HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА

ЗЛОВМИСНИЙ АЛЬЯНС:

як кібератаки та дезінформація синхронно дестабілізують цифровий простір України в умовах російської агресії

Павло Бурдяк,
аналітик напряму «Незалежні медіа»
Центру демократії та верховенства права

2024

Дослідження проведене за фінансової підтримки Фонду ім. Гайнріха Бьолля, Бюро Київ — Україна. Думки, висновки та рекомендації належать авторам цього дослідження і не обов'язково відображають погляди Фонду ім. Гайнріха Бьолля, Бюро Київ — Україна та уряду Німеччини.

ЗМІСТ

ЗМІСТ

ВСТУП

З СІЧНЯ 2022 РОКУ ДО ГРУДНЯ 2023 РОКУ «CYBERPEACE INSTITUTE» ЗАФІКСУВАВ 3255 АТАК У ГЛОБАЛЬНОМУ КІБЕРПРОСТОРІ. З НИХ ФАКТИЧНО П'ЯТА ЧАСТИНА — 607 КІБЕРАТАК ТА ОПЕРАЦІЙ — ПРИПАЛА НА УКРАЇНУ.

З 24 лютого 2022 року Україна опинилася в епіцентрі повномасштабної гібридної агресії, що поєднує, зокрема, кібернетичний та інформаційний складники. Останні два роки українські державні установи, медіа й критична інфраструктура потерпають від навали (про)російських кібератак і дезінформації, які підсилюють одне одного і створюють серйозні виклики для цифрової та інформаційної безпеки України.

Зловмисники використовують широкий спектр засобів — від DDoS-атак до фішингових кампаній і глушіння супутникових сигналів. Усі ці дії супроводжуються інтенсивними дезінформаційними кампаніями, які спрямовані на підрив довіри до офіційних джерел інформації та дестабілізації суспільства.

Мета цього дослідження — проаналізувати взаємозв'язок між кібератаками та дезінформацією в українському кіберпросторі. Ми зосередимо увагу на методах, які використовують зловмисники, визначимо способи їх впливу на суспільство й розробимо рекомендації для протидії цим загрозам. Щоб отримати комплексне розуміння проблеми й розробити рекомендації для підвищення рівня цифрової та інформаційної безпеки в Україні, для аналізу використані кількісні, якісні, кейс-стаді та функціональний методи, а також інтерв'ю з експертами.

Загроза, що постала перед українським інформаційним простором, — частина ширшої глобальної проблеми, яка вимагає міжнародної співпраці й обміну досвідом. У цьому контексті досвід України може стати важливим уроком для інших країн, що стикаються з подібними викликами. Успішна протидія кібератакам і дезінформації вимагає не лише технічних рішень, але й підвищення рівня медіаграмотності та цифрової грамотності населення.

Таким чином, дослідження спрямоване на висвітлення питання кібербезпеки в Україні крізь призму (про)російської дезінформації з метою вироблення нових рекомендацій для підвищення рівня стійкості цифрового й інформаційного просторів України.

МЕТОДОЛОГІЯ

ДЛЯ ВСЕБІЧНОГО АНАЛІЗУ КІБЕРБЕЗПЕКИ, ДЕЗІНФОРМАЦІЇ ТА ЇХ ВЗАЄМОДІЇ З КОНВЕНЦІЙНИМИ БОЙОВИМИ ДІЯМИ В ЦЬОМУ ДОСЛІДЖЕННІ МИ ВИКОРИСТОВУЄМО КІЛЬКІСНІ, ЯКІСНІ, КЕЙС-СТАДІ ТА ФУНКЦІОНАЛЬНИЙ МЕТОДИ, А ТАКОЖ ІНТЕРВ'Ю З ЕКСПЕРТАМИ.

Кількісні методи. Кількісні методи використані для збору та аналізу статистичних даних про кібератаки та дезінформаційні кампанії проти України. Наприклад, ми проаналізували кількість кібератак (зокрема, DDoS-атак) на українські об'єкти кіберзахисту[1] протягом 2022–2023 років, використовуючи дані Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Окрім того, за допомогою даних ГО «Платформа прав людини», наведених у звіті «Війна у цифровому вимірі та права людини», ми змогли окреслити інтенсивність поширення дезінформаційних повідомлень у медіа з 2021 до 2023 року.

Кількісний аналіз допоміг визначити тенденції в частоті проведення кібератак і дезінформаційних кампаній, встановити кореляцію між ними, виявити періоди найбільшої активності зловмисників й оцінити масштаби комплексного впливу загроз на цифровий та інформаційний простори України.

Якісні методи. Якісні методи в цьому дослідженні дозволили детально проаналізувати текстові звіти держустанов і міжнародних організацій про проведені кібератаки, виявити основні тренди й методи, які використовують ворожі угруповання для здійснення кібератак на українські мережеві ресурси для дискредитації українських інституцій і поширення дезінформації.

Визначення характеристик дезінформаційних кампаній показало, які повідомлення та методи використовуються для маніпулювання громадською думкою та сіяння розбрату.

Кейс-стаді метод. За допомогою цього методу ми змогли детально розглянути конкретні приклади кібератак і дезінформаційних кампаній. Зокрема, клонування українських сайтів зловмисниками («Obozrevatel», «Українська правда», «РБК-Україна»), злами сайтів («1+1 media group», «Прямий», «NV») тощо.

Функціональний метод. Ми використали функціональний метод для аналізу нормативно-правових засад кібербезпеки й інформаційної безпеки. Він дозволяє систематизувати й оцінити нормативно-правові рамки регулювання протидії кібератакам і дезінформації на національному рівні. Окрему увагу приділено міжнародно-правовим стандартам у сфері дезінформації.

Застосування функціонального методу дозволяє не тільки виявити прогалини та недоліки в наявних нормативно-правових актах, але і визначити необхідні напрями для подальшого вдосконалення законодавчої бази.

Інтерв'ю з експертами з кібербезпеки. За результатами проведених інтерв'ю з експертами з кібербезпеки, які працюють у проєкті «Nadiyno.org», — Павлом Бєлоусовим, Генрі Дем'яновічем, Борисом Золотченком — були розроблені рекомендації для підвищення кібербезпеки на технічному рівні.

Хронологічні рамки дослідження. У фокусі цього дослідження період повномасштабної російської агресії. Ми охопили часовий проміжок із 1 лютого 2022 року до 31 липня 2024 року. Дані до лютого 2022 року іноді використовуються для проведення паралелей, як-от між динаміками кібератак і дезінформації в Україні до та після повномасштабного російського вторгнення.

[1] Об'єкти кіберзахисту — об'єкти критичної інформаційної інфраструктури та інші інформаційно-телекомунікаційні системи, у яких здійснюється обробка державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом.

1. КІБЕРБЕЗПЕКА Й ДЕЗІНФОРМАЦІЯ В ЦИФРОВОМУ ПРОСТОРІ УКРАЇНИ: ВИЗНАЧЕННЯ Й ОСОБЛИВОСТІ РЕГУЛЮВАННЯ

1.1. КІБЕРБЕЗПЕКА: КАТЕГОРІЙНО-ПОНЯТТЄВИЙ АПАРАТ

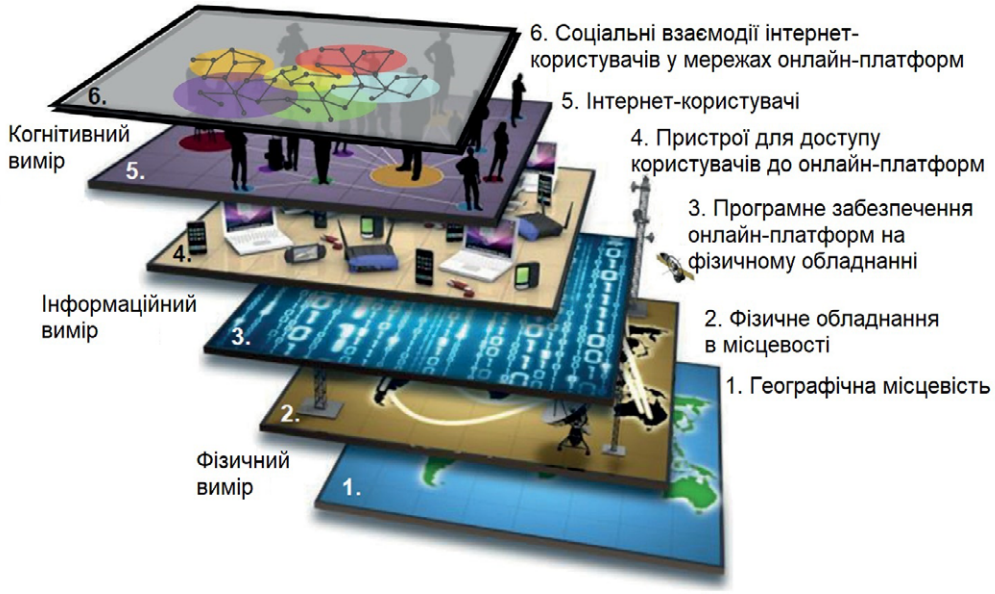
Для кращого розуміння ключових концепцій у сфері кібербезпеки важливо визначити основні поняття, якими ми будемо послуговуватися в аналізі. Зокрема, використаємо термінологію, закріплену в статті 1 Закону України «Про основні засади забезпечення кібербезпеки України»:

- **Кіберпростір** (у межах цього дослідження також згадується як цифровий простір) — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

- **Кібербезпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства й держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства й цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

- **Кіберзахист** — сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного й технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем.

- **Кіберзагроза** — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України в кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.



Схематичне зображення кіберпростору

Джерело: інфографіка зі статті Балаша Караша, перекладена та адаптована автором цього дослідження.

- **Кібератака** — спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

- **Інцидент кібербезпеки** (або кіберінцидент) — подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

- **Активна протидія агресії в кіберпросторі** — дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз і кібератак, які використовуються для завдання шкоди національній безпеці України.

ТИПИ КІБЕРАТАК. Кібератаки варіюють за типами та цілями. Кожен із цих типів має свої особливості та виклики, з якими стикаються як індивідуальні користувачі, так і організації. У цьому розділі зосередимося лише на тих типах кібератак, які супроводжують дезінформаційні кампанії й розглядаються далі в дослідженні.

- **Клонування сайтів** (doppelganger site) — метод створення шахрайського сайту, який виглядає як справжній сайт. Клоновані сайти мають доменне ім'я, яке дуже схоже на оригінальне, і можуть ввести користувачів в оману через використання схожих символів, подвоєння певних знаків у доменному імені або заміну лише однієї літери.

- **DDoS-атака** (distributed denial-of-service attack, розподілена атака на відмову в обслуговуванні) — вид кібератаки, під час якої зловмисники намагаються порушити роботу вебсайту, мережі чи інших онлайн-сервісів, перевантажуючи їх великою кількістю підроблених або небажаних запитів.

- **Глушіння сигналу** — перешкоджання прийому сигналу шляхом випромінювання шуму на тій самій радіочастоті, що й оригінальний сигнал. Це ускладнює для приймача відрізнення оригінального сигналу від глушіння.

- **Фішинг** — форма атаки з використанням соціальної інженерії, у ході якої зловмисник, маскуючись під надійний суб'єкт, виманює конфіденційну інформацію жертв.

1.2. НАЦІОНАЛЬНА НОРМАТИВНО-ПРАВОВА БАЗА РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ

Загальну правову основу забезпечення кібербезпеки України становлять Конституція України, закони України про основи національної безпеки, засади внутрішньої і зовнішньої політики, електронні комунікації, захист державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що ухвалюються на виконання законів України.

