КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.682
УДК 004.056.5

Івкова Валерія Сергіївна
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ ТА КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ ПРОТИДІЇ OSINT

Анотація. У сучасному світі питання захисту персональних даних набуває особливої актуальності, оскільки розвиток технологій та широке використання відкритих джерел інформації створюють нові виклики для безпеки. Стаття розглядає законодавчі аспекти регулювання використання даних у різних юрисдикціях, зокрема в Україні та ЄС, а також практичні загрози, такі як соціальна інженерія, фішинг та доксинг. На основі аналізу положень Загального регламенту захисту даних (GDPR) та Закону України «Про захист персональних даних», автори відзначають суттєві розбіжності у законодавстві, що регулює конфіденційність інформації. Особливу увагу приділено актуальним загрозам для персональних даних у контексті інформаційної безпеки, таким як атаки, що здійснюються за допомогою соціальної інженерії. Досліджується діяльність хакерських угрупувань, що використовують особисті дані для створення підроблених профілів у месенджерах, з метою отримання чутливих даних або доступу до облікових записів. Розглядаються приклади OSINT-технологій, що застосовуються зловмисниками для збору даних з відкритих джерел, а також їх використання для доксингу, де без згоди осіб публікуються їхні персональні дані, що несе потенційну загрозу їхній безпеці. Також вказано на зростаючі ризики фішингових атак, спрямованих на користувачів електронної пошти та браузерів, а також нові тактики, такі як багатоступеневий фішинг, що ускладнює виявлення та блокування таких атак. Окрім того, підкреслюється значення медіаграмотності та кібергігієни для зниження ризиків порушення конфіденційності та підвищення обізнаності про правила безпечної роботи з інформаційними технологіями. Стаття робить висновок про необхідність системного підходу до захисту конфіденційності даних, що включає правове регулювання, впровадження сучасних технологій для захисту інформації, а також підвищення рівня медіаграмотності серед населення. Запропоновано заходи, що включають імплементацію європейських стандартів захисту даних, які могли б стати надійною основою для посилення захисту персональних даних в Україні.

Ключові слова: персональні дані; конфіденційна інформація; доксінг; OSINT; кібербезпека.

ВСТУП

В епоху цифровізації величезні обсяги інформації, включаючи персональні дані, можуть бути отримані за допомогою розвідки по відкритих джерелах (OSINT). Проблема захисту інформації стає ще більш актуальною через збільшення кібератак та зловмисних дій, які спрямовані на несанкціонований збір та використання персональних і конфіденційних даних, особливо в умовах збройної агресії російської федерації проти

України. OSINT дозволяє зловмисникам та ворогу знаходити вразливі місця в системах безпеки, використовуючи відкриті джерела: соціальні мережі, веб-сайти, новинні ресурси та інші загальнодоступні інформаційні платформи.

Це загрожує конфіденційності користувачів, безпеці організацій та державних установ. Разом з тим, інновації в законодавстві повною мірою не закривають потребу в регламентації дій, пов'язаних з обробкою конфіденційної інформації, а також жодним чином не визначають регламент використання OSINT-технології.

Постановка проблеми. Технологічний прогрес створює можливості та загрози, пов'язані з потенціалом швидкого отримання інформації, нові технології допомагають локалізувати, обробляти та поширювати великі обсяги даних з відкритих джерел інформації.

В той же час, відсутність системного підходу до захисту персональних даних та конфіденційної інформації у відкритих джерелах інформації створюють додаткові загрози для конфіденційності користувачів, а державний сектор та приватні компанії несуть додаткові збитки, в наслідок кібератак або витоку інформації.

