formed BB. It is emphasized that with an increased dimensionality of the BB, the combinatorics of the multiplex of series parameters is limited. The dimension of the BB and the way of organizing the series scanning are elements of the composite key of the data extractor. The use of the principle of encoding series lengths significantly reduces the computational complexity of the algorithm and creates conditions for the implementation of inter-block multiplexing procedures. It is concluded that the use of the parameter of series lengths destroys the correlation relations of the source data more than in the case of using only BB. The main elements at the stage of inter-block content processing are BB and their parameters of series lengths. The modeling results confirm the key role of the «series length» parameter in the procedure of legitimizing content extraction. The variability of the sampling order of the used parameters of the BB series significantly enhances the resistance of the content to unauthorized extraction attempts. Attention is drawn to the fact that the principle of encoding series lengths is limited in the background areas of images, which makes it possible to preserve highly informative image areas and determine the structure of visual artifacts. According to the modeling results, it is concluded that the use of the method of encoding series lengths in inter-block multiplexing procedures additionally strengthens the protection and complicates the work of the steganoanalyst and determines the further course of the attack.*

Keywords: *Encoding Series lengths, Steganography, Content, Hacking, Stack.*

1. Introduction

The specialists in the field of image processing are well aware of the method of series length encoding, which is differed by simplicity of realization and has a low computational complexity. Its use in video data compression systems and formats of graphic information representation allows to obtain good results when processing images with limited color or brightness palette (*grayscale images*), and/or containing extended background areas with more or less homogeneous fill [1-4].

Taking into consideration the specificity of the human visual system and the features of the method of the series lengths encoding when processing images with different statistical characteristics [1, 3-5], an assumption is made about the possibility of its use to provide procedures inter-block data multiplexing, within the framework of the chosen concept of realization of a low-resource hybrid steganoalgorithm [6]. This possibility is due to the presence of 3 important circumstances characteristic of this method: 1 - undemanding to hardware resources (*orientation on mobile gadgets*); 2 - high speed of processing (*support of real-time mode*); 3 - creation of conditions for realization of procedures of inter-block porting of parameters of series lengths, as a tool of counteraction to attempts at unauthorized extraction of content.

The procedure of inter-block multiplex of series parameters, precedes the stage coding with transform [1,4] for all base blocks (*BB*) of the image-content [6], which reduces the overall operating time of the algorithm. The inter-block data multiplex is provided by decomposing the original array of *BB* and corresponding series length values, through mutual permutations of these elements

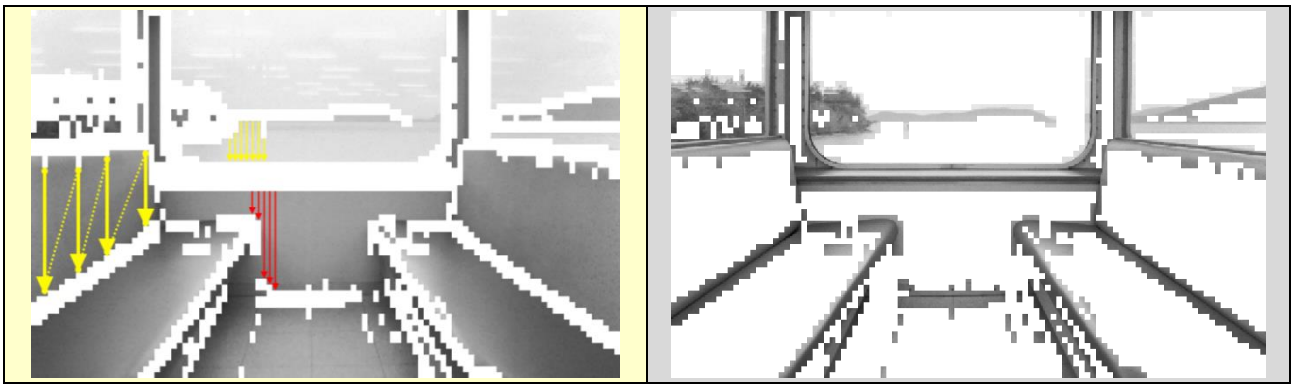
within the current combinatorics of the mixing mask. The number of formed BB depends on: - the realized way of smoothing original images and the threshold value of the difference «P_Z» between the elements of image blocks [6]; - the set dimensionality of blocks at the stage of formation of the series array [7]; - statistical characteristics and type of image-content [3-5, 8].

It is important to emphasize that in addition to the block dimensionality, the most important parameter providing legitimization of the procedure of content extraction is the way used to organize the scanning of the series. These two parameters are elements of the composite key of the data extractor and determine the order of realization of content encoding-decoding procedures at the level of inter-block processing of video data-content [6].

2. Main part

This work aims to demonstrate the possibility of implementing the series length encoding method [1-2] to provide procedures for two-level multiplexing of original data [6-7]. Multiplexing of the active parameters of the series length array provides the solution of two problems: 1 - reduces the computational complexity of the whole algorithm; 2 - counteracts attempts of illegitimate extraction of data (image-content) from the container. The way of forming series from blocks of the original image used in the modeling, is schematically represented in Fig. 1.

a) Original test image;



*b) Marking of **BB**;* *c) Marking of **All Series**;*

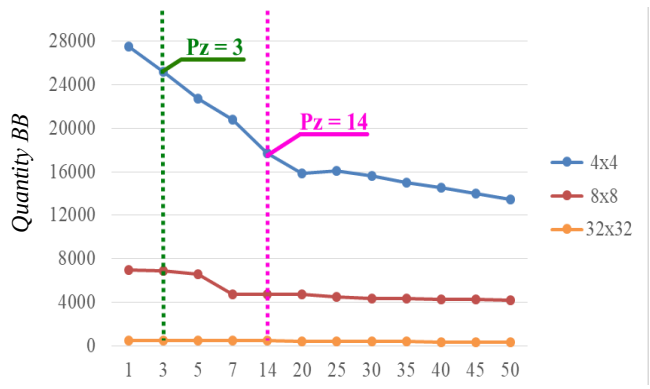
Fig. 1 - Scanning of blocks by columns and marking of the main elements of the series array (***BB*** *- white blocks on the sample (b);* ***All Series*** *- white areas on the sample (c);*
The working size of blocks - 8×8 el.)

It is schematically presented the realized scheme of blocks scanning (*by columns, from top to bottom and from left to right*) and characteristic arrangement of BB in each new series (*marked in white color, Fig. 1(b)*). In Fig. 1(c), all formed series of BB, regardless of their content, are highlighted in white color. In general, Fig. 1: - visualizes the total number of blocks to be encoded with

transformation at the next stage of the algorithm (*i.e., everything that is NOT white in Fig. 1(b)*); – allows to judge the potential combinatorics of mutual permutations of the parameter of series lengths for *BB* of size 8×8 el *(Fig. 1(c)).*

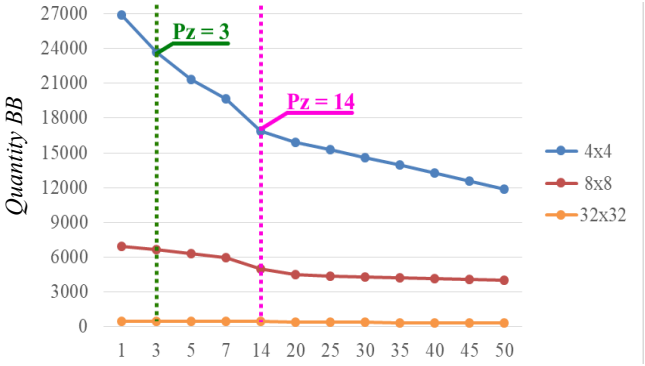
For presentation purposes of the obtained effects, the modeling results are presented on the example of one test halftone image of the type «landscape - city» (*see Fig. 2*). During the modeling process, the implementation of different variants of smoothing [6] of the original data was performed (*see Fig.5 (a-d)*). The graphs in Fig. 2 *(a, c, d)* reflect the nature of the dependence of the number of formed blocks (*respectively, and the combinatorics of permutations*) on the set values of the threshold of coarsening of the brightness of neighboring image elements *(P_Z)* and the dimensionality of the blocks themselves for different ways of smoothing the original images [5,6].

As can be seen from the presented dependences, the difference between different ways of data pre-processing practically disappears when choosing the P_Z value more than 14 brightness gradations (*dashed-cutoff P_Z = 14 in Fig. 2*).

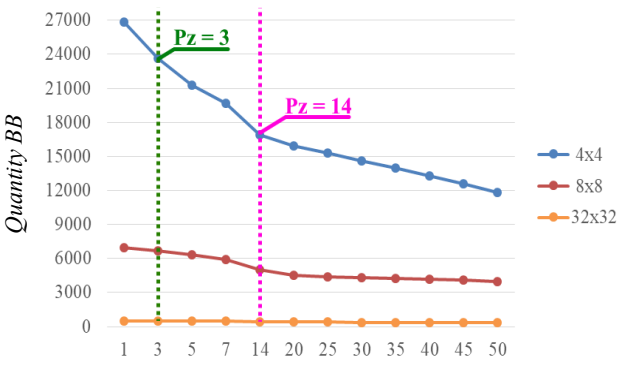


a) Number of BB without pre-processing;

b) Original test image;



c) Number of blocks for var.2 (P_Z = 3);



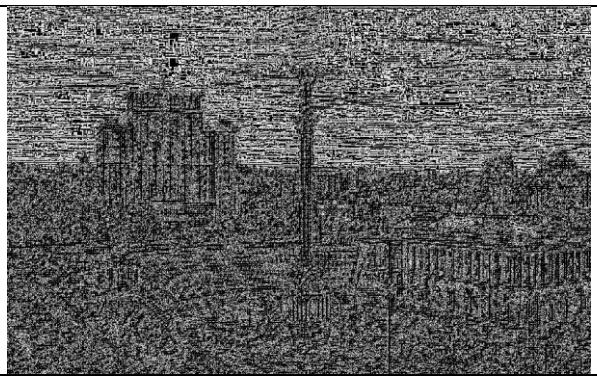
d) Number of blocks for var.3 (P_Z = 3);

Fig. 2 - Sample test image *(b)* and the number of formed blocks *(a, c, d)* for different values of P_Z, and ways of smoothing the original data.

Figs. 3-5 are presented images demonstrating the modeling results of attempts of illegitimate extraction/cracking of content on the assumption that the attacker knows only two processing parameters: - the size of the *BB* and the realized principle of scanning series [9], but he fails to determine the active parameters of the inter-block [10] data multiplex. This development of the situation predetermines three outcomes of events: 1 - incorrect determination of the valid *BB* arrangement parameter *(Fig. 3(a)); 2 - incorrect determination of the multiplex of the series length parameter (Fig. 3.c)*; 3 - mistake in determining two processing parameters at once, i.e., the *BB* and the series length parameter (*see Fig. 3(d)*). To demonstrate the characteristic structure of test image artifacts *(Fig. 3 (a, c, e))*, which are a consequence of unsuccessful content hacking, a short sampling stack *(length in 4 series)* was used. Naturally, this significantly limits the general combinatorics of per-

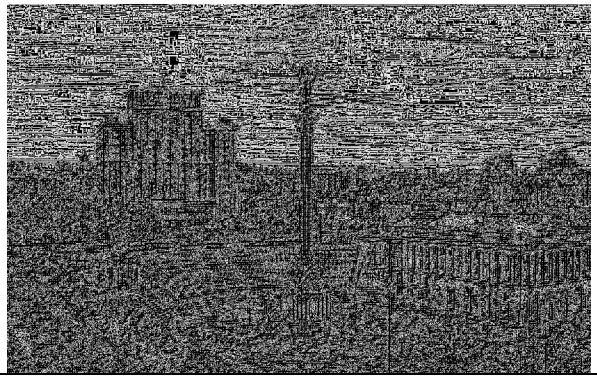
mutations of the investigated parameters, but the destruction of the original image, even on such a limited base, is more than indicative.

a) mix BB;



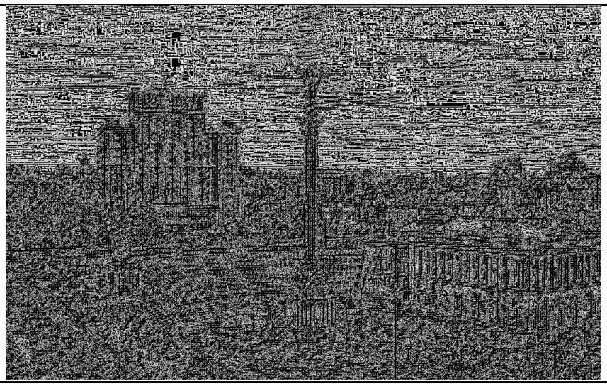
b) difference for mix BB;

c) mix Series;



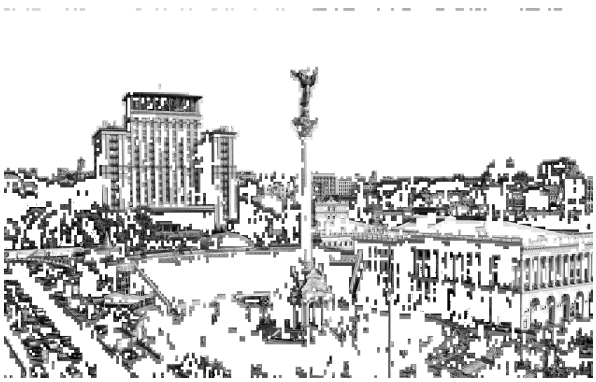
d) difference for mix Series;

e) mix BB + Series;



f) difference mix BB + Series;

g) marking BB in the original image (Fig.2(b));



h) marking Series in the original image (Fig.2(b));

Fig. 3 - Results of unsuccessful hacking of an image of the type city and visualization of artifacts for *BB* size 4×4 el. (*2nd var. processing;* $P_Z = 3$)

Naturally, the extension base of sampling will lead to a significant disruption of correlation relations between the active series *BB*. In turn, this will lead to intensification of the process of content defragmentation as a result of attempts of its unauthorized extraction [9,10].

Fig. 3*(b, d, e)* presents visualization of the difference between the original and «attacked» image-content, typical for the above three event outcomes. In this case, the darker the image fragments, the smaller the difference between the original and the obtained brightness values of their constituent elements and, accordingly, the brighter the element, the greater this difference. Samples *(g,h)* in Fig. 3 demonstrate the factual location of *BB* and their series in the test image when mistakenly selecting two parameters at once *(Fig. 3(e)). Conceptually, Fig. 3(g,h)* is similar to Fig. 1, but characterizes the situation with respect to the selected test image.

In Fig. 4 presents an enlarged fragment of the upper corner (proportional to 1/6) of the test image in Fig. 2*(b)*. The presented labeled fragments give a more detailed view of the actual location of the *BB* and their series directly in the test image (highlighted in blue color) by analogy with Fig. 1. This example vividly demonstrates the difference in the impact of the existing parameters of the *BB* series (*series length and BB content*), emphasizing the importance of the accuracy of their recovery in the content extraction process.