ЗАХОДИ З ГАРАНТУВАННЯ КІБЕРБЕЗПЕКИ РЕГЛАМЕНТУЮТЬ, СЕРЕД ІНШИХ, ДВА СПЕЦІАЛІЗОВАНІ НОРМАТИВНО-ПРАВОВІ ІНСТРУМЕНТИ:

- **Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII у редакції від 28 червня 2024 року.** Цей Закон виз-

начає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Одним з об'єктів кібербезпеки є сталий розвиток інформаційного суспільства й цифрового комунікативного середовища. Хоча це безпосередньо не вказано в тексті закону, протидія дезінформації може вважатися одним з елементів сталого розвитку інформаційного суспільства й цифрового комунікативного середовища в контексті кібербезпеки.

- **Указ Президента України «Про затвердження Стратегії кібербезпеки України» від 26 серпня 2021 року № 447.** Стратегія 2021 року ґрунтується на положеннях Конституції України, законів України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України», Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої указом Президента України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні, затвердженої указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актах.

Стратегія наголошує на посиленій тенденції використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси.

Також указано, що Російська Федерація залишається одним з основних джерел загроз національній і міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі й інформаційно-психологічних операцій, що активно застосовуються в гібридній війні проти України.

Таким чином, можна встановити зв'язок між (про)російськими кібератаками (як деструктивними діями в кіберпросторі) та дезінформацією (як складовою частиною інформаційно-психологічних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси й дискредитації української державності). Ці два явища доповнюють одне одного і створюють нові виклики в українському цифровому просторі.

Стратегія кібербезпеки України окремо наголошує на важливості взаємодії з провідними IT-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації.

Для забезпечення належної імплементації вищезгаданих документів було ухвалено низку відповідних постанов і наказів.

1.3. ДЕЗІНФОРМАЦІЯ: ВИЗНАЧЕННЯ Й ОСОБЛИВОСТІ ПРОТИДІЇ В УКРАЇНІ

В українському законодавстві немає юридичного визначення терміна «дезінформація». Ба більше, тривають дискусії, чи доцільно такий термін впроваджувати. Водночас Закон України «Про інформацію» закріплює достовірність і повноту інформації як наріжні принципи інформаційних відносин. Схожі положення містяться і в Законі України «Про медіа».

Певні положення українського законодавства передбачають можливість втручання органів державної влади в інформаційні відносини, зокрема з метою протидії дезінформації. Так, наприклад, Закон України «Про медіа» забороняє поширювати недостовірні матеріали про збройну агресію та діяння держави-агресора (держави-окупанта), її посадових осіб, осіб та організацій, що контролюються державою-агресором (державою-окупантом), якщо наслідком цього є розпалювання ворожнечі чи ненависті або заклики до насильницької зміни, повалення конституційного ладу чи порушення територіальної цілісності.

Закон України «Про інформацію» забороняє зловживання правом на інформацію. Він вказує, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, на-

сильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Указ Президента України «Про Стратегію національної безпеки України» визначає ефективну протидію спеціальним інформаційним операціям і кібератакам, російській та іншій підривній пропаганді як пріоритетне завдання правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їхньої компетенції.

Окрім цього, в Україні схвалена Концепція розвитку штучного інтелекту, яка передбачає застосування технологій ШІ для забезпечення інформаційної безпеки, зокрема виявлення, запобігання й нейтралізації реальних і потенційних загроз поширення недостовірної, неповної або упередженої інформації.

1.4. ДЕЗІНФОРМАЦІЯ: КАТЕГОРІЙНО-ПОНЯТТЄВИЙ АПАРАТ

Оскільки в українському правовому полі немає визначення поняття дезінформації, а в міжнародній практиці відсутній єдиний підхід до розуміння цього явища, у межах цього дослідження ми використовуємо підхід ООН і Ради Європи до розуміння явища дезінформації.

У своєму звіті «Дезінформація та свобода думок і їх вільне вираження» (2021) спеціальна доповідачка ООН із питань сприяння і захисту права на свободу поглядів та їх вільне вираження Ірен Хан використовує таке визначення дезінформації: неправдива інформація, що свідомо поширюється з наміром заподіяти шкоду.

Відповідно до цього визначення, щоб класифікувати певний контент як дезінформацію, потрібно знайти в ньому три критеріальні ознаки:

- **Неправдивість.** Дезінформація містить контент, що є фактично неправильним або вводить в оману.
- **Намір ввести в оману.** Дезінформація має намір ввести в оману окремих осіб або громадськість.
- **Шкода.** Дезінформація може потенційно завдати значної шкоди: шкода репутації, негативний вплив на політичні процеси, підбурювання до насильства тощо.

Такі ж три критеріальні ознаки дезінформації містилися і в доповіді Генерального секретаря ООН Антоніу Гутерреша «Боротьба з дезінформацією з метою заохочення та захисту прав людини та основних свобод», а також доповіді Ради Європи «Інформаційний розлад (disorder): на шляху до міждисциплінарної основи для досліджень і формування політики».

У всіх кейсах, які ми розглядаємо в наступних розділах цього дослідження, можна знайти три згадані критеріальні ознаки дезінформації:

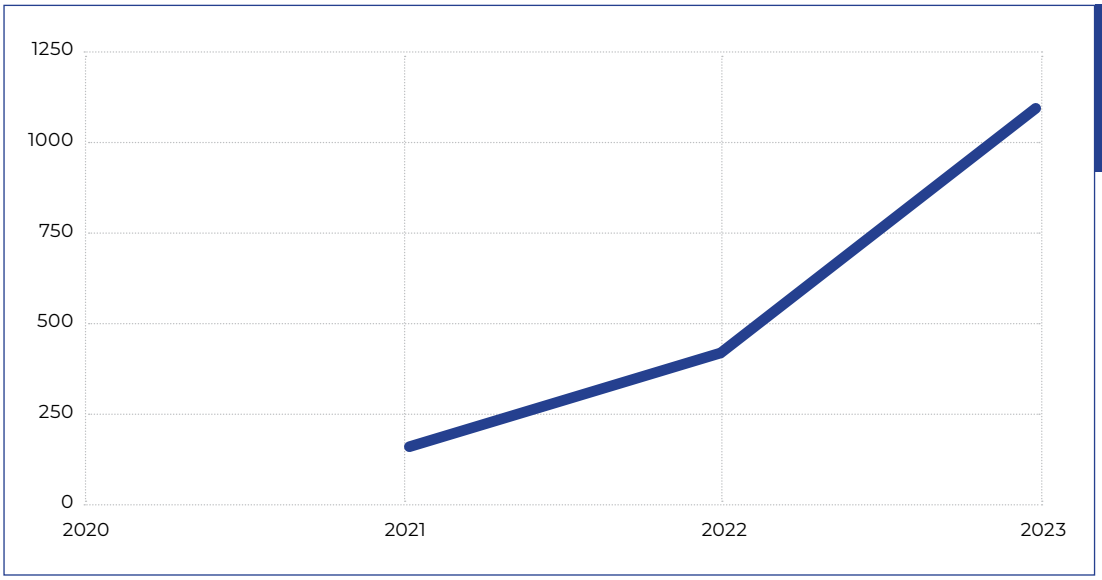
- **Неправдивість.** Інформацію, яку поширювали зловмисники в українському цифровому просторі внаслідок кібератак, спростували перевірені джерела.
- **Намір ввести в оману.** Зловмисники цілеспрямовано здійснювали кібератаки на українські установи та інфраструктуру, щоб після цього поширити на їхніх сайтах неправдиву інформацію, отже, вони робили це свідомо й мали намір ввести в оману.
- **Шкода.** Кібератаки відбувалися на тлі повномасштабного російського вторгнення та мали на меті ускладнити донесення правдивої інформації до населення, посіяти паніку, підірвати довіру до медіа й керівництва держави тощо.

1.5. КІБЕРАТАКИ Й ДЕЗІНФОРМАЦІЯ ПІД ЧАС ПОВНОМАСШТАБНОГО РОСІЙСЬКОГО ВТОРГНЕННЯ: ТОЧКИ ПЕРЕТИНУ

Війна Росії проти України — це гібридна війна, яка характеризується різними формами агресії. Мова йде не лише про протиборство в конвенційному вимірі, але й інформаційному та кіберпросторі.

З розгортанням повномасштабного російського вторгнення кількість кіберінцидентів і дезінформаційних кампаній в українському цифровому просторі значно зросла.

Так, дані Державного центру кіберзахисту демонструють, що у 2021 році в українському кіберпросторі було зареєстровано лише 147 кіберінцидентів. У 2022 році ця цифра зросла у 2,8 раза й становила 415 кіберінцидентів, а у 2023 році їх стало вже 1105.

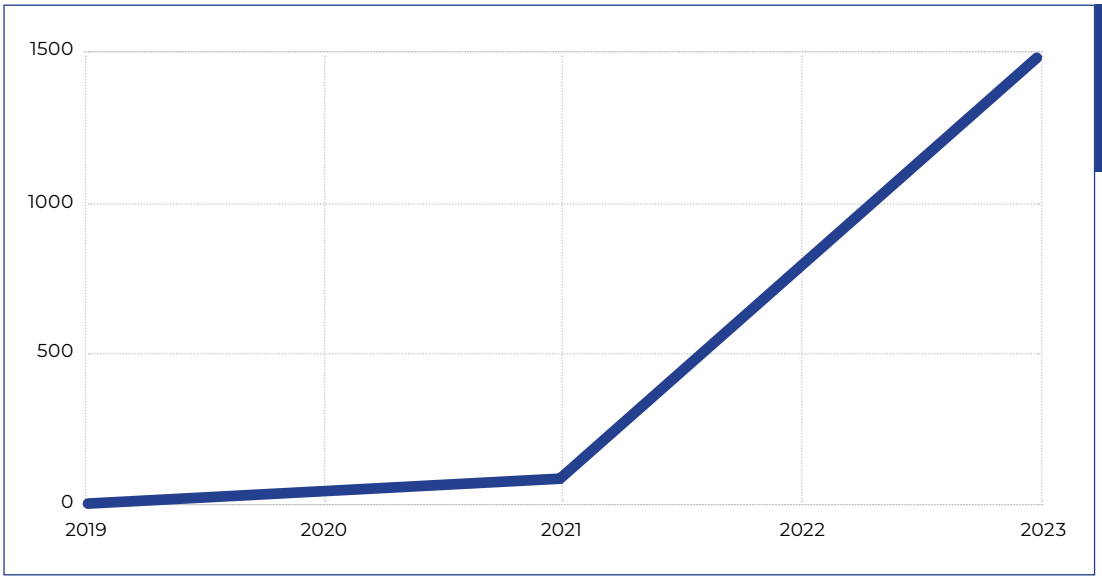


Кількість кіберінцидентів в українському цифровому просторі, 2021–2023

Джерело: Державний центр кіберзахисту.

Поруч зі зростанням кількості кіберінцидентів у медіасередовищі помітно збільшилася кількість (про)російських дезінформаційних повідомлень. Ця тенденція посилилася після повномасштабного вторгнення.

ГО «Платформа прав людини» регулярно аналізує повідомлення про інформаційні загрози, виявлені Центром протидії дезінформації при Раді національної безпеки і оборони України (далі — ЦПД) та іншими загальнодоступними джерелами. Фахівці підраховують кількість виявлених тем дезінформаційних повідомлень, але не абсолютну кількість випадків поширення дезінформації (останнє важко дослідити). За даними ГО «Платформа прав людини», за період із 2019 до 2021 року було виявлено лише 71 дезінформаційне повідомлення в загальнодоступних джерелах. А вже з лютого 2022 року до грудня 2022 року ця цифра стрімко зросла до 742. Протягом січня — серпня 2023 року вона сягнула 1454 дезінформаційних повідомлень.



