КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.881
УДК 004.056.55:004.9:005.8

Прокопович-Ткаченко Дмитро Ігорович
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів, Дніпро, Україна
старший науковий співробітник
Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», Київ, Україна
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Бакута Артем Ігорович
експерт з кібербезпеки
Національний координаційний центр кібербезпеки при РНБО України
ORCID ID: 0009-0001-5661-789X
ar.bakuta@gmail.com

Звєрєв Володимир Павлович
кандидат технічних наук
старший науковий співробітник
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державного торговельно-економічного університету, Київ, Україна
ORCID ID: 0000-0002-0907-0705
zwer172@gmail.com

Козаченко Ігор Миколайович
начальник підрозділу Державного центру кіберзахисту
Державної служби спеціального зв'язку та захисту інформації України
Київ, Україна
ORCID ID: 000-0002-0774-7284
kinkin2267@gmail.com

Черкаський Олександр Валерійович
незалежний дослідник у сфері кібербезпеки
Національний технічний університет «Дніпровська політехніка»
Дніпро, Україна.
ORCID ID: 0009-0006-3105-5217
asherjoseph.c@gmail.com

МОДЕЛЮВАННЯ ФІШИНГОВИХ СЦЕНАРІЇВ У КІБЕРПРОСТОРІ УКРАЇНИ: АНАЛІТИЧНИЙ ПІДХІД З ВИКОРИСТАННЯМ GRAFANA-ДОШКИ

Анотація. У статті представлено інноваційну методологію моделювання фішингових сценаріїв в українському кіберпросторі на основі інтеграції даних у середовищі Grafana. Основна увага приділена виявленню, класифікації та типізації фішингових доменів і каналів доставки шкідливого контенту (соціальні мережі, SMS, месенджери, мобільні застосунки). Запропоновано використання даних з HTTP-проксі-логів, DNS API та NetFlow-трафіку для побудови інтерактивних дашбордів, що візуалізують часові патерни, топ-домени, канали доставки й кампанії. Окрема увага приділяється економічній оцінці шкоди: розраховано фінансові втрати користувачів із врахуванням кількості переходів, середніх збитків на інцидент та тематики атак. У роботі також розглянуто застосування алгоритмів машинного навчання (decision trees, XGBoost) для автоматизованого виявлення фішингових URL на основі поведінкових, контентних і технічних ознак. Запропоновано концепцію інтеграції результатів візуалізації в SIEM-системи (Splunk, QRadar) для оперативного реагування на загрози. Результати дослідження мають практичне значення для формування національних платформ кіберзахисту, розробки державних реєстрів фішингових доменів, а також впровадження освітніх програм з кібергігієни. Представлений підхід поєднує технічну, аналітичну та політико-

освітню компоненти, що забезпечує його комплексний характер та релевантність в умовах сучасної гібридної війни проти України. Особливу увагу приділено візуальним інструментам: реалізовані дашборди Grafana дозволяють відстежувати піки фішингової активності, оцінювати канали доставки, тематику атак та регіональні особливості розповсюдження. Запропонована візуалізаційна модель сприяє підвищенню ефективності реагування на кіберінциденти завдяки інтерактивності, адаптивності та можливості глибокого аналізу даних у реальному часі. Дослідження також враховує соціо-культурний контекст України — аналізуються україномовні шаблони соціальної інженерії та демографічні чинники, що впливають на результативність фішингових кампаній. Застосування регіоналізованих підходів дозволяє підвищити точність прогнозування загроз і гнучкість захисних механізмів. Запропонована методика може бути адаптована до потреб державних органів, банківських структур та корпоративного сектору для побудови ефективних стратегій цифрової безпеки.

Ключові слова: аналітика фішингу; панель інструментів Grafana; український кіберпростір; SIEM; фінансові втрати; розвідка кіберзагроз; виявлення на основі штучного інтелекту; таксономія фішингу.

ВСТУП

В умовах сучасних геополітичних викликів та інформаційно-психологічного протистояння питання кібербезпеки набувають особливого значення. Україна, яка перебуває в епіцентрі гібридної війни, стала мішенню безпрецедентної хвилі кіберзагроз, серед яких особливе місце займають фішингові кампанії. Фішинг виступає одним з найефективніших інструментів соціальної інженерії, орієнтованих на масове ураження користувачів шляхом викрадення конфіденційних даних, фінансових ресурсів або втручання у роботу інформаційних систем держави [1], [7], [8]. Особливу увагу фішинговим атакам приділяють дослідники з різних країн, розглядаючи їх як невід'ємну складову сучасних гібридних воєн. Наприклад, Barichella зазначає, що саме кіберкомпонент відіграє одну з провідних ролей у російсько-українському конфлікті, а фішинг є важливим елементом у досягненні стратегічних цілей [1]. За даними Microsoft, український кіберпростір став ареною активних операцій, де фішинг і дезінформація тісно переплітаються, створюючи ефективні механізми психологічного впливу на користувачів [9]. Сучасні дослідження показують, що фішингові кампанії стають дедалі складнішими та різноманітнішими. Наприклад, дослідники з ETH Zurich вказують на зростання атак, що використовують тематичні повідомлення, адаптовані під локальний контекст, зокрема, український [12]. Це підтверджується практичними кейсами використання фейкових повідомлень від фінансових установ, поштових служб або державних органів України, таких як Monobank, PrivatBank або Nova Poshta [3], [5]. З огляду на різноманіття джерел фішингових атак, важливою складовою сучасних методологій аналізу кіберзагроз стала інтеграція даних у системи керування подіями та інформацією безпеки (SIEM). Проведені дослідження підтверджують, що використання таких систем як Splunk або QRadar у поєднанні з інтерактивними аналітичними платформами типу Grafana дозволяє ефективно виявляти, класифікувати та протидіяти фішинговим загрозам [2], [24]. Grafana як інструмент візуалізації даних займає центральне місце у представленому дослідженні завдяки широким можливостям інтеграції та високій інформативності своїх панелей. Останні дослідження підкреслюють ефективність використання Grafana для виявлення часових патернів і піків активності фішингових атак, які зазвичай синхронізуються з важливими політичними або суспільними подіями [25], [26]. Ще одним аспектом, який потребує особливої уваги, є економічна складова фішингових атак. Дослідження показують, що втрати від таких кіберінцидентів можуть бути досить суттєвими, особливо з огляду на те, що Україна є країною з великою кількістю активних користувачів онлайн-сервісів, мобільного банкінгу

та державних цифрових послуг [3], [4]. Враховуючи регіональні демографічні особливості та статистичні тренди, можна стверджувати, що фінансові втрати через фішинг стають значущим фактором ризику національної економіки [3], [23].

