НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

ЛАНДШАФТ КІБЕРЗАГРОЗ УКРАЇНИ У 2023 РОЦІ

Дослідження «Ландшафт кіберзагроз України у 2023 році» підготовлене Інститутом дослідження кібервійни завдяки підтримці, наданій Агентством США з міжнародного розвитку (USAID), через Проєкт USAID «Кібербезпека критично важливої інфраструктури України». Думки авторів, висловлені в цьому дослідженні, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США

ЗМІСТ

КОРОТКИЙ ОГЛЯД ЗВІТУ

Звіт «Ландшафт кіберзагроз Украни в 2023 році» подає інформацію про період з 1 січня 2023 року до 31 грудня 2023 року. Такий звіт підготовлено вперше, тому він не містить порівнянь з попередніми роками.

Основними цілями дослідження ландшафту кіберзагроз України є управління ризиками кібербезпеки, підтримка прийняття рішень на стратегічному рівні, визначення пріоритетів у розробці політик і процедур у сфері кібербезпеки, поширення інформації щодо кіберзагроз та способів протидії ним. Результати дослідження орієнтовані на аудиторію стратегічного та тактичного рівнів: розробників стратегій кібербезпеки, керівників організацій, керівників із кібербезпеки державного і приватного секторів та представників міжнародних партнерів.

Звіт підготовлений з використанням адаптованого варіанту методології ENISA[1] «Методологія ENISA з побудови ландшафту загроз кібербезпеки, Липень 2022 року» (ENISA Cybersecurity Threat Landscape Methodology, July 2022»). Інформацію про адаптовану методологію ENISA наведено в додатку.

Для підготовки звіту було використано інформацію з відкритих джерел, включно з публікацією з аналітикою кіберзагроз провідних компаній з кібербезпеки, даними про кіберінциденти та кібератаки з власних джерел, інформацією з систем обміну індикаторами компрометації MISP та аналітикою кіберзагроз OpenCTI, а також даними інтерв'ю з українськими експертами в галузі кібербезпеки та опитуванням представників державних органів, об'єктів критичної інфраструктури, громадського та приватного сектору методом анкетування. За сприяння Національного координаційного центру кібербезпеки (НКЦК) анкети заповнили 398 респондентів.

Мовою звіту «Ландшафт кіберзагроз України в 2023 році» є українська, передбачається його переклад англійською для поширення та отримання зворотного зв'язку від ENISA та країн-партнерів України.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology?v2=1

ВСТУП

На фоні повномасштабного вторгнення рф в Україну основну загрозу для українських організацій у 2023 році становила активність хакерських груп, пов'язаних із спецслужбами росії.

Основні суб'єкти забезпечення кібербезпеки України за підсумками звітного періоду повідомляють про зростання кількості зафіксованих кіберінцидентів та кібератак у порівнянні з 2022 роком. За даними СБУ, у 2023 році зафіксовано 4500 кібератак[2]; за даними Держспецзв'язку, Урядовою командою реагування CERT-UA опрацьовано 2543 кіберінцидентів[3], Державним центром кіберзахисту зафіксовано 1105 кіберінцидентів[4]; за даними Microsoft, Україна є найбільш атакованою країною в Європі[5]. Свій внесок у таке зростання зробили також збільшення кількості повідомлень про інциденти від організацій як державного, так і приватного секторів, покращення обміну аналітикою кіберзагроз (cyber threat intelligence, CTI) як всередині держави, так і з міжнародними партнерами, а також краща ситуаційна обізнаність завдяки впровадженню систем та сенсорів кібербезпеки в організаціях[6]. Тому, незважаючи на зростання загальної кількості інцидентів, кількість кіберінцидентів із критичними наслідками є незначною, зважаючи на виклики кібервійни, з якими зіткнулась Україна.

Найбільша кількість кібератак з боку російських APT-груп була спрямована на державні органи, Сили оборони України, організації та підприємства оборонної промисловості, сектори телекомунікацій, енергетики та IT. Також серед найбільш таргетованих є сектор засобів масової інформації, атаки на який були частиною більш широких інформаційних операцій російських спецслужб.

Активність з боку інших країн, що підтримують росію або не підтримують Україну, була спрямована насамперед на присутність в інформаційних системах державних органів та підприємств оборонного сектору з метою шпигунства[7]. На початку 2023 року зафіксовано

[2] Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500: СБУ назвала організаторів, https://minfin.com.ua/ua/2024/05/07/126427603/

[3] Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти, https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

[4, 6] 2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5%: звіт оперативного центру реагування на кіберінциденти ДЦКЗ, https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz

[5] Espionage fuels global cyberattacks, https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

[7] Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

спроби в тому числі деструктивних атак з боку іранських груп після оприлюднення інформації про поставки росії озброєння з цієї країни.

Для приватних осіб – громадян України, насамперед переміщених осіб, основну загрозу створюють фішингові веб-сайти та інтернет-шахрайство, що експлуатують тематики фінансової допомоги та компенсацій за пошкоджене майно від українського Уряду та міжнародних організацій. Фінансово-мотивовані кіберзлочинці використовують методи соціальної інженерії, вони швидко реагують на події в країні та безперервно удосконалюють шахрайські схеми[8].

Основні кіберзагрози, які були ідентифіковані та проаналізовані під час підготовки звіту «Ландшафт кіберзагроз України в 2023 році»:

- соціальна інженерія;
- шкідливе програмне забезпечення;
- DDoS-атаки;
- Інтернет-шахрайство;
- використання кібератак для підтримки інформаційних та гібридних операцій;
- компрометація облікових записів та витоки інформації;
- порушення доступності внаслідок збоїв або пошкодження обладнання або мереж;
- деструктивні атаки.

Варто зазначити, що під час підготовки звіту було розглянуто також інші кіберзагрози: атаки на ланцюги постачання, використання вразливостей нульового дня, атаки здирників (ransomware) тощо. Проте недостатній обсяг доступної інформації, незначна кількість описаних кіберінцидентів, а також загальна низька оцінка ймовірності їх реалізації з боку опитаних експертів не дозволила включити такі кіберзагрози до звіту про ландшафт кіберзагроз.

[8] https://csirt.bank.gov.ua/cyber-fraud

КЛЮЧОВІ ТЕНДЕНЦІЇ ТА ВИСНОВКИ

Більш складні та таргетовані атаки на організації, які становлять інтерес, з використанням соціальної інженерії.

Витоки інформації, дані OSINT та викрадені в результаті попередніх атак дані, ретельно аналізуються та використовуються для наступних таргетованих кібератак. Для поширення фішингових повідомлень активно використовуються мобільні пристрої. У багатьох випадках викрадені облікові дані використовуються для початкового доступу всередину мереж організацій.

Атаки на облікові записи.

Основною ціллю зловмисників є облікові записи та дані автентифікації до онлайн-сервісів. Значно зросла кількість атак такого типу: підбір паролів, password spraying, зловмисник посередині (Adversary-in-the-Middle). Для викрадення облікових записів використовуються шкідливе програмне забезпечення, що збирає паролі із браузерів, токени авторизації із скомпрометованих хостів, а також фішингові ресурси.

Використання легальних сервісів та інструментів під час кібератак.

І підтримувані державами, і фінансово-мотивовані хакерські групи все частіше використовують довірені легальні сервіси та інструменти для приховування своєї активності під час отримання доступу до мереж організацій. Наприклад, платформа Telegram активно застосовується для розповсюдження шкідливого програмного забезпечення, як канал поширення фішингу та в якості командно-контрольних серверів.

Краща координація між кібератаками та воєнними і інформаційними операціями.

Починаючи з осені 2022 року, росія доклала зусиль щодо погодження кібероперацій із воєнними задачами, в 2023 році ця тенденція посилилась. Інтенсивність кібератак, вибір пріоритетних цілей на рівні об'єктів, регіонів та секторів корелюється із веденням воєнних дій і цілями кінетичних атак на українську інфраструктуру. Компрометація інформаційних систем організацій, зокрема OT-пристроїв (камер спостережень), у місцях обстрілів використовується в тому числі для аналізу їх наслідків. Дані, викрадені в ході кібератак, дефейси державних органів та засобів масової інформації використовуються в операціях впливу.

Контроль над діяльністю груп псевдо-хактивістів з боку спецслужб.

Починаючи з кінця 2022 – початку 2023 року, російські спецслужби взяли під повний контроль всі проросійські групи хактивістів, спрямовуючи їхню діяльність на досягнення військово-політичних цілей рф. Водночас росія розробила «технологію» формування, легендування та підтримки таких груп псевдо-хактивістів «під ключ» залежно від геополітичних завдань та застосовує її для здійснення кібератак та операцій впливу. Наприклад, на початку ізраїльського конфлікту після теракту 7 жовтня 2023 року було створено десятки нових псевдо-хактивістських груп, які атакували інфраструктуру Ізраїлю, водночас в цей період в Україні були найнижчі показники кількості інцидентів за останні декілька років. У кінці 2023 року з'явилась тенденція з «монетизації послуг» низки псевдо-хактивістських груп, підконтрольних спецслужбам рф.

ОГЛЯД ЛАНДШАФТУ КІБЕРЗАГРОЗ

Триваюча війна росії проти України була основним фактором 2023 року, який впливав на ландшафт кіберзагроз. Основну небезпеку для українських організацій становила активність хакерських груп, пов'язаних із спецслужбами росії.

Це безпосередньо впливало на вибір цілей кібератак. Найбільш атакованими у 2023 році були такі сектори: державного управління, безпеки і оборони, телекомунікацій та енергетики, фінансовий і банківський, логістика, IT та підприємства оборонної промисловості. Також серед найбільш таргетованих секторів є сектор засобів масової інформації, атаки на який були частиною більш широких інформаційних операцій російських спецслужб. На рисунку наведено дані Урядової команди реагування CERT-UA[9] щодо кількості кіберінцидентів за секторами, порівнюючи перше та друге півріччя 2023 року.

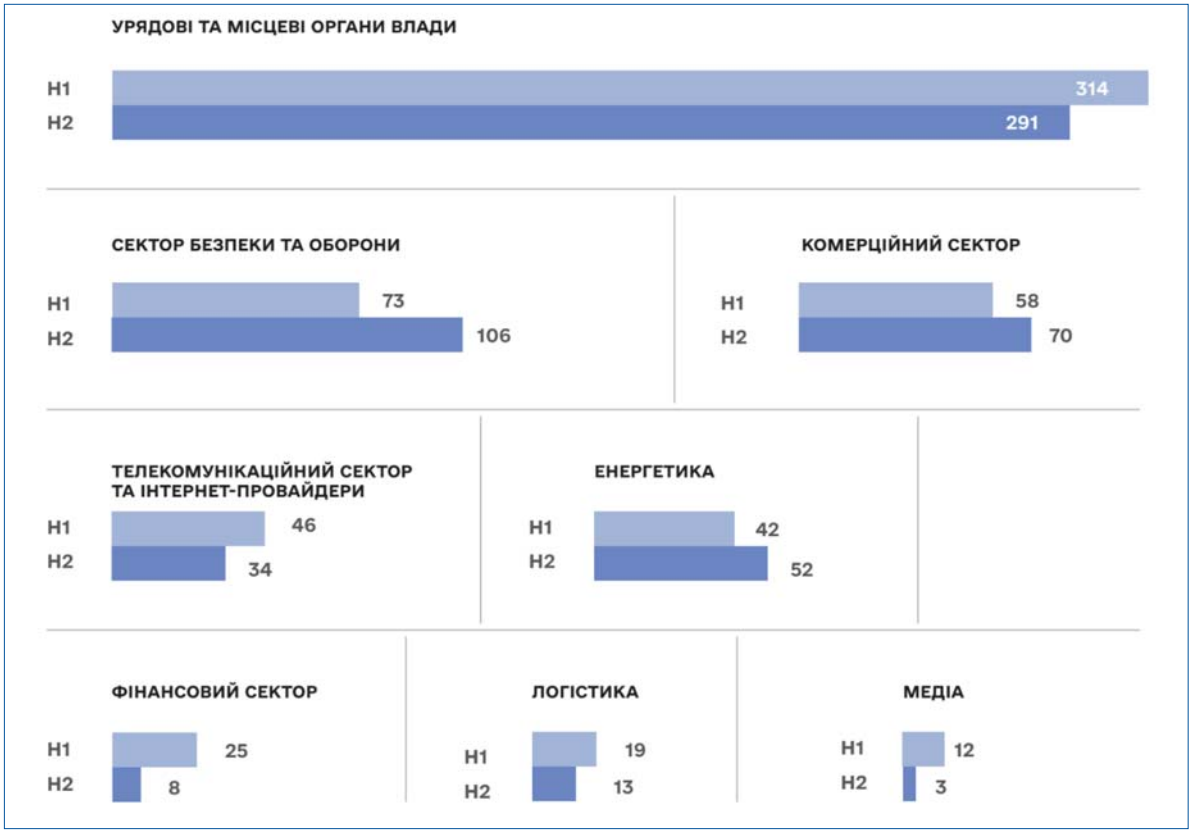


Рис 1. *Кількість кіберінцидентів за секторами, порівнюючи перше та друге півріччя 2023 року*