Аналіз останніх досліджень і публікацій. Згідно зі звітом Державної служби спеціального зв'язку та захисту інформації у першому півріччі 2024 року кількість російських хакерських атак на українські об'єкти зросла на 19% у порівнянні з другим півріччям 2023 року. Відповідно до даних, зібраних Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, у першому півріччі 2024 року зафіксовано 1739 кібератак, порівняно з 1463 у другому півріччі 2023 року. Попри зменшення інцидентів критичного та високого рівнів на 85%, число атак з розповсюдженням шкідливого програмного забезпечення зросло на 40%, основними з яких є кібершпіонаж та викрадення акаунтів в месенджерах [1].

Таблиця 1

Статистичні дані основних суб'єктів забезпечення кібербезпеки в Україні, цілями кібератак з початку повномасштабного вторгнення

Вектор атаки	Кількість зареєстрованих інцидентів:
Витік конфіденційної інформації та персональних даних	4300
Порушення роботи критичної інфраструктури	3800
Економічне шпигунство	2800
Заволодіння фінансовими активами	2300
Психологічний вплив та дезінформація	2000

За час повномасштабного вторгнення хакери активно збирали персональні дані громадян України, в тому числі військовослужбовців. Прізвище та ім'я, паспортні дані, а найголовніше — місце їх служби та посада. Саме ці дані надають змогу зловмисникам сконцентруватися на конкретних особах, комп'ютерному обладнання, на якому з високою ймовірністю є важливі документи.

Метою статті є дослідження і аналіз національного та зарубіжного досвіду забезпечення безпеки персональних даних та конфіденційної інформації в контексті протидії OSINT-технологіям, алгоритмів для захисту персональних і конфіденційних даних та визначення проблематики і перспективних напрямів їх застосування в Україні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Законодавче регулювання використання даних

У сучасному світі, де інформація легко доступна, а технології постійно розвиваються, захист особистих даних стає критично важливим завданням для держави, організацій і окремих осіб. Дані стають все більш цінним активом, тому важливо знайти оптимальну модель управління, яка б враховувала інтереси як організацій, так і користувачів, а також забезпечувала баланс між доступністю інформації та потребами в конфіденційності.

Одночасно з цим, гостро постає питання захисту конфіденційної інформації та персональних даних, від несанкціонованого збору та використання.

Зокрема, згідно ч. 2 ст. 21 ЗУ «Про інформацію» під конфіденційною інформацію необхідно розуміти інформацію про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом. [2].

Водночас, персональні дані — це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, відповідно до ЗУ «Про захист персональних даних», вказані відомості можуть оброблятися лише за умови надання добровільної згоди суб'єкта персональних даних [3].

Проте, згідно з статтею 4 Загального регламенту захисту даних (GDPR), прийнятого у 2016 році, під персональними даними визначено «будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи» [4].

Враховую, що Україна отримала статус кандидата на членство в ЄС, наступним кроком стане імплементація законодавства ЄС.

На даний час, відомості про логіни, паролі, контактна інформація (сторінки в соціальних мережах, нікнейми в месенджерах, номери мобільних телефонів або адреси сервісів електронної пошти), фотографії, тощо, розміщені у відкритому доступі, не підпадають під вище вказані визначення, зафіксовані в національному законодавстві, а їх використання в Україні регламентоване лише політиками конфіденційності окремих електронних ресурсів, які кожен утримувач такого ресурсу визначає самостійно.

Крім того, збір інформації з відкритих джерел не підпадає під законодавче регулювання, та широко використовується в діяльності правоохоронних органів, журналістів та кіберактивістів.

Соціальна інженерія та доксинг

У більшості корпоративних поштових серверів використовуються засоби захисту, тому зловмисники дедалі частіше відмовляються від надсилання шкідливого програмного забезпечення на поштові скриньки жертв та віддають перевагу атакам через інші засоби комунікації. Зокрема в такому випадку, основними цілями стають месенджери, якими також користується велика кількість військових або працівників критичних підприємств, установ, організацій.