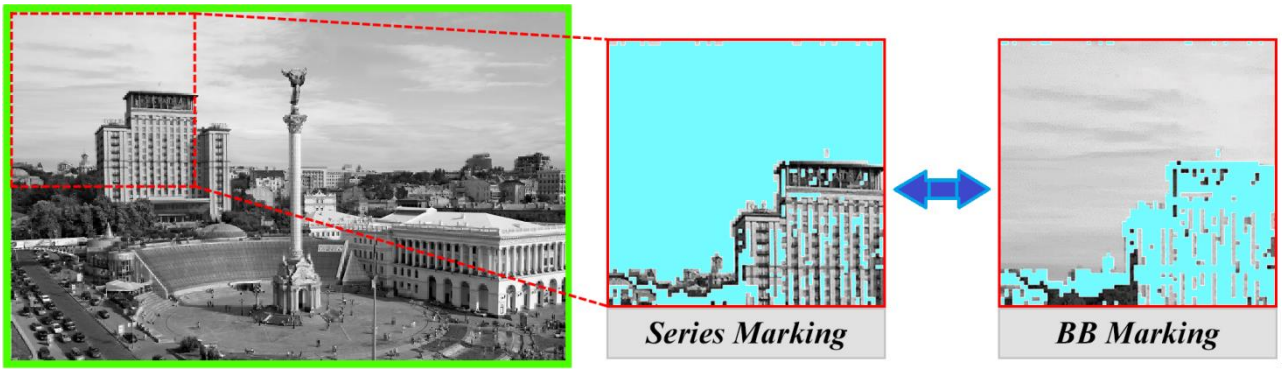


Fig. 4 - Enlarged fragment of a test image of the type city for *BB* size 8×8 el.
(*2nd var. processing;* $P_Z = 3$)

Results similar for the case of Fig. 3, but for different variants of content pre-processing *(i.e., smoothing)*, are presented in *Fig. 5(a-d)*. In this case, the modeling results are backed up by the corresponding values of *PSNR* (peak signal-to-noise ratio) and MSE *(mean square error)* that correspond to different options for their processing [6].

It should be noted that from the point of view of visual visibility of appearing artifacts, the value $P_Z = 14$ is a limiting value for almost all types of images. Therefore, in the interest of providing videodata steganographic insertion procedures, the most «interesting» results are obtained when using smoothing matrices of small dimensionality *(3×3 el.)*, *«*P_Z*»* values from 3 to 7 gradations and the dimensionality of the *BB* series in the range of *4÷8 el*. It is for such, processing parameters in *Figs. 2,3,5* presents the results of the attack of test content samples. In general, *Figs. 2,3,5* clearly show the possible consequences of selection the active parameters of the inter-block multiplex of BB series implemented on a small stack length of series sampling.

3. Conclusions

1. The use of the principle of series length encoding in the implementation of procedures for inter-block data multiplexing creates a good basis for counteracting attempts at unauthorized extraction of content.

2. Applying the principle of encoding series length decreases the computational complexity of the whole algorithm *(by reducing the total number of BB)* and creates the necessary original conditions for the implementation of inter-block data multiplexing procedures.

a) incorrect mix BB for Var.2;
(MSE = 52.08; PSNR = 30.964)

b) incorrect mix BB for Var.3;
(MSE = 52.952; PSNR = 30.892)

c) incorrect mix of Series parameter (Var.2);
(MSE = 110.176; PSNR = 27.71)

d) incorrect mix of Series parameter (Var.3);
(MSE = 106.367; PSNR = 27.863)

Fig. 5. Results of unsuccessful extraction *(i.e. attack)* of a test image of type city *(a-d)* for different smoothing variants of the original data *($P_Z = 3$; BB 8×8 el.)*

3. Basic blocks and their parameters of series lengths are the main procedural elements in the inter-block content processing stage.

4. The modeling results confirmed the leading role of the series length parameter *(see Fig.3 (a-e))* as a key element of the content extraction legitimization procedure. This thesis is confirmed already at a small stack length of the *BB* series sampling.

5. The inter-block multiplex of the series length parameter destroys the correlation relations of the original data to a much greater extent than when using only *BB*. The combined use of both parameters (*BB and Series lengths BB*) further enhances the required effect *(see Fig.3 (e))*.

6. An increase in the dimensionality of the *BB* significantly limits the combinatorics of the multiplex of series parameters, due to the reduction of the base stack sampling *(Fig. 2(a,c,d))*. The optimal dimensionality of the *BB* should be considered blocks in the range from *4×4* to *12×12 el.* with the value of $P_Z \leq 7$.

7. The use of various ways of content pre-processing allows to improve the combinatorics of the series multiplex, which is well confirmed by comparing the hacking results of the test image in *Fig.5(c, d)*.

8. The use of various ways of smoothing the input data, even with the same P_Z values, provides a significant difference in the number of formed *BB*.

9. The dimensionality of the *BB* and the way of organizing the scanning of series are the elements of the composite key of the data extractor [6], which determine the order of implementation of inter-block data processing procedures as a tool for legitimizing access to video content data.

10. The variability of the sampling order of the used parameters of the *BB* series when implementing any way of their scanning [9], strengthens the resistance of the content to attempts of its unauthorized extraction.

11. The use of the principle of series length encoding is largely limited in the background areas of images, which is clearly visible in the example images in *Fig.4*. Such data processing practically does not affect highly informative image areas, for instance, contour boundaries *(building details in Fig. 4)*. Therefore, for blocks forming similar image areas, it is necessary to use the intra-block data multiplexing mechanism *(for example, in parts of the transformation coefficients characterizing the average brightness of the BB)* [6,8].

References

[1] Прэтт У. (1985). Цифровая обработка изображений (Д. С. Лебедева, пер. с англ.). т. 1,2. Москва: Мир.

[2] Бутаков Е. А., Островский В. И., & Фадеев И. Л. (1987). Обработка изображений на ЭВМ. Москва: Радио и связь.

[3] Ярославский Л. П. (1979). Введение в цифровую обработку изображений. Москва: Сов. Радио.

[4] Зубарев Ю. Б., Дворкович В. П. Цифровая обработка телевизионных и компьютерных изображений. Москва: МЦНТИ, 1997. – 212 с.

[5] Красильников Н. Н. (1976). Статистическая теория передачи изображений. Москва: Связь.

[6] Лесная, Ю., Гончаров, Н., & Малахов, С. (2021). ОТРАБОТКА КОНЦЕПТА МНОГОУРОВНЕВОГО МУЛЬТИПЛЕКСА ДАННЫХ ГИБРИДНОГО СТЕГАНОАЛГОРИТМА. Збірник наукових праць SCIENTIA. Вилучено із: https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17666.

[7] Гончаров О., Лєсная Ю., Погоріла К., Богданова Є., Малахов С. Дослідження параметру «серій опорних блоків», як елементу композитного ключа екстрактора даних стеганоалгоритму // Problems of science and practice, tasks and ways to solve them. Proceedings of the XX International Scientific and Practical Conference. Warsaw, Poland. 2022. Pp. 779-785. URL: http://www.isg-konf.com/wp-content/uploads/2022/05/Problems-of-science-and-practice-tasks-and-ways-to-solve-them.pdf.

[8] Гончаров, Н., & Малахов, С. (2022). Использование параметра длин серий, как элемента межблочного мультиплекса данных стеганоалгоритма. Збірник наукових праць ΛΌГОΣ, 180-187. https://doi.org/10.36074/logos-08.07.2022.050.

[9] Лєсная, Ю., Гончаров, М., Семенов, А. & Малахов, С. (2023) Моделювання розгортки серій опорних блоків зображення, як інструменту з протидії спробам несанкціонованої екстракції стеганоконтенту. Grundlagen der modernen wissenschaftlichen Forschung: coll. of scientific papers «ΛΌГОΣ» with Proceeding of the International Scientific and Practical Conf. (Pp.109-115). March 31, 2023, Zurich, Switzerland: BOLESWA Publishers & Europäische Wissenschafts plattform. Вилучено із: https://archive.logos-science.com/index.php/conference-proceedings/article/view/631

[10] Honcharov, M., Pavlova, L., & Lesnaya, Y. (2022). Modeling steganocontent extraction attempts with different lengths stack sampling series of images blocks. Computer Science and Cybersecurity, (2), 22-27. Вилучено із: https://periodicals.karazin.ua/cscs/article/view/21036/19743

Надійшла: Жовтень 2023. **Прийнята**: Листопад 2023.

Автори:
Гончаров Микита, аспірант кафедри безпеки інформаційних систем та технологій Харківського національного університету імені В.Н. Каразіна, Україна.
ORCID ID: https://orcid.org/0000-0002-9790-7260
E-mail: m.honcharov@student.karazin.ua

Ольга Мелкозьорова, к.т.н, доцент кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна, Україна.
ORCID ID: https://orcid.org/0000-0002-1134-2925
E-mail: olha.melkozerova@karazin.ua

Імплементація методу кодування довжин серій для забезпечення процедур стеганографічної вставки зображень.

Анотація. Метою даного матеріалу є ознайомлення з принципом кодування довжин серій для забезпечення міжблочного мультиплексу даних гібридного стеганоалгоритму. У рамках моделювання зроблено припущення, що атакуючий вдало визначив один із двох параметрів обробки контенту: розмір опорних (базових) блоків (ОБ) і реалізований принцип розгортання серій. Моделювання проводилося на прикладі одного тестового напівтонового зображення типу «місто». Представлені зразки атакованого тестового зображення отримані для короткого стеку вибірки (довжиною в 4 серії). Виконано аналіз результатів атаки контенту при використанні різних способів згладжування вихідних зображень. Реалізація різних способів згладжування дає змогу поліпшити комбінаторику мультиплексу серій та кількість сформованих ОБ. Підкреслено, що при збільшені розмірності ОБ обмежує комбінаторику мультиплексу параметрів серій. Розмірність ОБ і спосіб організації роз-

гортки серій є елементами складеного ключа екстрактора даних. Використання принципу кодування довжин серій значно зменшує обчислювальну складність алгоритму та створює умови для реалізації процедур міжблочного мультиплексування. Зроблено висновок, що використання параметра довжин серій руйнує кореляційні зв'язки вихідних даних більше, ніж у разі використання тільки ОБ. Основними елементами на етапі міжблокової обробки контенту є ОБ та їхні параметри довжин серій. Результати моделювання, підтверджують ключову роль параметра «довжин серій» у процедурі легітимації вилучення контенту. Варіативність порядку вибірки використовуваних параметрів серій опорних блоків, значно посилює стійкість контенту до спроб його несанкціонованого вилучення. Звернуто увагу, що принцип кодування довжин серій дещо обмежений у фонових областях зображень, що дає змогу зберегти високоінформативні області зображень та визначити структуру візуальних артефактів. За результатами моделювання зроблено висновок, що використання методу кодування довжин серій у процедурах міжблочного мультиплексування додатково підсилює захист та ускладнює роботу стеганоаналітика і визначає подальший хід атаки.

Ключові слова: *кодування довжин серій, стеганографія, контент, атака, стек.*

УДК 004.056: 004.056.53

ОСОБЛИВОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО РЕАЛІЗУЄ МЕТОД ПОШУКУ ЗА ПРЕФІКСОМ В КРИПТОГРАФІЧНО ЗАХИЩЕНИХ БАЗАХ ДАНИХ

Сергій Лілікович, Віталій Єсін

Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
serhii.lilikovych@student.karazin.ua, v.i.yesin@karazin.ua

Надійшла: жовтень 2023. Прийнята: листопад 2023.

***Анотація**: У роботі розглядаються особливості розробки програмного забезпечення (ПЗ), що реалізує метод пошуку за префіксом в криптографічно захищених базах даних. Цей метод є різновидом симетричного шифрування із можливістю пошуку. Він дозволяє виконувати пошук за префіксом серед зашифрованих даних без необхідності їх розшифрування. Такий підхід дозволяє розв'язати проблему збереження конфіденційності даних, що зберігаються на віддалених або хмарних серверах. Однак його використання обумовлює ряд особливостей, які необхідно враховувати при розробці відповідного ПЗ, що його реалізує. У роботі аналізуються вимоги до ПЗ, що розробляється, яке реалізує метод пошуку за префіксом, визначається архітектура ПЗ, обґрунтовується вибір технологій та інструментальних засобів реалізації ПЗ, зокрема, технології ASP.NET, мов програмування Java, JavaScript, PHP, Python, СКБД MongoDB та фреймворку FastAPI, наводиться опис процесу розгортання відповідного програмного забезпечення. Для тестування швидкодії розробленого програмного забезпечення використовувався відомий інструмент для проведення навантажувального тестування Apache JMeter. Отримані оцінки продуктивності запропонованого рішення свідчать про прийнятність часових затримок на обробку відповідних запитів з пошуку даних.*

***Ключові слова:** база даних, шифрування з можливістю пошуку, конфіденційність, програмне забезпечення.*

1. Вступ

Сьогодні зберігання та обробка даних на сторонніх віддалених хмарних серверах знаходить широке застосування. Однак у міру збільшення масштабу, цінності та централізації даних виявляється зворотний бік цього процесу – загострюються проблеми забезпечення безпеки та приватності даних, що викликає серйозне занепокоєння у власників та користувачів даних. Існує виявлений ризик, що дані, які зберігаються в базах даних, можуть бути скомпрометовані [1-2]. Відомим способом розв'язання цієї проблеми та забезпечення конфіденційності даних є їх шифрування. При цьому, використання традиційних методів шифрування стикається зі специфічними труднощами, а саме – як дозволити ненадійним хмарним серверам виконувати пошукові операції так, щоб шукані дані залишалися конфіденційними. В цілому, проблематика пошуку даних у зашифрованих базах даних (БД) викликала великий інтерес, як у наукових колах, так і в цілому, в індустрії інформаційних технологій - IT [2-3]. Для розв'язання питань пошуку потрібної інформації в криптографічно захищених БД були проведені відповідні дослідження, що пов'язані з розробкою нових криптографічних примітивів, нових структур даних для шифрування з можливістю пошуку, розвитком поглядів на безпеку [4-5]. Однак попри велику різноманітність запропонованих на сьогодні рішень, немає домінуючої думки, що універсальною для всіх відомих випадків використання. Як і не існує найбільш захищеної пошукової системи або набору відповідних методів. Тому власники та користувачі даних повинні чітко усвідомлювати наскільки підходять для їх різних застосунків досить широкий існуючий спектр захищених систем БД і які саме компроміси для їхнього варіанта використання, допустимі. Все це стимулювало дослідження в галузі безпечного управління даними та підвищило їх актуальність [2].

У цій роботі розглядаються основні аспекти розробки *(аналіз вимог, вибір патерну системної архітектури, вибір технологій)* та особливості програмного забезпечення (ПЗ), що

реалізує один з методів пошуку даних у криптографічно захищених базах даних, а саме метод пошуку за префіксом, який представлено у роботі [6].

2. Аналіз вимог до програмного забезпечення, що реалізує метод пошуку за префіксом

Програмне забезпечення, що реалізує відповідні різні методи шифрування з можливістю пошуку (*SE – Searchable Encryption*), природно відрізняється набором вимог. Аналіз вимог є критичним для успішної розробки проекту. Для визначення відповідних функціональних і не функціональних вимог, щодо безпеки що пред'являються до ПЗ, можна скористатися діаграмою потоків даних для процесу пошуку в симетричних системах *SE* (див. рис.1):

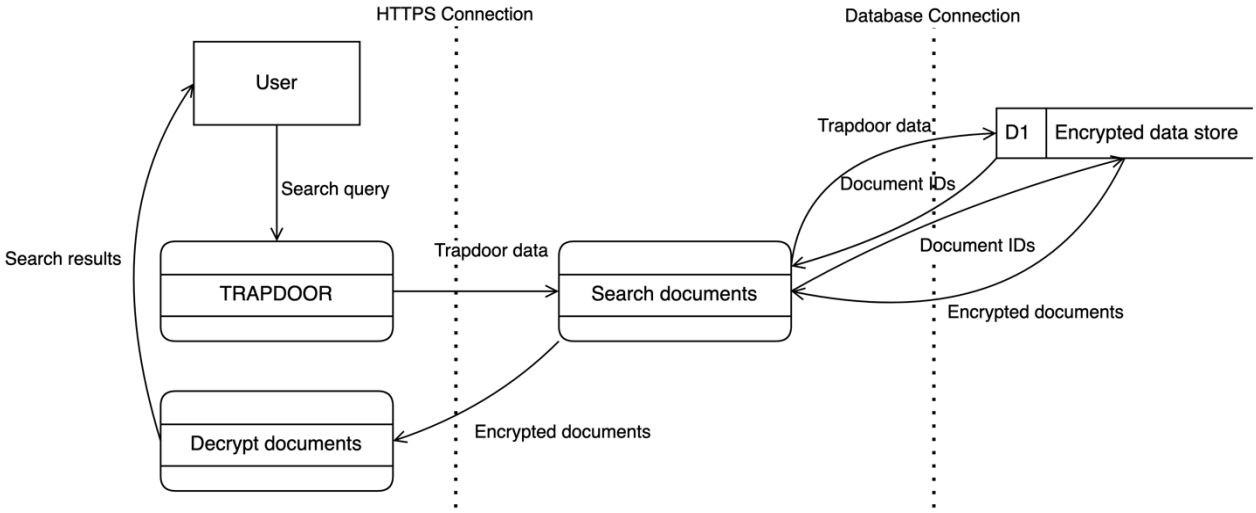


Рис. 1 – Діаграма потоків даних в симетричних системах *SE*
Fig. 1 – Diagram of data flows in symmetric systems *SE*

На діаграмі показано, що пошуковий запит (*search query*) перетворюється на спеціальну «лазівку» (*trapdoor data*) за допомогою алгоритму TRAPDOOR на клієнтському вузлі. «Лазівка» передається на вузол застосунку, який виконує з її використанням запити до БД. Тільки вузол клієнта має доступ до секретних ключів, що використовуються для формування «лазівок».