[9] Російські кібероперації. Аналітика за II півріччя 2023 року, https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi

Починаючи з осені 2022 року, росія доклала зусиль щодо узгодження кібероперацій із воєнними задачами, в 2023 році ця тенденція посилилась. Інтенсивність кібератак, вибір пріоритетних цілей на рівні об'єктів, регіонів та секторів корелюється із веденням воєнних дій і цілями кінетичних атак на українську інфраструктуру, а також з операціями Сил оборони України. У відповідь на підрив Кримського мосту 17 липня 2023 року впродовж наступних тижнів помітно зросла активність усіх основних хакерських APT-груп росії та Білорусі щодо українських організацій, зокрема спроби проведення деструктивних операцій. Кібератаки рф на підприємства енергетичного сектору, зокрема деструктивні, кількість яких зросла у другому півріччі, стали підготовкою для наступних кінетичних ударів по об’єктах енергетики.

Водночас, порівняно з попередніми етапами кібервійни, у 2023 році зменшилась кількість деструктивних операцій, пов'язаних із знищенням даних та/або пошкодженням функціонування інформаційних систем. Активність російських APT-груп стала більш спрямованою на шпигунство та проведення інформаційних операцій. За цих обставин росія розширила свої кібер- та інформаційні операції на країни Заходу, які надають підтримку Україні.

Розділ не містить вичерпного переліку усіх виявлених впродовж 2023 року тенденцій, а скоріше відображає погляд на важливі тенденції та кіберзагрози, що спостерігаються на стратегічному рівні.

Соціальна інженерія

Соціальна інженерія охоплює широкий спектр діяльності, спрямованої на експлуатацію людської поведінки або помилок, з метою отримання доступу до даних чи сервісів. Вона використовує різні форми маніпуляції, щоб обманом змусити жертв зробити помилку або передати конфіденційну інформацію. Користувачів можуть спонукати відкрити документи, файли чи електронні листи, перейти за посиланнями, заповнити онлайн-форму або надати доступ до систем чи сервісів. Соціальна інженерія є зручним вектором атаки через свою простоту, низьку вартість, легкість в експлуатації.

> Фішинг, тобто розсилка повідомлень електронної пошти, спрямованих на викрадення важливої інформації, такої як паролі або номери кредитних карток, є основним вектором початкової компрометації. Впродовж 2023 року його використовували практично всі хакерські групи[10].

Залежно від аудиторії та мотивації хакерської групи використовувались різні тематики та приманки. Серед них – закінчення терміну дії паролю або облікового запису, фейкові документи від органів державної влади, від правоохоронних органів, платіжні документи тощо.

[10] Microsoft Digital Defense Report. Building and improving cyber resilience. October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

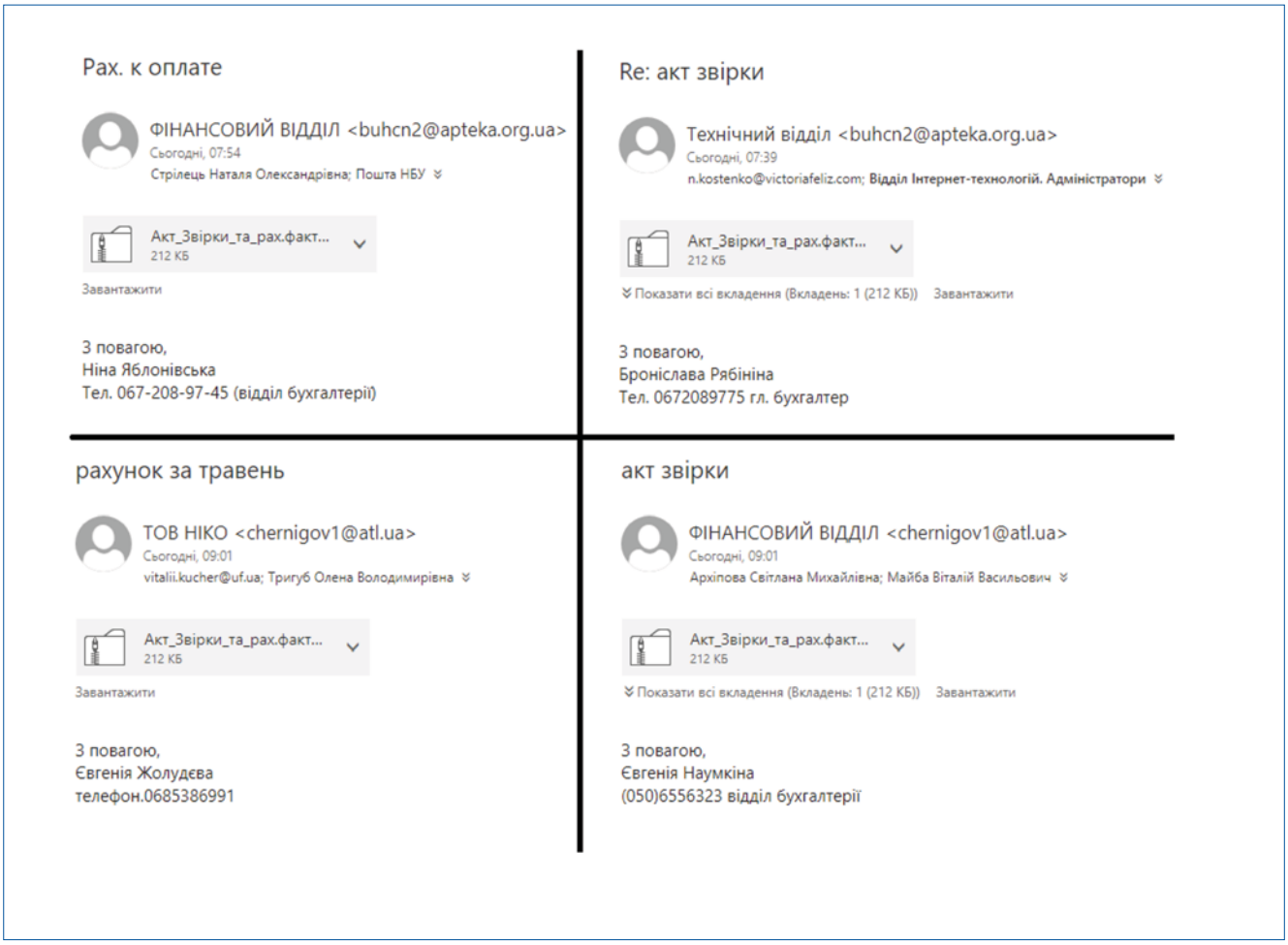


Рис 2. *Зразок фішингового листа групи UAC-0006 із шкідливим вкладенням SmokeLoader*

Окремою тематикою фішингових повідомлень є пропозиція співпраці з боку російських спецслужб. Як правило, такі повідомлення надсилаються через месенджери та містять посилання на канал в месенджері Telegram для зв'язку та отримання подальших інструкцій.

З метою обходу засобів захисту використовуються запаролені архіви з паролем у тексті листа, файли ISO, LNK, скрипти та документи з макросами, посилання на легітимні хмарні сервіси. Незважаючи на вимкнення за замовчанням у 2022 році компанією Microsoft виконання макросів, у багатьох організаціях використовуються неоновлені версії операційних систем та пакету Office, що підтримує використання вбудованих макросів зловмисниками.

Для підвищення рівня довіри до фішингових листів розсилки здійснюються із скомпрометованих поштових акаунтів органів державної влади чи відомих підприємств. Зафіксовані розсилки, таргетовані під конкретний сектор. У такому таргетованому фішингу розсилка всередині сектора здійснюється зі скомпрометованих електронних адрес організацій відповідного сектору. Для державних установ використовуються скомпрометовані акаунти інших державних установ, для підприємств сектору енергетики – скомпрометована електронна адреса підприємства з сектору енергетики і т.д.

Зафіксовано значне зростання використання фішингових розсилок через засоби мобільного зв'язку – СМС та популярні месенджери. У ході підготовки звіту ідентифіковано,

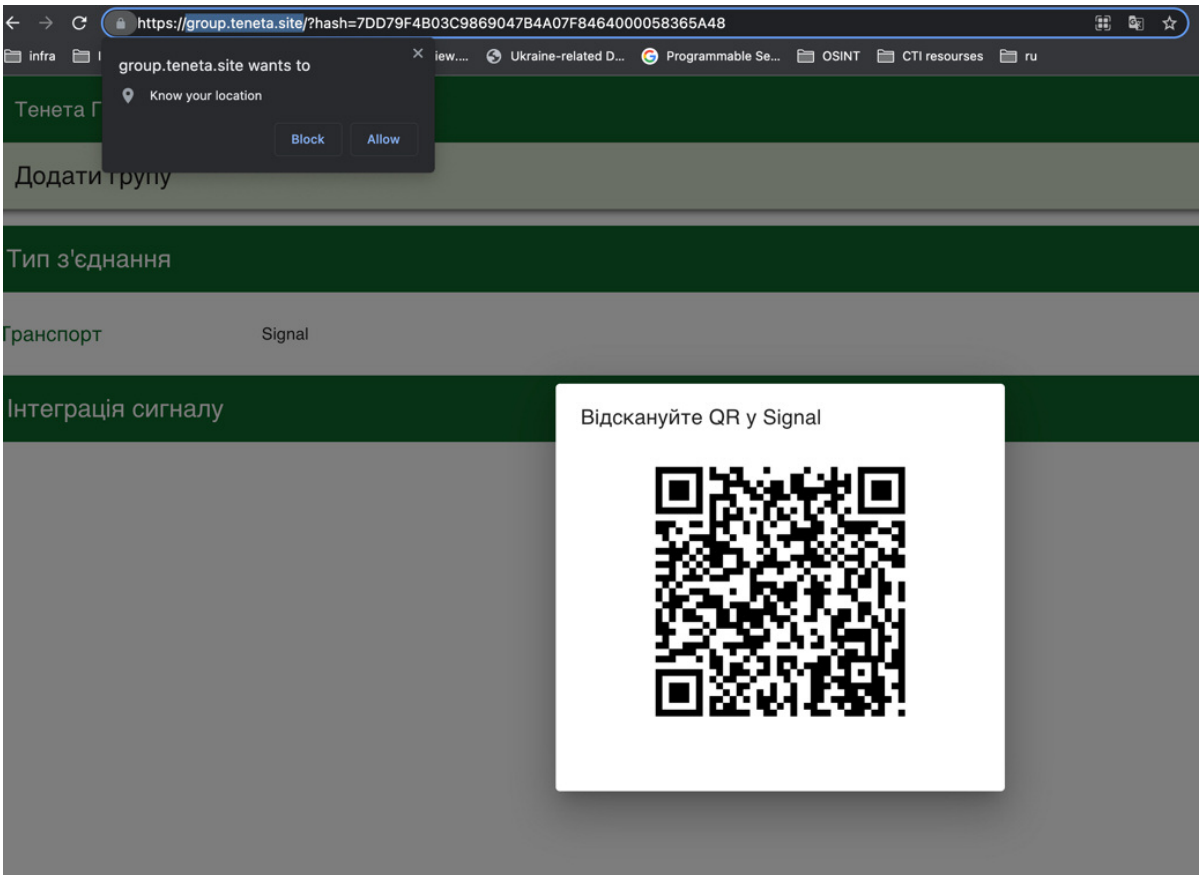


Рис 3. *Розсилка через SMS та Signal фішингових посилань для викрадення сесії Signal військовослужбовців*

що актуальність цієї загрози навіть вища, ніж традиційного фішингу через електронну пошту. Фінансово-мотивовані актори активно використовують тематику отримання посилки або листа через служби доставки, повідомлення містять посилання на фішингові веб-сайти служби доставки. Основною метою хакерських груп, пов'язаних із спецслужбами рф, є отримання доступу до акаунтів, зареєстрованих на мобільних телефонах, включно з платформами обміну повідомленнями, з метою отримання доступу до командних чатів та систем ситуаційної обізнаності Сил оборони України.