Як приклад, маючи у розпорядженні масив даних про особу, отриманий з інших скомпрометованих акаунтів та відкритих джерел інформації, контактний телефон, хакери з угруповання UAC-0184, використовуючи засоби соціальної інженерії, видають себе за інших осіб та розпочинають спілкування з майбутньою жертвою, зазвичай за допомогою месенджеру «Signal». Слід відмітити, що для впливу на жертву та отримання від неї інформації, використовуються будь-які доступні ресурси, навіть платформи для знайомств [1].

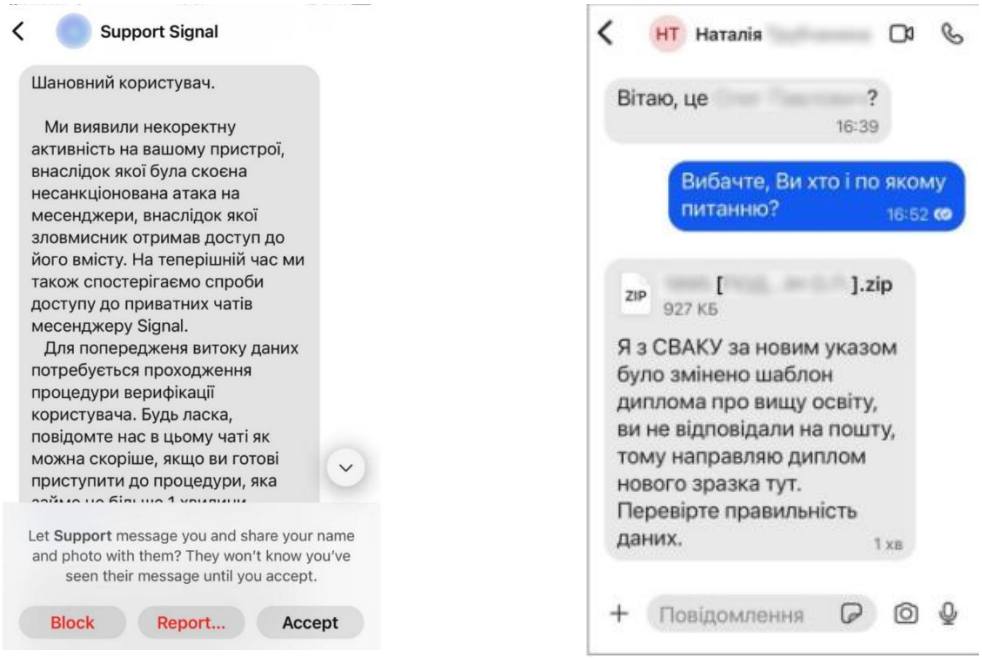

Рис. 1. Приклади фішингових атак на військовослужбовців — користувачів месенджеру «Signal».

Окремо слід зауважити, що OSINT-технології використовуються для так званого «doxing», коли без згоди особи, здійснюється збір персональної або конфіденційної інформації, з метою її подальшого несанкціонованого використання.

Термін «doxing» походить від фрази «dropping documents» або «dropping dox», що було формою помсти в хакерській культурі поза законом 1990-х років, яка включала публічне розкриття осіб, які підтримували анонімність (Honan 2014).

Термін «doxing», став настільки вживаним, що його дефініцію включили до офіційних словників. Наприклад, Оксфордський словник британської та світової англійської мови визначає доксинг як «пошук і публікація приватної чи ідентифікаційної інформації про (конкретну особу) в Інтернеті, як правило, зі зловмисними намірами» (Оксфордські словники 2015) [5].

Таким чином, під доксингом необхідно розуміти практику збору та публікації особистої інформації про осіб без їхньої згоди, що може призводити до серйозних наслідків та загроз для їхньої конфіденційності та безпеки, що може включати поширення фізичних адрес перебування особи, контактних номерів телефонів, електронних поштових адрес та інших чутливих даних, які використовуються для погроз, переслідувань або навіть завдання фізичної шкоди потерпілому.