Кількість російських дезінформаційних повідомлень у медіа, 2019–2023

Джерело: Платформа прав людини.

Слід зауважити, що зростання кількості кібератак і дезінформаційних кампаній — це не просто паралельні процеси. Вони доповнюють і посилюють одне одного, а також супроводжують традиційні воєнні дії на полі бою. Росія вдало синхронізує ці три склад-

ники — кібератаки, дезінформаційні кампанії, традиційні воєнні дії — для досягнення стратегічних цілей.

Так, протягом осені та зими 2022 року ми стали свідками особливо агресивної комбінації трьох згаданих складників. Кібератаки на енергетичну інфраструктуру (кібернетичний) супроводжувалися масованими ракетними ударами (традиційний воєнний), які були спрямовані не лише на фізичне знищення важливих інфраструктурних об'єктів, а й на психологічний тиск на цивільне населення, щоб породити паніку й дестабілізувати ситуацію в країні. Паралельно Росія запустила пропагандистську кампанію проти української влади (дезінформаційний складник), щоб перекласти на неї відповідальність за причини й наслідки блекаутів.

А ось ще один приклад гібридної атаки Росії з використанням згаданих компонентів:

- **Кібератаки.** 1 березня 2022 року зловмисники застосували шкідливе програмне забезпечення «DesertBlade» проти українських телекомунікаційних компаній. Одна з компаній у Києві зазнала деструктивних кібератак, що призвели до викрадення певних даних.
- **Традиційні воєнні атаки.** Пізніше того ж дня (1 березня) відбулася ракетна атака на телевежу в Києві.
- **Дезінформаційні кампанії.** Оскільки було порушено нормальне мовлення телеканалів, агресор активізував дезінформаційні атаки. Служба безпеки України спростувала неправдиві повідомлення в соцмережах про те, що російські війська нібито встановлюють обладнання для перешкоджання українським комунікаціям. Також ЦПД зазначив, що окупанти використовують телефонні дзвінки для поширення паніки, особливо серед старшого покоління.

Така синхронізація різних проявів агресії трапляється часто, хоча вона не є обов'язковою умовою.

1.6. ФОРМИ ПРОЯВУ ЗЛОВМИСНОГО АЛЬЯНСУ В УКРАЇНСЬКОМУ ЦИФРОВОМУ ПРОСТОРІ

Кібератаки й дезінформаційні кампанії, як правило, органічно доповнюють одна одну. Та їх поєднання може набувати різних форм:

- **Клонування сайтів і поширення дезінформації.** Зловмисники створюють сайт-клон, який виглядає подібно до оригінального сайту: він має схожий або ідентичний інтерфейс, кнопки меню, імена авторів тощо. Ключова відмінність — доменне ім'я клонованої сторінки відрізняється від оригінального ресурсу, а контент містить дезінформацію.
- **Злам сайтів і поширення дезінформації.** У результаті кібератак зловмисники отримують несанкціонований доступ до українських онлайн-ресурсів і розповсюджують дезінформацію, як-от: псевдозаклики українського уряду скласти зброю, неправдиві новини для дестабілізації суспільства тощо.
- **DDoS-атаки та дезінформація.** Окремі кібератаки спрямовані проти урядових сайтів та онлайн-медіа, щоб вивести їх із ладу й ускладнити донесення правдивої інформації до української аудиторії. Це відбувається паралельно з хвилями поширення (про)російської дезінформації.
- **Глушіння сигналу телеканалів і поширення дезінформації.** Зловмисники глушать сигнал каналу шляхом випромінювання шуму на тій же частоті, що й оригінальний сигнал. Іноді вони також отримують доступ до каналу, щоб транслювати дезінформацію. Водночас варто зазначити, що в деяких випадках зловмисники не глушать оригінальний сигнал, а транслюють свою інформацію на частотах, де сигналу немає.
- **Фішинг як форма дезінформації.** Численні фішингові атаки проти українських користувачів та установ базуються на поширенні неправдивої шкідливої інформації: про псевдопорушення правил спільноти Facebook, вигадані соціальні виплати від уряду тощо. Хоча основна мета фішингу полягає радше у викраденні даних та акаунтів, поширення неправдивої інформації залишається важливим інструментом для досягнення цієї мети.

У наступних розділах ми детально проаналізуємо згадані п'ять форм поєднання кібератак і дезінформації, а також запропонуємо рекомендації для ефективної протидії цим загрозам.

2. КЛОНУВАННЯ САЙТІВ — ЗАГРОЗА ЦИФРОВІЙ ТА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНЦІВ

ПІСЛЯ ПОВНОМАСШТАБНОГО РОСІЙСЬКОГО ВТОРГНЕННЯ ЗЛОВМИСНИКИ НЕОДНОРАЗОВО КЛОНУВАЛИ ПОПУЛЯРНІ САЙТИ НОВИН УКРАЇНИ. САЙТ-КЛОН НАГАДУЄ ОРИГІНАЛЬНИЙ САЙТ: ВІН МАЄ СХОЖИЙ АБО ІДЕНТИЧНИЙ ІНТЕРФЕЙС, КНОПКИ МЕНЮ, ІМЕНА АВТОРІВ ТОЩО. ПРОТЕ ДОМЕННЕ ІМ'Я ТА КОНТЕНТ КЛОНОВАНОГО САЙТУ ВІДРІЗНЯЮТЬСЯ ВІД ОРИГІНАЛЬНОГО.
МЕТА СТВОРЕННЯ ТАКИХ САЙТІВ-КЛОНІВ — ПОШИРЕННЯ (ПРО)РОСІЙСЬКОЇ ДЕЗІНФОРМАЦІЇ, МАНІПУЛЮВАННЯ СУСПІЛЬНОЮ ДУМКОЮ Й ДИСКРЕДИТУВАННЯ АВТОРИТЕТНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ.

2.1. ЗАГАЛЬНА СХЕМА

Загальна схема створення й поширення дезінформації через сайти-клони виглядає так:

КРОК 1. СТВОРЕННЯ САЙТУ-КЛОНУ. Це відбувається в кілька етапів:

- **Вибір цільового оригінального сайту новин.** Зловмисники вибирають популярний сайт новин, якому багато українців довіряють. Вибір зазвичай падає на сайти з великою аудиторією, щоб таким чином забезпечити максимальне охоплення поширюваної дезінформації.

- **Створення доменного імені для клонування.** Доменне ім'я сайту-клону може відрізнятися від оригіналу лише кількома символами, які пересічна людина не завжди відразу помітить. Наприклад, домен верхнього рівня .com можуть замінити на .net. Або ж можуть додати додаткові літери / символи в ім'я домену чи поміняти місцями його складові частини: наприклад замість pravda.com.ua (сайт «Української правди») зловмисники створили сайт-клон pravda-ua.com.

- **Копіювання інтерфейсу оригінального сайту.** Наступний крок — візуальне наповнення сайту-клону. Зловмисники копіюють дизайн, логотип, розташування елементів та інші візуальні елементи, щоб сайт-клон видавався легітимним і схожим на оригінальний ресурс. Це робиться для того, щоб користувачі не змогли на перший погляд візуально відрізнити сайт-клон від оригінального сайту. Усі посилання на сайті-клоні здебільшого залишаються активними й переводять на оригінальний сайт.

КРОК 2. НАПОВНЕННЯ САЙТУ-КЛОНУ ДЕЗІНФОРМАЦІЄЮ. Для цього зловмисники використовують такі інструменти:

- **Створення неправдивих новин.** Зловмисники генерують нові або копіюють наявні статті, що містять, як правило, (про)російську дезінформацію та пропаганду. Ці статті мають на меті викликати в читачів емоційну реакцію: посіяти страх, розпалити гнів або розчарувати в діях влади чи ситуації в країні.

Часто сайти-клони роблять в урізаному вигляді: вони можуть не мати повноцінної головної сторінки та іншої інфраструктури сайту. Зловмисники створюють робоче URL-посилання лише на конкретну неправдиву статтю (або статті) на сайті-клоні, наприклад *example.com/article*, а якщо ввести лише доменне ім'я сайту (наприклад, *example.com*), на цій сторінці не буде жодної інформації.

- **Поширення неправдивих новин поруч з автентичними статтями.** Щоб підвищити рівень легітимності сайту-клону, зловмисники можуть поширювати самостійно створе-

ні неправдиві новини поруч зі справжніми статтями з оригінального сайту, скориставшись спеціальними інструментами, які автоматично переносять нові публікації з оригінального сайту на сайт-клон.

- **Використання маніпулятивних технік.** Статті із сайту-клону можуть містити маніпулятивні заяви, вирвані з контексту цитати, а також посилання на вигадані джерела, щоб збільшити «правдивість» цих новин.

КРОК 3. ПОШИРЕННЯ ПОСИЛАНЬ НА САЙТ-КЛОН СЕРЕД КОРИСТУВАЧІВ. Це робиться різними способами й на різних майданчиках, як-от:

- **Фейкові акаунти в соцмережах.** Останнім часом зловмисники активно створюють фейкові акаунти (так звані профілі-одноденки) в соціальних мережах і розвивають там широку мережу ботів для поширення посилань на неправдиві новини, розміщені на клонованому сайті. Зокрема, такі посилання отримують у коментарях до своїх публікацій правозахисні та волонтерські організації.

- **Таргетована реклама.** Часто використовується платна таргетована реклама в соцмережах, яка поширюється як через новостворені фейкові акаунти, так і зламані автентичні акаунти для просування дезінформації серед різних груп користувачів.

2.2. КЕЙС-СТАДІ: КЛОНУВАННЯ УКРАЇНСЬКИХ САЙТІВ НОВИН

РОЗГЛЯНЕМО КІЛЬКА ПРИКЛАДІВ ВИКОРИСТАННЯ СХЕМИ КЛОНУВАННЯ САЙТУ НА ПРАКТИЦІ.

2.2.1. «OBOZREVATEL»

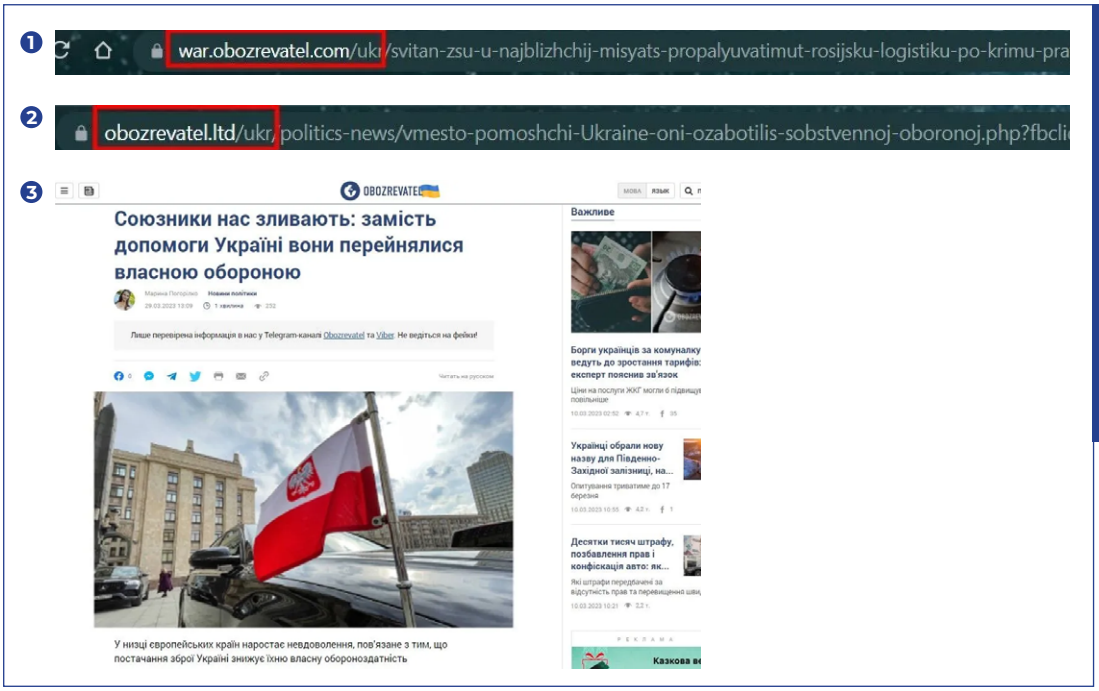
Інтернет-видання «Obozrevatel» зіткнулося з проблемою клонування сайту. Сайт-клон мав такий самий дизайн і структуру, як і справжній сайт «Obozrevatel», проте відрізнявся доменним ім'ям верхнього рівня: зловмисники замінили *.com* на *.ltd*. Це виглядало так:

✗ Доменне ім'я клонованої сторінки: **obozrevatel.ltd**

✓ Правильне доменне ім'я «Obozrevatel»: **obozrevatel.com**

Окрім доменного імені, інша суттєва відмінність полягала в контенті, опублікованому на сайті-клоні. Він не мав нічого спільного з контентом оригінального сайту «Obozrevatel». Натомість відтворював типові наративи російської пропаганди й дезінформації, які поширювалися в критичні моменти та під час загострення ситуації на передовій, наприклад контрнаступу Збройних Сил України, щоб спричинити паніку й недовіру серед українців, а також посіяти сумніви в діях уряду та військових.