Шкідливе програмне забезпечення

Шкідливе програмне забезпечення (ШПЗ) – це загальний термін, що описує будь-який програмний продукт або прошивку, які призначені для виконання несанкціонованих процесів у системі, що матиме наслідком порушення цілісності, конфіденційності чи доступності інформації. Одним із варіантів поширення шкідливого програмного забезпечення є модель ШПЗ як послуга (Malware-as-a-Service), що дозволяє зловмисникам не займатися розробкою коду, а сфокусуватися на здійснені атак, отримані несанкціонованого доступу до систем, досягнені цілей атаки після компрометації.

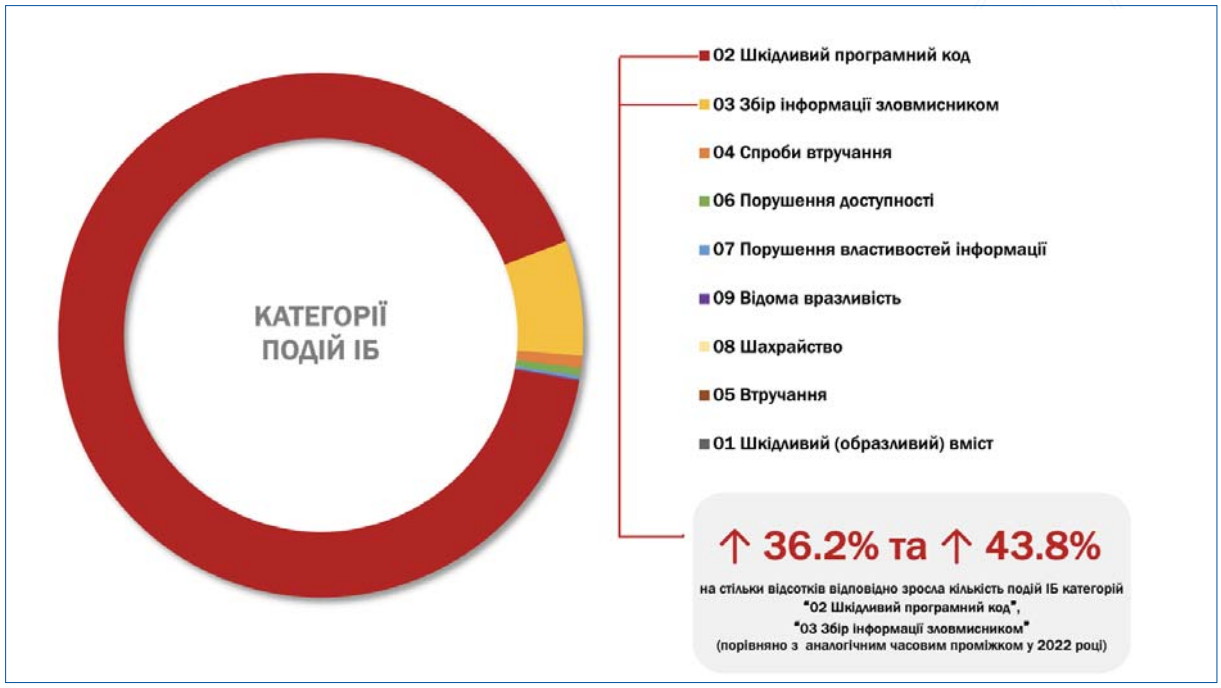


Рис 4. *Застосування шкідливого програмного коду*[11]

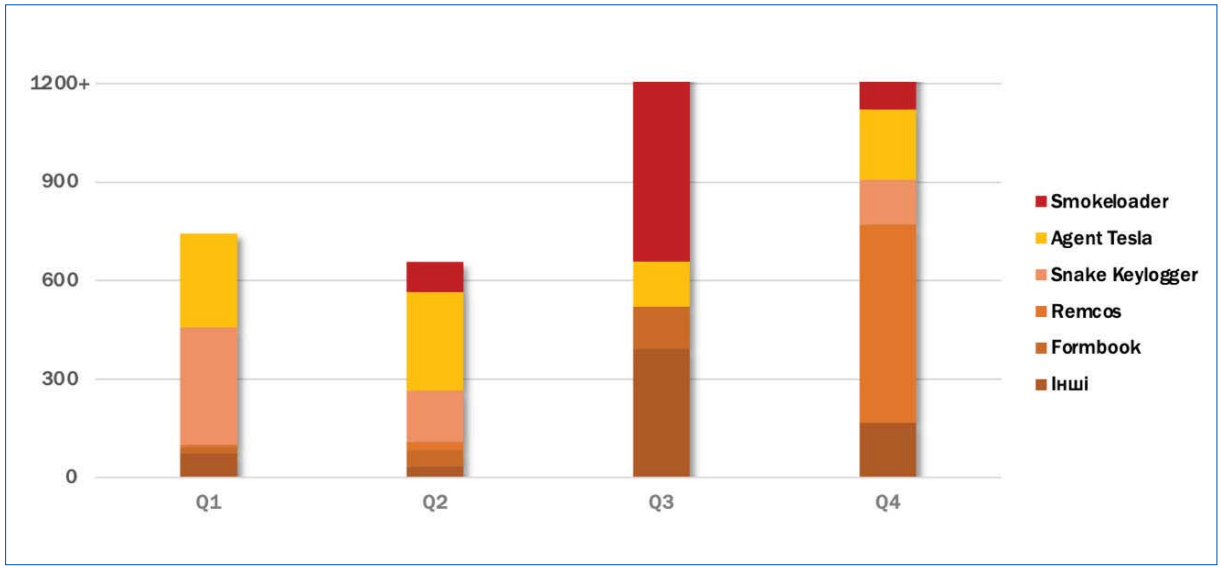


Рис 5. *Основні сімейства шкідливого ПЗ*[12]

DDoS-атаки

DDoS-атака – це вид кібератаки, скерованої на порушення доступності, під час якої зловмисник намагається порушити роботу веб-ресурсу, мережі, онлайн-сервісу, перевантажуючи їх великою кількістю підроблених або небажаних запитів.

[11] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки 2023, https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

[12] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки 2023, https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

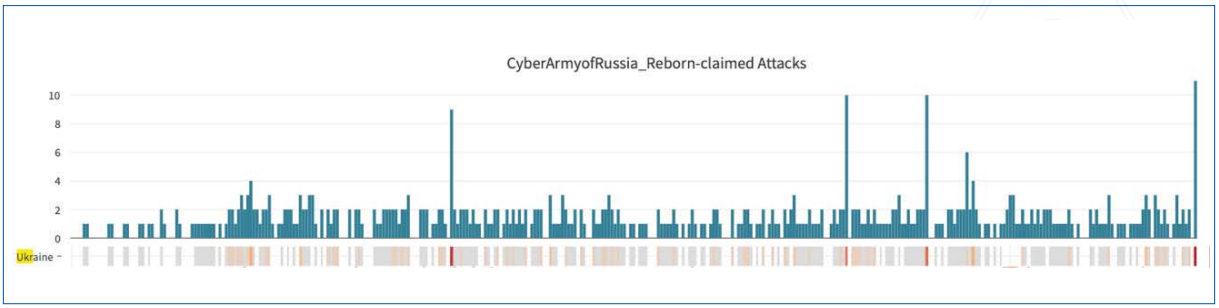


Рис 6. *У 2023 році псевдо-хактивістська група CyberArmy of Russia Reborn заявила про 341 DDoS-атаку на Україну*

Впродовж року зафіксовано тисячі DDoS-атак на українські організації[13], значний вплив на кількість таких атак веде діяльність груп псевдо-хактивістів, пов'язаних із спецслужбами рф[14].

У період з кінця 2022 – початку 2023 року російські спецслужби взяли під повний контроль всі проросійські групи хактивістів, спрямовуючи їх діяльність на досягнення військово-політичних цілей рф. Тому значна кількість DDoS-атак у 2023 році була спрямована на інформаційні ресурси та мережі державних органів, пріоритетом здебільшого є установи, які надають публічні сервіси громадянам або забезпечують роботу державних реєстрів. Тактика проросійських псевдо-хактивістських груп включає публікацію організацій-цілей до початку атак та звітів про недоступність під час DDoS-атаки. Тривалість атак зазвичай становить декілька годин.

DDoS-активність з боку груп псевдо-хактивістів не мають суттєвого впливу на роботу інформаційних систем державних органів. З одного боку, причиною цього є низький рівень спроможностей більшості таких груп, з іншого боку, багато державних установ завдяки підтримці міжнародних партерів з початку повномасштабного вторгнення рф в Україну використовують сервіси протидії DDoS-атакам від компаній Cloudflare, Akamai та ін.

Водночас фіксуються спроби складних DDoS-атак рівня застосунків, переважно в банківському секторі та секторі послуг.