Таблиця 2

Дані, які найчастіше підпадають під доксинг

Тип інформації	Дані, що підлягають збору та публікації
Ідентифікаційна інформація:	– Повне прізвище, ім'я, по батькові. – Адреса реєстрації та адреса проживання / фактичного перебування особи. – Номер мобільного телефону. – Адреса електронної пошти. – Інформація про документи, що посвідчують особу (паспорт, ідентифікаційний код платника податків, водійське посвідчення, дозвіл на зброю, участь у громадських організаціях, тощо) – Інформація з державних реєстрів, що не потребують спеціального доступу.
Онлайн-акаунти та логіни:	– Логіни, нікнейми, псевдоніми, імена користувачів. – Паролі та паролі від акаунтів. – Дані про прив'язані облікові записи (наприклад, інші соціальні мережі, блоги, форуми, месенджери, онлайн-магазини, тощо). – Інформація про типи пристроїв та операційних систем, якими користується жертва. – Інформація про зв'язки на основі аналізу лайків, коментарів та взаємних підписок.
Фінансова інформація:	– Банківські та фінансові установи, в яких обслуговується особа. – Банківські рахунки та номери карток. – Дані про платежі, квитанції, фінансові звіти. – Інформація про кредитну історію та кредитні рейтинги. – Інформація про майно та доходи. – Дані про використання криптоактивів та електронних грошей.
Особиста інформація:	– Сімейний стан – Дані членів сім'ї, включаючи контакту інформацію та акаунти в соціальних мережах, месенджерах. – Фото та відео, що показують особисте життя, в т.ч. компроментуючі. – Відомості про місцезнаходження (геолокаційні дані, метадані).
Робоча інформація:	– Місце роботи, посада. – Контактні дані колег та/або керівників. – Інформація про зарплати, бонуси або трудовий стаж. – Інформація про участь в проектах.
Інша інформація, що може завдати шкоди:	– Медичні дані, історія хвороби, діагнози або результати аналізів/досліджень. – Секрети, компромат або інші конфіденційні дані. – Відомості про судимість або минулі правопорушення. – Інформація про участь в судових засіданнях, тощо.

Ця проблема в Україні останнім часом привертає значну увагу через зростання використання соціальних мереж і відкритих джерел інформації. Вказані технології експлуатуються зловмисниками, для отримання значущої інформації про військові події, та для залучення підлітків до деструктивних рухів, з метою скоєння диверсій на території України, шляхом їх залякування та маніпуляцій [6].

Спостерігається тенденція щодо втрати інформацією, яка підлягає захисту, головної властивості — конфіденційності. Дані про особу, її контактна інформація, фото — стали товаром в руках зловмисників. Соціальна інженерія стала однією з найбільш поширених форм атаки, заснованих на домінуванні психологічних маніпуляцій. Зловмисники використовують інформацію, отриману з відкритих джерел, для створення «переконливих» фейкових профілів, що вводять в оману жертви, спричиняючи, наприклад, перехоплення даних для авторизації в облікових записів або отримання чутливої інформації.

Медіаграмотність та кібергігієна

Другим викликом, щодо забезпечення безпеки персональних даних та конфіденційної інформації, після використання засобів соціальної інженерії та доксингу, є недостатній рівень медіаграмотності та обізнаності населення щодо правил використання кіберпростору.

Медіаграмотність — це вміння аналізувати, оцінювати та створювати медіа-контент. У дослідженні «Критичне сприйняття інформації в медіапейзаже України» (Мельник, 2022) зазначено, що більшість українців не здатні адекватно оцінювати достовірність інформації, що робить їх вразливими до дезінформації та маніпуляцій. Неправильне сприйняття медіа може призвести до легкого поширення конфіденційної інформації та особистих даних, які відкрито діляться в онлайн-середовищі.

Кібергігієна, що включає в себе знання про безпечне використання інформаційних технологій та Інтернету, також залишається на низькому рівні. За даними статті «Кібербезпека в Україні: виклики та можливості» (Савченко, 2023), лише 30% користувачів мають базові знання про захист своїх даних в Інтернеті. Це включає незахищені паролі, несанкціонований доступ до особистої інформації та недостатню обережність при відкритті електронних листів від невідомих відправників.