Виходячи з представленої діаграми, можна ідентифікувати такі загрози:

1. Атака «людина посередині» між вузлами системи, що мають мережеве з'єднання. Зловмисник зможе отримати відомості про «лазівки» та перехопити шифротексти документів (*encrypted documents*). Він також зможе перехопити ідентифікатори відповідних документів (*document IDs*).
2. Атака на алгоритм TRAPDOOR, що дозволить зловмиснику генерувати власні "лазівки" без знання ключової інформації.
3. Атака на вузол сховища даних «*encrypted data store*» – атака «відомого шифртексту», що дозволить зловмиснику отримати зашифровані дані без належної автентифікації, або відомості про зв'язки між документами тощо.

Таким чином, до програмного забезпечення висуваються такі нефункціональні вимоги:

1. Секретний ключ повинен використовуватись та зберігатись тільки на клієнтському вузлі.
2. Пошуковий індекс та документи, що зберігаються в БД, повинні бути криптографічно захищені, а їх зміст не повинен розкриватись на будь-якому вузлі системи, окрім клієнтського.
3. Алгоритм TRAPDOOR повинен бути криптографічно стійким.

4. Канали зв'язку між вузлами системи повинні бути захищеними.

Набір функціональних вимог та інших не функціональних вимог визначаються в залежності від конкретних завдань, які повинна вирішувати програмна система. При аналізі вимог корисно враховувати існуючі моделі безпеки для методів *SE* – вони можуть стати джерелом додаткових вимог до програмної системи. Деякі з цих моделей описані в [7]. В рамках даної роботи щодо функціональних вимог достатньо визначити, що серед них є вимога надавати користувачу можливість пошуку в криптографічно захищений БД за префіксом, з використанням обраного методу *SE*.

3. Визначення системної архітектури ПЗ

В застосунках де передбачається використання шифрування з можливістю пошуку доцільно використовувати 3-х рівневу клієнт-серверну архітектуру *(як шаблон або патерн (pattern))*, за допомогою якої розробники можуть створювати гнучке та повторно використовуване ПЗ. Такий архітектурний шаблон допомагає структурувати програми, які можна розкласти на групи підзавдань, у яких кожна група підзавдань знаходиться на певному рівні абстракції [8]. В цьому випадку такий патерн клієнт-серверної архітектури дозволяє перенести криптографічні функції на бік клієнтського застосунку, доступ до даних може бути обмеженим за допомогою серверу БД, а сервер застосунку може приховати деталі взаємодії з пошуковим індексом та БД. Приклад діаграми розгортання застосунку, що використовує такий патерн системної архітектури для реалізації пошуку за методом SE показано на рис.2.

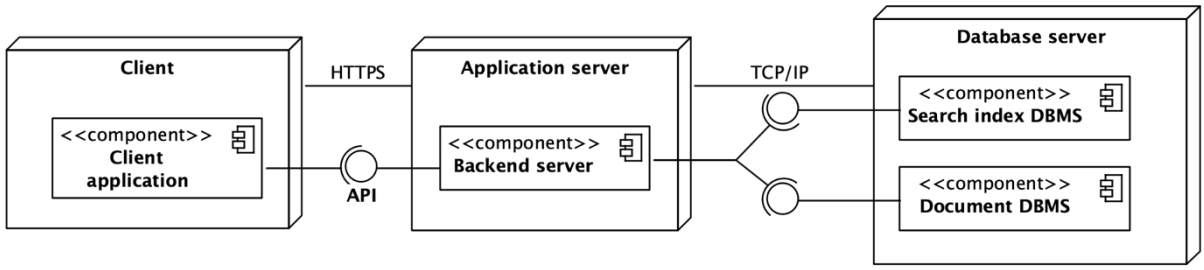


Рис. 2 – Діаграма розгортання ПЗ
Fig. 2 - Software deployment diagram

На діаграмі видно, що у порівнянні з типовою діаграмою розгортання 3-х рівневого застосунку, на фізичному рівні використання SE не призводить до значних змін в архітектурі, окрім можливого додавання нового компонента БД, що може зберігати пошуковий індекс.

4. Вибір технологій реалізації ПЗ

Основною особливістю при виборі технологій реалізації ПЗ пошуку в криптографічно захищених БД є необхідність враховувати, що окрім зашифрованих документів, для забезпечення можливості пошуку методами симетричного *SE* необхідно додатково зберігати та обслуговувати пошуковий індекс, за рахунок якого стає можливою операція пошуку без розшифрування даних. У випадку використання методу пошуку за префіксом, індекс має деревовидну структуру, що впливає на вибір типу СКБД *(системи управління/керування базами даних* СКБД/СУБД*, від англ. Database Management System, DBMS))* для його зберігання.

У разі використання реляційної СКБД, зберігання деревовидної структури даних потребує додаткових супутніх витрат на її обслуговування. В деяких СКБД, таких як *PostgreSQL* і *MongoDB,* деревовидні структури даних підтримуються на рівні розширень або в основному функціоналі, що впливає на вибір конкретного рішення для зберігання даних пошукового індексу. З урахуванням цієї особливості, застосовується документ-орієнтована *MongoDB*, яка

підтримує не тільки збереження деревовидних структур даних, а й виконання складних запитів до них, що може бути використано для оптимізації операцій з індексом. Одночасно з цим, зберігання великих за обсягом записів в *MongoDB* значно знижує швидкодію роботи з такою БД, тому у випадку використання цієї СКБД з документами великого обсягу, необхідно забезпечити їх окреме зберігання поза межами БД індексу.

Особливості вибору інших технологій реалізації полягають у необхідності вибору сучасних підтримуваних технологій, з достатньою кількістю інструментів підтримки якості, наприклад аналізаторів коду, сканерів вразливостей тощо. Далі розглядається обґрунтування вибору інструментальних засобів ПЗ для конкретної реалізації.

4.1 Вибір інструментальних засобів

На сьогодні ринок надає широкий вибір технологій реалізації програмного забезпечення. В якості потенційних засобів розробки програмного забезпечення розглядалися наступні технології: - *Java, JavaScript, Python, ASP.NET, PHP*. Список з цих технологій був складений виходячи з практичної можливості використання кожної з них. При цьому в процесі вибору інструментарію були сформульовані відповідні критерії:

1. Багатоплатформність – один і той же програмний код повинен покрити якомога більше платформ.
2. Доступність – розробка повинна бути максимально дешевою.
3. Простота розробки – час розробки має бути мінімальним.
4. Наявність зручного та сучасного GUI-фреймворку для швидкої розробки графічного інтерфейсу.
5. Наявність простих інструментів статичного аналізу коду для підтримки його якості.

Детальніше розглянемо властивості зазначених засобів розробки.

Мова програмування Java

Java – це об’єктно орієнтована мова програмування, яка була вперше представлена в 1995 році компанією Sun Microsystems як ключовий компонент платформи Java. З 2009 року розвитком та підтримкою мови займається компанія Oracle, яка того року придбала Sun Microsystems. Офіційна реалізація програм на Java компілюється в байт-код, який потім виконується віртуальною машиною, специфічною для конкретної платформи.

Oracle надає компілятор *Java* та віртуальну машину Java, які відповідають специфікаціям *Java Community Process*, і це відбувається під ліцензією *GNU General Public License*.

Синтаксис Java схожий на C та C++, але з істотними відмінностями. Розробники технології врахували досвід розробки за допомогою цих двох мов, що призвело до усунення можливості виникнення деяких конфліктних ситуацій, які могли виникнути через помилки програміста, і спростило процес розробки об’єктно орієнтованих програм. Багато з тих дій, які вимагаються в C/C++, тепер виконує віртуальна машина. Головною метою *Java* завжди було створення мови, яка була б платформонезалежною, і це визначає її обмеження в роботі з апаратним забезпеченням порівняно з, наприклад, C++. Таким чином, швидкість роботи програми може бути меншою. Проте, *Java* надає можливість викликати підпрограми, написані іншими мовами програмування, коли це необхідно. Приклад програми мовою *Java* в середовищі *IntelliJ IDEA* наведено на рис. 3.

Java мала значний вплив на розвиток мови програмування J++, яку розробляла компанія Microsoft. Роботу над J++ було припинено через судовий позов, поданий *Sun Microsystems*, оскільки ця мова програмування була модифікацією *Java*. Пізніше, при створенні нової платформи .NET компанією Microsoft, була представлена мова J#, яка спрощувала міграцію програмістів, які вже володіли *J++* або *Java*, на нову платформу. З часом нова мова програ-

мування C# стала основною мовою платформи .NET, позичивши багато ідей з Java. J# включали востаннє в версію *Microsoft Visual Studio 2005*.

Іншою технологією, що має широкі можливості як клієнтських, так і серверних застосунків є *JavaScript*.

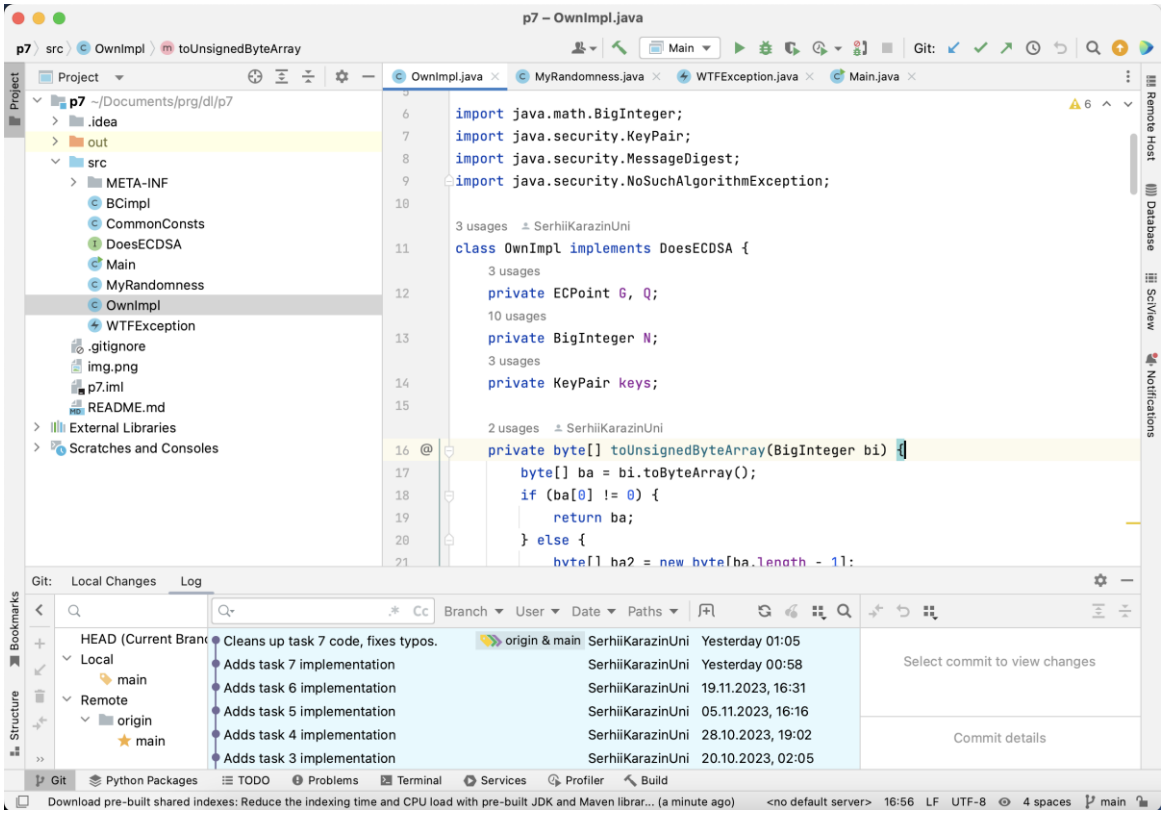


Рис. 3 – Приклад програми мовою *Java* (*в середовищі IntelliJ IDEA)*

Fig. 3 – Example of *Java* program (*in the environment IntelliJ IDEA*)

Мова програмування JavaScript

JavaScript є однією з найпоширеніших мов програмування у світі. Вона підтримується всіма основними браузерами, включаючи *Chrome, Firefox, Edge* та *Safari*. *JS* також є основою для багатьох популярних фреймворків, таких як *React, Angular* та *Vue.JS*.

Серед основних переваг *JavaScript* можна назвати такі:

1. Має простий синтаксис, подібний до C та C++.
2. Є широко поширеною мовою, що робить її легко доступною для розробників.
3. Де-факто є стандартом для сучасних веб-застосунків, підтримується більшістю веб-браузерів.
4. Деякі реалізації *JavaScript* є проектами відкритого коду, що дозволяє розробникам робити свій внесок у розвиток мови, проводити незалежні аудити безпеки тощо.

Серед основних недоліків *JavaScrip*t виділяють:

1. Програми на *JavaScript* інтерпретуються на стороні клієнта, а отже передаються туди у вигляді відкритого тексту. Це може впливати на безпеку застосунків, адже клієнт може модифікувати код.

2. *JavaScript* є динамічною мовою без статичної типізації, що може призводити до помилок.

Приклад програми мовою JavaScript, в середовищі *IntelliJ IDEA* наведено на рис. 4. Для JavaScript існують фреймворки та численні інструменти підтримки якості коду, що можуть значно полегшити розробку програмного забезпечення роботи. Одним з них є *Vue.JS* – фрей-

мворк для створення односторінкових веб-застосунків, що прискорює розробку. Іншим фреймворком, що може бути використаним в роботі, є *Vuetify* – фреймворк для створення інтерфейсів користувача на основі *Vue.JS*. *Vuetify* надає широкий спектр готових компонентів, які можна використовувати для швидкого створення красивих і зручних у використанні інтерфейсів.

Альтернативою до використання *JavaScript* є технології на платформі .NET, зокрема *ASP.NET*.