Новизна представленого дослідження полягає у поєднанні графічного аналізу фішингових кампаній через Grafana з кіберфорензичними підходами, економічною оцінкою потенційних втрат і застосуванням штучного інтелекту для превентивного виявлення загроз. Впровадження методів машинного навчання, таких як дерева рішень (decision trees) і алгоритми типу XGBoost, дозволяє значно підвищити ефективність автоматизованого виявлення нових і раніше невідомих сценаріїв атак [5], [6]. У сучасних умовах зростає необхідність активної інтеграції методик виявлення фішингових загроз в державні та приватні інформаційні системи України. Провідні дослідники та фахівці пропонують розробляти державні реєстри фішингових доменів, посилювати відповідальність операторів зв'язку за протидію поширенню шкідливого контенту, а також впроваджувати інтерактивні освітні програми з кібергігієни для населення [30]. Таким чином, метою даної публікації є аналіз кампаній фішингу через візуальні панелі Grafana з фокусом на загрози для користувачів у національному кіберпросторі України, враховуючи економічну складову та потенціал інтеграції штучного інтелекту для автоматизованого виявлення і протидії фішинговим загрозам. Запропонований підхід має на меті сприяти покращенню ефективності систем кібербезпеки та надавати практичні рекомендації щодо створення національних платформ кіберзахисту.

Постановка проблеми. У сучасних умовах гібридної війни проти України фішингові атаки набули особливої актуальності як інструмент кібернетичної та інформаційно-психологічної дестабілізації. Зловмисники дедалі активніше застосовують методи соціальної інженерії, спрямовані на масове викрадення конфіденційних даних, фінансових ресурсів, а також порушення функціонування інформаційних систем органів державної влади та стратегічних підприємств [1], [2]. Уразливість користувачів, посилена інформаційною перенасиченістю, низьким рівнем цифрової гігієни та обмеженою здатністю до розпізнавання маніпулятивного контенту, створює сприятливе середовище для масштабного розгортання фішингових кампаній.

Особливої загрози набувають фішингові сценарії, орієнтовані на локальні реалії — з використанням україномовних шаблонів, підроблених брендів національних банків, логістичних компаній та державних установ [3], [4]. Через складність структури таких атак традиційні системи виявлення, що спираються на сигнатурний аналіз або статичні чорні списки, виявляються неефективними або недостатньо оперативними [5]. Крім того, наявність різноманітних каналів доставки — від SMS і месенджерів до push-сповіщень і соціальних мереж — ускладнює централізований моніторинг загроз і прийняття рішень у реальному часі.

Зростаюча складність та варіативність фішингових атак потребує впровадження нових підходів до їх виявлення, аналізу та прогнозування. Зокрема, актуальним є створення інтегрованих систем, здатних оперативно обробляти великі обсяги різнорідних даних (логи проксі-серверів, DNS-запити, NetFlow-трафік) та надавати візуалізовану аналітику у форматі, зручному для експертів з кібербезпеки [6], [7]. Окрему проблему становить відсутність достатньо гнучких інструментів для класифікації атак, визначення їх джерел, каналів поширення та економічних наслідків.

Таким чином, постає необхідність у розробці комплексної методології, яка б поєднувала графічну аналітику (наприклад, на базі Grafana), елементи штучного інтелекту для прогнозування нових сценаріїв, а також механізми інтеграції з SIEM-системами. Такий підхід дозволить не лише підвищити ефективність реагування на

фішингові загрози, а й сформувати основу для національних платформ кіберзахисту, адаптованих до специфіки українського кіберпростору [8], [9].

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі питання фішингових атак розглядається як одна з ключових проблем цифрової безпеки, особливо в контексті гібридних загроз. Дослідники відзначають, що фішинг є ефективним методом соціальної інженерії, здатним паралізувати діяльність організацій, отримати несанкціонований доступ до конфіденційних даних і завдати фінансових збитків [1], [2]. Особливої уваги заслуговують дослідження, присвячені аналізу фішингових кампаній у контексті війни в Україні, де кіберпростір розглядається як поле бойових дій [1], [8], [9]. Окремий науковий напрям присвячено вивченню так званого «локалізованого фішингу», що передбачає адаптацію фішингових повідомлень до мовних, культурних та регіональних особливостей цільової аудиторії. Зокрема, аналітики з ETH Zurich наголошують на зростанні кількості україномовних фішингових шаблонів із використанням брендів українських банків і державних сервісів [12]. Подібні приклади підтверджуються дослідженнями, які демонструють активне підроблення сайтів таких компаній, як Monobank, PrivatBank та Nova Poshta [3], [5]. Інформаційно-аналітичні платформи, зокрема Grafana, активно розглядаються у працях сучасних дослідників як ефективний засіб для візуалізації та моніторингу фішингових загроз у реальному часі [2], [21], [22]. У поєднанні з SIEM-системами, такими як Splunk або QRadar, вони забезпечують можливість оперативного реагування на інциденти, а також аналітичну підтримку кіберзахисних центрів [6], [24].

Також слід відзначити зростання ролі штучного інтелекту у виявленні фішингових атак. У ряді робіт продемонстровано, що застосування алгоритмів машинного навчання — таких як дерева рішень, XGBoost або нейронні мережі — значно підвищує точність класифікації шкідливих URL і дозволяє виявляти нові, раніше невідомі сценарії атак [5], [6], [19]. Дослідження Hazell [4] і Chrysanthou [5] підтверджують потенціал таких підходів у межах реальних інфраструктур кіберзахисту. Таким чином, огляд наукової літератури підтверджує актуальність розробки інтегрованих рішень для виявлення фішингових загроз із використанням сучасних візуалізаційних інструментів, інтелектуального аналізу даних і урахуванням специфіки локального інформаційного середовища.

Мета статті. Метою статті є розроблення комплексного підходу до моделювання фішингових сценаріїв у кіберпросторі України з використанням інтерактивної аналітики в середовищі Grafana. У межах цього підходу передбачено побудову системи візуалізації кіберзагроз на основі багатоканальних мережевих даних (HTTP-проксі, DNS-запити, NetFlow-трафік), інтегрованої з SIEM-системами та підсиленої алгоритмами штучного інтелекту для автоматизованого виявлення нових атак.

Також мета статті полягає у виявленні зв’язків між тематикою фішингових кампаній, каналами їх доставки та рівнем фінансових втрат користувачів, що дозволяє формувати ефективні механізми реагування та прогнозування. Запропонований підхід спрямований на підвищення рівня ситуаційної обізнаності аналітиків кіберзахисту, оптимізацію аналітичної візуалізації, а також удосконалення державної політики у сфері протидії фішингу шляхом створення національних платформ для моніторингу загроз і просвітницьких ініціатив з цифрової гігієни [1], [3], [6].

МЕТОДИКА ДОСЛІДЖЕННЯ

Методологія дослідження передбачає комплексний аналіз фішингових кампаній на основі різноманітних цифрових джерел даних, отриманих із кількох незалежних каналів.