Інтернет-шахрайство

З середини 2022 року спостерігається стрімке зростання інтернет-шахрайства стосовно громадян України, яке експлуатувало теми допомоги від держави та міжнародних організацій, таких як ООН, Червоний Хрест, ЮНІСЕФ, НАТО тощо. Типова схема передбачала заповнення форми із персональними даними та номером банківської карти нібито для отримання виплати

[13] 2023 in Review: DDoS Attacks Report by StormWall, https://stormwall.network/ddos-attack-report-2023

[14] Radware Global Threat Analysis Report, https://www.radware.com/threat-analysis-report/

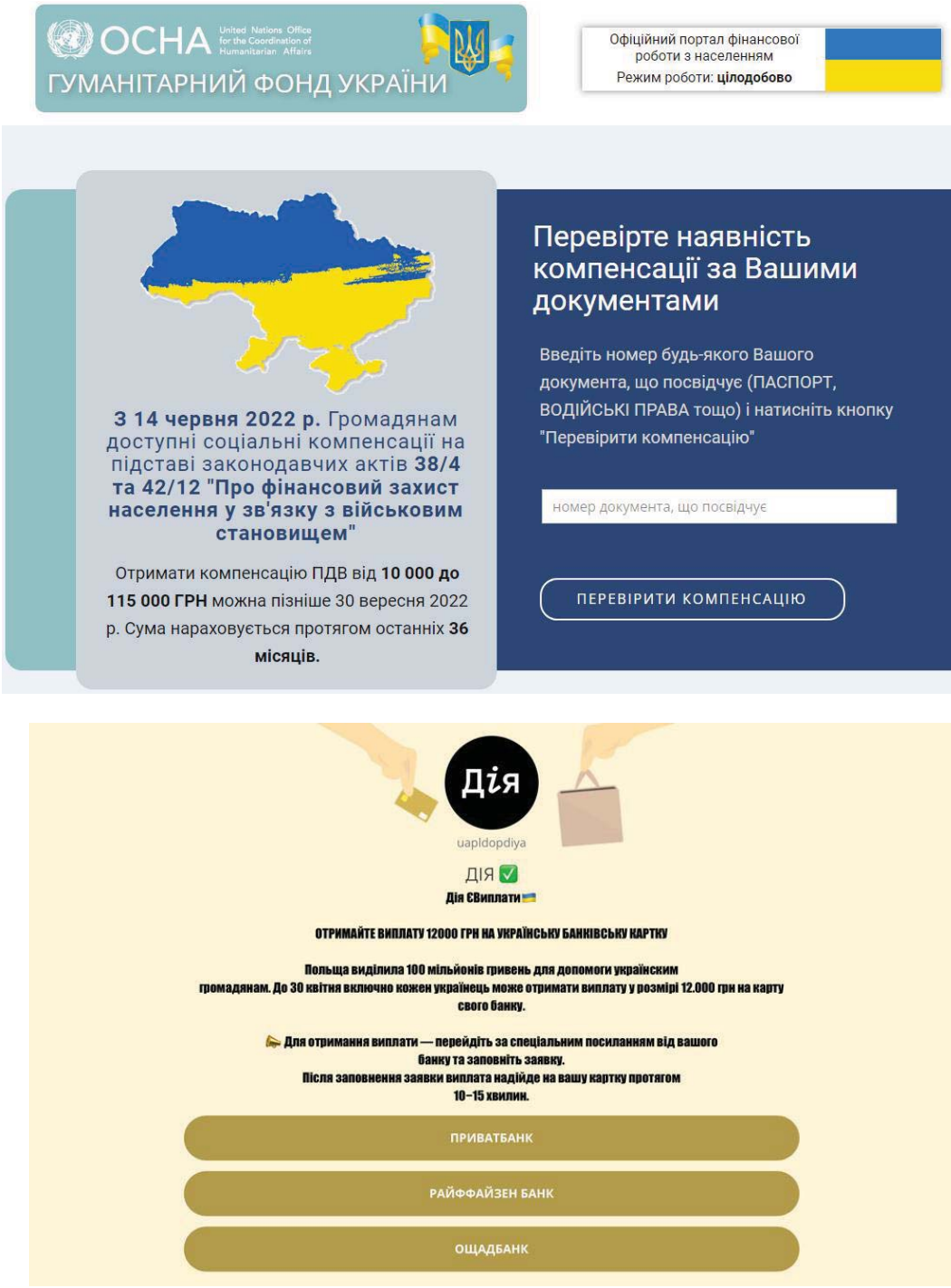


Рис 7. *Шахрайські схеми, за допомогою яких експлуатують теми виплат і компенсацій громадянам України*[15]

Також активно використовуються фішингові сайти, що імітують офіційні ресурси державних органів та волонтерських організацій, з метою збору пожертв.

Підтримувані державою російські групи використовують аналогічний підхід для збору персональних даних військовослужбовців та членів їхніх сімей. Створені ними фішингові

[15] https://csirt.bank.gov.ua/cyber-fraud

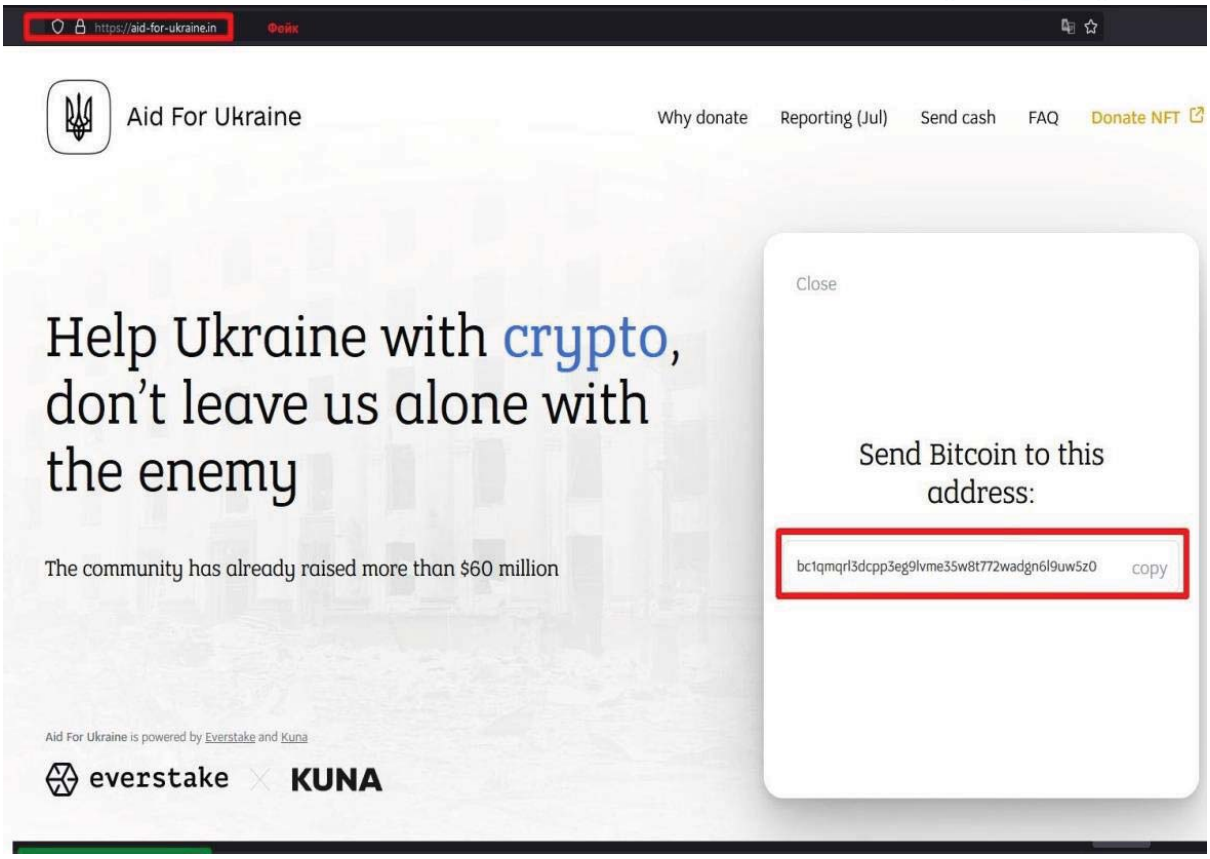


Рис 8. *Фейковий сайт збору пожертв, що імітує офіційний ресурс Мінцифри*[15]

сайти, що імітують допомогу переміщеним особам, містять детальні форми для збору персональних даних, включно з фотографіями у військовій формі, нібито для підтвердження служби у Силах оборони України.

Кіберзлочинці швидко змінюють тематики та створюють нові шахрайські ресурси. У середньому фішинговий сайт використовується від декількох годин до доби, після чого його власники переміщують його на новий домен.

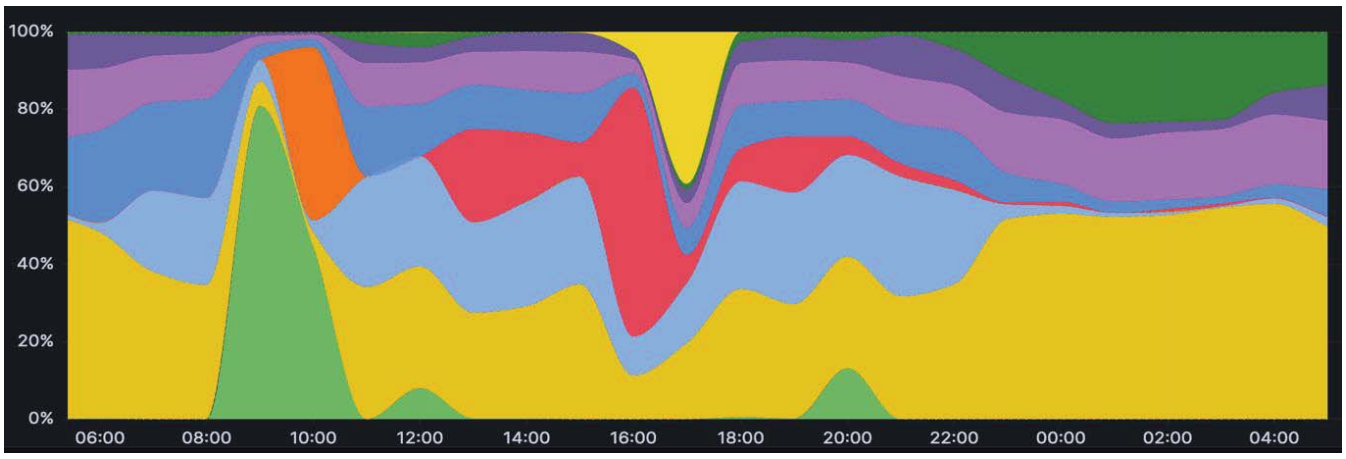


Рис 9. *Тривалість життя фішингових доменів може складати декілька годин. Дані НКЦК*

Зафіксовано тактику щодо створення фішингових доменів у національних зонах країн-партнерів, у яких проживають багато українських громадян, та обмеження (геофільтрацію) запитів з України для уникнення виявлення таких доменів.

У четвертому кварталі 2023 року найбільш активні шахрайські фішингові кампанії скеровані на фішингові схеми з сервісами доставки Укрпошта, Нова пошта, DHL та ін. Для розповсюдження такого фішингу часто використовуються розсилки повідомлень через СМС та популярні месенджери.

Google, Facebook, Telegram є основними каналами реклами і поширення фішингових лінків, зафіксовано також використання TikTok.

За результатами аналізу даних реєстрації та розміщення (хостингу) шахрайських ресурсів встановлено, що впродовж 2023 року понад 80-90% фішингових доменів використовують сервіси компанії Cloudflare для приховування реальних IP-адрес та протидії алгоритмам автоматизованого виявлення та блокування фішингу.

Використання кібератак для підтримки інформаційних та гібридних операцій

Підтримувані державою російські групи використовують кібератаки для сприяння інформаційних та гібридних операцій.

Дефейси веб-сайтів органів державної влади, компрометація інформаційних систем засобів масової інформації використовуються для поширення дезінформації та пропаганди.

23 лютого 2023 року росіяни провели масштабну кібератаку на органи державної влади, аналогічну операції BleedingBear 13 січня 2022 року, в ході якої здійснювались спроби знищення інформації, дефейси офіційних сайтів держаних органів, волонтерських організацій, засобів масової інформації. Одночасно відбулась компрометація телеканалу «Інтер», яка призвела до підміни трансляції під час інтерв'ю Секретаря РНБО України (почав грати гімн СССР).

Тактикою проросійських псевдо-хактивістських груп є публікація повідомлень про плани проведення DDoS-атак і досягнуті результати на власних сайтах та в мережі Telegram-каналів.

Частина мережі підконтрольних спецслужбам рф Telegram-каналів на постійній основі публікує персональні дані військовослужбовців, різноманітні бази даних та доступи, отримані внаслідок кібератак на українські організації.