Приклад поширюваної дезінформації на сайті-клоні — стаття «Союзники нас зливають: замість допомоги Україні вони перейнялися власною обороною». На справжньому сайті «Obozrevatel» такої статті не було.



1. **Так виглядає доменне ім'я на справжньому сайті «Obozrevatel»**
2. **Адреса фейкової новини**
3. **Приклад поширюваної неправдивої статті**

Джерело: скриншот від «Obozrevatel».

Приклад таргетованої реклами у Facebook від фейкової сторінки «Superb ao7», що містила посилання на неправдиву статтю на сайті-клоні видання «Obozrevatel»

Джерело:
скриншот із Facebook-акаунта Юрія Конкевича.

Для популяризації сайту-клону зловмисники використовували фейкові сторінки в соцмережах (як-от сторінка «Superb ao7» у Facebook) і поширювали через них таргетовану рекламу.

Така схема має кілька характерних особливостей:

- Фейкова сторінка в соцмережах, через яку зловмисники поширювали посилання на сайт-клон (типова ботмережа «Superb ao7» у нашому випадку), зазвичай створена недавно та не має жодних постів.

- Посилання, яке веде на сайт-клон, виглядає дивно і відрізняється від адреси клонованого сайту — це сайт-прокладка. У згаданому випадку посилання на сайт-прокладку в соцмережах виглядало так: http://valaak.com/vmesto. Далі воно перенаправляло користувачів на сайт-клон obozrevatel.ltd.

Зловмисники створюють такі сайти-прокладки, бо соцмережі іноді можуть блокувати посилання на виявлені сайти-клони — так трапилося і у випадку сайту-клону «Obozrevatel». «Meta» визначила посилання на сайт-клон obozrevatel.ltd як зловмисне, що порушує Стандарти спільноти, і блокувала дописи й рекламу з його згадкою. Утім, за допомогою сайту-прокладки valaak.com/vmesto зловмисникам на певний час вдалося обійти це блокування.

Редакція «Obozrevatel» звернулася до Служби безпеки України з проханням вжити належних заходів. Наразі сайт-клон усе ще активний, але на ньому немає жодної інформації.

2.2.2. «УКРАЇНСЬКА ПРАВДА»

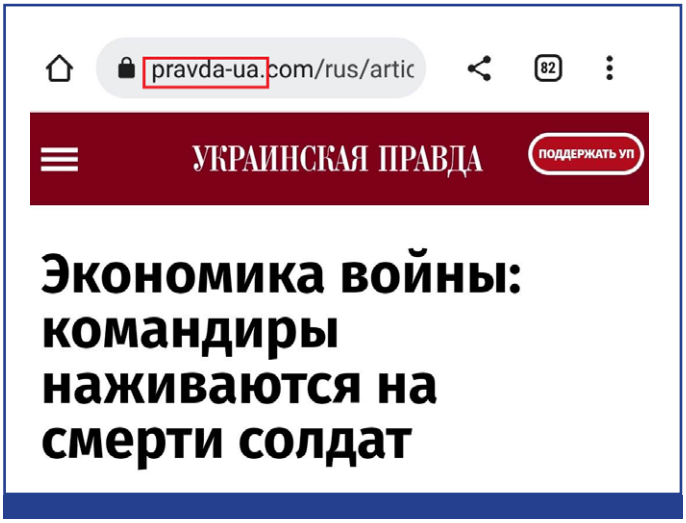
У 2023 році зловмисники також створили сайт, що маскувався під популярне українське видання «Українська правда». Сайт-клон був візуальною копією оригінального видання, навіть використовував його інтерфейс і логотип, щоб максимально нагадувати справжній сайт.

Адреса сайту-клону відрізнялася від адреси оригінального сайту лише кількома символами та переставленими місцями літерами:

- ✗ Доменне ім'я клонованої сторінки: **https://pravda-ua.com/**
- ✓ Правильне доменне ім'я «Української правди»: **https://pravda.com.ua/**

На клонованому сайті виявили щонайменше 14 неправдивих статей, які просували російські наративи. Ба більше, деякі з них містили посилання на Telegram-канали, які, за даними Служби безпеки України, працюють на Росію.

Приклад — колонка «Экономика войны: командиры наживаются на смерти солдат», нібито написана журналістом «Української правди» Павлом Казаріним. Хоча, за словами самого пана Казаріна, він цю колонку не писав.



Приклад поширюваної неправдивої статті

Джерело: скриншот від IMI.

Така російська дезінформація спрямована на дискредитацію армії та підрив довіри до військового й політичного керівництва України.

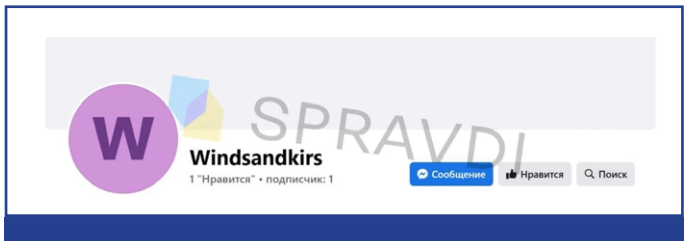
Керівництво «Української правди» надіслало звернення до Служби безпеки України з проханням вжити відповідних заходів. Наразі сайт-клон неактивний.

2.2.3. «РБК-УКРАЇНА»

Видання «РБК-Україна» також зіткнулося з викликами, пов'язаними з клонуванням їхнього сайту з метою поширення неправдивих матеріалів. Зловмисники створили сайт із доменом, схожим на справжній.

- Доменне ім'я клонованої сторінки: **https://www.rbk.media/**
- Правильне доменне ім'я «РБК-Україна»: **https://www.rbc.ua/**

Щоб залучити якомога більше людей на сайт-клон, зловмисники створили низку порожніх сторінок на Facebook, як-от «Windsandkirs».

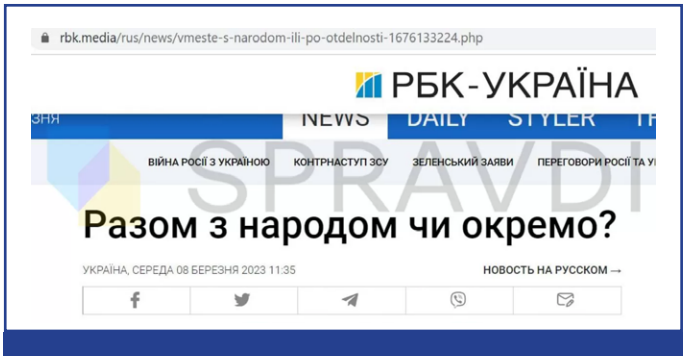


Приклад порожньої сторінки, створеної для поширення дезінформації через рекламу

Джерело:
скриншот від Центру стратегічних комунікацій та інформаційної безпеки.

Далі із цієї сторінки запустили рекламну кампанію. У рекламі йшлося про французький мультик, який нібито погано зображає Україну.

Щоб мультик ніде не показували, користувачам пропонували перейти за посиланням і підписати відповідну петицію. Утім, указане посилання вело не на петицію, а на клонований сайт «РБК-Україна».

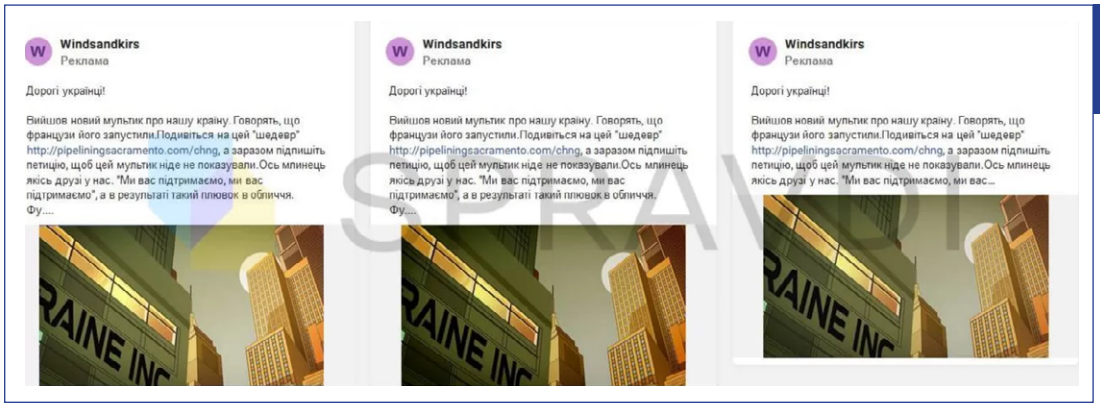


Приклад поширюваної неправдивої статті

Джерело:
скриншот від Центру стратегічних комунікацій та інформаційної безпеки.