Основним джерелом інформації є HTTP-проксі-логи, які дозволяють реєструвати та аналізувати користувацький трафік, визначати патерни переходів за шкідливими посиланнями, а також виявляти джерела початкових інфікувань. Другим джерелом даних виступають API-логи DNS, що містять інформацію про запити до шкідливих доменів, дають змогу відстежувати динаміку поширення атак і забезпечують оперативне оновлення інформації щодо нових загроз. Третім джерелом є NetFlow-трафік, що фіксує потоки даних у мережах, дозволяючи детально аналізувати характер трафіку, визначати аномальні сплески активності та встановлювати взаємозв'язки між різними сегментами мережі. Для обробки та візуалізації отриманих даних використовуються Grafana та ELK (Elasticsearch, Logstash, Kibana) dashboards. Ці платформи дозволяють інтегрувати різні джерела даних у єдину систему, що забезпечує високу швидкість аналізу, зручність інтерпретації результатів, а також можливість оперативно реагувати на виявлені загрози. Dashboards у Grafana та ELK використовуються для надання вичерпних аналітичних звітів, що включають в себе метрики активності, часові піки інцидентів та класифікацію атак за типами та категоріями даних для виявлення й аналітики фішингових кампаній у національному кіберпросторі України. Вона структурно ілюструє взаємодію між основними джерелами даних, системами їх обробки й візуалізації та кінцевим користувачем аналітичної інформації.

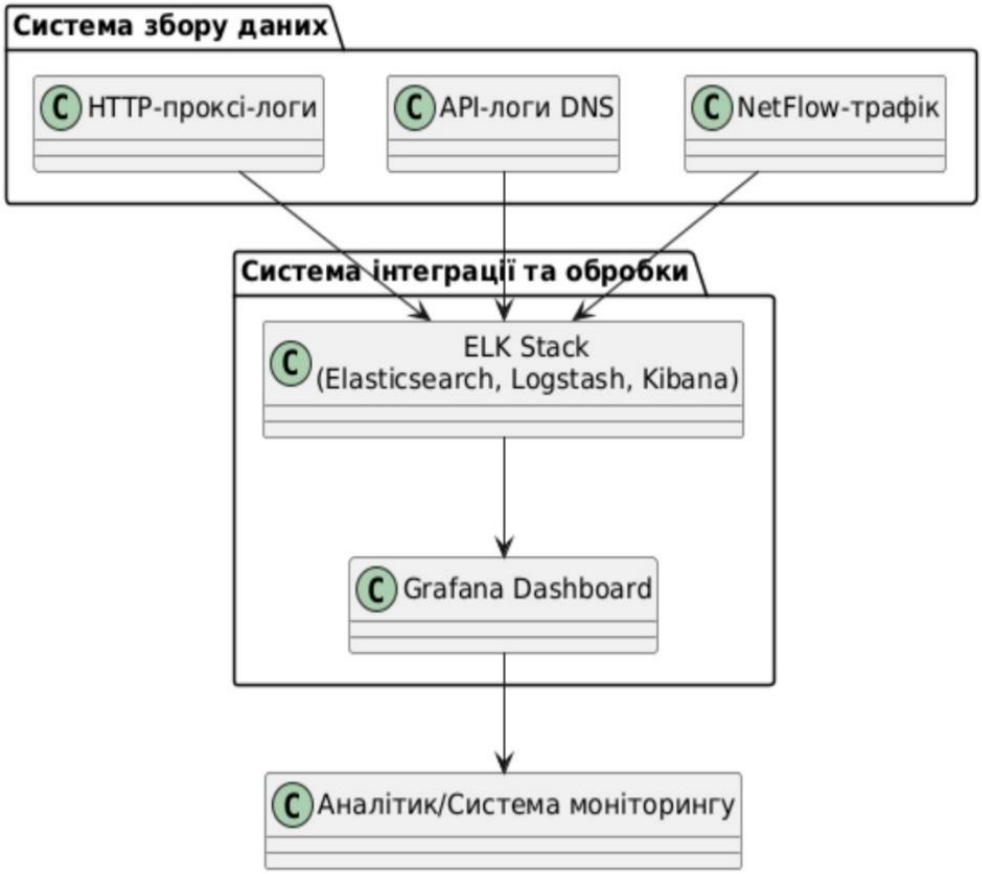

Рис. 1. Логіка та послідовність обробки та збору даних

Система збору даних.

HTTP-проксі-логи:

Фіксують всі веб-запити користувачів через корпоративні або організаційні проксі-сервери. Дозволяють визначити патерни переходів, джерела фішингових посилань і основні маршрути поширення атак.

API-логи DNS:

Зберігають інформацію про всі DNS-запити, що дозволяє ідентифікувати підозрілі або шкідливі домени, пов'язані з фішинговими кампаніями, а також відстежувати динаміку появи нових загроз.

NetFlow-трафік:

Мережеві потоки, що надають інформацію про характер взаємодії різних пристроїв і сегментів мережі. Дозволяють виявити аномальні піки активності, характерні для масових розсилок або атак.

Система інтеграції та обробки

ELK Stack (Elasticsearch, Logstash, Kibana):

Використовується для агрегації, обробки, зберігання й пошуку великих обсягів логів. Дані з різних джерел централізовано обробляються, збагачуються і готуються до подальшого аналізу.

Grafana Dashboard:

Виступає інструментом для побудови інтерактивних дашбордів. Візуалізує основні метрики: кількість унікальних переходів, активність за часом, топ-домени, канали доставки фішингу, кампанії тощо.

Аналітик/Система моніторингу

На виході з Grafana підготовлені аналітичні панелі, які споживаються аналітиками SOC (Security Operations Center) чи автоматизованими системами моніторингу для:

- Прийняття рішень щодо реагування на інциденти.
- Швидкого виявлення нових патернів атак.
- Генерації звітів для менеджменту або відповідальних державних органів.

Усі дані з різних мережевих джерел централізовано збираються, інтегруються й обробляються в ELK-стеку, після чого інтерактивно візуалізуються у Grafana для оперативного аналізу та реагування на кіберзагрози.

Візуалізаційна модель.

Одним з ключових аспектів методології є побудова комплексної моделі візуалізації даних, яка дозволяє ефективно представляти результати аналізу фішингових атак у зрозумілому для користувачів форматі. В рамках дослідження активно застосовуються такі методи візуалізації, як теплові карти (heatmaps), які дають можливість швидко оцінити географічне поширення атак та їхню інтенсивність за регіонами. Використання часових рядів (time series) дозволяє визначати періоди активності фішингових кампаній, виявляти часові патерни, які часто збігаються з певними подіями чи інформаційними приводами. Sankey-діаграми забезпечують візуалізацію потоку трафіку від джерел поширення до кінцевих користувачів, що допомагає ідентифікувати найбільш впливові канали доставки фішингових повідомлень. У дослідженні також представлені інтерактивні панелі Grafana, які забезпечують детальну розбивку інформації за різними параметрами. Панелі дозволяють візуалізувати джерела трафіку (наприклад, соціальні мережі, SMS-розсилки, мобільні застосунки), розподіл фішингових атак за регіонами України, а також типізацію атак за тематикою (банківський фішинг, фейкові служби доставки тощо). Інтерактивний характер Grafana-панелей дозволяє користувачам самостійно досліджувати дані, отримуючи глибші

ISSN 2663 - 4023

інсайти через застосування фільтрів і динамічних запитів, що значно полегшує завдання оперативного моніторингу та реагування на кіберзагрози. В умовах гібридної війни проти України, що супроводжується масштабними інформаційними та кібернетичними атаками, питання забезпечення кібербезпеки та захисту користувачів від фішингових кампаній набувають особливої актуальності . Сучасний фішинг — це не лише масове викрадення фінансових і персональних даних, а й інструмент впливу на критичні інформаційні потоки, фінансову стабільність і довіру громадян до цифрових сервісів держави. Відповіддю на ці виклики стає впровадження комплексних аналітичних платформ, які дозволяють автоматизовано виявляти, візуалізувати й аналізувати динаміку фішингових загроз у реальному часі.