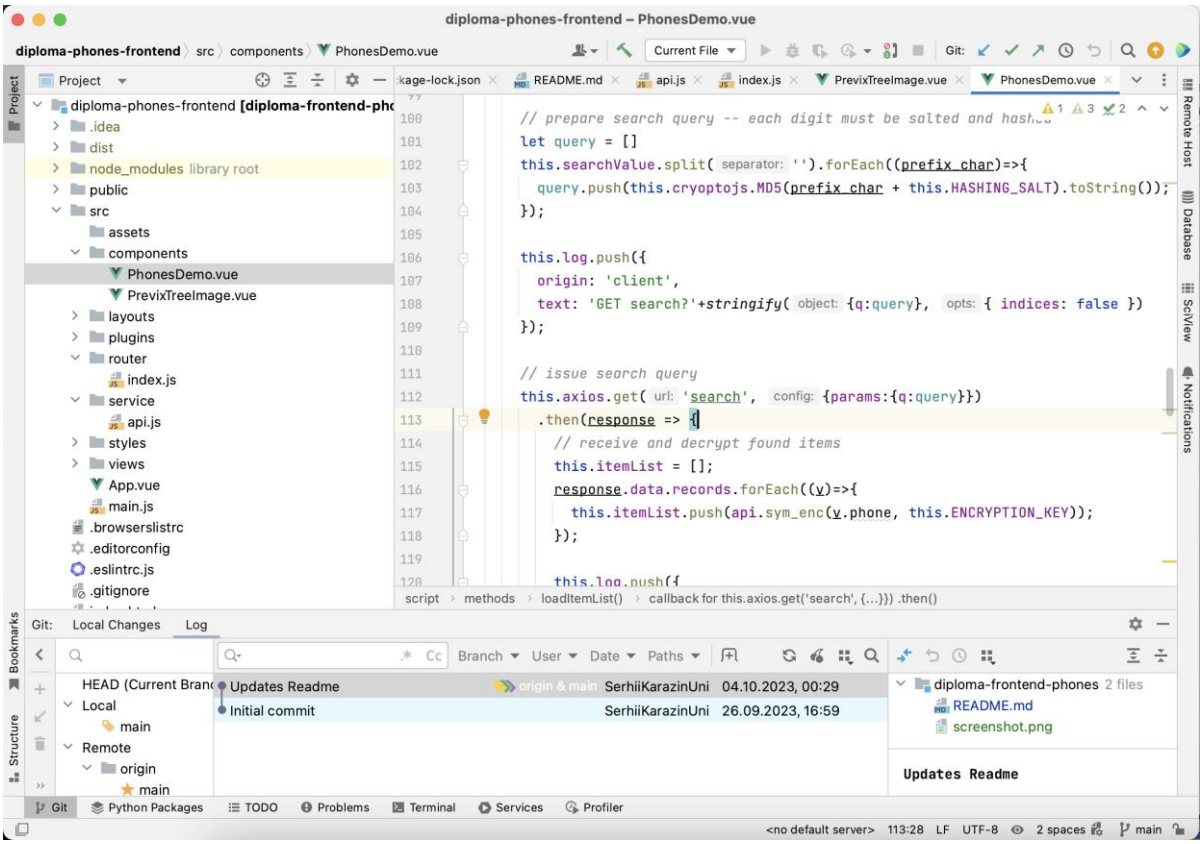


Рис. 4 – Приклад програми мовою *JavaScript (в середовищі IntelliJ IDEA)*

Fig. 4 – Example of *JavaScript* program (*in the environment IntelliJ IDEA*)

Технологія ASP.NET

ASP.NET – це технологія створення веб застосунків і веб сервісів від компанії Microsoft, і вона є важливою частиною платформи *Microsoft.NET*. Ця технологія являє собою еволюцію попередньої версії – *Microsoft ASP*. На сьогодні останньою версією *ASP.NET* є *ASP.NET 6*.

ASP.NET має багато спільних рис зі своєю попередницею ASP, що дозволяє розробникам переходити на *ASP.NET* досить легко. Проте внутрішня структура *ASP.NET* суттєво відрізняється від *ASP*, оскільки *ASP.NET* базується на платформі .NET і використовує всі переваги цієї платформи. Приклад програми для платформи *ASP.NET* в середовищі Microsoft *Visual Studio* наведено на рис. 5.

Microsoft повністю переробила *ASP.NET*, використовуючи Common Language Runtime як основу, яка є фундаментальною для всіх застосунків *Microsoft .NET*. Один із головних плюсів *ASP.NET* полягає в тому, що розробники можуть писати код для *ASP.NET*, використовуючи практично будь-яку мову програмування, доступну в *.NET Framework* (такі як C#).

Основною перевагою *ASP.NET* є його продуктивність. Під час першого запиту код компілюється і зберігається в спеціальному кеші, що дозволяє його швидше виконувати в подальших запитах, і не потребує синтаксичного аналізу (*parsing*), оптимізації та інших проміжних операцій, що заощаджує час.

Іншою популярною технологією є *Python*.

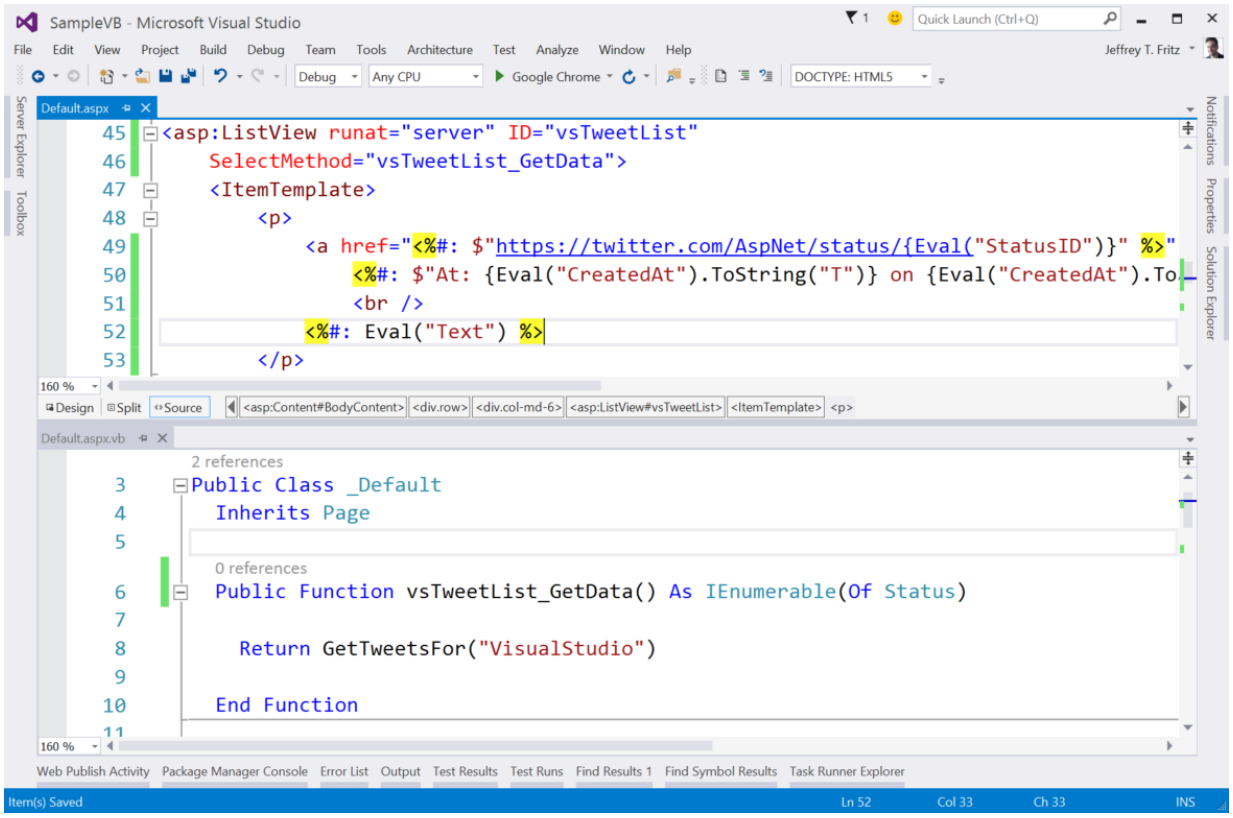


Рис. 5 – Приклад застосування технології *ASP.NET* в середовищі *Visual Studio*

Fig. 5 – Application example of the implementation of *ASP.NET* technology in the middle of *Visual Studio*

Мова програмування Python

Python – це інтерпретована об'єктно-орієнтована мова програмування високого рівня зі строгою динамічною типізацією. Структури даних високого рівня разом із динамічною семантикою та динамічним зв'язуванням роблять її привабливою для швидкої розробки програм, а також як засіб поєднання існуючих компонентів. *Python* підтримує модулі та пакети модулів, що сприяє модульності та повторному використанню коду. Інтерпретатор *Python* та стандартні бібліотеки доступні як у скомпільованій, так і у вихідній формі на всіх основних платформах.

В мові програмування *Python* підтримується декілька парадигм програмування, зокрема: об'єктно-орієнтована, процедурна, функціональна та аспектно-орієнтована.

Серед основних її переваг можна назвати такі:

1. Доступний для розробників різного рівня досвіду синтаксис мови.
2. Переносність програм (що властиве більшості інтерпретованих мов).
3. Зручний для розв'язання математичних задач (має засоби роботи з комплексними числами, може оперувати з цілими числами довільної величини).
4. Відкритий код.

До недоліків *Python* можна віднести:

1. Низьку швидкодію (*у порівнянні з мовами більш низького рівня*).
2. Відсутність статичної типізації.

Для Python існують інструменти підтримки якості коду, та фреймворки, що можуть значно полегшити розробку програмного забезпечення прототипу. Одним з них є *FastAPI* – високопродуктивний веб-фреймворк для створення *API*. Приклад програми мовою *Python* з використанням *FastAPI*, в середовищі *IntelliJ IDEA* наведено на рис. 6.

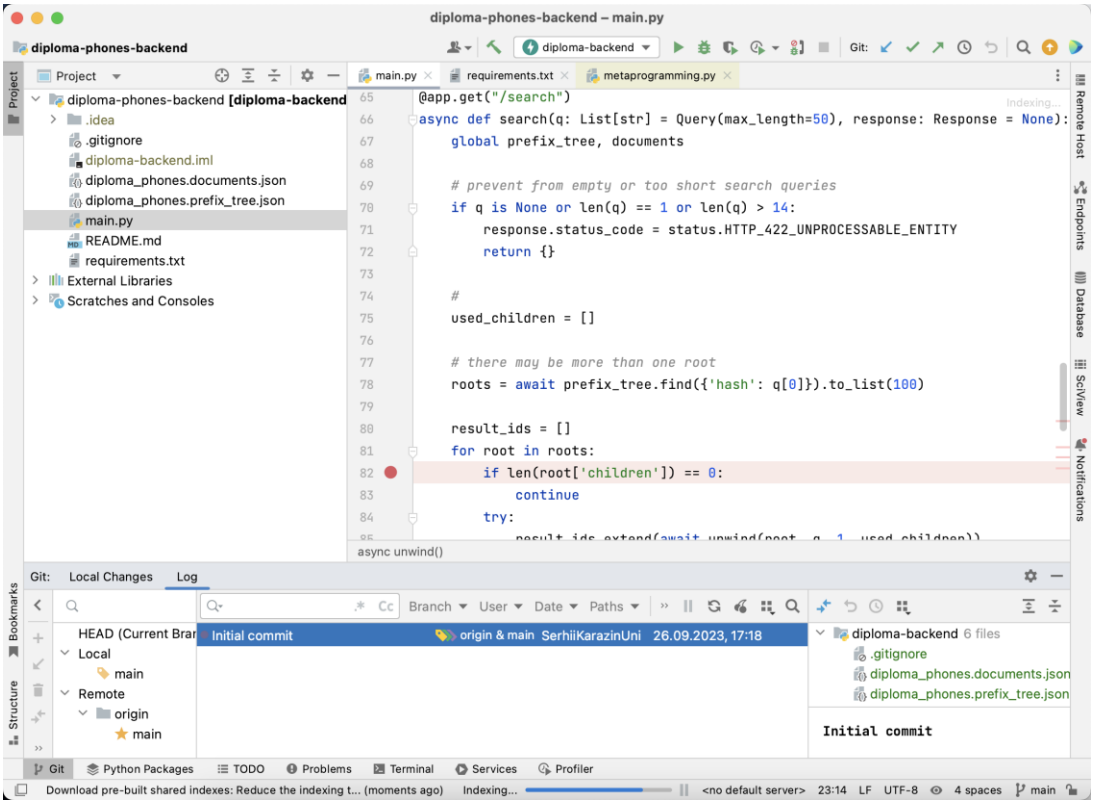


Рис. 6 – Приклад програми мовою *Python* (*в середовищі IntelliJ IDEA)*

Fig. 6 – Application example of *Python* program (*in the environment IntelliJ IDEA*)

Важливі властивості *FastAPI*:

1. Один з найшвидших веб фреймворків для *Python*. Він досягає високої продуктивності шляхом використання асинхронного запиту та відповіді, а також оптимізації коду.
2. Має простий і інтуїтивно зрозумілий синтаксис. Він також має ряд вбудованих функцій, які спрощують створення *API*.
3. Має вбудовані функції для документування *API* та тестування.

Крім того, при розробці веб-додатків однією з найпопулярніших є технологія *PHP*.

Мова програмування PHP

PHP – це скриптова мова програмування, створена для генерації *HTML*-сторінок на стороні веб сервера. *PHP* є однією з найпоширеніших мов, використовуваних у сфері веб розробки, разом з *Java, .NET, Python* та *Ruby*.

PHP була розроблена в 1994 році, а наразі є однією з найпоширеніших мов програмування для веб розробки. Велика кількість веб сайтів, включаючи популярні соціальні мережі, електронні комерційні платформи та блоги, побудовані з використанням *PHP*. Однією з переваг *PHP* є те, що вона підтримується більшістю хостинг-провайдерів, що робить її доступною для широкого кола веб розробників.

Завдяки вдосконаленням у внутрішній архітектурі та оптимізаціям, зараз *PHP* здатна конкурувати з іншими популярними мовами програмування, такими як *Java* та *Python*. Швидкодія стала особливо помітною в *PHP 7*, яка отримала значне прискорення завдяки оптимізації в роботі з пам'яттю й виконанню опкоду.

Основні переваги *PHP* включають:

1. *PHP* – мова програмування з синтаксисом, схожим на мови з родини «C».
2. Спрямованість на веб розробку – *PHP* призначена для розв'язання задач, пов'язаних з веб розробкою, і не вимагає від програміста глибоких знань інших технологій.
3. Висока популярність серед веб-розробників та спільноти користувачів.

4. Ліцензія відкритого ПЗ, що дозволяє вільне використання і розповсюдження.

Приклад програми мовою *PHP*, в середовищі *IntelliJ IDEA* наведено на рис. 7.