Хоча здебільшого опубліковані дані про «успішні кібератаки» не підтверджуються, це забирає час для перевірки такої інформації та формує уявлення про високий рівень спроможностей таких груп.

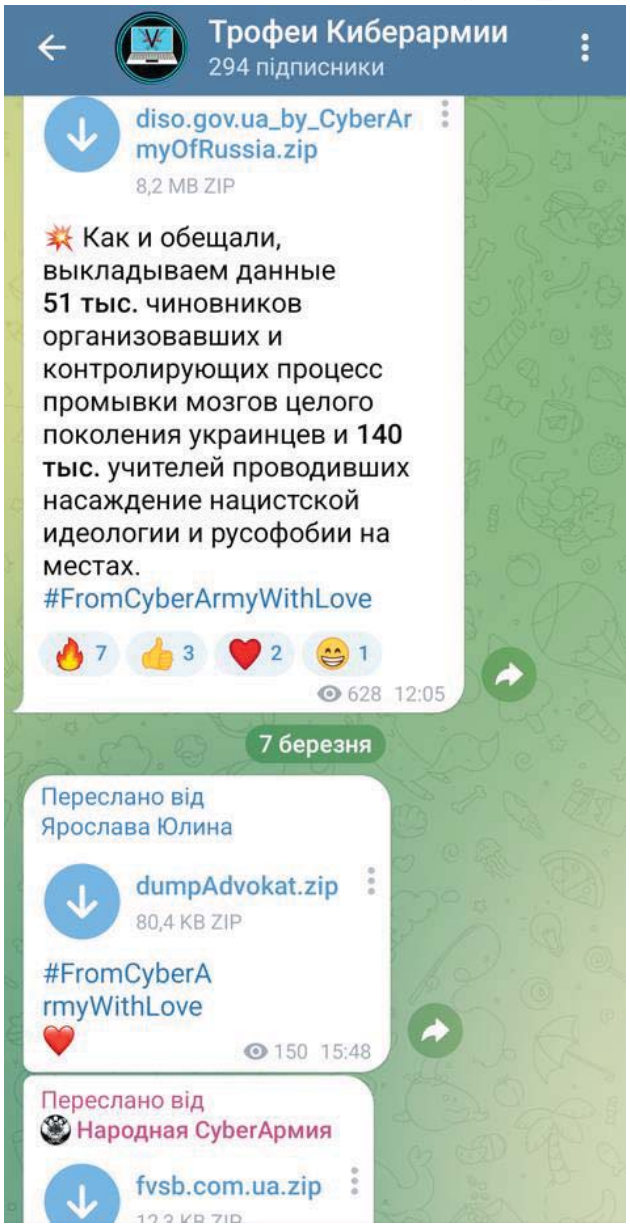


Рис 10. *Скриншот з Telegram-каналу «Трофеи Киберармии»*

Компрометація облікових записів та витоки інформації

Тенденцією 2023 року є використання валідних облікових записів для початкового доступу до мереж організацій. Витоки інформації, дані OSINT та викрадені в результаті попередніх кібератак даних ретельно аналізуються та використовуються під час наступних таргетованих кібератак.

У багатьох випадках ціллю атакувальників є облікові записи та дані автентифікації до онлайн-сервісів. Значно зросла кількість атак типу підбір паролів, password spraying, зловмисник посередині (Adversary-in-the-Middle). Для викрадення облікових записів використовуються шкідливе програмне забезпечення, що збирає паролі із браузерів, токени авторизації із скомпрометованих хостів, а також фішингові ресурси.

Порушення доступності внаслідок збоїв або пошкодження обладнання чи мереж

Внаслідок російської агресії в Україні пошкоджено 25% фіксованих мереж, знищено або пошкоджено 4,3 тис. базових станцій мобільного зв'язку[16]

В умовах війни для українських організацій загрозу становлять не тільки ворожі дії в кіберпросторі, але й порушення доступності внаслідок збоїв або пошкодження обладнання чи мереж. Вимкнення електроенергії, пошкодження ліній зв'язку можуть мати наслідком - недоступність інформації або сервісів.

Більшість організацій з важливими бізнес-процесами забезпечили резервування даних, живлення, каналів зв'язку, в тому числі із застосуванням хмарних технологій, проте опитані експерти визначають таку загрозу як актуальну.

Деструктивні атаки

У 2023 році значно зменшилася кількість деструктивних кібератак.

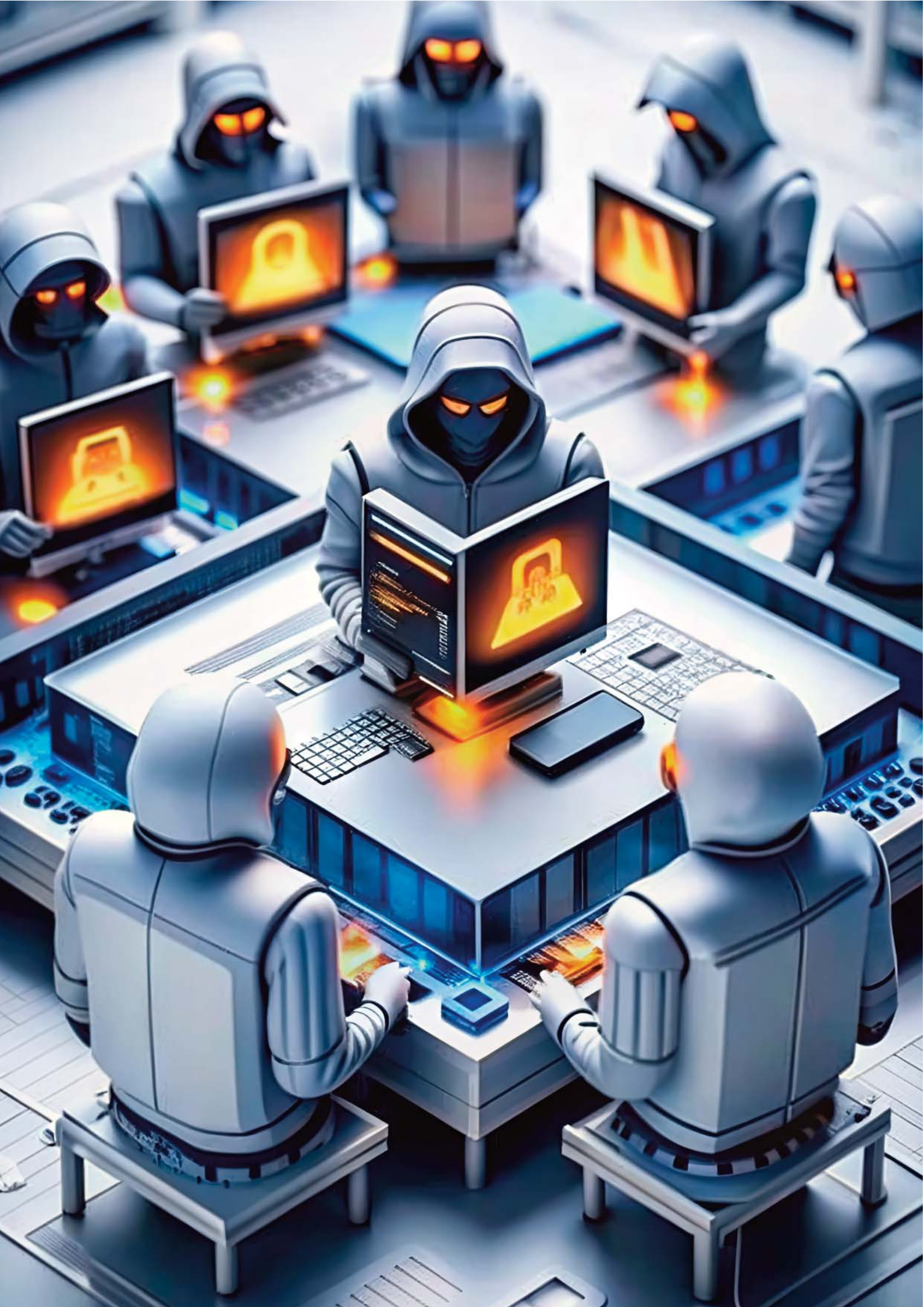
Деструктивні атаки у звітний період були спрямовані і на знищення даних, і на пошкодження мережевої інфраструктури.

Для знищення даних на окремих хостах використовувалися модифіковані версії утиліти Sdelete. Для її розповсюдження використовувались засоби ActiveDirectory, у разі їх наявності / компрометації, або інструменти типу Impacket.

Зафіксована тактика отримання доступу до консолі керування систем управління віртуальними машинами та масового видалення віртуальних машин та/або віртуальних дискових сховищ.

У секторі електронних комунікацій тактикою атакувальників є також пошкодження або видалення конфігурацій мережевого обладнання, що призводить до припинення функціонування мережі. 12 грудня 2023 року зафіксовано таку деструктивну атаку на оператора зв'язку «Київстар», наслідком якої була тимчасова недоступність зв'язку для мільйонів українських громадян.

[16] Пошкоджено 25% мереж фіксованого зв'язку та 4 тисячі мобільних вишок, – Федоров, https://mbiz.censor.net/news/3489565/v_ukrayini_poshkodjeno_25_merej_fiksovanogo_zvyazku_ta_4_tysyachi_vyshok



НАЙАКТИВНІШІ ХАКЕРСЬКІ ГРУПИ

У таблиці наведено хакерські групи, які здійснювали найбільшу активність щодо України у 2023 році.

Група	Приналежність	Основні цілі	Спроможності
APT28	в/ч 26165 ГРУ, росія	Військові організації, енергетична інфраструктура, державні установи, дипломатичні установи	Oceanmap, Masepie, Steelhook, Impacket, Headlace, CVE-2023-23397, CVE-2023-38831
APT29	СЗР росія	Військові організації, дипломатичні установи	Envyscout, Halfrig, Quarterrig, Snowyamber, Cobalt Strike, Brute Ratel, CVE-2023-38831
Sandworm	в/ч 74455 ГРУ, росія	Провайдери телекомунікацій, критична інфраструктура	BIASBOAT, QueueSeed, LOADGRIP, AcidRain, AcidPour, Poemgate, Poseidon, Whitecat
Turla	в/ч 71330 ФСБ, росія	Військові організації	Kazuar
Callisto	в/ч 64829 ФСБ, росія	Державні та дипломатичні установи	Spear-phishing, Evilginx
Gamaredon	Управління ФСБ у Криму	Військові організації, правоохоронні органи, державні та дипломатичні установи	LoadShort, GammaLoad, GammaDrop, HockSeat, LakeFlash,
WinterVivern	Активність в інтересах росії та Білорусі	Військові організації, державні установи	CVE-2023-5631, CVE-2022-27926,
Ghostwriter	Військові, Білорусь	Державні установи	CVE-2023-38831, PicassoLoader, Cobalt Strike
DaVinci Group (UAC-0050)	Правоохоронні органи, росія	Підприємства і організації приватного та державного секторів	LummaStealer, RemoteUtilities, Remcos, Quasar, Venom
Smokeloader Group (UAC-0006)	Фінансово мотивовані злочинці, росія	Підприємства і організації приватного та державного секторів	Smokeloader, Taleshot, RDPWrapper, Hangthread
NoName057(16)	Псевдо-хактивісти, ГРУ росія	Підприємства і організації приватного та державного секторів	DDoSia
CyberArmyofRussia	Псевдо-хактивісти, ГРУ росія	Підприємства і організації приватного та державного секторів	Killweb, CA_DDoS

ОЦІНКА ВПЛИВУ КІБЕРЗАГРОЗ

Здебільшого українські організації не оцінюють масштаб збитків та наслідків кібератак, обмежуючись заходами із відновлення після інциденту, або не роблять таку інформацію доступною публічно.