Зокрема, відповідно до дослідження «Аналіз рівня медіаграмотності у населення України» (Коваленко, 2021), відзначається, що молодь, хоч і більш підкована в технологічному плані, часто не усвідомлює потенційних загроз через недостатній рівень критичного мислення. Ця ситуація стосується не лише особистої безпеки, але і безпеки інформації, з якою підприємства ведуть бізнес.

Так, згідно опитування «Безпека дітей в Інтернеті: опитування для батьківської громадськості», проведеного у Львівській області протягом квітня 2024 року було встановлено, що 77% опитаних батьків, не знають про програми та ресурси з підвищення рівня кіберграмотності, і лише 23% респондентів дотримуються загальних правил кібергігієни в мережі Інтернет, крім того, 43% опитаних не знають, що таке кіберзлочини та переліку заходів, які необхідно вжити, щоб не стати жертвою таких правопорушень, або запобігти їх вчиненню.

За результатами вищевказаного опитування було сформовано узагальнені потреби населення на прикладі Львівської області в розрізі медіаграмотності та кібергігієни:

Рис. 2. Потреби населення в проведенні профілактичної та роз'яснювальної роботи на прикладі Львівської області

Відсутність сталої системної роботи, щодо впровадження алгоритмів та правил публікації персональних даних та конфіденційної інформації у відкритих джерелах, спричинила збільшення кількості випадків несанкціонованого збору, обробки та використання даних.

Фішингові атаки

Фішингові атаки дедалі частіше використовуються з метою підтвердження даних, отриманих шляхом проведення OSINT. Фішинг є однією з найпоширеніших та найнебезпечніших форм кіберзлочинності, що ставить під загрозу персональні дані та конфіденційну інформацію користувачів. Цей тип атаки передбачає спробу заволодіти особистими даними, такими як логіни, паролі та фінансова інформація, через скомпроментовані електронні листи, веб-сайти або інші комунікаційні канали.

Згідно звіту H1 2024 Cybersecurity Trends & Insights, у першому півріччі 2024 року фішинг становив 75% усіх атак, спрямованих на засоби електронної пошти. Це узгоджується з показниками першого півріччя 2023 року, що свідчить про те, що зловмисники надають перевагу фішингу як надійному методу атак, щоб змусити користувачів розкрити конфіденційну інформацію.