Grafana — одна з провідних платформ для побудови інтерактивних дашбордів, яка дає змогу об’єднати різноманітні джерела даних (HTTP-проксі-логи, API-логи DNS, NetFlow-трафік) та представити результати аналізу у зручному для експертів форматі. Візуалізація даних у Grafana підвищує оперативність реагування на інциденти, дозволяє швидко ідентифікувати пікові періоди активності та джерела поширення загроз, а також здійснювати інтеграцію з SIEM-системами для подальшої автоматизації процесів кіберзахисту.

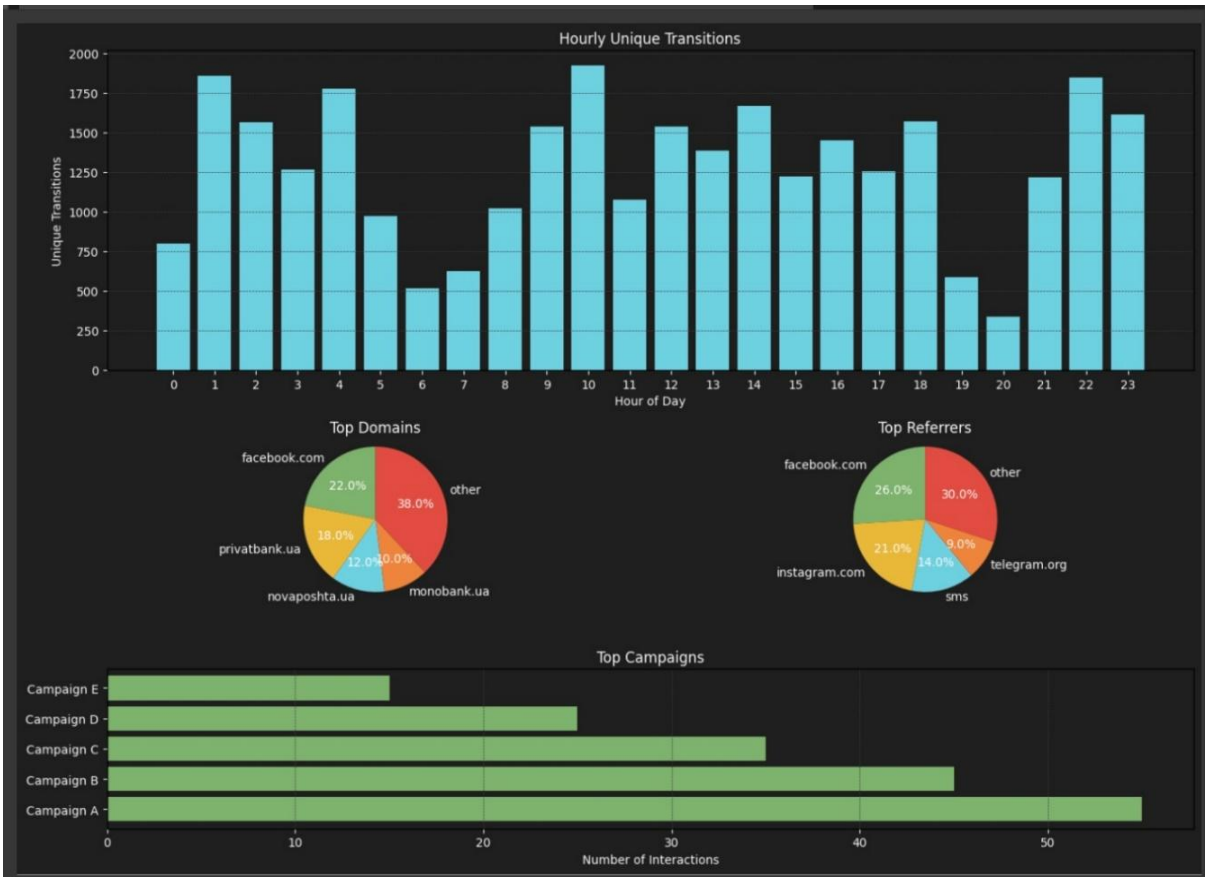

Рис. 2. Інтегрований дашборд, стилізований під інтерфейс Grafana з використанням темної кольорової палітри та характерних графічних елементів

Опис візуалізації дашборду.

1. Графік унікальних переходів (Hourly Unique Transitions):

Вгорі дашборду розміщено гістограму, яка відображає динаміку унікальних переходів за фішинговими посиланнями протягом доби. Цей графік дозволяє виявляти часові піки активності, що часто співпадають із зовнішніми тригерами (інформаційні кампанії, новинні анонси, кризові події) та сигналізують про початок масових атак.

2. Статистичні показники:

На панелі виділено основні кількісні метрики — загальна сума фінансових втрат, кількість унікальних і загальних переходів. Такі метрики є ключовими для експрес-оцінки масштабів інциденту та прийняття оперативних рішень.

3. Діаграми розподілу (Top Domains / Top Referrers):

Середній рядок містить дві кругові діаграми. Перша відображає структуру топових доменів, на які було здійснено найбільше переходів, що допомагає ідентифікувати основні цілі атак (наприклад, facebook.com, privatbank.ua, novaposhta.ua). Друга діаграма ілюструє основні джерела трафіку — соцмережі, SMS, месенджери, що використовуються як головні канали доставки фішингових повідомлень.

4. Горизонтальна гістограма кампаній (Top Campaigns):

У нижній частині дашборду розташовано горизонтальний bar chart, який ілюструє розподіл фішингової активності за різними кампаніями або сценаріями. Цей блок дозволяє оцінити вплив кожної окремої фішингової хвилі, порівняти ефективність тактик зловмисників та визначити пріоритети для реагування.

5. Графічне оформлення:

Всі компоненти дашборду витримані у фірмовому темному стилі Grafana з використанням характерної палітри: сині, зелені, жовті, помаранчеві й червоні відтінки для чіткої диференціації категорій. Така кольорова схема не лише відповідає візуальній ідентиці Grafana, а й забезпечує високу контрастність та зручність для швидкого сприйняття результатів аналітики.