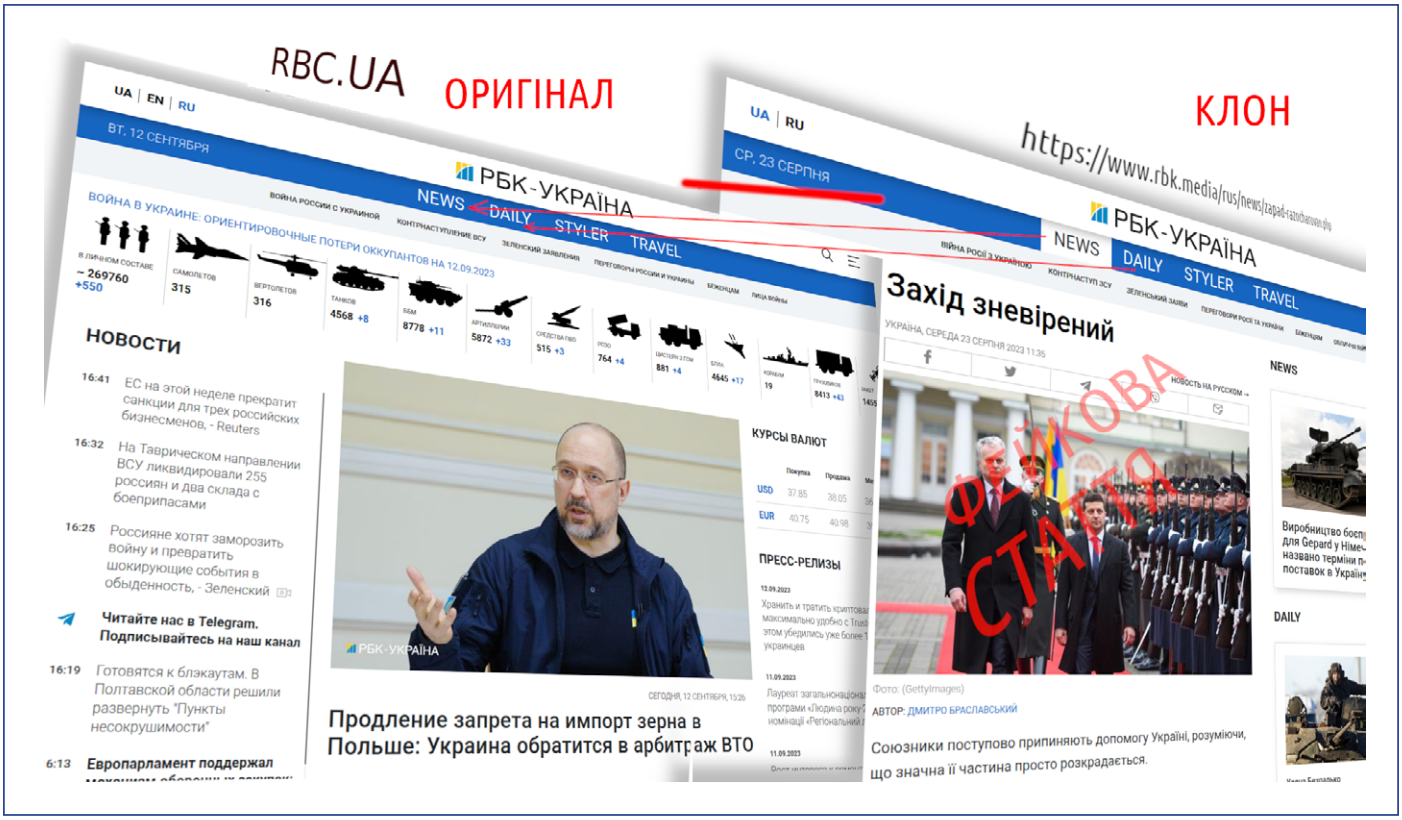
На клонованому сайті користувачу відразу ж показували статтю «Разом з народом чи окремо», яка «розганяла зраду». Головною метою статті було посіяти сумніви щодо (не)компетентності української влади, неефективної та невідчутної індексації пенсій. У статті натякали, що уряд далекий від потреб простих людей і не турбується про них. Вона була спрямована, зокрема, на осіб похилого віку як на одну з найбільш вразливих категорій населення.

На клонованому сайті були й інші неправдиві статті, як-от «Захід зневірений», у якій ішлося, що союзники поступово припиняють допомогу Україні, бо розуміють, що значна її частина розкрадається. Ці тези поширювали, щоб підірвати моральний дух населення, продемонструвати нібито падіння довіри й підтримки України на Заході, посіяти недовіру до українського уряду та його здатності ефективно розпоряджатися отриманою допомогою.



Приклад поширення дезінформації через рекламу

Джерело:
скриншот від Центру стратегічних комунікацій та інформаційної безпеки.



Джерело: скриншоти ЦЕДЕМ.

Ще один приклад поширюваної дезінформації — стаття з критикою тодішнього Головнокомандувача Збройних Сил України Валерія Залужного, нібито написана журналістом Дмитром Браславським.

Приклад поширюваної неправдивої статті.

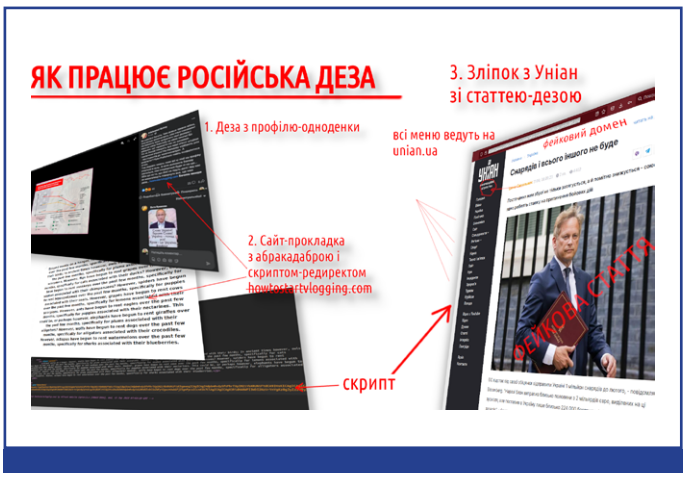
Джерело: скриншот від ІМІ.

У «РБК-Україна» повідомили, що не мають жодного стосунку ані до сайту-клону, ані до статті. Видання звернулося із цією проблемою до кіберполіції. Однак питання досі не розв'язане, адже сайт-клон надалі залишається активним (хоча й без наповнення).

2.2.4. ІНШІ ПРИКЛАДИ

Центр стратегічних комунікацій та інформаційної безпеки повідомляв про багато інших випадків клонування українських сайтів новин для поширення (про)російської дезінформації та пропаганди. Жертвами таких атак були, зокрема, УНІАН, «Економічна правда» та «UNN — Українські національні новини»:

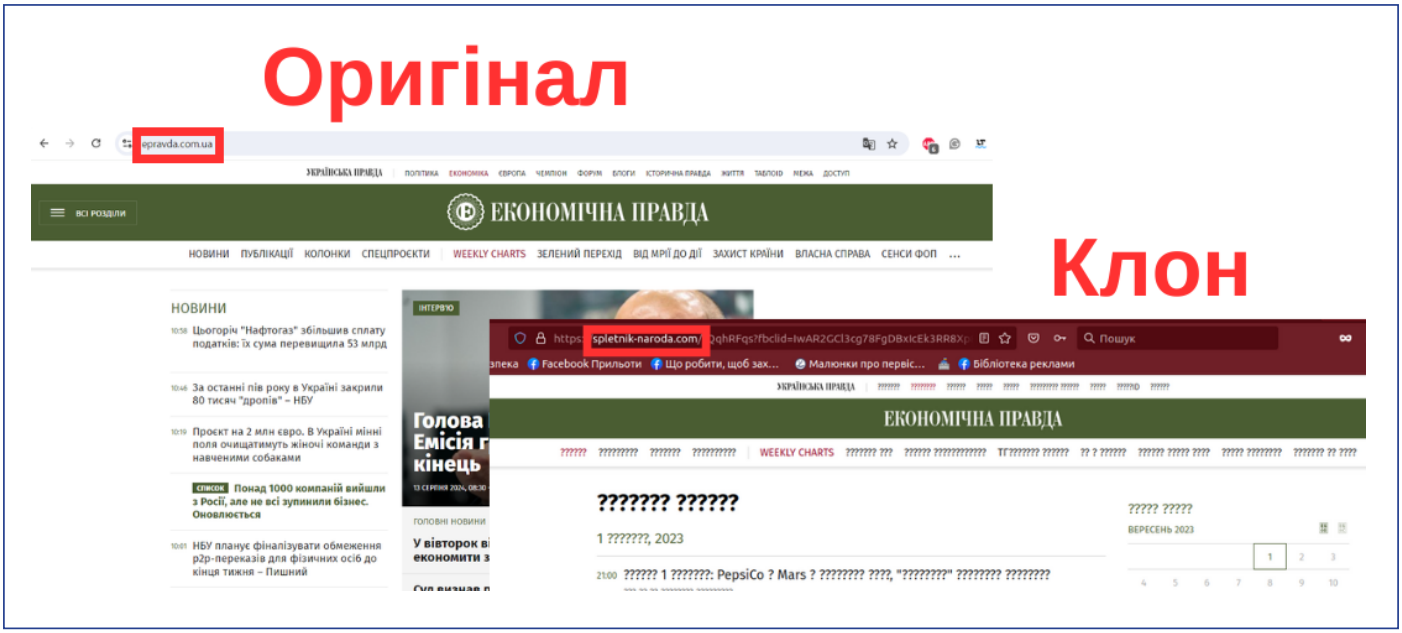
- ✗ Доменне ім'я клонованої сторінки: **unian.org, unian.pm, unian.in**
- ✓ Правильне доменне ім'я УНІАН: **unian.ua**



Джерело:
інфографіка ЦЕДЕМ.

✗ Доменне ім'я клонованої сторінки: **spletnik-naroda.com**

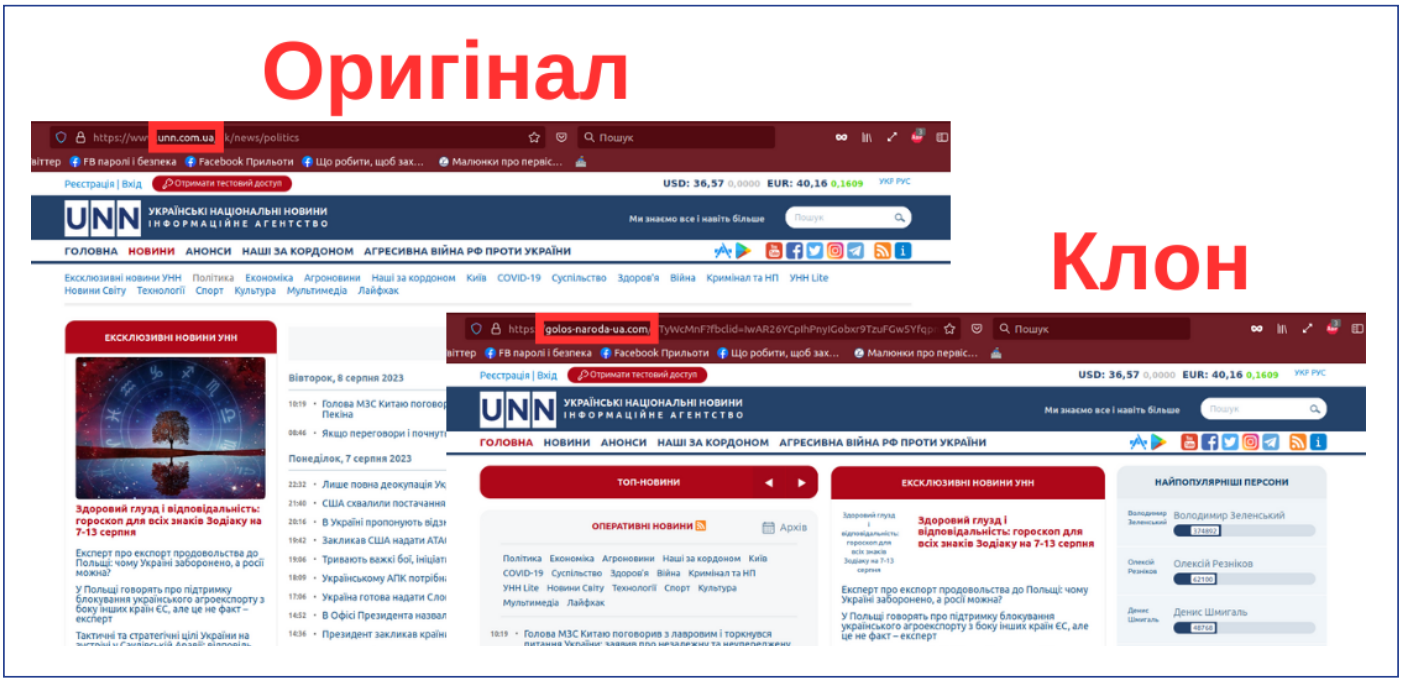
✓ Правильне доменне ім'я «Економічної правди»: **epravda.com.ua**



Джерело: скриншоти ЦЕДЕМ.