Для оцінки загальних наслідків кібератак використовувалися результати опитування експертів державного і приватного секторів та якісного аналізу, що має дещо суб'єктивний характер. В рамках цього звіту були обрані наступні види наслідків кіберінцидентів:

☑ Цифрові наслідки, що стосуються недоступності систем, пошкодження даних або витоків інформації.

☑ Економічні наслідки, що стосуються прямих і непрямих фінансових втрат.

☑ Соціальні наслідки, що стосуються втрати довіри внаслідок порушення важливих публічних сервісів, або витоку персональних даних громадян.

☑ Репутаційні наслідки, що стосуються можливого негативного сприйняття громадськістю організації, яка стала жертвою кіберінциденту.

☑ Фізичні наслідки, що стосуються травм чи шкоди громадянам.

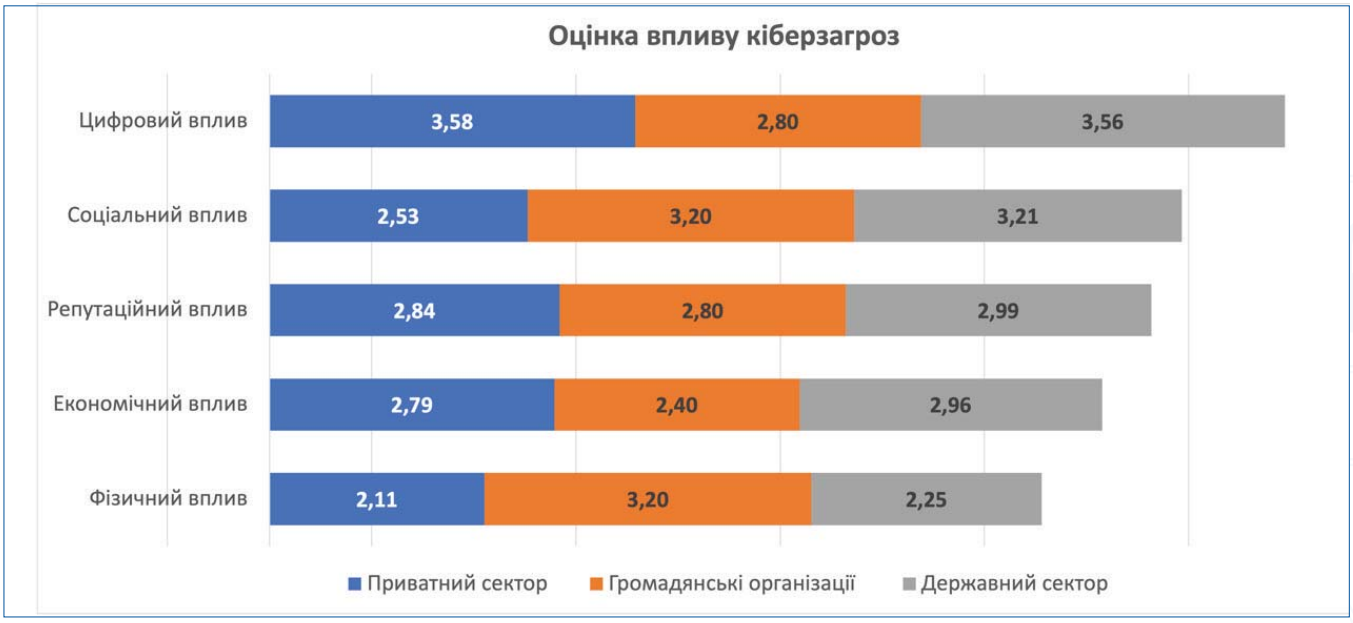


***Рис 11**. Оцінка наслідків реалізації кіберзагроз*

Найбільшими наслідками від кібератак у 2023 році є цифрові та соціальні наслідки, економічні та репутаційні втрати вважаються менш важливими, фізичні наслідки кібератак не розглядаються як суттєві.

ВРАЗЛИВОСТІ

Відповідно до даних «Звіту про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 рік» Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку України найчастіше фіксувалися спроби експлуатації вразливостей CVE-2022-20776, CVE-2021-26084, CVE-2021-40438, CVE-2022-31699, CVE-2023-45802, CVE-2022-25762, CVE-2022-20920, CVE-2021-34699, CVE-2021-21974, CVE-2023-34048. Водночас не всі з цих вразливостей виявлені в продуктах, поширених в Україні.

Урядова команда реагування CERT-UA опублікувала декілька звітів, які містять інформацію щодо вразливостей, які використовуються під час атак на українську інфраструктуру, а саме

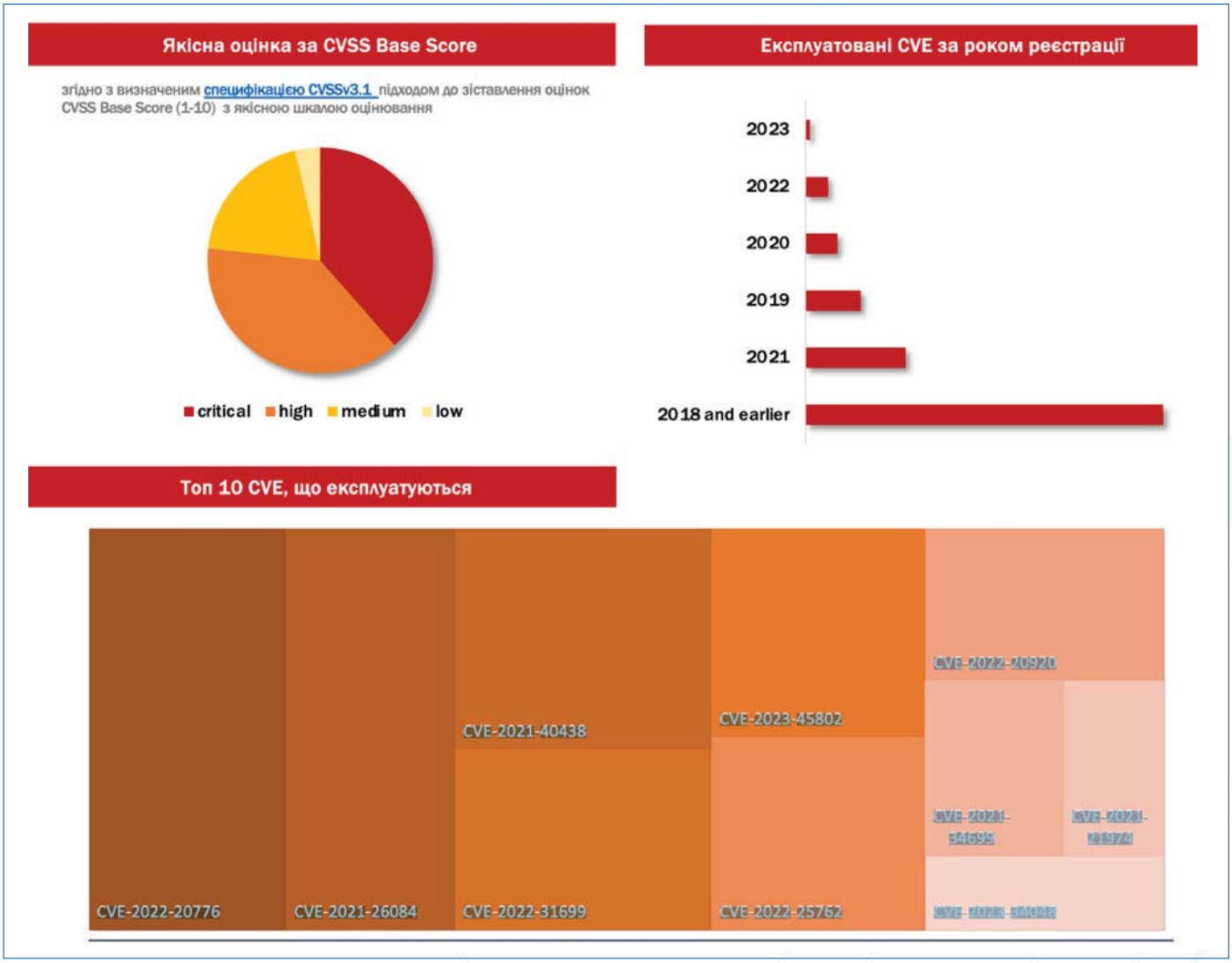


Рис 12. *Основні вразливості*

вразливості у Zabbix (CVE-2022-23131, CVE-2022-23134), WinRAR (CVE-2023-38831), Roundcube (CVE-2020-35730, CVE-2021-44026, CVE-2020-12641).

За результатами опитування експерти зазначили додаткові вразливості, які експлуатувались у 2023 році: Zimbra Collaboration Suite (CVE-2018-6882), Fortinet FortiGate SSL-VPN (CVE-2023-27997), Fortinet FortiOS (CVE-2018-13379), Microsoft Outlook (CVE-2023-23397), Apache Log4j (CVE-2021-44228).

ДОДАТОК. ІНФОРМАЦІЯ ПРО АДАПТОВАНИЙ ВАРІАНТ МЕТОДОЛОГІЇ ENISA

Для проведення дослідження ландшафту кіберзагроз України та підготовки звіту було використано методологію ENISA «Методологія ENISA з побудови ландшафту загроз кібербезпеки, Липень 2022 року» (ENISA Cybersecurity Threat Landscape Methodology, July 2022». Враховуючи стратегічний характер діяльності НКЦК, методологію було адаптовано з використанням наступних принципів.

Узагальнений процес створення звіту про ландшафт кіберзагроз відповідно до методології наведено на рис.

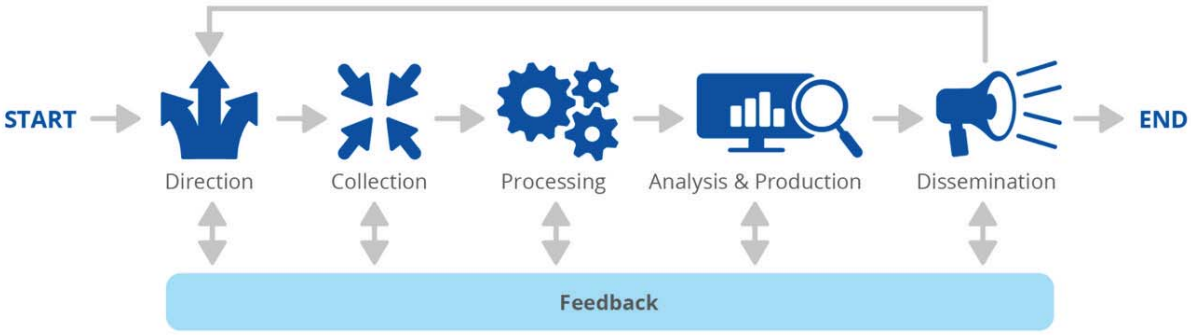


Рис 13. *Узагальнений процес створення звіту про ландшафт кіберзагроз*

Він складається з п’яти основних етапів: визначення спрямування, збір даних, обробка даних, аналіз даних та підготовка і розповсюдження звіту. На кожному з етапів передбачено механізм зворотного зв'язку.

Визначення спрямування

Метою етапу є визначення цілей, аудиторії та сфери дослідження. За результатами консультацій з НКЦК та з урахуванням рекомендацій ENISA було визначено такі цілі звіту:

- ☑ прийняття рішень стратегічного рівня;
- ☑ управління ризиками;
- ☑ пріоритезація рекомендацій щодо політик кібербезпеки;
- ☑ визначення напрямів для навчань та розвитку спроможностей;
- ☑ поширення інформації, корисної для забезпечення кіберзахисту.