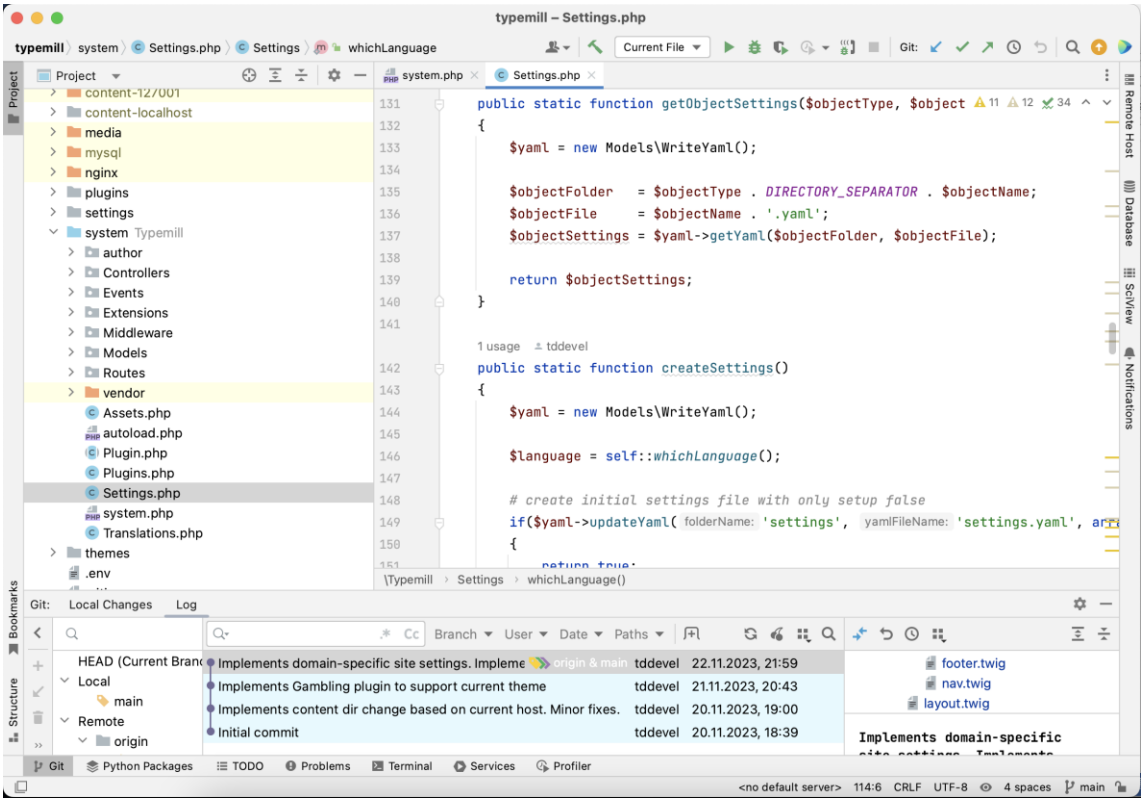


Рис. 7 – Приклад програми мовою *PHP* (*в середовищі IntelliJ IDEA*)

Fig. 7 – Application example of *PHP* program (*in the environment IntelliJ IDEA*)

Серед недоліків можна виділити:

1. Забезпечення безпеки. PHP в минулому мав деякі серйозні проблеми із забезпеченням безпекою (*наприклад, такі як вразливості SQL-ін'єкції, вразливості з крос-сайт скриптінгом тощо; відтоді в PHP були внесені покращення, такі як впровадження підготованих виразів (prepared statements) для SQL та бібліотеки PDO, але питання безпеки є актуальним для PHP і сьогодні*).

2. Складні назви деяких поширених функцій, таких як *htmlspecialchars*, *mysql_select_db*, *nl2br* тощо. У *PHP* можуть існувати кілька функцій, які виконують схожі завдання, і це може призвести до плутанини та невизначеності у виборі правильної функції. Крім того, у різних функціях *PHP* можуть існувати різні стандарти назв функцій та порядку аргументів, що може призвести до плутанини та помилок.

Для *PHP* існують численні фреймворки та інструменти підтримки якості коду, проте в швидкодії *Python* зазвичай має перевагу над *PHP*.

Порівняння технологій

Для порівняння та вибору технологій можна прибігти до методу експертних оцінок за критеріями, які були сформульовані вище. Для цього розглянуті технології були оцінені за трьома критеріями: - кросплатформність, доступність, та простота розробки. В табл.1 наведені оцінки за кожним з критеріїв в діапазоні [1;5] для кожної із технологій.

З урахуванням отриманих оцінок прийнято рішення про використання *Python* з фреймворком *FastAPI* для реалізації сервера застосунку та *JavaScript* з фреймворком *Vuetify* для клієнтського ПЗ. В якості СКБД/СУІБ може бути обрана будь-яка з підтриманих в *Python*, але з міркувань простоти реалізації роботи з деревовидними структурами даних була обрана *MongoDB*.

Таблиця 1 – Порівняння інструментальних засобів реалізації ПЗ
Table 1 – Comparison of software implementation tools

Критерій/ Засіб	Крос-платформність	Доступність	Простота розробки	Сума
Java	5 – Виконується у віртуальній машині, що доступна для більшості платформ	5 – Вільна ліцензія, багато безкоштовних інструментів	3 – Висока складність для швидкої розробки	13
JavaScript	5 – Скриптова мова програмування	5 – Вільна ліцензія, відкритий код, багато безкоштовних інструментів	4 – Можуть бути проблеми сумісності при виконанні в різних браузерах	14
ASP.NET	3 – Виконується у віртуальній машині з обмеженою підтримкою	4 – Вільна ліцензія, відкритий код	3 – Висока складність для швидкої розробки	10
PHP	5 – Скриптова мова програмування	5 – Вільна ліцензія, відкритий код, багато безкоштовних інструментів	5 – Підтримує SDLC швидкої розробки	15
Python	5 – Скриптова мова програмування	5 – Вільна ліцензія, відкритий код, багато безкоштовних інструментів	5 – Підтримує SDLC швидкої розробки	15

Таким чином, за результатами огляду різних технологій реалізації, діаграма розгортання застосунку котра реалізує пошук з використанням запропонованого методу *SE*, набула наступного вигляду (рис. 8).

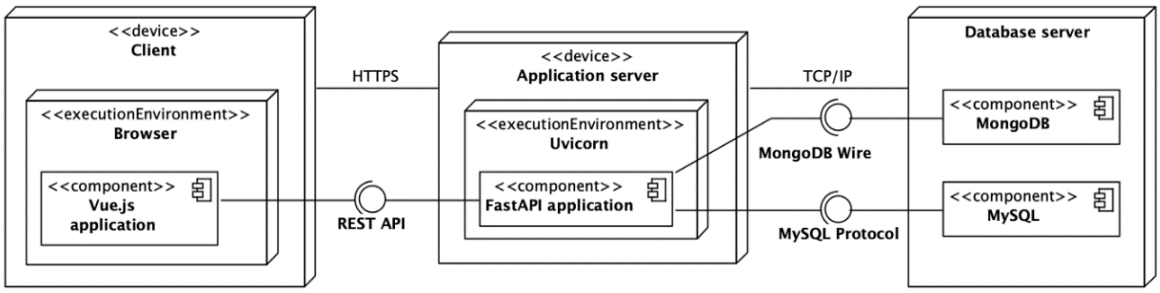


Рис. 8 – Уточнена діаграма розгортання для застосунку
Fig. 8 – Adjusted application deployment diagram

Вимоги до апаратного і програмного забезпечення

Обраний набір інструментів реалізації ПЗ визначає початкові вимоги до ПЗ і апаратного забезпечення кожного з вузлів майбутньої системи. Для коректної роботи ПЗ вузла *«Client»* необхідно забезпечити функціонування сучасної версії веб-браузера, тому в залежності від операційної системи (ОС) висуваються наступні вимоги (див.табл. 2).

Таблиця 2 – Вимоги до вузлу *«Client»* в залежності від ОС
Table 2 – Requirements for the "Client" node depending on the OS used

ОС	Вимоги
Windows	Win 10 або новіша, 4 ГБ ОЗУ (або більше), не менше 128 ГБ дискового простору. Браузер Google Chrome або будь-який інший сумісний.
Mac	MacOS Catalina 10.15 або новіша, 4 ГБ ОЗУ, не менше 128 ГБ дискового простору. Браузер Google Chrome або будь-який, сумісний.
Linux	64-бітна система Ubuntu 18.04, Debian 10, OpenSUSE 15.2, Fedora Linux 32 або новіші, 4 ГБ ОЗУ (чи більше), не менше 128 ГБ дискового простору, підтримка інструкцій SSE3. Браузер Google Chrome або будь-який інший сумісний.
Android	Android 8.0 або новіша, 1 ГБ оперативної пам'яті (чи більше), 32 ГБ дискового простору (або більше). Браузер Google Chrome або будь-який інший, сумісний.

ПЗ вузла *«Application server»* використовує мову *Python*, яка дозволяє виконувати однаковий код на різних платформах, тому для цього вузла висуваються однакові вимоги для всіх підтриманих платформ (*Windows, Linux, MacOS або будь-яка інша, що підтримує Python 3.11*):

1. 4 ГБ оперативної пам'яті (ОЗУ), не менше 128 ГБ дискового простору.
2. Інтерпретатор *Python* 3.11 (або сумісний).
3. Бібліотеки залежностей: FastAPI 0.103.2 (або сумісна), *PyMongo* 4.5.0 (*або сумісна*), python-dotenv 1.0.0 (*або сумісна*).

Для вузла сервера баз даних необхідно забезпечити функціонування сучасної версії СКБД *MongoDB*, тому висуваються такі вимоги:

1. 4 ГБ оперативної пам'яті (*або більше*), не менше 10 ГБ дискового простору (в залежності від обсягу даних що зберігаються, ця вимога може бути більше).
2. Процесор 64-бітної архітектури.
3. MongoDB 7.0.1 community (*або будь-яка сумісна*).

При цьому, хмарне рішення *MongoDB Atlas* надає декілька варіантів готових віртуальних машин для простого розгортання СКБД. Один з таких варіантів – *«M0 Sandbox»*. Він має суттєві обмеження в ресурсах, проте задовольняє мінімальним вимогам до програмного та апаратного забезпечення прототипу.

Процес інсталяції програмного забезпечення

Для ознайомлення з ПЗ прототипу користувачам необхідно перейти за адресою *https://se-uavs.lilikovych.name* – окрім браузера *Google Chrome* (*або сумісного*) з боку користувача встановлювати будь-яке інше ПЗ не потрібно.

Вихідний код програмного забезпечення прототипу доступний за адресами:
https://github.com/SerhiiKarazinUni/diploma-uavs-frontend (інтерфейс користувача).
https://github.com/SerhiiKarazinUni/diploma-uavs-backend (ПЗ вузла серверу застосунку).

Інсталяція сервера застосунку

Для інсталяції власної копії ПЗ вузла *"Application server"* необхідно:

1. Встановити *Git* та інтерпретатор *Python* версії 3.11 (*або новішої сумісної*).
2. Виконати команду *«git clone https://github.com/SerhiiKarazinUni/diploma-uavs-backend»*, перейти в директорію *«diploma-uavs-backend»*.
3. Виконати команду встановлення залежностей *«py -m pip install -r requirements.txt»*.
4. Окремо встановити сервер *Uvicorn* за допомогою команди *«py -m pip install uvicorn[standard]»*.
5. Перейменувати файл *"example.env"* в *".env"*, налаштувати актуальні значення змінних оточення.
6. Після збереження файлу, сервер застосунку можна запустити командою *"py -m uvicorn main:app --port 3000 --host 127.0.0.1"*.

Після виконання цих дій, ПЗ сервера застосунку буде доступне по протоколу *HTTP* на порт 3000.

Інсталяція користувальницького інтерфейсу застосунку

Для встановлення ПЗ користувальницького інтерфейсу необхідно:

1. Встановити Git та актуальну версію Node.JS.
2. Виконати команду *"git clone https://github.com/SerhiiKarazinUni/diploma-uavs-frontend"*, перейти в директорію *"diploma-uavs-frontend"*.
3. Виконати команду встановлення залежностей *"npm install"*.
4. Відкрити для редагування файл *"src/plugins/index.js"*, та в рядках 14 і 15 налаштувати відповідну адресу сервера застосунку. Крім того, необхідно переконатися, що в ряд-

ку 16 встановлено актуальне значення токена клієнта, таке що відповідає *"API_TOKEN"* з налаштувань сервера. Зберегти файл.

5. Виконати команду *"npm run dev -- --port 80"* .

Після виконання цих дій, ПЗ вузла «Client» буде доступне по протоколу *HTTP* на порту 80, як показано на рис. 9.

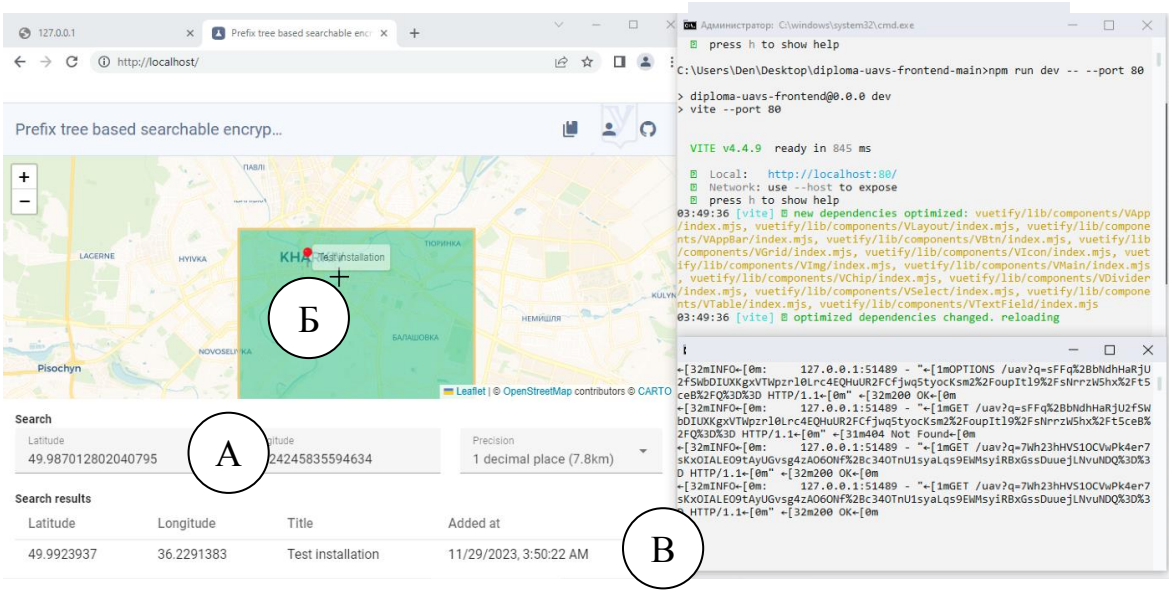


Рис. 9 – Вікно браузера з користувальницьким інтерфейсом та вікна терміналів
Fig. 9 – Browser window with user interface and terminals windows

Літерами на рисунку позначено: (А) панель пошуку, де можна задати або переглянути поточні координати центральної точки, навколо якої відбувається пошук, (Б) інтерактивну карту, яка відображає поточну центральну точку, зону пошуку, та дозволяє подвійним кліком змінити місцезнаходження центральної точки, (В) результати пошуку у вигляді таблиці. Додатково в інтерфейсі застосунку доступне поле вводу для створення нового об'єкту на карті, та вікно відомостей про обмін даних між клієнтським застосунком та сервером застосунку, де можна бачити, що в ході пошуку не відбувається обміну даними пошукового запиту у відкритому вигляді, і дані про збережені документи (*відомості про точки на карті*) надходять до клієнтського застосунку в зашифрованому вигляді. Для тестування швидкодії ПЗ прототипу, використано *Apache JMeter*, який був сконфигурирован, як показано на рис. 10.