Загалом, представлена візуалізація Grafana дозволяє:

- Оперативно моніторити ситуацію з фішинговими атаками у реальному часі.
- Виявляти критичні періоди і найуразливіші канали.
- Здійснювати глибоку аналітику інцидентів для подальшої автоматизації протидії кіберзагрозам та підготовки рекомендацій для державних і корпоративних центрів кібербезпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У рамках аналізу даних використовуються реєстри шкідливих доменів, а також open-source threat feeds, що дозволяє ідентифікувати найбільш активні та небезпечні домени, задіяні у фішингових кампаніях. Згідно з отриманими результатами, основними каналами доставки шкідливого контенту є SMS-фішинг, соціальні мережі, push-сповіщення та месенджери. SMS-фішинг залишається одним з найбільш популярних методів через його простоту та ефективність, тоді як соціальні мережі забезпечують високу швидкість розповсюдження інформації та значну аудиторію.

ISSN 2663 - 4023

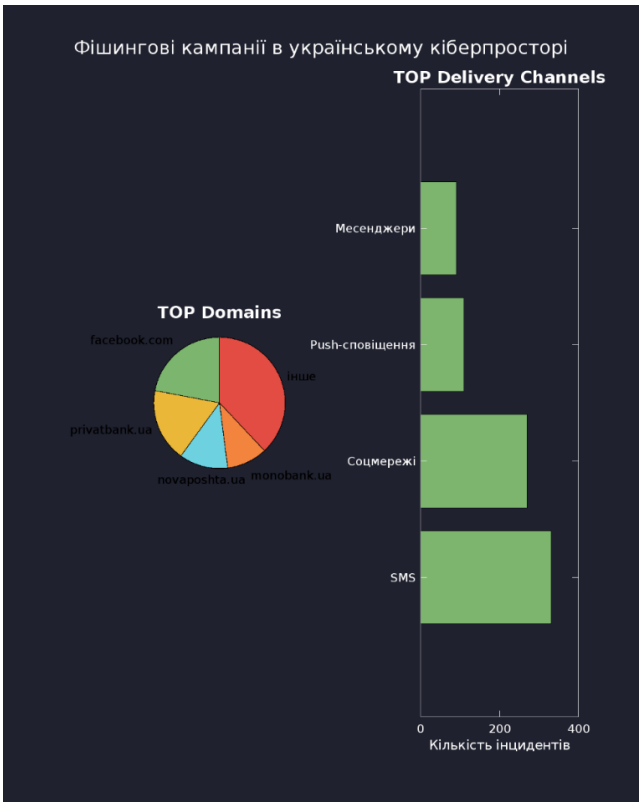

Рис. 3. Аналітичний дашборд для дослідження фішингових кампаній у національному кіберпросторі України

Візуалізація на рис. 3 складається з таких блоків:

1. Кругова діаграма «TOP Domains»

Ця діаграма ілюструє розподіл найактивніших доменів, що використовуються для фішингових атак.

facebook.com, privatbank.ua, novaposhta.ua, monobank.ua — відомі домени, що часто підробляються у фішингових кампаніях, оскільки користувачі їм довіряють.

«Інше» — сукупність менш поширених доменів, які також фіксуються у реєстрах шкідливих адрес.

За допомогою кругової діаграми можна швидко оцінити, які ресурси є найпривабливішими цілями для зловмисників і на які напрямки варто звернути увагу під час моніторингу.

2. Горизонтальна гістограма «TOP Delivery Channels»

Даний графік демонструє, які канали найчастіше використовуються для доставки шкідливого контенту до жертв:

SMS-фішинг — залишається наймасовішим і найпростішим каналом через доступність і відсутність складних технічних бар'єрів.

Соціальні мережі — забезпечують швидке поширення фішингових посилань серед великої аудиторії.

Push-сповіщення та месенджери — використовуються для персоніфікованої доставки, особливо під час масових атак або таргетованих кампаній.

Такий розподіл дозволяє аналітикам SOC чи CERT:

Виявляти найуразливіші канали доставки,

Фокусувати превентивні дії на тих векторах, які мають найбільший вплив,

Оцінювати ефективність впроваджених фільтрів і захисних механізмів.

Візуалізація стилізована під сучасний dark dashboard (темний фон, насичені кольори секторів), що забезпечує зручність для роботи вночі, високу контрастність і швидке сприйняття основних аналітичних висновків.

Пікова активність

Аналіз часових вікон пікової активності фішингових атак дозволив виявити кореляцію між посиленням атак та ключовими суспільно-політичними подіями, такими як державні оголошення, значні новини або кризові ситуації. Такі періоди характеризуються різким зростанням кількості атак та інтенсивності взаємодії з користувачами, що свідчить про використання зловмисниками психологічних факторів для досягнення максимальної ефективності кампаній.

Типізація тем

Типізація тем фішингових атак виявила, що найбільш поширеними є банківський фішинг, включаючи атаки на користувачів Monobank і PrivatBank, шахрайські повідомлення щодо «митної оплати» та фейкові служби доставки, такі як Nova Poshta. Ці теми є актуальними для українських користувачів і активно використовуються для обману жертв через їхню довіру до зазначених брендів та сервісів.

Оцінка збитків

Для комплексної оцінки фінансових втрат, пов’язаних з фішинговими атаками, використовується комбінований підхід, який включає кількісні та якісні методи аналізу. Центральним компонентом кількісної оцінки є визначення потенційних фінансових втрат на основі кількості унікальних переходів за фішинговими посиланнями та середньої суми викрадених коштів. В основі такого методу лежить ідея, що кожен зафіксований перехід є потенційною загрозою втрати коштів, отже, важливо обчислювати загальні збитки за формулою:

$$\text{Загальні збитки} = \text{Кількість унікальних переходів} \times \text{Середня сума викрадених коштів}$$

Середня сума викрадених коштів розраховується на базі аналітичних даних про попередні інциденти, враховуючи типи атак і категорії цільових аудиторій. Ця інформація регулярно оновлюється завдяки інтеграції даних із правоохоронних органів, банківських установ і незалежних аналітичних агентств. Додатково враховується регіональна демографія користувачів, що дозволяє уточнити оцінку шляхом корекції на специфіку різних регіонів України. Наприклад, в регіонах з більш високою цифровою грамотністю населення рівень фінансових втрат може бути меншим завдяки швидшому виявленню загроз. У регіонах з нижчим рівнем цифрової обізнаності населення спостерігається вища частота інцидентів та більші суми викрадених коштів, що підкреслює важливість врахування демографічних факторів при моделюванні збитків.