Аудиторією звіту є фахівці та керівники, які оперують на стратегічному та частково тактичному рівнях:

☑ представники організацій-членів НКЦК, які беруть участь у розробці Стратегії кібербезпеки;

☑ керівники з кібербезпеки органів влади, об'єктів критичної інфраструктури;

☑керівники приватних підприємств;

☑ представники міжнародних організацій і національних агентств та установ у сфері кібербезпеки.

З огляду на стратегічний характер звіту, у його структурі передбачено розділ «Ключові тенденції та висновки», який дозволяє цільовій аудиторії швидко ознайомитись з основними результатами дослідження.

Оскільки дослідження проводилось в інтересах НКЦК, а основним стейкхолдером виступали працівники Апарату РНБО України, які надавали інформацію про пріоритети, забезпечували загальне керівництво процесом та зворотній зв'язок.

Сфера дослідження включає в себе підготовку відповідей на наступні питання: найбільш атаковані сектори, основні тенденції, типи кіберзагроз, вразливості, актори, оцінка впливу кіберзагроз. Звіт подає інформацію про період з 1 січня 2023 року до 31 грудня 2023 року. Під час підготовки використовувався зовнішньо-орієнтований підхід.

Збір даних

На етапі збору даних використовувалась інформація з відкритих джерел, включно з публікаціїями аналітики кіберзагроз провідних компаній з кібербезпеки, даними про кіберінциденти та кібератаки з соціальних мереж, власниими джерелами, інформацією з систем обміну індикаторами компрометації MISP та аналітики кіберзагроз OpenCTI, а також матеріалами НКЦК, даними інтерв'ю з українськими експертами в галузі кібербезпеки та опитуваннями представників державних органів, об'єктів критичної інфраструктури, громадського та приватного сектору методом анкетування.

В Україні відсутній механізм обов'язкового інформування про кіберінциденти та кібератаки. Механізми і процедури обміну інформації про кіберінциденти частково врегульовані у різних підзаконних актах та на практиці є добровільними для державних органів, об'єктів критичної інфраструктури та підприємств приватного сектору. Крім того, в багатьох випадках основною метою організацій під час реагування на інциденти є усунення їх наслідків без встановлення точних причин та способів втручання в їх інформаційні системи, а також масштабу впливу інцидентів.

Прийняту в Україні таксономію кіберінцидентів, схвалену Національним координаційним центром кібербезпеки у 2021 році[17], використовують здебільшого державні органи. Вона розроблена з використанням рекомендацій ENISA від січня 2018 року (ENISA Reference Incident

[17] Перелік категорій кіберінцидентів, https://cert.gov.ua/recommendation/16904

Classification Taxonomy[18]), а також спільного документа ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs[19]) та орієнтована передусім на обмін інформацією на рівні команд реагування CERT/CSIRT, тобто на технічний/тактичний обмін інформацією.

В Україні відсутня узгоджена на національному рівні система іменування хакерських груп (акторів). Найчастіше під час атрибуції використовується таксономія Урядової команди реагування CERT-UA (UAC-xxxx) або застосовуються назви хакерських груп, запропоновані Microsoft, Mandiant, ESET, Recorded Future та іншими компаніями.

Ці фактори ускладнюють порівняння інформації з різних джерел та обмежують можливості кількісного аналізу.

Для аналізу було зібрано інформацію з сайту Урядової команди CERT-UA (37 публікацій за 2023 рік); (пів)річні звіти CERT-UA та ДЦК3; деперсоналізовані дані щодо кіберінцидентів, надані низкою українських компаній з кібербезпеки (27 звітів); публікації з сайтів компаній Cisco Talos, Cloudflare, Crowdstrike, Darktrace, ESET, Fortinet, Google TAG, Mandiant, Microsoft, PaloAlto, Radware, Recorded Future, Sophos, StormWall та ін. (143 публікації); дані OSINT, матеріали сайтів новин та соціальних мереж, що містили інформацію та заяви організацій про атаки на них. З системи MISP НКЦК було отримано дані про 241 подію, з власної CTI-системи було отримано 103,701 звітів про кібератаки і кіберінциденти. Також НКЦК було надано 50 інформаційних тижневих звітів про ситуацію в кіберпросторі.

Оскільки дослідження здійснювалось вперше та впродовж досить короткого проміжку часу, дані для звіту збирались протягом обмеженого часу. Надалі, відповідно до методології ENISA, передбачено збір даних на постійній основі, згідно з наступним планом.

Джерело даних	Тип даних	Час збирання даних
Основні суб'єкти	Тактичні, стратегічні	Упродовж року, річні та піврічні звіти
Публікації компаній з кібербезпеки, постачальників CTI	Операційні, тактичні	Упродовж року
Соціальні мережі	Операційні, тактичні	Упродовж року
Новини з кібербезпеки	Операційні, тактичні, стратегічні	Упродовж року
Дані про вразливості	Операційні, тактичні	Упродовж року
Наукові матеріали	Тактичні, стратегічні	Упродовж року
Дані OSINT	Операційні, тактичні	Упродовж року
Дані з технічних систем обміну	Операційні, тактичні	Упродовж року
Звіти ситуаційної обізнаності від партнерів	Операційні, тактичні, стратегічні	На періодичній основі, упродовж року

[18] Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[19] Common Taxonomy for Law Enforcement and CSIRTs, https://www.europol.europa.eu/publications-events/publications/common-taxonomy-for-law-enforcement-and-csirts

Відповідно до методології, різним джерелам було присвоєно відповідні рівні довіри: низький, середній та високий. Високий рівень довіри надається інформації від основних суб'єктів, середній – даним з власних технічних систем обміну та даних власного OSINT та досліджень, низький рівень – зовнішнім джерелам та даним опитувань.

За сприяння НКЦК було проведено опитування представників державних органів, приватного сектору (компанії з кібербезпеки та об’єкти критичної інфраструктури) та громадського сектору. Загалом на питання анкети відповіли 398 респондентів: 373 з державного сектору, 19 з приватного сектору, 5 з громадського сектору, 1 респондент зазначив «інше» (ЗСУ).

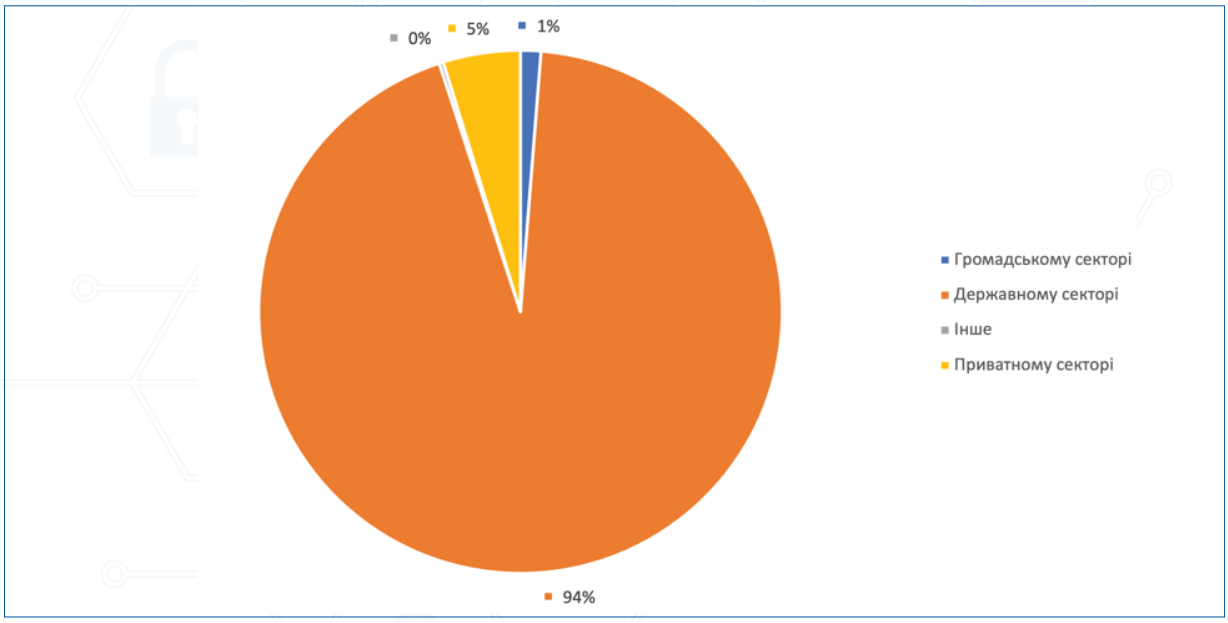


Рис 14. *Структура респондентів*

Анкета містила 13 запитань, згрупованих за темами: інформація про респондента (1 питання); актуальні загрози (2 питання); джерела, цілі і наслідки кібератак (4 питання); інструментарій (3 питання); оцінки респондента (3 питання).

З метою визначення актуальних загроз анкета містила питання «Які загрози були найбільш актуальними для українських організацій і громадян у 2023 році?» з варіантами вибору зі списку загроз, визначених у звіті ENISA про ландшафт загроз за 2023 рік (ENISA Threat Landscape 2023[20]) та можливістю визначити ступінь їх актуальності за шкалою від 1 (менш актуальні) до 5 (більш актуальні). Варто зазначити, що незважаючи на те, що фішинг на мобільні пристрої є елементом соціальної інженерії, цю загрозу було виокремлено через велику кількість пов'язаних із цим типом загроз інцидентів.

Найбільш актуальними загрозами, які виділили респонденти, стали шкідливе програмне забезпечення, фішинг на мобільні пристрої, DDoS-атаки. Представники різних секторів мають дуже схоже сприйняття загроз, проте є й відмінності.

[20] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Для представників приватного сектору шкідливе програмне забезпечення становить меншу загрозу (лише 5 місце), для представників державного сектору ця загроза розділила 1 місце з фішингом на мобільні пристрої. Натомість загрози від DDoS-атак, деструктивних атак та витоків інформації бізнес оцінює на 5-15 процентних пункти вище, ніж держава, що ймовірно пов'язано із більш жорсткими вимогами до безперервності процесів та репутаційними ризиками. Цікаво, що всі респонденти відзначили високий рівень загрози від кібератак, метою яких є підтримка інформаційних та гібридних операцій, хоча для приватного сектору рівень цієї загрози вищий, порівнюючи з іншими секторами.