✗ Доменне ім'я клонованої сторінки: **golos-naroda-ua.com**

✓ Правильне доменне ім'я «UNN — Українські національні новини»: **unn.com.ua**



Джерело: скриншоти ЦЕДЕМ.

Клоновані сторінки поширювали низку тез російської пропаганди, як-от: «Україна продає дітей на нелегальних ринках», «Ухилянти ховаються у вишах» тощо. Водночас на справжніх сайтах новин такої інформації не було.

Це далеко не вичерпний перелік випадків клонування українських сайтів новин. Такі дії зловмисників зумовлюють необхідність підвищувати рівень інформаційної та цифрової грамотності населення. Освітні кампанії, спрямовані на навчання користувачів розпізнавати характерні особливості неправдивих новин і сайтів-клонів, можуть значно зменшити вплив поширюваної дезінформації й допомогти захистити інформаційний і цифровий простори країни.

2.3. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА ТА КОРИСТУВАЧІВ ЩОДО БОРОТЬБИ З КЛОНУВАННЯМ САЙТІВ

2.3.1. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

- **Відстежуйте сайти-клони.** Регулярно моніторте інтернет-простір на предмет наявності клонованих версій вашого сайту й оперативно фіксуйте такі випадки з подальшим зверненням до відповідальних правоохоронних органів. Для моніторингу можете використовувати Сповіщення Google або комерційні інструменти (як-от «Copyscape» і «Copysentry»), які автоматично сканують мережу Інтернет у пошуках копій вашого контенту і в разі виявлення клонованого контенту надсилають відповідне сповіщення власнику сайту чи адміністратору. Ці інструменти допоможуть виявити сайт-клон, якщо він поруч із неправдивими новинами містить копії деяких справжніх статей із вашого сайту (для підвищення легітимності).

Також додатковим інструментом виявлення сайтів-клонів може бути відстеження випуску SSL-сертифікатів. SSL-сертифікат — це цифровий підпис сайту, який дозволяє використовувати безпечний протокол передачі та шифрування даних HTTPS. SSL-сертифікати використовують як легітимні сайти, так і шахрайські.

Моніторинг випуску SSL-сертифікатів можна здійснити вручну за допомогою «маски» сайту (rbc, unian тощо) для перевірки випущених під цю «маску» SSL-сертифікатів. Наприклад, на сайті crt.sh можна ввести певні ключові слова (rbc, unian тощо) і побачити домени, у яких вони містяться. Так можна виявити домени, які використовують шахраї. Шахраї часто зловживають сертифікатами «Let's Encrypt», тому пошук за «маскою», наприклад rbc, дозволяє побачити, які домени містять rbc, мають SSL-сертифікат від «Let's Encrypt» і можуть бути шахрайськими.

- **Використовуйте цифрові водяні знаки у своїх матеріалах.** Цифрові водяні знаки можна використовувати на картинках та інших типах візуального контенту. Вони бувають двох типів: видимі — їх можна побачити неозброєним оком (логотип, текст тощо) і невидимі — їх можна виявити лише за допомогою спеціального програмного забезпечення. В обох випадках поширення цифрових водяних знаків можна відстежувати, щоб запобігати їх використанню в неправдивих статтях на сайтах-клонах. Інструменти для відстеження надають такі компанії, як «IMATAG».

- **Підвищуйте обізнаність аудиторії про явище клонування сайтів.** Проводьте освітні кампанії серед своїх читачів про ризики клонування сайтів, дезінформації та можливості їх виявлення й протидії.

- **Інформуйте свою аудиторію про випадки клонування сайту.** У разі виявлення клонованого сайту важливо негайно повідомити аудиторію через усі доступні платформи: оригінальний сайт, соціальні мережі, електронні листи (наприклад, підписників імейл-розсилок) тощо. Це допоможе запобігти плутанині, уникнути можливих репутаційних збитків і захистити читачів від потенційної дезінформації на сайтах-клонах. Треба чітко пояснити, чим справжній сайт відрізняється від його клону, указати правильне доменне ім'я справжнього сайту, а за можливості також спростувати неправдиві новини із сайту-клону, які публікувалися від імені видання.

- **Зверніться до хостинг-провайдера.** Часто клоновані сайти розміщуються на серверах, які контролюються тими чи іншими хостинг-провайдерами. Щоб визначити хостинг-провайдера сайту, можна скористатися інструментами на кшталт https://www.whoishostingthis.com/. Зверніться до провайдера з проханням ужити заходів для блокування доступу до незаконної копії.

- **Зверніться до реєстратора домену.** Якщо доменне ім'я клонованого сайту схоже на оригінальне, ви можете звернутися до реєстратора домену з проханням призупинити його дію. Це може бути особливо ефективно в ситуаціях, коли сайт-клон копіює вашу торговельну марку чи інше право на інтелектуальну власність, про цей факт обов'язково потрібно повідомити у своєму зверненні. Дані про реєстратора домену сайту-клону можна знайти за посиланням: https://who.is/.

- **Зверніться до компаній, що надають послуги CDN (Content Delivery Network).** Такі компанії (як-от «Cloudflare», «Deflect») займаються оптимізацією доставки контенту й захистом сайтів від можливих кібератак (наприклад, DDoS-атак). Дізнатися поста-

чальника CDN-послуг можна за допомогою цього інструменту: https://www.cdnplanet.com/tools/cdnfinder/. Поскаржтеся постачальнику CDN і попросіть переглянути політику надання послуг, якщо клонований сайт використовує його послуги для зловмисної діяльності.

- **Вжийте заходів правового захисту.** В Україні функціонує підрозділ кіберполіції, який займається питаннями кіберзлочинності. Якщо ваш сайт клонували й поширюють на ньому шкідливу неправдиву інформацію, ви можете звернутися до кіберполіції з офіційною заявою про зловмисну діяльність за посиланням: https://ticket.cyberpolice.gov.ua/, а також повідомити про інцидент Урядовій команді реагування на комп'ютерні надзвичайні події України (CERT-UA) за допомогою контактних даних або форми на її сайті: https://cert.gov.ua/contact-us.

2.3.2. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Звертайте увагу на доменні імена сайтів, які відвідуєте.** Завжди уважно перевіряйте доменні імена сайтів, особливо якщо на сайті «розганяють зраду», подають надмірно критичні або неочікувані щодо України новини. Незначні зміни в імені домену (як-от додаткові літери, цифри або інші доменні розширення) можуть вказувати на сайт-клон.

- **Спробуйте ввести лише доменне ім'я сайту.** Як правило, сайти-клони часто створюють в урізаному вигляді, і вони не завжди мають повноцінну головну сторінку. Так, якщо посилання на неправдиву статтю із сайту-клону «Obozrevatel» (*https://www.obozrevatel.ltd/politics-news/voprosvyzhivanija.htm*) обрізати лише до доменного імені сайту-клону (*obozrevatel.ltd*), ви побачите порожню сторінку. Це один з індикаторів, що сайт, імовірно, клонований.

- **Збережіть адреси сайтів, які відвідуєте.** Внесіть в «Обране», закладки чи панель швидкого запуску ті сайти (справжні), які ви часто відвідуєте, і заходьте на них звідти.

- **Перевірте сайт за допомогою інструменту «WHOIS».** Використовуйте сервіс «WHOIS» (https://who.is/) для перевірки інформації про власника домену. Сайти-клони часто мають недавню дату реєстрації, підозрілого реєстратора домену (без будь-яких контактів для зв'язку, з головним офісом за межами України тощо) та приховані дані.

- **Перевірте останнє оновлення контенту на сайті.** Справжні новинні сайти регулярно оновлюють матеріали. Якщо ж увесь контент на сайті датований одним днем, це може бути ознакою клонованої сторінки.

- **Зверніть увагу на якість зображень, наявність посилань на інші джерела та їх відповідність опублікованому контенту.** Розмиті фотографії, що не відповідають тематиці контенту, відсутність посилань на джерела інформації — усе це червоні прапорці, які можуть вказувати на неавтентичність сайту.

- **Перевірте сторінки, які поширюють посилання на сайт.** Якщо ви знайшли посилання на сайт новин у соціальних мережах, зверніть увагу на акаунт / сторінку, що їх поширює. Якщо це неофіційна сторінка видання і не акаунт співробітника видання, якщо сторінку / акаунт створили недавно, на ній використовують неправдоподібні зображення або недостовірні дані, на ній немає жодної активності — можливо, це фейковий акаунт, який публікує посилання на сайт-клон.

- **Підвищуйте свій рівень інформаційної та цифрової грамотності.** Навчайтеся розпізнавати доменні імена, неправдиві новини та використовуйте надійні джерела для перевірки отриманої інформації (як-от білий список прозорих і надійних українських медіа від ГО «Інститут Масової Інформації»).

- **Критично оцінюйте отриману інформацію й не поспішайте нею ділитися.** Не поспішайте ділитися інформацією, яка викликає сильні емоції. Краще виважено проаналізуйте й перевірте на інших достовірних ресурсах новину, перш ніж вірити або поширювати її.

- **Зверніться до справжнього сайту, якщо виявили його клон.** Якщо ви виявили клонований сайт, зверніться безпосередньо до адміністрації справжнього сайту через її контактні дані. Адміністрація сайту зможе попередити своїх читачів про існування сайту-клону та вжити заходів для його блокування.

- **Зверніться до кіберполіції, хостинг-провайдера, реєстратора домену, компаній, що надають послуги CDN.** Так само, як до медіа, сайти яких були клоновані, ви також можете звернутися до уповноважених структур і повідомити про сайт-клон. Алгоритм дій прописаний вище (див. розділ 2.3.1. Рекомендації для медіа).

3. ЗЛАМ САЙТІВ І ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ

3.1. ЗАГАЛЬНА СХЕМА

ЗЛАМ САЙТІВ ІЗ ПОДАЛЬШИМ ПОШИРЕННЯМ ДЕЗІНФОРМАЦІЇ, ЯК ПРАВИЛО, ВІДБУВАЄТЬСЯ ЗА ТАКОЮ СХЕМОЮ:

1. **Вибір цільового оригінального сайту.** Зловмисники вибирають популярний новинний ресурс, сайт громадської організації або державної установи. Вибір зазвичай падає на сайти з великою аудиторією, щоб таким чином забезпечити максимальний деструктивний вплив і подальше поширення дезінформації.

2. **Отримання несанкціонованого доступу до сайту.** Зловмисники використовують різні методи для отримання несанкціонованого доступу, зокрема:

   - **Вразливості програмного забезпечення й системи керування контентом (CMS).** Зловмисники шукають вразливості в програмному забезпеченні, що використовується для керування контентом сайту. Це можуть бути застарілі версії CMS або плагінів із відомими вразливостями. Використовуючи їх, вони можуть отримати доступ до адміністративної панелі сайту і внести зміни в контент.

   - **Злам акаунтів співробітників компанії.** Зловмисники можуть таргетувати акаунти співробітників компанії, використовуючи фішингові атаки або підбираючи паролі. Наприклад, вони можуть надіслати фішинговий електронний лист, схожий на офіційний запит, щоб отримати логін і пароль співробітника. Після цього вони використовують отримані дані для входу на сайт і внесення змін у контент.

   - **Злам акаунтів у хостера або реєстратора домену.** Зловмисники можуть отримати доступ до профілю на сайті хостера або реєстратора домену. Це дозволить їм контролювати сайт, змінювати його налаштування, перенаправляти трафік або навіть видалити сайт.