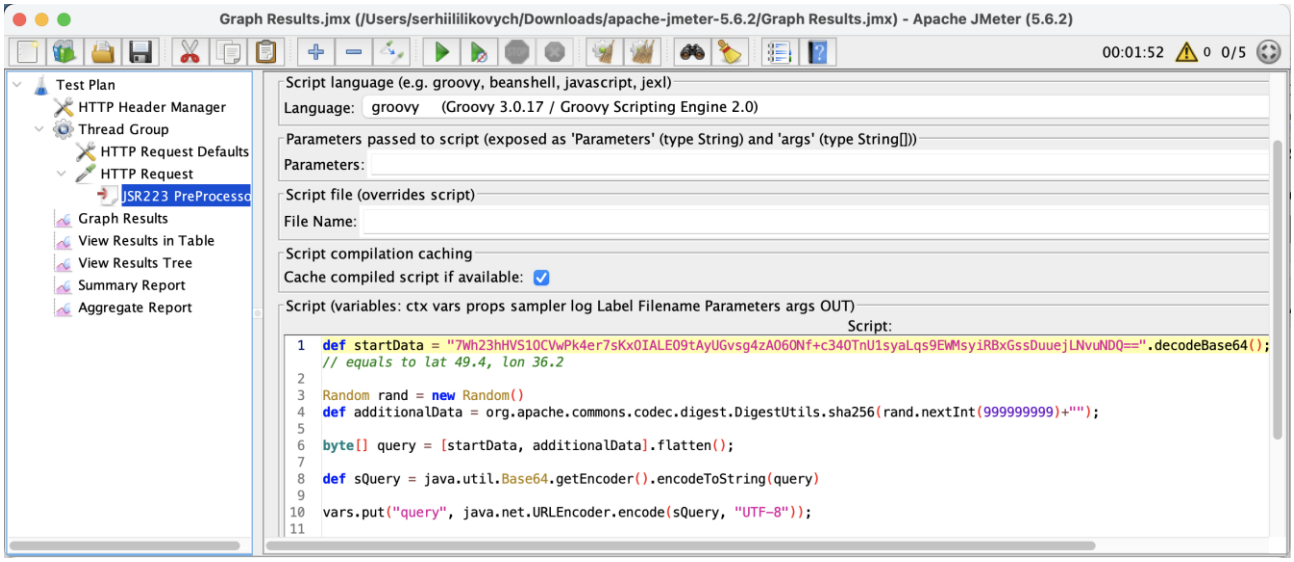


Рис. 10 – Інтерфейс *Apache JMeter* в ході тестування швидкодії
Fig. 10 – *Apache JMeter* interface during performance testing

З рис.10 видно, що тестування складається з одної групи потоків (*thread group*), яка виконує *HTTP*-запити таким чином, що кожен наступний відрізняється від попередніх, за що відповідає спеціально створений об'єкт *"JSR223 PreProcessor"* – програма, яка генерує випадкові, але коректні «*лазівки*». Група потоків сконфігурована таким чином, що імітує одночасне виконання пошукових запитів від імені п'яти користувачів. Кожен користувач виконує по 200 запитів, тобто сумарне навантаження досягає 1000 пошукових запитів. Графік пропускної здатності прототипу ПЗ за результатами тестування швидкодії *Apache JMeter*, показано нижче, на рис.11. Як можна бачити, пропускна здатність ПЗ прототипу – 535.26 запити на 1 хв, а отже приблизно 8.9 запитів на секунду, або 0.11 секунд на один запит.

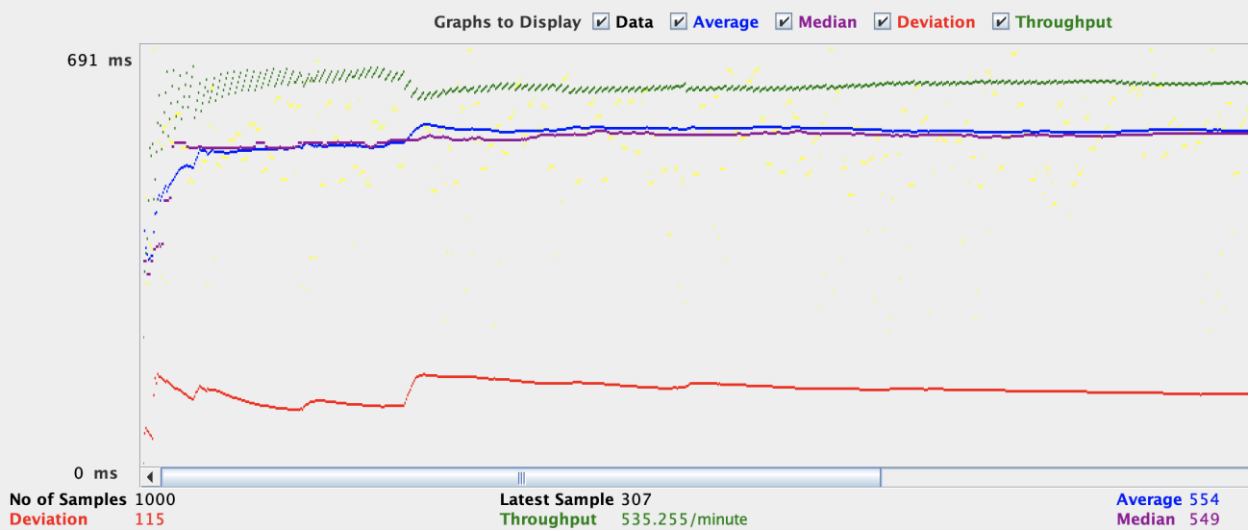


Рис. 11 – Пропускна здатність прототипу ПЗ (*за результатами Apache JMeter)*
Fig. 11 – Bandwidth of the software prototype *(according to the results of Apache JMeter)*

3. Висновки

При розробці ПЗ, яке забезпечує пошук за допомогою розглянутого методу були:

1. Сформульовані вимоги до нього, що враховують результати проведеного аналізу загроз та відомих моделей безпеки.
2. Визначено архітектуру та інструментальні засоби для реалізації ПЗ.
3. Розроблено програмну модель відповідного прототипу додатку/рішення.
4. Проведено оцінку продуктивності запропонованого рішення. Середній час обробки запиту під час тестування швидкодії склав 0.11 с.

Список літератури

[1] SoK: Cryptographically Protected Database Search / Benjamin Fuller [et al.] // 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017. – Mode of access: https://doi.org/10.1109/sp.2017.10 (date of access: 05.01.2024)

[2] Technique for Searching Data in a Cryptographically Protected SQL Database / Vitalii Yesin [et al.] // Applied Sciences. – 2023. – Vol. 13, no. 20. – P. 11525. – Mode of access: https://doi.org/10.3390/app132011525 (date of access: 05.01.2024)

[3] Azraoui M. Framework for Searchable Encryption with SQL Databases / Monir Azraoui, Melek Önen, Refik Molva // 8th International Conference on Cloud Computing and Services Science, Funchal, Madeira, Portugal, 19–21 March 2018. – Mode of access: https://doi.org/10.5220/0006666100570067 (date of access: 05.01.2024)

[4] A Survey of Provably Secure Searchable Encryption / Christoph Bösch [et al.] // ACM Computing Surveys. – 2015. – Vol. 47, no. 2. – P. 1–51. – Mode of access: https://doi.org/10.1145/2636328 (date of access: 05.01.2024)

[5] Dynamic Verifiable Encrypted Keyword Search Using Bitmap Index and Homomorphic MAC / Rajkumar Ramasamy [et al.] // 2017 IEEE 4th International Conference on Cyber-Security and Cloud Computing (CSCloud), New York, NY, 26–28 June 2017.– Mode of access: https://doi.org/10.1109/cscloud.2017.47 (date of access: 05.01.2024)

[6] Лілікович С.О. Метод пошуку за префіксом в зашифрованих базах даних / Лілікович С.О., Єсін В.І. // Комп'ютерне моделювання в наукоємних технологіях : Зб. наук. пр. міжнар. науково-техн. конф., Харків, 25–27 жовт. 2023 р.– С. 105–108.

[7] Handa R. Searchable encryption: A survey on privacy preserving search schemes on encrypted outsourced data / Rohit Handa, C. Rama Krishna, Naveen Aggarwal // Concurrency and Computation: Practice and Experience. – 2019. – P. e5201. – Mode of access: https://doi.org/10.1002/cpe.5201 (date of access: 05.01.2024)
[8] Pattern-Oriented Software Architecture Volume 1: A System of Patterns / Frank Buschmann [et al.]: Wiley, 1996. – 476 p.

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

Authors:
Serhii Lilikovych, CSD Student (magistrate), Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.
ORCID: https://orcid.org/0009-0003-4407-1281
E-mail: serhii.lilikovych@student.karazin.ua
Vitalii Yesin, Doctor of Engineering Sciences, Full Professor, Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.
ORCID: https://orcid.org/0000-0003-1977-7269
E-mail: v.i.yesin@karazin.ua

Features of software implementing the prefix search method in cryptographically protected databases.

Abstract. The article addresses the specific considerations associated with the development of software implementing the prefix search method in cryptographically protected databases. This method is a variant of symmetric searchable encryption, which allows search among the encrypted data. The prefix search method allows searching for prefixes among encrypted data without the need for decryption. Such an approach resolves the issue of maintaining data confidentiality stored on remote or cloud servers. However, its usage introduces a set of issues that must be considered during the development of the corresponding software. The paper analyzes the requirements for software that implements the prefix search method, defines the software architecture, and justifies the choice of technologies and tools for software implementation, including *ASP.NET*, *Java*, *JavaScript*, *PHP*, *Python* programming languages, *MongoDB* database management system, and the *FastAPI* framework. A description of the deployment process of the corresponding software is provided. To assess the performance of the developed software, the well-known *Apache JMeter* tool for conducting load testing was utilized. The obtained performance evaluations of the proposed solution indicate acceptable time delays in processing relevant data search queries.

Keywords: *Database, Searchable Encryption, Confidentiality, Software.*

УДК 004.056.5

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У БАНКІВСЬКИХ МОБІЛЬНИХ ДОДАТКАХ

Єлизавета Логачова[1], Марина Єсіна[1,2], Всеволод Бобух[2]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
lohachova2020kb11@student.karazin.ua, m.v.yesina@karazin.ua
[2] АТ «ІІТ», вул. Коломенська, 15, Харків, 61166, Україна
jsciitua@gmail.com

Надійшла: листопад 2023. Прийнята: грудень 2023.

Анотація: *В даній статті розглядаються важливі аспекти забезпечення кібербезпеки в мобільних банківських додатках. В роботі аналізуються потенційні загрози безпеки та ефективні стратегії, щодо їх запобігання та протидії. У зв'язку зі стрімким розвитком цифрових технологій у банківській галузі, мобільні застосунки та онлайн сервіси стали необхідною складовою фінансового взаємодії клієнтів, забезпечуючи зручні та ефективні фінансові операції. Однак, розвиток функціоналу таких застосунків породжує нові виклики у сфері кібербезпеки, на які активно відповідають фахівці з інформаційної безпеки. Стаття присвячена оглядовому аналізу міжнародних та вітчизняних стандартів кібербезпеки в банківському секторі, а також містить аналіз мобільних додатків відомих українських банків. На основі цього аналізу формулюються конкретні рекомендації, стосовно можливостей подальшого вдосконалення кібербезпеки в таких застосунках. Розглядається вплив комфорту клієнтів на рівень безпеки. Крім того, в роботі розглядається вплив рівня безпеки в банківському секторі на загальну діджиталізацію фінансової галузі. Автори роблять акцент на тому, як підвищення рівня безпеки може стимулювати та підтримувати процеси діджиталізації, забезпечуючи довіру клієнтів та оптимальне використання мобільних банківських застосунків. Комплексний підхід до оцінки рівня безпеки, порівняння різних додатків і стандартів (як українських, так і міжнародних), а також розгляд взаємозв'язку питань безпеки та інновацій в банкінгу, роблять цю роботу корисною для розуміння ґенези кібербезпеки у сфері мобільного банкінгу.*

Ключові слова: *банківська система, безпека, загрози, кібербезпека, банкінг, мобільні додатки.*

1. Вступ

З приходом діджиталізації більшість сфер побутового життя значно полегшились. Банківська сфера також зазнала змін – на ринку з’явились мобільні банкінги – застосунки банківських установ, за допомогою яких з легкістю можна виконати більшість банківських операцій фізично не відвідуючи саму установу. Заради приваблювання клієнтів розробники вимушені йти на поступки і зменшувати потужність захисту задля зручності, бо навряд когось із користувачів привабить довге і незручне проходження автентифікації, коли легше буде піти у найближче відділення. То ж переважна більшість користувачів вимагають від банківських застосунків більшого комфорту, не замислюючись при цьому про ризики безпеки.

Фінансовий сектор був і залишається привабливим для кіберзлочинців, зі збільшенням розвитку технологій, збільшується кількість атак. У контексті України з 2022 року кількість кібератак зросла на 2.8%, де кожна 10-та атака була здійснена на фінансовий сектор. На жаль, країна-агресор продовжує потуги розбити фінансову систему нашої країни, таким чином наносячи велику шкоду роботі держави [1]. Банківські застосунки мають низку особливостей з точки зору кібербезпеки, адже, на відмінну від більшості додатків, зберігають особисту інформацію клієнта і поєднуються безпосередньо із самою банківською установою.

2. Актуальні загрози та вразливості банківських додатків

Важливо усвідомлювати, що розвиток технологій та стратегій захисту будь-яких додатків, у тому числі і банківських, призводить до росту і розвитку іншої сторони – кіберзлочинності. Починаючи з 2020 року діджиталізація (цифровізація) різних сфер життя набула попу-

лярності і досі є одним з важливих аспектів ведення бізнесу чи іншої діяльності. Задля підвищення рівня конкурентоспроможності, банки додають все більше функцій та часом нехтують безпекою заради зручності.

Банкінги, як і інші програмні застосунки, що можуть надавати доступ до грошей, є привабливою мішенню для злочинців. То ж сьогодні клієнти банків мають турбуватись не тільки про те, як вберегти свою фізичну банківську картку й особисті дані, а і як убезпечити себе від мобільних-шахраїв, які мають у своєму розпорядженні «вагомий» арсенал різних злочинних схем та методик проведення атак для здобуття доступу до їх грошей.

Мобільний банкінг означає використання спеціального програмного застосунку, розробленого банком. Це відрізняється від банкінгу онлайн, який передбачає вхід на веб-сайт банку на телефоні та/чи через комп'ютер. Як не дивно, але це має певне значення при розгляді питань безпеки.

Банки мають більше контролю над безпекою рахунку при користуванні застосунком, ніж при використанні веб-сайту. Наприклад, шахраї можуть створювати фішингові сайти, схожі на сторінку входу банку, або перехоплювати користувацьку мережу *Wi-Fi*. Але злочинцям набагато важче вдатися до шахрайства у випадку програмного застосунку. Однак це не означає, що у такому випадку використання банкінгу є цілком безпечним [2].

Програми мобільного банку передають дані між пристроєм клієнта та сервером банку. З цього виділяється три основні можливості здійснення шахрайств пов'язаних з банкінгами:

1. Доступ на пристрої користувача;
2. Під час передачі даних;
3. Доступ на сервері самого банку.

Тож усі дії шахраїв будуть засновані на цих трьох аспектах. Варто також пам'ятати, що кіберзлочинці несуть загрозу не тільки клієнтам, а і самому банку для якого найголовнішим пріоритетом є довіра клієнтів [2].

Атаки соціальної інженерії. Атаки соціальної інженерії використовують психологію та «терміновість», щоб обманом змусити жертв піти на розкриття облікових даних, які пропонують шахраям доступ до фінансових рахунків. Такі дії можуть включати у себе повідомлення та дзвінки, що надходять нібито з банку. Насправді ж, злочинці змушують повірити клієнта, що його рахунок якимось чином під загрозою і усе, що необхідно зробити – надати необхідні секретні дані.

Також поширеним є погроза «зламу» картки і маніпуляція про необхідність здійснення переказу на інший рахунок. Якщо клієнт погоджується, то фактично власноруч здійснює переказ, який неможливо скасувати, на реквізити зловмисника [2].

Фішинг. Фішинг є однією з найулюбленіших стратегій шахраїв для викрадення інформації або компрометацію пристроїв потенційних жертв. Фішинг-лист, що надходить під виглядом звичайного і містить у собі посилання, файли і так далі, у випадку завантаження активізує свої зловмисні наміри. Ці електронні листи можуть виглядати так само, як листи, які клієнти звикли отримувати від свого банку, і відправник може навіть підробити ім'я «від» для того, щоб виглядати легітимним [2]. Найгіршим у такий спосіб є той факт, що посилання у фішингових електронних листах можуть завантажити на пристрій жертви зловмисне програмне забезпечення (ПЗ), яке в наступному надасть хакерам доступ до мобільної банківської програми. Фішингові електронні листи також не обов'язково надходять від банку, наприклад можна отримати зловмисний електронний лист від шахраїв, які видають себе за *Netflix*, кур'єрську службу тощо [2].

Фізична крадіжка пристрою. Мабуть, один з найпримітивніших способів, проте також небезпечний – викрадення пристрою. У деяких випадках, пристрій навіть не потрібно викра-

дати, клієнт сам віддає його у руки, наприклад, відносячи телефон до ремонту у неперевірені сервіси. Хакери з відносною легкість зможуть знайти доступ до такого пристрою і до банківських додатків, використовуючи надалі пристрій клієнта для своїх дій [2].