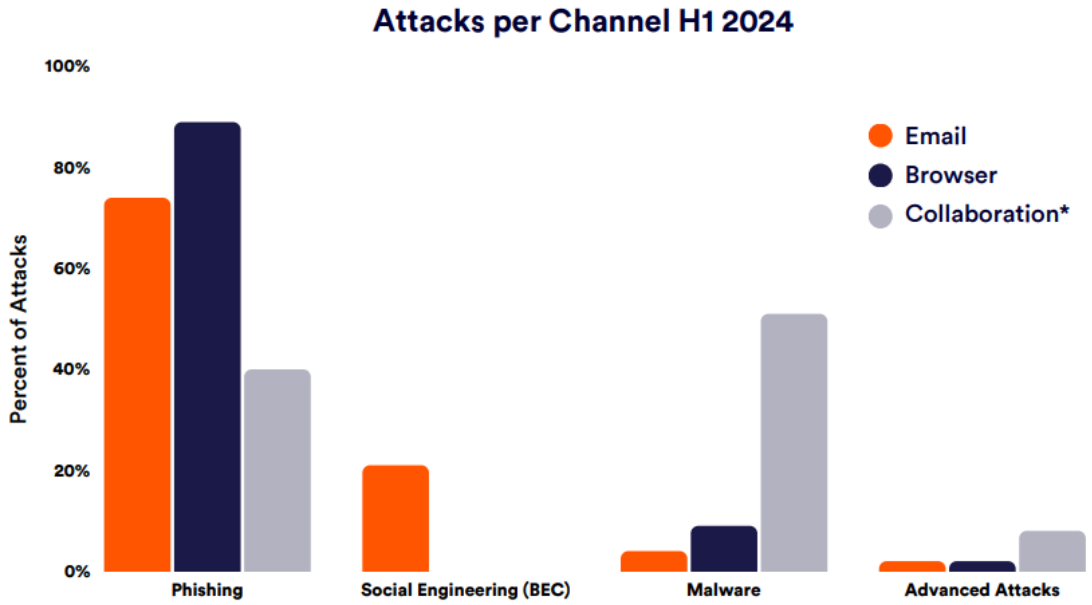

Рис. 3. Вектори кібератак за результатами звіту H1 2024 Cybersecurity Trends & Insights

Крім того, важливо зазначити, що фішинг не лише загрожує особистим даним, але й може стати причиною серйозних наслідків для компаній. Дослідження, проведене Міжнародною асоціацією кібербезпеки, показує, що 60% компаній, які стали жертвами фішингових атак, зазнали фінансових втрат або репутаційних пошкоджень (Smith, 2022). Ці фінансові втрати пов’язані не лише з викраденими коштами, але й з витратами на відновлення даних та покращення систем безпеки.

Удосконалення систем безпеки та антивірусного захисту електронних поштових сервісів, призвело до удосконалення методології використання фішингу.

Так, наразі зловмисниками активно використовується тактика багатоетапного фішингу, яка заснована на перенаправленні користувача від одного ресурсу до іншого, щоб уникнути виявлення. Ці складні атаки зросли на 175% у 2023 році та залишаються значною загрозою у 2024 році. Багатоетапний фішинг часто передбачає надсилання нешкідливих посилань, які згодом переспрямовують на фішингові сторінки, що ускладнює виявлення та блокування таких атак за допомогою традиційних заходів безпеки.

Рис. 4. Схема багатоетапної фішингової атаки

Що стосується атак на браузери та збір інформації з них, фішинг використовувався у 89% усіх атак через у першому півріччі 2024 року, порівняно з 83% у першому півріччі 2023 року. Ці атаки зазвичай стосуються підроблених веб-сайтів або імітації брендів, призначених для викрадення особистої інформації користувачів. Браузер залишається важливим вектором для фішингу через його широке використання для доступу до професійних інструментів і служб.

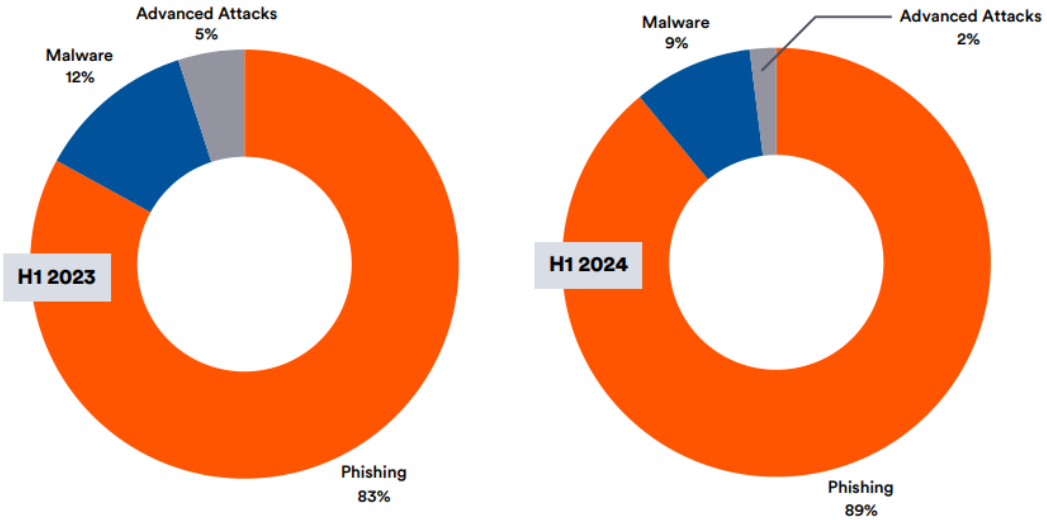

Рис. 5. Вектори кібератак на браузери за результатами звіту H1 2024 Cybersecurity Trends & Insights