Статистичні тренди

Статистичний аналіз динаміки втрат дозволяє відслідковувати тенденції в активності фішингових кампаній та їхньому економічному впливі протягом певних періодів, зокрема кварталів. Аналіз втрат протягом кварталу демонструє чіткі патерни сезонності та реакції на зовнішні події. Як правило, пікові значення втрат припадають на періоди політичних, соціальних чи економічних потрясінь, коли рівень суспільної тривоги зростає, що посилює вразливість користувачів до соціальної інженерії. Важливим аспектом статистичного аналізу є сегментація втрат за типами пристроїв, операційними системами та мовними

локалізаціями користувачів. Ця сегментація виявила, що найбільш уразливими до фішингових атак залишаються мобільні пристрої, які використовують ОС Android, оскільки вони мають широку аудиторію, менш строгі стандарти безпеки та частіше стають мішенню шкідливих повідомлень через push-сповіщення і SMS. Водночас користувачі пристроїв на базі iOS демонструють нижчі показники втрат через більш строгі системи безпеки, які ускладнюють поширення шкідливого контенту. Крім того, мовна локалізація повідомлень відіграє важливу роль у визначенні ефективності фішингових атак. Згідно з даними дослідження, україномовні та російськомовні повідомлення демонструють найвищу ефективність серед населення України, тоді як англомовні фішингові повідомлення виявляються менш результативними через меншу довіру та нижчий рівень залученості цільової аудиторії. Загалом, отримані статистичні тренди дозволяють прогнозувати майбутню активність фішингових кампаній, підвищувати точність оцінки збитків та вдосконалювати механізми реагування на загрози, адаптуючи їх до особливостей різних сегментів користувачів.

Одним з ключових результатів дослідження стало формування ефективних сценаріїв інтеграції даних про фішингові атаки в системи керування подіями та інформацією безпеки (SIEM), зокрема Splunk та QRadar. Запропонована модель інтеграції забезпечує двонаправлену взаємодію між Grafana та SIEM-платформами, дозволяючи оперативно виявляти, аналізувати і реагувати на фішингові загрози. Завдяки цій інтеграції події, зафіксовані у Grafana, автоматично корелюються з логами інших джерел в Splunk чи QRadar, що дає змогу формувати комплексні сценарії реагування на основі широкого спектру даних. Важливим елементом інтеграції є виявлення аномальних переходів у реальному часі. Це здійснюється за допомогою алгоритмів автоматичного аналізу поведінкових шаблонів користувачів. Система ідентифікує аномалії у поведінці (наприклад, незвично часті переходи за фішинговими посиланнями, підозрілі часові патерни або нестандартні джерела трафіку) і автоматично надсилає сповіщення у SIEM-системи для подальшого аналізу фахівцями з кібербезпеки. Такий підхід забезпечує високу оперативність виявлення загроз і скорочує час реагування на інциденти, мінімізуючи потенційні втрати.

AI/ML-моделі

Значні результати отримані також у сфері застосування методів штучного інтелекту і машинного навчання (AI/ML) для класифікації і виявлення фішингових URL. У рамках дослідження розроблено та апробовано модель, засновану на алгоритмах дерев рішень (decision trees) і XGBoost, які продемонстрували високий рівень точності класифікації фішингових посилань. В основу моделей покладено детальну генерацію ознак, таких як специфіка доменного імені (довжина, використання символів, дата реєстрації), структура веб-сторінки (наявність форм авторизації, типові патерни розміщення елементів), а також геолокаційні параметри (аналіз походження запитів). Використання AI/ML-моделей дозволило не лише автоматизувати процес виявлення шкідливих URL, а й значно підвищити точність прогнозування нових атак. Ці моделі демонструють високу адаптивність до зміни стратегій зловмисників, ефективно розпізнають нові, раніше невідомі типи фішингових атак. Інтеграція таких рішень у реальні системи моніторингу дозволяє суттєво посилити кібербезпеку на національному рівні.

Блокування і попередження

Ефективне блокування фішингових загроз і своєчасне інформування користувачів є критичними елементами комплексної стратегії протидії фішингу. В ході дослідження виявлено, що найбільш результативним підходом є впровадження інтегрованих фільтрів

у браузери користувачів. Ці фільтри працюють на основі динамічно оновлюваних чорних списків, створених за допомогою даних з Grafana, SIEM-систем та AI-моделей. Блокування шкідливих URL на рівні браузерів дозволяє запобігти безпосередньому контакту користувача з потенційно небезпечним контентом. Ще одним ефективним методом виявилося повідомлення користувачів через мобільні застосунки банків. Цей канал комунікації забезпечує швидке інформування про актуальні фішингові загрози і рекомендації щодо запобіжних дій. У рамках дослідження було встановлено, що користувачі, які отримували регулярні сповіщення про фішингові загрози через мобільні додатки банків, демонстрували значно нижчі показники взаємодії з шкідливими посиланнями. Таким чином, інтеграція автоматичних засобів блокування шкідливих ресурсів і активна інформаційна кампанія серед користувачів сприяють значному зменшенню успішності фішингових атак. Ці заходи рекомендується розглядати як ключові складові державних стратегій кібербезпеки, впроваджувати на рівні національних платформ і приватних організацій, з метою створення безпечного кіберпростору для громадян України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження дозволяє стверджувати, що фішингові атаки в українському кіберпросторі залишаються однією з наймасштабніших та найдинамічніших форм кіберзагроз. У контексті гібридної війни фішинг перетворюється не лише на інструмент крадіжки даних і фінансових ресурсів, а й на механізм інформаційно-психологічного впливу на користувачів [1], [8], [9]. Аналіз сучасних підходів засвідчив обмеженість традиційних рішень на основі сигнатурних методів та статичних списків — вони виявляють низьку адаптивність до нових сценаріїв атак і не забезпечують оперативного реагування [5], [6].

Запропонована в статті методологія базується на трьох ключових компонентах: інтерактивній візуалізації даних у середовищі Grafana, інтеграції з SIEM-системами (Splunk, QRadar), а також застосуванні алгоритмів машинного навчання (XGBoost, decision trees) для виявлення нових фішингових шаблонів. Такий підхід демонструє значну гнучкість, масштабованість і здатність до адаптації у швидкозмінному середовищі кіберзагроз [2], [19], [24].

Особливу увагу приділено візуалізації фішингових кампаній, що включає графічне представлення часових піків активності, географічного розподілу, каналів доставки та фінансових наслідків. Завдяки використанню Grafana-дошок аналітики отримують зручний інструмент для моніторингу в реальному часі, ідентифікації аномалій та генерації звітів для оперативного реагування [21]–[23]. У поєднанні з механізмами SIEM-платформ така візуалізація дозволяє не лише виявляти, а й автоматизовано блокувати фішингові загрози.

Застосування AI/ML-моделей у межах дослідження продемонструвало високу точність класифікації фішингових URL. Врахування таких ознак, як структура домену, геолокація, шаблони веб-сторінки та поведінкові характеристики, дозволило системам виявляти навіть раніше невідомі атаки [5], [6], [19]. Це підтверджує перспективність включення інтелектуального аналізу в державні кіберзахисні стратегії.

Окремий акцент зроблено на соціально-освітній складовій: як показали результати, найбільш ефективними є гібридні підходи, що поєднують технічні фільтри (блокування через браузери, мобільні додатки банків) та активне інформування користувачів про

поточні фішингові загрози. Такі заходи знижують ймовірність переходу за шкідливими посиланнями, особливо у користувачів з нижчим рівнем цифрової грамотності [4], [30].