Підробка банківських додатків. Якщо шахраї не зможуть отримати доступ до вашої мобільної банківської програми, вони спробують обманом змусити вас використовувати шахрайську програму. Так, наприклад, за 2020 рік ФБР (*Федеральне Бюро Розслідувань*) повідомило, що було виявлено майже 65000 підроблених банківських програм [3]. Ці підроблені програми виглядають, як цілком законні, але після вводу облікових даних, замість входу, користувач отримує повідомлення про помилку. У той же час шахрай отримав облікову інформацію жертви буде намагатися увійти у обліковий запис у справжньому додатку, а коли ж користувач зрозуміє, що його вже ошукали, то може бути вже пізно [2].

Зловмисне програмне забезпечення – кейлогери

Хакери використовують тип зловмисного ПЗ, яке записує всю інформацію, яка вводиться власником гаджету з якого відбувається сеанс банкінгу, зокрема банківські рахунки і паролі. При завантаженні додатків під контролем кейлогерів, злочинці зможуть легко зайти у відповідну банківську програму. Навіть гірше, можна випадково завантажити зловмисне ПЗ на свій пристрій, просто від сканувавши відповідний *QR*-код у відкритому доступі [2]. Тож навіть, якщо не завантажувати шахрайську банківську програму, шахраї все одно можуть отримати доступ до рахунків через інші заражені шкідливим ПЗ, програмні додатки.

Інші види шахрайств. Окрім вже перерахованих видів є ще багато зловмисних дій направлених на викрадення клієнтських статків, які варті не меншої уваги.

- *Трояни Android, такі, як SharkBot*. Основна мета *SharkBot* – ініціювати грошові перекази зі зламаних пристроїв за допомогою технології автоматичних систем переказу (*ATS*) в обхід механізмів багатофакторної автентифікації [4].
- *Атаки за допомогою програм вимагачів* – при виконанні атаки шахраї викрадають і шифрують важливі фінансові документи, блокують клієнтів у системах, паралізують банківські системи і за спокій вимагають викуп [5].
- *Незашифровані дані* – здебільшого уся важлива інформація шифрується, проте деякі дані лишаються незашифрованими на банківському сервері, зловмисники націлені знайти ці дані про клієнтів [5].
- *Атаки на одноразові паролі* – часто елементом безпеки є використання одноразових паролів, зловмисники можуть намагатись перехопити паролі з мобільних пристроїв користувачів, щоб використати їх на свою користь [5].
- *Атаки на зв'язок* – у даній атаці кіберзлочинці використовують шкідливе ПЗ для перехоплення комунікації між мобільним застосунком і банківським сервером, та інші [5].

Враховуючи все вищезазначене слід підкреслити, що загрозу мобільним банкінгам несуть не тільки кіберзлочинці, а і необізнаність працівників та користувачів гаджетів та послуг відповідних сервісів, з питань ІБ.

3. Стандарти кібербезпеки мобільних банкінгів у Європі та світі

Довіра є основою функціонування банківської системи, руйнування іміджу банку призводить до стрімкого спадання клієнтського потоку та негативно впливає на усю подальшу роботу організації. Саме тому банківські установи не шкодують витрат на розвиток кібербезпеки і постійно оновлюють свої системи згідно нових стандартизацій.

Сфера банківських мобільних застосунків не стала виключенням, а навпаки потребує все більшої уваги. Зважаючи на європейський досвід, можна помітити, що через важливість

кібербезпеки у банківському секторі, самі банки не можуть визначати, які стандарти безпеки їм використовувати. У країнах Європейського Союзу (ЄС) право приймати такі рішення не надається окремій країні чи організації, а безпосередньо відбувається на рівні ЄС і є чинними та однаковими для всіх країн учасників. Прикладами таких рішень є *PSD2* – директива про платіжні послуги. А також *RTS* – делегований регламент комісії ЄС 2018/389, який називають доповненням до *PSD2* [6].

RTS доповнює Директиву (ЄС) 2015/2366 Європейського Парламенту та Ради стосовно нормативних технічних стандартів для надійної автентифікації клієнта та загальних і безпечних відкритих стандартів зв'язку. 16 серпня 2022 року Європейська Комісія опублікувала Делегований Регламент Комісії (ЄС) від 3.8.2022, який вносить зміни до регуляторних технічних стандартів (РТС), викладених у Делегованому Регламенті 2018/389, зазначеному вище. Зміни стосувались 90-денного звільнення для доступу до рахунку [7].

Однією з ключових ініціатив в напрямку безпеки є Директива *PSD2*. Одним з основних положень цієї директиви стало введення двофакторної автентифікації для клієнтів банків. Тепер банки повинні вимагати від своїх клієнтів використання принаймні двох компонентів для автентифікації, забезпечуючи високий рівень захисту [6].

Ці компоненти можуть належати до трьох основних категорій: - *«щось, що ви знаєте»*, наприклад, пароль; - *«щось, що ви маєте»*, наприклад, документи, які знаходяться у вас; - та *«щось, що ви є»*, наприклад, біометричні дані. Унікальність цього підходу полягає в тому, що ці компоненти можуть діяти незалежно один від одного, таким чином зменшуючи вразливість системи до порушень [6].

Директива *PSD2* покладає велику частку відповідальності за інциденти на банки, змушуючи їх активно турбуватись про покращення систем безпеки. Однак вона також полегшує відповідальність клієнтів за можливі інциденти, роблячи банківські застосунки більш надійними та безпечними [6].

Поточний *RTS* для надійної автентифікації клієнта та спільного і безпечного зв'язку (*SCA*) дозволяє не вимагати виконувати надійну автентифікацію клієнтів за умови, що: доступ обмежений лише до балансу рахунку та/або недавньої історії транзакцій, конфіденційні платіжні дані не розкриваються, а також *SCA* застосовується, коли доступ до інформації здійснюється вперше та принаймні кожні 90 днів після цього. У 2021 році було запропоновано ввести певні правки до директиви, а саме [7]:

- запровадження обов'язкового винятку для *SCA* для конкретного випадку, коли доступ здійснюється через AISP і лише за умови виконання певних умов;
- обмеження сфери дії добровільного виключення випадками, коли клієнт безпосередньо отримує доступ до інформації про обліковий запис;
- подовжувати терміни оновлення *SCA* від кожні 90 днів до кожні 180 днів, коли доступ до інформації здійснюється через *AISP* або безпосередньо клієнтом.

Додатково, банки, що пропонують електронні банківські послуги, вживають заходів для мінімізації ризиків використання різноманітних атак, таких як фішинг та інших. Тут важливою стає роль токенів, які використовуються для забезпечення безпеки автентифікації. Ці токени можуть бути апаратними або мобільними, прикладами є *tProc ECC* та *tPro Mobile* [6].

Comarch tPro ECC ідеально відповідає вимогам клієнтів, які висувають високі стандарти щодо швидкості, ефективності та комфорту в сфері безпеки онлайн банкінгу. Цей невеликий та легкий *USB*-токен, який не вимагає встановлення драйверів, призначений переважно для авторизації документів та онлайн-транзакцій, а також для підтвердження особи за допомогою електронного підпису [6].

Процес підписання передбачає автентифікацію користувача за допомогою кнопки, вбудованої в пристрій. Це забезпечує захист транзакцій від віддалених атак, гарантуючи, що жодна третя сторона не матиме доступу до інструкцій без відома користувача.

tPro Mobile – це мобільна платформа, яка підтримує надійну автентифікацію користувачів і авторизацію транзакцій відповідно до директиви *PSD2*. Вона складається із зовнішньої програми та бібліотек розробки, які інтегруються з існуючими продуктами [6].

Більшість банків також використовують *PUSH*-повідомлення та біометричні методи для надання додаткових гарантій безпеки в процесі використання мобільного банкінгу.

Варто також зазначити кілька нових вимог до мобільного банкінгу, які були опубліковані в період з 2021 по 2022 рік у різних країнах світу. Такі нові вимоги можна поділити на дві категорії: вимоги про покращення цифрової ідентифікації та вимоги щодо захисту персональних даних. Про покращення захисту цифрової ідентифікації [8]:

- Данія замінює *NemID* на вдосконалений *MitID* для схвалення платежів і входів;
- Канада запускає програму *Voila Verified Trustmark*, яка видає знаки довіри організаціям, що демонструють відповідність компонентам *PCTF*;
- Європейська комісія завершує роботу над інструментарієм для країн-членів, який міститиме перелік конкретних архітектур, найкращих практик, стандартів, посилань та рекомендацій щодо створення цифрових гаманців;
- уряд Федеральної ради Швейцарії розробляє державну інфраструктуру *E-ID*. Вона буде використовуватися постачальниками ідентифікаційних даних, агентами, довіреними особами або постачальниками ідентифікаційних гаманців;
- Національний інститут стандартів і технологій США випускає для громадського обговорення проект Керівництва з цифрової ідентичності для протидії фішинговим атакам з використанням фіш-стійких автентифікаторів.

Вимоги щодо захисту персональних даних [8]:

- в Японії 1 квітня 2022 року набули чинності правила застосування Закону про захист персональних даних, які зобов'язують суб'єктів повідомляти про порушення даних до комісії із захисту персональних даних та застосовувати норми щодо суб'єктів, які їх порушують;
- Швейцарія ухвалила Закон про захист даних, який зобов'язує компанії негайно повідомляти про серйозні порушення даних федеральному комісару із захисту даних та інформації.

4. Стандартизація кібербезпеки банківських застосунків в Україні

Основним документом для регулювання банківської діяльності в Україні є Закон про банки і банківську діяльність. Цей закон визначає організаційну структуру банківської системи, а також економічні та правові основи для створення, функціонування, реорганізації та ліквідації банків. Основною метою цього законодавства є юридичне забезпечення захисту законних інтересів вкладників та інших клієнтів банків. Також, воно спрямоване на забезпечення стійкого розвитку та стабільності банківської системи. Крім того, його ціль – створення сприятливих умов для економічного розвитку України та встановлення належного конкурентного середовища на фінансовому ринку. За допомогою цього закону створюються необхідні рамки для підтримки ефективності функціонування фінансових інститутів, що сприяє загальному економічному добробуту країни [9].

Вітчизняні системи мобільних банкінгів поки не регулюються повністю відповідно до стандартизацій ЄС, проте вже не перший рік проходить ряд змін. Так, з 1 квітня 2023 року, Україна почала використовувати міжнародний стандарт ISO 20022. Він дозволяє стандарти-

зувати обмін фінансовою інформацією, спрощуючи комунікацію між різними фінансовими установами та підвищуючи ефективність операцій. Його впровадження має на меті поліпшити якість та надійність фінансових послуг [10].

tProc ECC апаратний маркер (згаданий вище) віднедавна доступний і в Україні. Даний апаратний маркер є стійким до віддалених атак, адже використовує криптографію еліптичної кривої. Вітчизняна версія токену була розроблена в співпраці з локальним дистриб'ютором *Comarch IT Park* і відповідає державному стандарту електронного підпису. Крім того, вона підтримує геш-функцію «Купина». Це робить *tProc ECC* добре адаптованим до державних стандартів та легко інтегрованим в інфраструктуру будь-якого вітчизняного банку [6].

PCI DSS – ще один стандарт впроваджений в Україні. Загалом його створення ініціювали міжнародні платіжні системи *American Express, Visa, Mastercard, JCB* та *Discover*. Стандарт *PCI DSS* визначає 12 вимог, які складають комплекс заходів, обов'язкових для досягнення максимального рівня безпеки інформації про власників платіжних карток. Ці вимоги стосуються усіх етапів обробки даних – від їх передачі до зберігання та обробки в інформаційно-технологічних структурах організацій. Ці вимоги включають у себе [11]:

- захист системи включає у себе забезпечення безпеки систем, що обробляють платіжні дані;
- захист власницьких даних описує захист від доступу до даних власників платіжних карток;
- захист мережі для запобігання несанкціонованому доступу до мережі, що обробляє платіжні дані;
- захист від шкідливих програм;
- захист доступу описує обмеження доступу до даних лише авторизованим користувачам;
- розвиток та тестування системи безпеки;
- підтримка політик безпеки включає запровадження та підтримка ефективних політик безпеки;
- захист фізичного доступу вимагає обмеження фізичного доступу до приміщень, що містять обладнання для обробки платіжних даних;
- моніторинг та виявлення інцидентів;
- захист від зовнішніх атак;
- управління підтримкою та обслуговуванням;
- політики та процедури безпеки пропонують розробку та впровадження політик та процедур безпеки для забезпечення відповідності стандарту.

5. Мобільні банківські застосунки: огляд функцій та ризиків

У процесі розвитку банківські операції у мобільних застосунках постійно розширювали свій спектр і вже зараз користувачі мають змогу не тільки здійснювати прості транзакції та відслідкувати стан рахунку, а і оформити кредит, переглянути наявні комунальні платежі, оновити документи, що пов’язані з карткою, поповнити мобільний та ще багато іншого.

Можна сказати, що історія мобільних банкінгів бере свій початок з *«Bank of America»*, який впровадив систему під назвою *«Electronic Recording Machine, Accounting and Credit»* (*ERMA*) у 1950-х роках. *ERMA* була призначена для автоматизації банківських операцій, включаючи обробку чеків та інші транзакції. *ERMA* була революційною технологією, система визначалася, як комп'ютеризований облік чеків та банківських транзакцій, і вона використовувалася для автоматизації та полегшення роботи банківських операцій. Основні можливості *ERMA* включали: - читаючий пристрій для чеків; збереження інформації про транзакції;

передачу даних, тобто ця система дозволяла передавати інформацію між різними банківськими підрозділами та об'єктами [12].

Першим банкінгом в Україні став «Приват24». Приват24, як мобільний застосунок, був вперше представлений у 2011 році ПриватБанком, який вже на той момент був лідером вітчизняного банкінгового сектору. Цей мобільний застосунок став важливим інструментом для клієнтів банку, що дозволяє їм здійснювати різноманітні банківські операції саме через мобільні пристрої. Для створення Приват24 потрібна була сучасна технологічна інфраструктура для обробки та збереження фінансової інформації користувачів, забезпечення безпеки та зручності користування. З урахуванням чутливості фінансової інформації, важливим етапом було впровадження найвищих стандартів безпеки, таких як *PCI DSS*, щоб захистити дані користувачів від несанкціонованого доступу [11].

З часів створення Приват24 в Україні з'явилось багато банківських застосунків, таких як Monobank, Raiffeisen Online, Ощад24, Альфа-Мобайл та інші. Кожен з цих додатків надає клієнтам зручний доступ до банківських послуг за допомогою мобільного пристрою та має певні особливості безпеки та користувацького інтерфейсу. Асоціація ЄМА провела дослідження у якому було розглянуто дані аспекти. (табл.1-2) [14].

Таблиця 1 – Аспекти зручності

Table 1 – Convenience aspects

Банк	Кредитна лінія у застосунку	Підв'язка карток інших банків	Оплата будь-якого рахунку з застосунку	Відображення різних рахунків клієнта	Вимкнення подвійної конвертації	Відкриття валютного депозиту
Monobank	+	+	-	+	+	+
Sense bank	+	+	-	+	+	+
А-банк	+	+	-	+	+	+
Приват-Банк	+	+	+	+	+	+
ПУМБ	+	+	-	-	-	+
Укргазбанк	-	+	-	-	-	+
Укрсиббанк	-	+	-	-	-	-
Otpbank	-	+	-	-	-	-
Райффайзен банк	-	-	-	-	-	-
Ощадбанк	-	-	-	-	-	-

Таблиця 2 – Аспекти безпеки

Table 2 – Security Aspects

Банк	Зміна *PIN* у застосунку	*3D*-secure можливість вимкнути посилену автентифікацію	Керування перевіркою геолокації клієнта і отримувача платежу	Вибір власного *CVV* у додатку	Управління токенізованими застосунками	Керування підписками на ресурси застосунку
Monobank	+	+	+	+	+	+
Sense bank	+	-	+	-	+	+
А-банк	+	+	-	-	-	+
Приват-Банк	+	-	-	-	-	+
ПУМБ	+	-	+	-	-	-
Укргазбанк	+	-	-	-	-	-
Укрсиббанк	+	+	-	-	-	-
Otpbank	+	-	-	-	-	-
Райффайзен банк	+	-	-	-	-	-
Ощадбанк	-	+	-	-	-	-

За даними табл. 1, помітно, що такі додатки, як Monobank, Sense bank, А-банк, Приват-Банк є помітними лідерами за зручністю.