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Через розширення можливостей розвідки у відкритих джерелах, персональні дані стали більш вразливими. В Україні OSINT використовується для збору даних про громадян, що особливо критично під час збройної агресії з боку російської федерації та гібридної війни. Наявні правові норми не забезпечують достатнього захисту для персональних та конфіденційних даних у відкритих джерелах. Це свідчить про необхідність імплементації європейських стандартів захисту даних (як-от GDPR) для підвищення рівня безпеки.

Відсутність навичок медіаграмотності та низький рівень кібергігієни сприяють витоку даних та роблять людей більш вразливими до фішингових атак і соціальної інженерії. Це особливо актуально для молоді та підлітків, які часто недостатньо критично сприймають інформацію.

Фішинг залишається основним інструментом для крадіжки особистих даних, особливо через електронну пошту та браузери. В статті наведені статистичні дані, які підтверджують поширення багатоступеневих фішингових атак, що ускладнює їх виявлення.

Отже, стаття пропонує комплексний підхід до вирішення проблем конфіденційності, який поєднує правове регулювання, технологічні засоби захисту та підвищення обізнаності користувачів щодо кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Кібероперації рф: нові цілі, інструменти та групи. Аналітика хакерських атак проти України за 1 півріччя 2024 року.* (2024). Державна служба спеціального зв'язку та захисту інформації України. https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report
2. Про інформацію, Закон України № 2657-XII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Про захист персональних даних, Закон України № 2297-VI (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. *Загальний регламент захисту даних (GDPR).* (2016). https://gdpr-text.com/uk/
5. Douglas, D. M. (2016). Doxing: a conceptual analysis. Ethics and Information Technology, 18(3), 199–210. https://doi.org/10.1007/s10676-016-9406-0
6. *Вербування підлітків ворогом для скоєння диверсій: кіберполіція попереджає про небезпеку в інтернеті.* (2024). https://cyberpolice.gov.ua/article/verbuvannya-pidlitkiv-vorogom-dlya-skoyennya-dyversij-kiberpolicziya-poperedzhaye-pro-nebezpeku-v-interneti-2116/
7. Савченко, О. (2023). Кібербезпека в Україні: виклики та можливості. *Вісник національної академії правових наук України, 28(1)*, 78–92.
8. Мельник, І. (2022). Критичне сприйняття інформації в медіапейзаже України. *Журнал медіа і комунікацій, 4(2)*, 45–59.
9. Коваленко, Т. (2021). Аналіз рівня медіаграмотності у населення України. Соціологічні дослідження, 29, 102–113.
10. Григоренко, П. (2023). Кіберзлочинність в Україні: статистичний огляд. *Огляд кримінологічних досліджень, 12 (1),* 56–70.
11. *Безпека дітей в інтернеті: що варто знати батькам та як побудувати безпечний освітній простір з Cisco на Львівщині.* (2024). https://loda.gov.ua/news/103088
12. *H1 2024 Cybersecurity Trends & Insights.* (2024). https://perception-point.io/resources/report/2024-h1-report/
13. Cybersecurity in the European Union: Current Challenges and Future Perspectives. (2020). European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/cybersecurity-in-the-eu
14. Smith, J. (2022). The Impact of Phishing Attacks on Businesses: A Global Perspective. *International Journal of Cyber Security, 18,* 78–88.
15. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2024). *Інформаційна та кібернетична безпека підприємства.* Підручник. Львів : Видавець Марченко Т. В.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Valeriia Ivkova
Postgraduate student of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Ivan Opirskyy
Doctor of Science, Professor, Head of Information ProtectionDepartment
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