У результаті дослідження сформульовано низку практичних рекомендацій. По-перше, доцільним є впровадження національного реєстру фішингових доменів з відкритим API-доступом для комерційних і державних структур. По-друге, слід посилити відповідальність операторів мобільного зв'язку за розповсюдження шкідливих SMS. По-третє, варто розгорнути модульну освітню програму для держслужбовців і населення з акцентом на практики цифрової гігієни [3], [6], [30].

Таким чином, запропонована у статті концепція є цілісним підходом до моделювання, виявлення та попередження фішингових атак в Україні. Вона об'єднує технічні, аналітичні та освітні механізми захисту, адаптовані до українського контексту. Реалізація рекомендацій дозволить суттєво підвищити рівень національної кіберстійкості, мінімізувати фінансові втрати населення та державних структур, а також забезпечити інтеграцію сучасних рішень у стратегії цифрової трансформації країни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ACIG Journal. (2024). *Russia's cyber campaigns and the Ukraine war – from gray zone to red zone*. https://acigjournal.com/russia-cyber-campaigns-ukraine-war
2. Barichella, G. (2022). *The cybersecurity dimension of the war in Ukraine*. Institut Delors. https://institutdelors.eu/wp-content/uploads/2022/06/CybersecurityUkraine.pdf
3. Brandefense.io. (2022). *Analysis of hybrid warfare through Russia–Ukraine cyber war*. https://brandefense.io/hybrid-warfare-russia-ukraine-cyber
4. Center for Security Studies, ETH Zurich. (2018). *Hotspot analysis: Cyber and information warfare in the Ukrainian conflict*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Ukraine.pdf
5. Chrysanthou, A., Pantis, Y., & Patsakis, C. (2023). The anatomy of deception: Technical and human perspectives on a large-scale phishing campaign. *arXiv*. https://arxiv.org/abs/2305.03123
6. Center for Strategic & International Studies. (2025). *Russia's shadow war against the West*. https://www.csis.org/analysis/russias-shadow-war-against-west
7. Digital Front Lines. (2023). *The face of modern hybrid warfare*. https://www.digitalfrontlines.com/hybrid-warfare-ukraine
8. The Economist. (2025, March 2). *How Elon Musk's satellites have saved Ukraine and changed warfare*. https://economist.com/elon-musk-satellites-ukraine
9. Financial Times. (2023, February 10). *Europe battles "avalanche of disinformation" from Russia*. https://ft.com/europe-disinformation-russia
10. Finkle, J. (2016, January 7). U.S. firm blames Russian "Sandworm" hackers for Ukraine outage. *Reuters*. https://reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKCN0UL1ZZ20160107
11. Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2022). Russian propaganda on social media during the 2022 invasion of Ukraine. *arXiv*. https://arxiv.org/abs/2205.12382
12. Grafana Labs. (2025). *Success stories and case studies*. https://grafana.com/success
13. The Guardian. (2024, June 3). *Russia launching more sophisticated phishing attacks*. https://theguardian.com/russia-phishing-attacks-2024
14. Hazell, J. (2023). Spear phishing with large language models. *arXiv*. https://arxiv.org/abs/2305.06972
15. Ho, G., Thomas, K., Lee, K., & Grace, A. (2019). Detecting and characterizing lateral phishing at scale. *arXiv*. https://arxiv.org/abs/1908.00051
16. Microsoft. (2022, April 27). *The hybrid war in Ukraine*. Microsoft On the Issues. https://blogs.microsoft.com/hybrid-war-ukraine
17. NATO CCD COE & FireEye. (2015). *Cyber war in perspective: Russian aggression against Ukraine*. https://ccdcoe.org/uploads/2015/cyber-war-russian-aggression-ukraine.pdf
18. Nemec, M., Sys, M., Svenda, P., Klinc, D., & Matyas, V. (2017). The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security* (pp. 1637–1649). https://doi.org/10.1145/3139563.3139696

19. OpenThreat. (2025). *Real-time security analytics – Grafana dashboard integration with Wazuh*. https://openthreat.ro/real-time-security-analytics-grafana-dashboard-integration-with-wazuh
20. ProjectPro. (2025). *Grafana vs Power BI: Which tool is better?* https://www.projectpro.io/grafana-vs-power-bi-comparison
21. ResearchGate. (2023). *Cybersecurity in the context of hybrid warfare in Ukraine*. https://www.researchgate.net/publication/366774293
22. Reuters. (2024, August 5). *Russia's critics targeted with global hacking campaign*. https://reuters.com/russia-global-hacking-campaign
23. Sanger, D. E., & Barnes, J. E. (2021, December 21). U.S. and Britain help Ukraine prepare for potential Russian cyberassault. *The New York Times*. https://nytimes.com/us-britain-ukraine-cyberassault.html
24. SharePoint Europe. (2024). *Azure cost analysis dashboards on Grafana*. https://www.sharepointeurope.com/azure-cost-analysis-dashboards-grafana
25. Time Staff. (2022, December 14). *Inside the Kremlin's year of Ukraine propaganda*. *Time*. https://time.com/kremlin-ukraine-propaganda
26. UpGuard. (2025). *Grafana security rating, vendor risk report, and data breaches*. https://www.upguard.com/security-report/grafana
27. Wired. (2025, March 12). *Gamaredon: The turncoat spies relentlessly hacking Ukraine*. https://wired.com/gamaredon-ukraine-hacking
28. Wired. (2025, January 18). *A signal update fends off a phishing technique used in Russian espionage*. https://wired.com/signal-update-fends-off-phishing
29. Wikipedia contributors. (2025, July 18). *Emotet*. In *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Emotet
30. Wikipedia contributors. (2025, July 18). *Fancy Bear*. In *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Fancy_Bear

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Prokopovych-Tkachenko Dmytro
Candidate of Technical Sciences, Associate Professor
Head of the Department of Cybersecurity and Information Technologies,
University of Customs and Finance, Dnipro, Ukraine
Senior Researcher,
State Scientific Institution
"Institute of Information, Security and Law,
National Academy of Legal Sciences of Ukraine", Kyiv, Ukraine
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Artem Bakuta
Cybersecurity expert
National Coordination Center for Cybersecurity
at the National Security and Defense Council of Ukraine
ORCID ID: 0009-0001-5661-789X
ar.bakuta@gmail.com

Zverev Volodymyr
Candidate of Technical Sciences
Senior Researcher
Associate Professor, Department of Software Engineering and Cybersecurity,
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-0907-0705
zwer172@gmail.com

Kozachenko Igor
Head of the Department of the State Center for Cyber Defense
of the State Service for Special Communications and Information Protection of Ukraine
Kyiv, Ukraine
ORCID ID: 000-0002-0774-7284
kinkin2267@gmail.com

Cherkasky Oleksandr
Independent Researcher in Cybersecurity
National Technical University "Dnipro Polytechnic"
Dnipro, Ukraine
ORCID ID: 0009-0006-3105-5217
asherjoseph.c@gmail.com