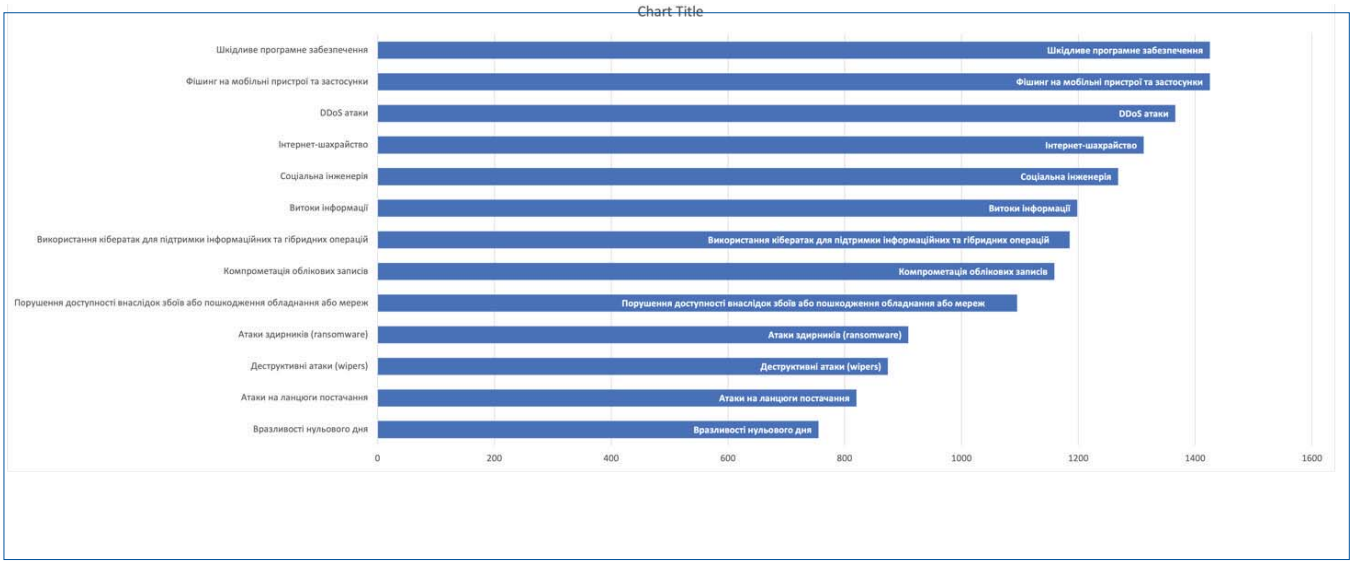


Рис 15. *Актуальні загрози*

Відповідно до результатів опитування та зібраних даних про кібератаки та кіберінциденти, для розгляду у цьому звіті були вибрані наступні основні загрози: соціальна інженерія, шкідливе програмне забезпечення, DDoS-атаки, інтернет-шахрайство, використання кібератак для підтримки інформаційних та гібридних операцій, компрометація облікових записів та витоки інформації, порушення доступності внаслідок збоїв або пошкодження обладнання чи мереж та деструктивні атаки.

Результати відповідей на питання «Які сектори та категорії громадян були найчастіше об'єктами кібератак у 2023 році?» використовувались під час аналізіу секторів, які зазнали найбільших атак. Отримані за результатами опитування дані в цілому корелюють з інформацією звіту Урядової команди CERT-UA. Цікаво, що і публічний, і приватний сектор визнають, що найбільше атак здійснюється на державні органи. Проте бізнес вважає, що наступними за кількістю атак є телекомунікації, IT та банківський сектор, а в державному секторі більш атакованими вважають сектори безпеки і оборони та енергетику.

Питання щодо мотивації атакувальників та наслідків їх впливу використовувались під час оцінки впливу кібератак. Незважаючи на порівняно невелику кількість деструктивних атак, саме пошкодження функціонування систем зайняло друге місце у відповідях на питання «Які основні цілі та мотивація кібератак на українські організації та громадян у 2023 році?». Це

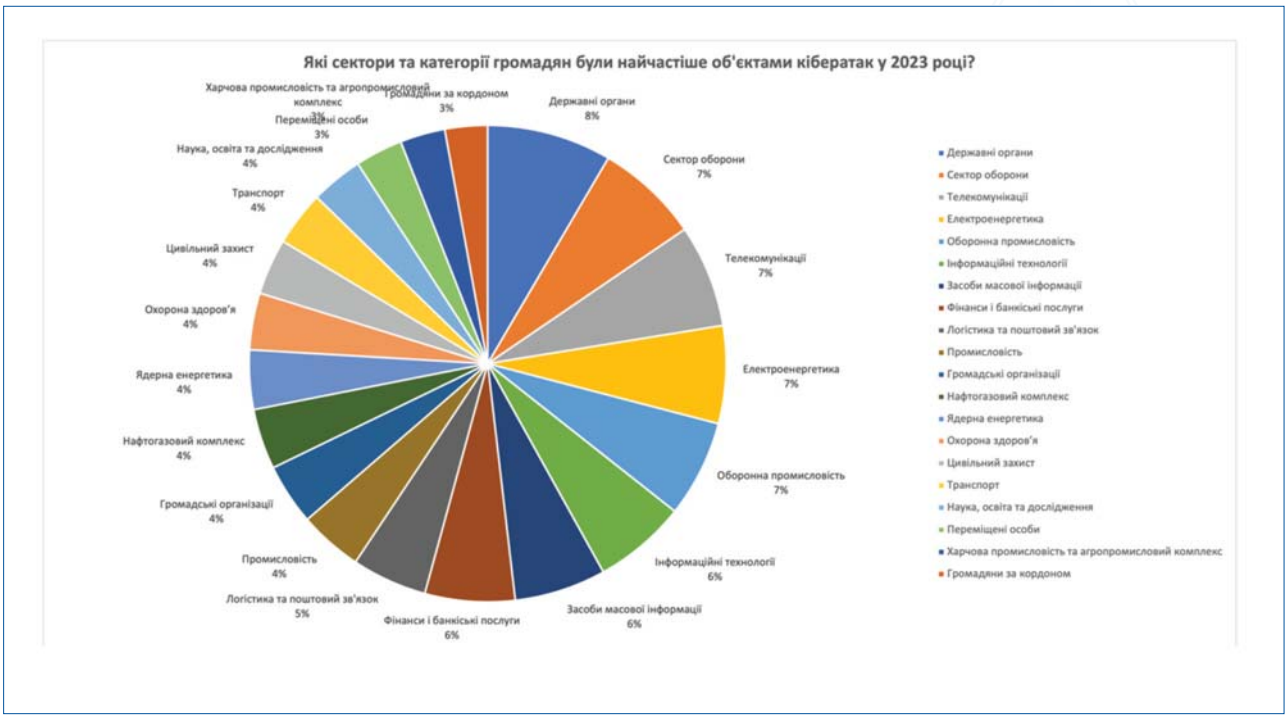


Рис 16. *Атаковані сектори та категорії громадян*

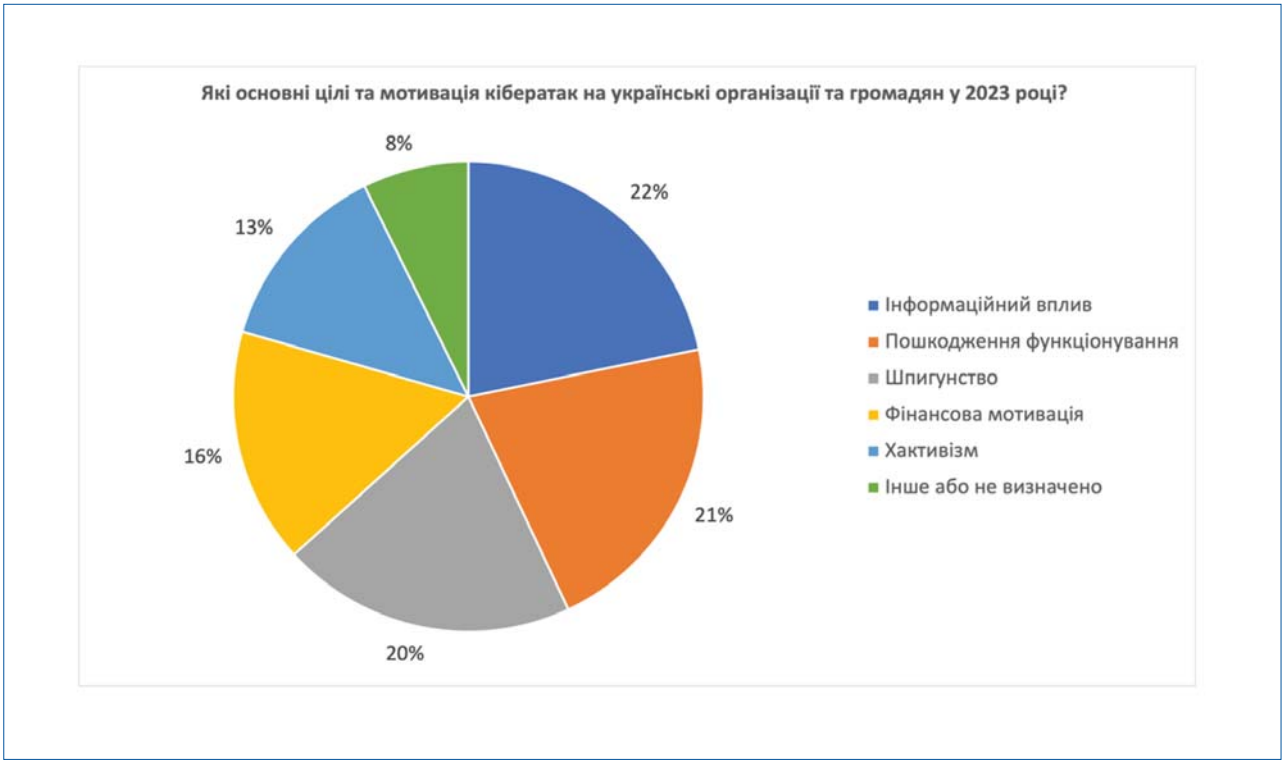


Рис 17. *Мотивація здійснення кібератак*

свідчить про більш високий рівень суб'єктивного сприйняття загроз від такого виду кібератак внаслідок більшої шкоди та їх реалізації, а також про більш широку інформованість про такі атаки завдяки публікаціям у засобах масової інформації.

Обробка даних та аналіз даних

На етапі обробки даних здійснюється перетворення зібраних даних у формат, що може бути використаний аналітиками кіберзагроз на етапах аналізу та формування звіту. Оскільки вихідні дані надходять у різних форматах (структурованих та неструктурованих), з різною глибиною деталізації, рівнями довіри тощо, основним завданням цього етапу є усунення дубльованої інформації, приведення даних до спільних форматів, що можуть оброблятися, зокрема в автоматизованих CTI-системах.

У процесі обробки здійснювалось перетворення даних до формату, що мінімально описує: дату, тип інциденту, опис інциденту, атакований сектор, атрибуцію, наслідки, рівень довіри тощо. Матеріали міжнародних компаній було перекладено українською мовою.

Методологія ENISA передбачає використання наступних таксономій кіберзагроз: ENISA Threat Taxonomy[21], JRC Taxonomy[22], Cybersecurity Incident Taxonomy[23], ENISA Reference Security Incident Classification Taxonomy[24]. Також рекомендовано використовувати результати перспективних досліджень та вимоги нормативних актів ЄС. Під час обробки даних необхідно забезпечити можливість зіставлення ENISA Threat Taxonomy та схваленої в Україні таксономією кіберінцидентів[25].

[21] ENISA Threat Taxonomy 2016, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[22] A Proposal for a European Cybersecurity Taxonomy, https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[23] Cybersecurity Incident Taxonomy, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[24] ENISA Reference Security Incident Classification Taxonomy, https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/reference-security-incident-taxonomy-working-group-2013-rsit-wg

[25] Перелік категорій кіберінцидентів, https://cert.gov.ua/recommendation/16904

У ролі CTI фреймворків залежно від даних Методологією ENISA передбачено використання наступних фреймворків: MITRE ATT&CK®, Cyber Kill Chain®, MITRE CVE®, OASIS Cyber Threat Intelligence (CTI) STIX™.

У ролі CTI фреймворків залежно від даних Методологією ENISA передбачено використання наступних фреймворків: MITRE ATT&CK®, Cyber Kill Chain®, MITRE CVE®, OASIS Cyber Threat Intelligence (CTI) STIX™.

У ролі технічного формату файлів як основного використовується JSON.

Залежно від типів даних було використано методики традиційного аналізу із застосуванням експертних оцінок та структуровані аналітичні методи.

Проміжні версії звіту було надано НКЦК для перевірки та зворотного зв'язку.

Підготовка та розповсюдження звіту

Звіт підготовлено українською мовою, в форматі pdf. Передбачено розповсюджувати його шляхом публікації на онлайн-ресурсах НКЦК, а також через презентації основним зацікавленим сторонам. Додатково розглядається переклад звіту англійською мовою для поширення міжнародним партнерам.