Спостерігається достатня увага до *аспектів зручності* у більшості найпопулярніших банківських додатків. Що ж стосується *аспектів безпеки (див. табл.2)*, то варто відмітити, що більшість банків не мають повного комплекту усіх аспектів. Єдиний банк, що містить у собі всі аспекти, це Monobank, який при цьому не має фізичної установи банку. Слід зазначити, що в усіх додатках присутні: - цифрова картка, онлайн підтримка та можливість відкриття депозиту. Також можна спостерігати те, що банки здебільшого не мають ніяких аспектів, окрім зміни *PIN* у застосунку, та при цьому включають у себе більше аспектів зручності, орієнтуючись при цьому на користувацькі побажання, але це не заважає більшості додатків працювати коректно і надійно та все ж викликає певні вразливості у їх системах.

Варто зазначити, що вітчизняний ринок мобільних банківських застосунків продовжує успішно розвиватись і вже на сьогодні є досягнення якими можна пишатись. На сучасному фінансовому ринку з'явилася значна кількість онлайн-банків, включаючи Monobank, які надають клієнтам можливість користуватися фінансовими послугами шляхом використання мобільних застосунків. Це докорінно змінює взаємодію з банківськими послугами, надаючи максимальний комфорт власним клієнтам. Крім того, інші впливові банки держави, такі як ПриватБанк, Raiffeisen Bank, Oschadbank, OTP Bank, також вирішили приєднатися до можливостей онлайн-банкінгу, надаючи своїм клієнтам широкий спектр можливостей. Цей вибір фінансових мобільних програм відкриває нові можливості для клієнтів, дозволяючи їм обирати оптимальний сервіс, який відповідає їхнім користувальницьким потребам [15].

Україна вийшла на лідируючі позиції, впроваджуючи QR-коди для безготівкових платежів та стаючи однією з перших країн у світі, що використовує цю технологію. Це механізм оплати рахунків й здійснення покупок помітно зменшує ризик помилкових транзакцій та скорочує черги в банківських відділеннях. Прогрес у цьому напрямі став можливим завдяки технологічним інноваціям, таким як мобільні платежі та електронні гаманці, що сприяють зручності та ефективності фінансових операцій.

Проте вітчизняна сфера мобільних банківських застосунків продовжує зіштовхуватись з проблемами, які затримують її розвиток, наприклад: - недовіра клієнтів; відсутність стандартів і єдиних правил, щодо безпеки мобільних банківських додатків; мала кількість точок доступу до якісного інтернет; недостатність необхідного регулювання з боку держави та ін. Але ці проблеми не заважають активному збільшенню кількості користувачів банківськими сервісами. Так, кількість користувачів мобільними банкінгами у 2018 році становила 4,7 млн. осіб, а вже у 2022 році зросла до 8,9 млн. осіб, що є майже вдвічі більше попереднього значення. Ця статистика свідчить про велику популярність таких застосунків та «обіцяє» і надалі помітний розвиток їх можливостей [15].

6. Приклади кібератак, основні помилки та практичні рекомендації

Зусілля кіберзлочинців проникнути у банківську систему та викрасти клієнтські гроші чи дані відбуваються постійно. Проте більшість банків успішно справляються з такими атаками. Нерідко, особливо у старшого покоління, мобільні банківські застосунки викликають недовіру, адже вони звикли користуватись фізичними картками чи готівкою. Тому розробники намагаються довести клієнтській аудиторії, що їм можна довіряти. На жаль, рівень безпеки залежить не тільки від того, наскільки надійно побудована система відповідного мобільного додатку, а і від того, наскільки люди, що працюють з цією програмою є обізнаними у сфері ІБ. Саме тому банківські корпорації не шкодують грошей для проведення тренінгів, щодо питань безпеки серед своїх клієнтів та працівників.

Нещодавня кібератака на оператора мобільного зв'язку «Київстар» не була напряму пов'язана із банківською системою, проте «навела безладу» у деяких мережах. Так, окрім збою у роботи деяких відділень та банкоматів, перебої мережі зв'язку також призвели до погіршення роботи деяких банківських застосунків. Наприклад, Ощад24, який при проведенні транзакцій вимагає проходження подвійної автентифікації не міг провести автентифікацію за sms-кодом належним чином, бо через проблеми зв'язку повідомлення не могло надійти до абонентів «Київстар». У той же день DDoS-атаки зазнав і Monobank, проте фахівці змогли її відбити [16]. Одним за умовно «найгірших» періодів у кібербезпеці банківських додатків в Україні можна вважати початок 2022 року. 15 лютого відбулись наймасовіші атаки на різні сфери функціонування держави, у тому числі і у банківському секторі. Атакуючі намагалися здійснити DDoS-атаки, навантажуючи трафік банківських додатків у значущу кількість разів більше, ніж звичайні користувачі. Атаки зазнали мобільні застосунки ведучих вітчизняних банків таких як: - ПриватБанк, Ощадбанк, АльфаБанк, Monobank та інші. Ця атака припинилась приблизно опівночі та до серйозних втрат вона не призвела, проте було порушено штатну роботу додатків ще на деякий час після її відбиття [17].

Важливо підкреслити, що фатальні (тобто такі, що мають серозні наслідки) помилки при захисті мобільного банківського додатку можуть допускати, як самі працівники банку, так і його клієнти. Помилки в дизайні, що супроводжуються «слабкою» безпекою, реалізованою під час розробки відповідного ПЗ, потенційно можуть призвести до компрометації (зломів) додатку. До таких недоліків насамперед відносять [18]:

- *недостатню перевірку вхідних даних* – це може дозволити зловмисникам впровадити шкідливий код у застосунок;
- *слабке управління сеансами* – призводить до несанкціонованого доступу до облікових записів користувачів;
- *недостатню обробку помилок* – дає можливість розкриття конфіденційної інформації потенційними зловмисниками;
- *погано реалізований контроль доступу* – може призвести до несанкціонованих дій у застосунку;
- *відсутність безпечних методів кодування* – робить мобільний застосунок вразливим до різних типів атак.

Також є інші помилки, яких варто всіляко уникати, наприклад помилки в кодуванні можуть порушити роботу мобільного застосунку, іноді спричиняючи непередбачені наслідки. Ці вразливості ПЗ можуть виникати через такі проблеми, як: - переповнення буферу та/чи помилки рядка форматування тощо. Щоб захистити програмний додаток від подібних проблем, дуже важливо коректне проведення етапу тестування відповідного ПЗ та мати надійний метод тестування безпеки мобільного банкінгу. Цей метод допомагає помітити та локалізувати можливі помилки кодування, перш ніж вони стануть джерелом проблем безпеки, забезпечуючи неперервну та безпечну роботу відповідного додатку [18].

Застосунки мобільного банкінгу часто потребують підключення до зовнішніх джерел, щоб працювати в повному обсязі. Однак, використання зовнішніх джерел потенційно забезпечує більше точок входу для кіберзлочинців, щоб отримати доступ до конфіденційної інформації в програмі мобільного банкінгу користувачів. Ось чому ретельне тестування банківських застосунків є найважливішим чинником для їх подальшої безпечної роботи [18].

Якщо клієнти не планують установку програми мобільного банкінгу належним чином та не знайомі з комп'ютерними системами, то це може в купі може призвести до помилок. Так наприклад, вони можуть забути видалити облікові записи налагодження або паролі. Чи можуть зіткнутися з проблемами управління різними версіями. Тому важливо налагоджувати

увесь весь процес таким чином, щоб користувач однозначно міг пройти процес встановлення та налагодження додатку правильно і безпечно. Наприклад, у 2018 році в основних магазинах програмних застосунків, службами США було виявлено майже 65000 підроблених програм. Тому США проводять ретельний контроль банківських застосунків у відповідних онлайн-маркетах, тобто постійно перевіряють мережу на наявність шахрайських підробок популярних мобільних банківських застосунків. До того ж більшість великих банків США надають посилання на свій мобільний додаток безпосередньо на своєму власному веб-сайті [3].

Як згадувалось вище, користувачі не менше відповідальні за безпеку своїх рахунків, ніж банки. Тому рекомендовано щомісяця оновлювати паролі застосунків, оновлювати програмне забезпечення, уникати загроз не тільки мобільним банкінгам, а і усьому мобільному пристрою, при виявленні підозрілої активності повідомляти відповідні служби.

4. Висновки

1. Останні роки на фінансовому ринку спостерігається велика потреба у діджиталізації, одним з таких рішень стало широке поширення мобільних банківських застосунків, які у свою чергу вирішили багато проблем, що виникли у процесі пандемії, а потім війни.

2. Чим більше розвивається індустрія мобільного банкінгу, в тим більшої мірі кіберзлочинці намагаються знайти шлях до отримання «легких» грошей. Вони так само, як і спеціалісти з ІБ, досліджують шляхи доступу до застосунку, проте мають зовсім інші наміри. Онлайн шахраї постійно розробляють нові комплексні сценарії проведення атак, до складу яких залучають: - трояни, кейлогери, методи соціальної інженерії, експлуатацію вразливостей цільових систем, необачність користувачів й працівників банку та ін..

3. Вітчизняна сфера мобільного банкінгу потребує певних довершень з точки зору забезпечуваного рівня безпеки. Такими можуть стати: - єдина обов’язкова стандартизація для всіх банків, встановлення більш стійких точок доступу до мережі інтернет, впровадження контролю над поширенням нелегітимних (в т.ч. невідомих) програмних застосунків, розповсюдження онлайн тренінгів з безпеки серед працівників та клієнтів банківських установ.

Список літератури

[1] Бегаль І. (2023). Броня фінтеху за сотні тисяч доларів. Під час війни кібератаки на фінансовий бізнес почастішали в рази. Як компанії захищаються від нападів. (http://surl.li/pgzrw)

[2] The Risks of Mobile Banking Apps: Keep Your Money Safe. (2023). (https://www.identityguard.com/news/risks-of-using-mobile-banking-apps)

[3] Increased Use of Mobile Banking Apps Could Lead to Exploitation. (2020). (https://www.ic3.gov/Media/Y2020/PSA200610)

[4] SharkBot: a new generation of Android Trojans is targeting banks in Europe. (2021). (https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe)

[5] The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. (2023).(https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/)

[6] Comarch Financial Services. (https://www.comarch.com/finance/articles/)

[7] Albert Weatherill. Commission Delegated Regulation amending the RTS as regards the 90-day exemption for account access. (2022). (https://www.regulationtomorrow.com/eu/commission-delegated-regulation-amending-the-rts-as-regards-the-90-day-exemption-for-account-access/)

[8] Mobile Banking Compliance Requirements: Does Your Product Comply with Latest Trends. (2022). (https://binariks.com/blog/mobile-banking-compliance-requirements/)

[9] Відомості Верховної Ради України. Закон України Про банки і банківську діяльність. № 5-6, ст.30. (2001). (https://zakon.rada.gov.ua/laws/show/2121-14#Text)

[10] Міжнародний стандарт ISO 20022 - з 01 квітня 2023 року в Україні. (2023) (https://dn.tax.gov.ua/media-ark/news-ark/667242.html)

[11] PCI DSS Certification (https://getpci.com/)

[12] Our Heritage: Bank of America revolutionizes banking industry. (2020) (https://about.bankofamerica.com/en/our-company)

[13] ПриватБанк. (https://privatbank.ua/)

[14] ЄМА. (2023). (https://www.ema.com.ua/)

[15] Мірошник, Р., Кухта, І. (2023). ДІДЖИТАЛІЗАЦІЯ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ В СУЧАСНИХ УМОВАХ. Економіка та Суспільство, (49).
[16] Як кібератака на «Київстар» вплинула на роботу НБУ та банківської інфраструктури. (2023). (https://minfin.com.ua/ua/2023/12/14/117801942/)
[17] ПриватБанк, Ощадбанк, monobank, Альфа-Банк, урядові сайти та портал «Дія» зазнали кібератаки. (2022). (https://forbes.ua/news/dzherela-v-nbu-privatbank-ta-oshchadbank-zaznali-kiberataki-servisi-vzhe-vidnovlyuyut-robotu-15022022-3691)
[18] Enhancing Mobile Banking App Security: Top Threats and Solutions. (2023). (https://cybersecurity.asee.co/blog/mobile-security/enhancing-mobile-banking-app-security-top-threats-and-solutions/)

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

Authors:
Yelyzaveta Lohachova, CSD Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: lohachova2020kb11@student.karazin.ua

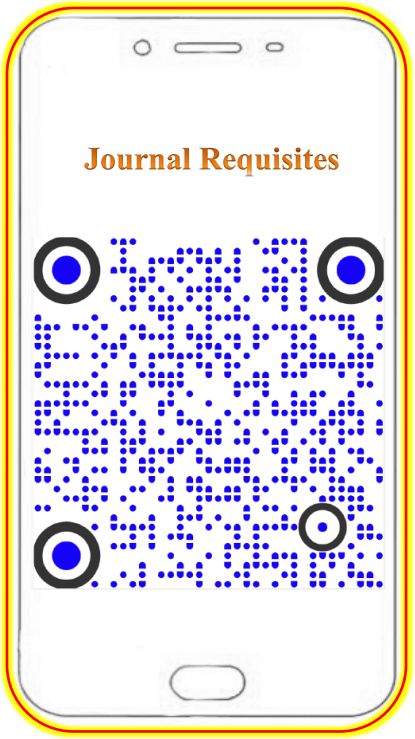
Maryna Yesina, Ph.D., Associate Professor, Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
ORCID: https://orcid.org/0000-0002-1252-7606
E-mail: m.v.yesina@karazin.ua

Vsevolod Bobukh, Ph.D., head of the information protection hardware department of JSC "IIT", Kharkiv, Ukraine.
E-mail: jsciitua@gmail.com

Analysis of cybersecurity features in banking mobile applications.

Abstract. This article discusses important aspects of cybersecurity in mobile banking applications. The article analyses in detail potential threats and effective strategies for their prevention and counteraction. Due to the rapid development of digital technologies in the banking industry, mobile applications and online services have become a necessary component of financial interaction between customers, providing convenient and efficient financial transactions. However, the development of the functionality of such applications gives rise to new cybersecurity challenges that information security professionals are actively addressing. The article is devoted to a comprehensive review of international and Ukrainian cybersecurity standards in the banking sector, and also contains quick review of mobile applications of well-known Ukrainian banks. Based on this review basic recommendations for improving cybersecurity in such applications are formulated. The article considers the impact of customer comfort on the level of security. In addition, the article considers the impact of the level of security in the banking sector on the overall digitalisation of the financial industry. It is noted that improving the level of security can stimulate and support digitalisation processes, ensuring customer trust and optimal use of mobile banking applications. A comprehensive approach to assessing the level of security, comparing various applications and standards (both Ukrainian and international), as well as considering the relationship between security issues and innovations in banking, make this work useful for understanding the genesis of cyber security in mobile banking.

Keywords: *Banking System, Security, Threats, Cybersecurity, Banking, Mobile Apps.*



Publishing, cover design: V.N. Karazin Kharkiv National University, 2023

Наукове видання

КОМП’ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 1(23) 2023

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, *та ін. мовами*

Комп’ютерне верстання – Єсіна М.В., Федоренко В.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing

CS&CS

2023