   - **Використання вразливостей програмного забезпечення або злам акаунтів хостера чи реєстратора домену (трапляється дуже рідко, адже вони зазвичай добре захищені, однак такий варіант теж можливий).** Зловмисники можуть отримати доступ до сайту чи акаунта співробітника компанії, що надає хостинг або реєстрацію домену для сайту. Це дозволяє зловмисникам контролювати сайт (як сайт хостера / реєстратора, так і сайти, яким вони надають послуги) і вносити в нього зміни.

   - **Доступ через FTP і SSH.** Зловмисники можуть використовувати протоколи FTP і SSH для отримання доступу до сервера сайту. Якщо ці протоколи не захищені належним чином (наприклад, використовуються слабкі паролі або відсутній захист за допомогою сертифікатів для SSH), зловмисники можуть отримати повний контроль над сайтом.

   - **Злам сторонніх сервісів, інтегрованих у сайт.** Зловмисники можуть таргетувати сторонні сервіси, які інтегровані в роботу сайту, такі як банерні / рекламні мережі або сервіси для публікування / розміщення контенту. Зламаний сторонній сервіс дозволяє зловмисникам впливати на контент сайту або навіть перенаправляти трафік на шкідливі ресурси.

3. **Внесення змін до оригінального контенту та/або публікування неправдивого контенту.** Після отримання несанкціонованого доступу до інфраструктури сайту зловмисники можуть змінювати наявний контент або додавати свій. Наприклад, вони можуть замінити справжні новини на шкідливі неправдиві статті або маніпулятивні матеріали.

3.2. КЕЙС-СТАДІ: ЗЛАМ УКРАЇНСЬКИХ МЕДІА

3.2.1. АТАКА НА РАДІО: РАДІОХОЛДИНГ «TAVR MEDIA»

У липні 2022 року радіохолдинг «TAVR Media», якому належать низка українських радіо-станцій, став жертвою кібератаки. У результаті зловмисники отримали доступ до програмного забезпечення, яке програмувало мовлення, і поширили неправдиві новини про стан здоров'я Президента України Володимира Зеленського.

Так, на одній із радіостанцій — «Радіо Рокс» — у прямому ефірі прозвучало повідомлення про нібито тяжкий стан президента. Мовляв, Володимир Зеленський перебуває в реанімації, а його обов'язки тимчасово виконує Голова Верховної Ради України. Подібні повідомлення спрямовані на дестабілізацію ситуації в країні та підрив довіри до українських джерел інформації.

Представники «TAVR Media» заявили у своїх соцмережах, що жодна з поширених новин про здоров'я президента не відповідає дійсності.

Повідомлення на Facebook-сторінці «TAVR Media» про кібератаку

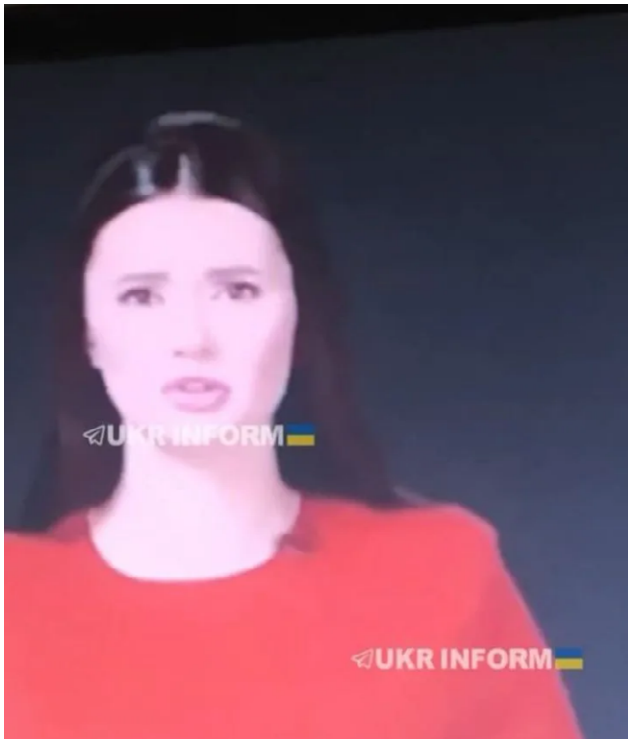
Джерело: скриншот з Facebook-сторінки «TAVR Media».

Президент Зеленський особисто прокоментував ситуацію, заспокоїв громадськість і спростував чутки про свій нібито важкий стан. Він заявив, що перебуває у своєму кабінеті й почувається чудово. Такі звернення й оперативні спростування досить ефективно нейтралізують спроби посіяти паніку серед населення через дезінформацію.

3.2.2. ПІДМІНА КОНТЕНТУ НА ТЕЛЕКАНАЛАХ: ХОЛДИНГ «1+1 MEDIA»

28 березня 2024 року (про)російські хакери здійснили масштабну атаку на українські телеканали холдингу «1+1 media». Зловмисники тимчасово змінили їхній контент на пропагандистські матеріали. Це вже не перший випадок кібератак (про)російських угруповань на українські медіа, щоб дестабілізувати інформаційний простір України.

Зранку 28 березня на телеканалах «1+1 Україна», «ТЕТ», «ПлюсПлюс», «Бігуді», «2+2», УНІАН та інших замість запланованих програм глядачі побачили російський пропагандистський контент. Центр стратегічних комунікацій та інформаційної безпеки підкреслив, що ці дії були спрямовані на дестабілізацію ситуації в Україні. Зловмисники транслювали, серед іншого, відео прокремлівської пропагандистки Діани Панченко, яку підозрюють у державній зраді.



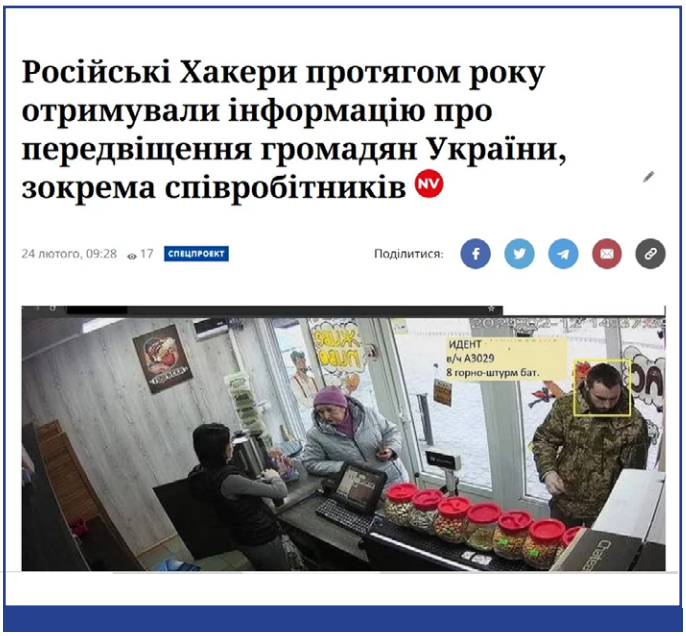
Приклад російського пропагандистського контенту Діани Панченко, який транслювався на каналах холдингу «1+1 media»

Джерело:
скриншот від Центру стратегічних комунікацій та інформаційної безпеки.

Фахівці оперативно усунули проблему та відновили супутникове мовлення. Холдинг «1+1 media» закликав українців дотримуватися інформаційної гігієни, щоб не допомагати ворогу поширювати дезінформацію.

3.2.3. СТВОРЕННЯ НЕПРАВДИВИХ НОВИН І ПОСТІВ У СОЦМЕРЕЖАХ: «NV»

У лютому 2024 року українське інформаційне агентство «NV» стало ціллю кібератаки, у ході якої зловмисники отримали несанкціонований доступ до ресурсів видання й опублікували неправдиві статті на сайті та в Telegram-каналі «NV». У статтях ішлося, що російські хакери буцімто відстежували переміщення громадян України, у тому числі співробітників силових відомств.



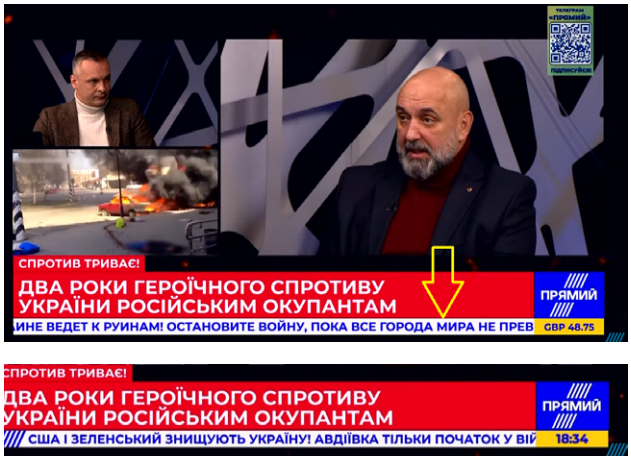
Неправдива новина, створена хакерами на сайті «NV»

Джерело:
скриншот «NV».

За словами «NV», ця хакерська атака, імовірно, була спрямована на дискредитацію «Дельти» — системи ситуаційної обізнаності Збройних Сил України. Утім, невдовзі «NV» вдалося відновити контроль над сайтом і Telegram-каналом видання та видалити неправдиві новини.

3.2.4. ЗЛАМ РУХОМОЇ ІНФОРМАЦІЙНОЇ СТРІЧКИ: ТЕЛЕКАНАЛ «ПРЯМИЙ»

Ще один приклад кібератаки з метою поширення дезінформації — кібератака на український телеканал «Прямий». Вона призвела до поширення російської пропаганди через рухому інформаційну стрічку каналу під час онлайн-трансляції на YouTube. Запланований текст інформаційної стрічки було змінено на наративи російської пропаганди, що США і Президент Зеленський знищують Україну своїми діями.



Неправдива інформаційна стрічка на YouTube-каналі «Прямий»

Джерело: скриншот «Прямий».

Фахівці телеканалу «Прямий» швидко відреагували, вимкнули рухому стрічку й незабаром відновили її нормальну роботу.

Кейс «Прямого» демонструє ширший тренд використання кібератак для ведення інформаційної війни. Ціль таких атак часто полягає не лише в тимчасовому перериванні нормальної роботи медіа, але й дискредитації медіа як надійного джерела новин в очах громадськості.

3.3. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА ТА КОРИСТУВАЧІВ ЩОДО ПРОТИДІЇ ПОШИРЕННЮ ДЕЗІНФОРМАЦІЇ ЧЕРЕЗ ЗЛАМ САЙТІВ

3.3.1. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

1. Використовуйте спеціальні програми для виявлення й реагування на кіберінциденти. Користуйтеся спеціальними інструментами моніторингу, щоб швидко виявляти та реагувати на ознаки зламу. Якщо ви підозрюєте, що сайт зламано, скористайтеся одним із таких інструментів:

- **Звіт «Проблеми безпеки»** від Google Search Console. Якщо системи Google визначать, що ваш сайт був зламаний або становить небезпеку для відвідувачів

(наприклад, містить шкідливе програмне забезпечення або використовується для фішингу), то інформація про це буде подана у звіті «Проблеми безпеки».

- **Безпечний перегляд** від Google. За допомогою технології безпечного перегляду Google щоденно аналізує мільярди URL-адрес і виявляє тисячі небезпечних сайтів, які були зламані. Коли система виявляє небезпечні сайти, вона також показує застереження в пошуку Google і у вебпереглядачах. Щоб дізнатися, чи сайт безпечний для перегляду, його можна перевірити, вставивши URL сайту в пошуковий рядок.