RESEARCH OF PROBLEMS OF ENSURING THE SECURITY OF PERSONAL DATA AND CONFIDENTIAL INFORMATION IN THE CONTEXT OF COUNTER-OSINT

Abstract. In today's world, the issue of personal data protection is becoming particularly relevant as technological advancements and the widespread use of open information sources create new security challenges. This article examines the legislative aspects of data regulation in various jurisdictions, particularly in Ukraine and the EU, as well as practical threats such as social engineering, phishing, and doxing. Based on an analysis of the General Data Protection Regulation (GDPR) and the Ukrainian Law "On the Protection of Personal Data", the authors highlight significant discrepancies in the legislation regulating data confidentiality. Special attention is given to current threats to personal data in the context of information security, such as attacks carried out through social engineering. The article investigates the activities of hacker groups that use personal data to create fake profiles in messaging platforms to obtain sensitive data or gain access to accounts. Examples of OSINT technologies used by attackers to gather data from open sources are discussed, along with their application in doxing, where personal data is published without individual consent, posing potential security risks. The article also addresses the growing risks of phishing attacks targeting email and browser users, including new tactics like multi-stage phishing, which complicates the detection and blocking of such attacks. Additionally, it emphasizes the importance of media literacy and cyber hygiene in reducing privacy risks and increasing awareness of safe practices for working with information technologies. The article concludes by underscoring the need for a systematic approach to data privacy protection, including legal regulation, the adoption of modern information protection technologies, and an increase in media literacy among the population. Proposed measures include the implementation of European data protection standards, which could provide a reliable foundation for strengthening personal data protection in Ukraine.

Keywords: personal data; confidential information; doxing; OSINT; cybersecurity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Russian cyber operations: new targets, tools and groups. Analytics of hacker attacks against Ukraine for the 1st half of 2024.* (2024). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report
2. On Information, Law of Ukraine No. 2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. On the Protection of Personal Data, Law of Ukraine No. 2297-VI (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. *General Data Protection Regulation (GDPR)*. (2016). https://gdpr-text.com/uk/
5. Douglas, D. M. (2016). Doxing: a conceptual analysis. *Ethics and Information Technology, 18(3),* 199–210.
6. Recruiting teenagers by the enemy to commit sabotage: cyber police warn of dangers on the Internet. (2024). https://cyberpolice.gov.ua/article/verbuvannya-pidlitkiv-vorogom-dlya-skoyennya-dyversij-kiberpolicziya-poperdzhaye-pro-nebezpeku-v-interneti-2116/

7. Savchenko, O. (2023). Cybersecurity in Ukraine: challenges and opportunities. *Bulletin of the National Academy of Legal Sciences of Ukraine, 28(1),* 78–92.
8. Melnyk, I. (2022). Critical perception of information in the media landscape of Ukraine. *Journal of media and communications, 4 (2),* 45–59.
9. Kovalenko, T. (2021). Analysis of the level of media literacy among the population of Ukraine. *Sociological studies, 29,* 102–113.
10. Grigorenko, P. (2023). Cybercrime in Ukraine: a statistical review. *Review of criminological research, 12(1),* 56–70.
11. *Children's safety on the Internet: what parents should know and how to build a safe educational space with Cisco in Lviv region.* (2024). https://loda.gov.ua/news/103088
12. *H1 2024 Cybersecurity Trends & Insights.* (2024). https://perception-point.io/resources/report/2024-h1-report/
13. *Cybersecurity in the European Union: Current Challenges and Future Perspectives.* (2020). European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/cybersecurity-in-the-eu
14. Smith, J. (2022). The Impact of Phishing Attacks on Businesses: A Global Perspective. International *Journal of Cyber Security, 18,* 78–88.
15. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.