MODELING PHISHING SCENARIOS IN UKRAINIAN CYBERSPACE: AN ANALYTICAL APPROACH USING GRAFANA-BOARD

Abstract. The article presents an innovative methodology for modeling phishing scenarios in Ukrainian cyberspace based on data integration in the Grafana environment. The main attention is paid to the detection, classification and typification of phishing domains and malicious content delivery channels (social networks, SMS, messengers, mobile applications). The use of data from HTTP proxy logs, DNS API and NetFlow traffic is proposed to build interactive dashboards that visualize time patterns, top domains, delivery channels and campaigns. Special attention is paid to the economic assessment of damage: financial losses of users are calculated taking into account the number of transitions, average losses per incident and attack topics. The paper also considers the use of machine learning algorithms (decision trees, XGBoost) for automated detection of phishing URLs based on behavioral, content and technical features. A concept for integrating visualization results into SIEM systems (Splunk, QRadar) for rapid response to threats is proposed. The research results are of practical importance for the formation of national cyber defense platforms, the development of state registries of phishing domains, and the implementation of educational programs on cyber

hygiene. The presented approach combines technical, analytical, and political and educational components, which ensures its comprehensive nature and relevance in the conditions of the modern hybrid war against Ukraine. Particular attention is paid to visual tools: the implemented Grafana dashboards allow you to track peaks of phishing activity, assess delivery channels, attack themes, and regional distribution features. The proposed visualization model helps increase the efficiency of responding to cyber incidents due to interactivity, adaptability, and the ability to perform deep data analysis in real time. The study also takes into account the socio-cultural context of Ukraine - Ukrainian-language social engineering patterns and demographic factors that affect the effectiveness of phishing campaigns are analyzed. The use of regionalized approaches allows for increased accuracy in threat prediction and flexibility of protective mechanisms. The proposed methodology can be adapted to the needs of government agencies, banking structures, and the corporate sector to build effective digital security strategies.

Keywords: phishing analytics; Grafana dashboard; Ukrainian cyberspace; SIEM; financial loss; cyber threat intelligence; AI-based detection; phishing taxonomy.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. ACIG Journal. (2024). *Russia's cyber campaigns and the Ukraine war – from gray zone to red zone*. https://acigjournal.com/russia-cyber-campaigns-ukraine-war
2. Barichella, G. (2022). *The cybersecurity dimension of the war in Ukraine*. Institut Delors. https://institutdelors.eu/wp-content/uploads/2022/06/CybersecurityUkraine.pdf
3. Brandefense.io. (2022). *Analysis of hybrid warfare through Russia–Ukraine cyber war*. https://brandefense.io/hybrid-warfare-russia-ukraine-cyber
4. Center for Security Studies, ETH Zurich. (2018). *Hotspot analysis: Cyber and information warfare in the Ukrainian conflict*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Ukraine.pdf
5. Chrysanthou, A., Pantis, Y., & Patsakis, C. (2023). The anatomy of deception: Technical and human perspectives on a large-scale phishing campaign. *arXiv*. https://arxiv.org/abs/2305.03123
6. Center for Strategic & International Studies. (2025). *Russia's shadow war against the West*. https://www.csis.org/analysis/russias-shadow-war-against-west
7. Digital Front Lines. (2023). *The face of modern hybrid warfare*. https://www.digitalfrontlines.com/hybrid-warfare-ukraine
8. The Economist. (2025, March 2). *How Elon Musk's satellites have saved Ukraine and changed warfare*. https://economist.com/elon-musk-satellites-ukraine
9. Financial Times. (2023, February 10). *Europe battles "avalanche of disinformation" from Russia*. https://ft.com/europe-disinformation-russia
10. Finkle, J. (2016, January 7). U.S. firm blames Russian "Sandworm" hackers for Ukraine outage. *Reuters*. https://reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKCN0UL1ZZ20160107
11. Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2022). Russian propaganda on social media during the 2022 invasion of Ukraine. *arXiv*. https://arxiv.org/abs/2205.12382
12. Grafana Labs. (2025). *Success stories and case studies*. https://grafana.com/success
13. The Guardian. (2024, June 3). *Russia launching more sophisticated phishing attacks*. https://theguardian.com/russia-phishing-attacks-2024
14. Hazell, J. (2023). Spear phishing with large language models. *arXiv*. https://arxiv.org/abs/2305.06972
15. Ho, G., Thomas, K., Lee, K., & Grace, A. (2019). Detecting and characterizing lateral phishing at scale. *arXiv*. https://arxiv.org/abs/1908.00051
16. Microsoft. (2022, April 27). *The hybrid war in Ukraine*. Microsoft On the Issues. https://blogs.microsoft.com/hybrid-war-ukraine
17. NATO CCD COE & FireEye. (2015). *Cyber war in perspective: Russian aggression against Ukraine*. https://ccdcoe.org/uploads/2015/cyber-war-russian-aggression-ukraine.pdf
18. Nemec, M., Sys, M., Svenda, P., Klinc, D., & Matyas, V. (2017). The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security* (pp. 1637–1649). https://doi.org/10.1145/3139563.3139696
19. OpenThreat. (2025). *Real-time security analytics – Grafana dashboard integration with Wazuh*. https://openthreat.ro/real-time-security-analytics-grafana-dashboard-integration-with-wazuh

20. ProjectPro. (2025). *Grafana vs Power BI: Which tool is better?* https://www.projectpro.io/grafana-vs-power-bi-comparison
21. ResearchGate. (2023). *Cybersecurity in the context of hybrid warfare in Ukraine*. https://www.researchgate.net/publication/366774293
22. Reuters. (2024, August 5). *Russia's critics targeted with global hacking campaign*. https://reuters.com/russia-global-hacking-campaign
23. Sanger, D. E., & Barnes, J. E. (2021, December 21). U.S. and Britain help Ukraine prepare for potential Russian cyberassault. *The New York Times*. https://nytimes.com/us-britain-ukraine-cyberassault.html
24. SharePoint Europe. (2024). *Azure cost analysis dashboards on Grafana*. https://www.sharepointeurope.com/azure-cost-analysis-dashboards-grafana
25. Time Staff. (2022, December 14). *Inside the Kremlin's year of Ukraine propaganda*. *Time*. https://time.com/kremlin-ukraine-propaganda
26. UpGuard. (2025). *Grafana security rating, vendor risk report, and data breaches*. https://www.upguard.com/security-report/grafana
27. Wired. (2025, March 12). *Gamaredon: The turncoat spies relentlessly hacking Ukraine*. https://wired.com/gamaredon-ukraine-hacking
28. Wired. (2025, January 18). *A signal update fends off a phishing technique used in Russian espionage*. https://wired.com/signal-update-fends-off-phishing
29. Wikipedia contributors. (2025, July 18). *Emotet*. In *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Emotet
30. Wikipedia contributors. (2025, July 18). *Fancy Bear*. In *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Fancy_Bear