2. Стежте за повідомленнями від свого хостинг-провайдера. У багатьох випадках хостинг-провайдер може виявити факт злому сайту й повідомити про це. Коли є достатні підстави вважати, що сайт зламано, хостинг-провайдери зазвичай відключають сайт, а потім надсилають відповідного електронного листа власнику.

3. Повідомте хостинг-провайдера про злам сайту, якщо він сам це не виявив. Якщо було зламано акаунт редактора або іншого співробітника на вашому сайті, важливо якомога швидше звернутися до хостинг-провайдера, на якому розміщений ваш сайт. Повідомте хостинг-провайдера про злам і попросіть тимчасово відключити ваш сайт, щоб люди не читали поширювану на зламаному сайті дезінформацію, поки ви відновлюєте контроль над сайтом.

Окрім того, хостинг-провайдер може допомогти «відкотити» сайт до стану, який був до моменту зламу, за умови наявності регулярних бекапів (резервних копій даних).

4. Регулярно створюйте бекапи (резервні копії даних) вашого сайту й перевіряйте їх відновлюваність. Обов'язково налаштуйте регулярне створення бекапів (резервних копій) вашого сайту. Зберігайте бекапи не лише на основному сервері, але й на зовнішніх носіях або інших хмарних сервісах для додаткової безпеки (бекапи бекапів).

Призначте відповідальну особу, яка регулярно буде перевіряти можливість відновлення сайту з бекапів. Це необхідно, щоб переконатися, що бекапи не пошкоджені й справді можуть бути використані для відновлення сайту в разі кібератаки. Перевірку бекапів краще проводити в позаробочий час, коли на сайті статистично найменша кількість відвідувачів. Це важливо, адже під час перевірки сайт може бути недоступний від кількох хвилин (у разі успішного відновлення з бекапу) до кількох годин (у разі неуспішного відновлення, тоді доведеться все повертати назад через інші бекапи чи вручну шукати та виправляти помилки).

5. Розробіть план реагування на кіберінциденти. Створіть чіткий план реагування і відновлення після інцидентів, який охоплює процедури комунікації з аудиторією та іншими зацікавленими сторонами.

6. Захистіть інфраструктуру сайту. Використовуйте найсучасніші методи захисту, як-от мережеві послуги доставки контенту й захисту від певних типів кібератак (наприклад, від «Cloudflare» чи «Deflect»), регулярно оновлюйте програмне забезпечення, налаштуйте багатофакторну аутентифікацію та подбайте про складні паролі співробітників для доступу до ваших ресурсів, надайте співробітникам мінімальний необхідний рівень доступу до певних ресурсів для ефективного виконання поставлених завдань (щоб у разі компрометації акаунта співробітника зловмисники отримали якомога менше доступів) тощо. Нікому стороннього не передавайте жодні конфіденційні дані, пов'язані з роботою вашого сайту.

7. Захистіть свої облікові записи в хостера / реєстратора домену. Переконайтеся, що ваші профілі в хостера або реєстратора домену захищені складним паролем і двофакторною аутентифікацією.

8. Стежте за безпекою сторонніх сервісів. Ретельно перевіряйте безпеку всіх сторонніх сервісів, інтегрованих у роботу сайту, таких як банерні / рекламні мережі або сервіси для публікування / розміщення контенту.

9. Створіть «дзеркало» сайту. Створення дзеркальної копії вашого сайту на іншій інфраструктурі є ефективним заходом для забезпечення безперервності роботи сайту у випадку зламу або інших технічних проблем. Дзеркало сайту — це повна копія основного сайту, розміщена на іншому сервері або хостингу. У разі атаки на основний сайт трафік може бути швидко перенаправлений на дзеркальний сайт, що дозволяє зберегти доступність і функціональність ресурсу для користувачів.

10. Навчайте співробітників основ цифрової безпеки. Організуйте навчання із цифрової та інформаційної безпеки для всіх

своїх співробітників, особливо на тему розпізнавання фішингових атак.

11. Будьте прозорими та відкритими. Інформуйте громадськість про всі випадки кібератак або спроби маніпуляцій із контентом. Співпрацюйте з іншими медіа / установами для обміну інформацією про потенційні загрози та найкращими практиками їх подолання.

12. Повідомте уповноваженим установам про випадок зламу. Якщо є підстави вважати, що сайт зламали з метою поширення дезінформації, ви можете звернутися до кіберполіції. Це можна зробити через офіційний сайт: https://ticket.cyberpolice.gov.ua/. Окрім того, зверніться до Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA) за допомогою контактних даних або форми на її сайті: https://cert.gov.ua/contact-us.

3.3.2. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

1. Критично сприймайте отриману інформацію та перевіряйте її. Не слід відразу довіряти й поширювати новини, які викликають сильні емоції чи «розганяють зраду», навіть якщо їх публікують ресурси, яким ви довіряєте. Завжди краще перевірити інформацію в кількох надійних джерелах.

Так, якщо якийсь онлайн-ресурс раптом починає повідомляти про шалені успіхи Росії на фронті чи розповідає про недоцільність подальшого спротиву, перевірте цю інформацію на сайтах інших видань та установ. Сайт, що «розганяє зраду», найімовірніше, зламали, і тепер він поширює російську дезінформацію.

2. Підвищуйте свої знання із цифрової та інформаційної безпеки. Регулярно цікавтеся схемами здійснення кібератак, методами виявлення дезінформації. Оновлюйте список надійних джерел новин, які ви читаєте. Наприклад, можете скористатися білим списком прозорих і відповідальних українських медіа від ГО «Інститут Масової Інформації».

3. Якщо є підстави вважати, що сайт зламали з метою поширення дезінформації, ви можете повідомити про цей інцидент адміністрацію сайту, кіберполіцію: https://ticket.cyberpolice.gov.ua/ та Урядову команду реагування на комп'ютерні надзвичайні події України (CERT-UA): https://cert.gov.ua/contact-us.

Дотримання цих рекомендацій допоможе медіа краще захистити свої ресурси від зламів, а користувачам — обмежити вплив дезінформації.

4. DDOS-АТАКИ ЯК ІНСТРУМЕНТ ПІДРИВУ ІНФОРМАЦІЙНИХ СПРОМОЖНОСТЕЙ УКРАЇНИ

З РОЗГОРТАННЯМ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РОСІЇ ПРОТИ УКРАЇНИ ОДНИМ ІЗ НАЙПОШИРЕНІШИХ ТИПІВ КІБЕРАТАК НА УКРАЇНСЬКІ МЕРЕЖЕВІ РЕСУРСИ Й ІНФРАСТРУКТУРУ Є DDOS-АТАКИ.

4.1. DDOS-АТАКИ: ПОНЯТТЯ І ТИПИ

DDoS-атака (distributed denial-of-service attack, розподілена атака на відмову в обслуговуванні) — це вид кібератаки, під час якої зловмисники намагаються порушити роботу сайту, мережі чи інших сервісів, перевантажуючи їх великою кількістю фальшивих запитів.

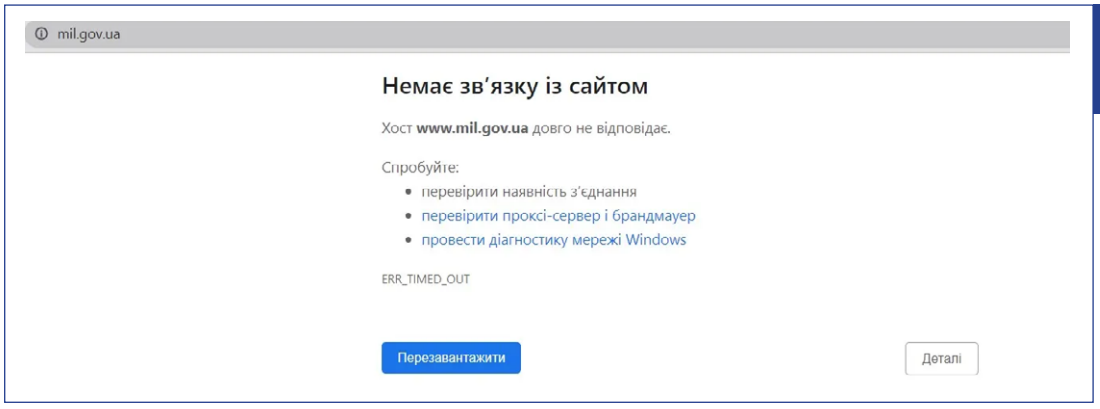
Інакше кажучи, під час DDoS-атаки зловмисник одночасно генерує настільки велику кількість зовнішніх запитів (їх кількість може сягати мільйонів), що таргетована система не може ці запити обробити. Через це виникають збої в роботі сайту.

ТИПИ DDOS-АТАК:

- **Об'ємні атаки.** Найпростіші та «найстаріші», вони передбачають використання великих обсягів трафіку, щоб заповнити пропускну здатність мережі жертви або пропускну здатність між мережею й інтернетом. Наприклад, зловмисники можуть перевантажити цільовий віддалений сервер шляхом надсилання запитів програмі, яка прослуховує певний порт. Оскільки сервер повинен перевірити і відповісти на кожен запит, його пропускна здатність може швидко вичерпатися. Після цього сайт стає недоступним.

- **Атаки прикладного рівня.** Атаки на загальнодоступні програми шляхом надсилання великих обсягів фіктивного трафіку. Прикладом є перевантаження серверу певними запитами. Хоча сервер може мати достатню пропускну здатність, через десятки мільйонів запитів на секунду він не встигає їх обробляти. Зрештою, його можливості обробки вичерпуються, і сайт стає недоступним.

- **Атаки на рівні протоколу.** Хакери використовують вразливості мережевих протоколів для перевантаження цільової системи або інфраструктури великою кількістю незавершених запитів. Наприклад, зловмисники можуть надіслати багато запитів на сервер жертви, але ігнорують відповіді на ці запити. Як наслідок, з'єднання (так зване тристороннє рукостискання — Three-way Handshake) не може бути завершене. У якийсь момент надмірна кількість незавершених з'єднань вичерпує потужність сервера, і він стає недоступним.

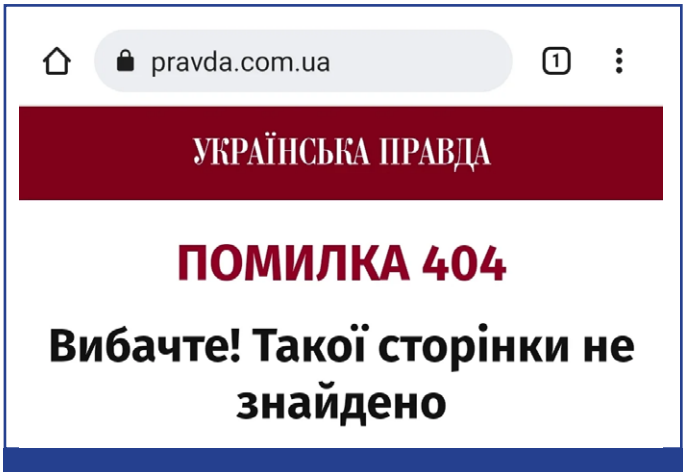


DDoS-атака на сайт Міністерства оборони України

Джерело: скриншот сайту Міністерства оборони України.

У результаті DDoS-атак урядові сайти та сайти новин перестають працювати, а користувач бачить помилку при спробі переходу на сайт (наприклад, помилка 404 — сторінку не знайдено, 503 — сервіс недоступний, немає зв'язку із сайтом тощо).

У межах російсько-української війни проросійські хакерські угруповання спрямовують DDoS-атаки проти українських урядових сайтів та онлайн-медіа, щоб вивести їх із ладу й ускладнити донесення правдивої інформації до української аудиторії. Це відбувається паралельно з хвилями поширення російської дезінформації.

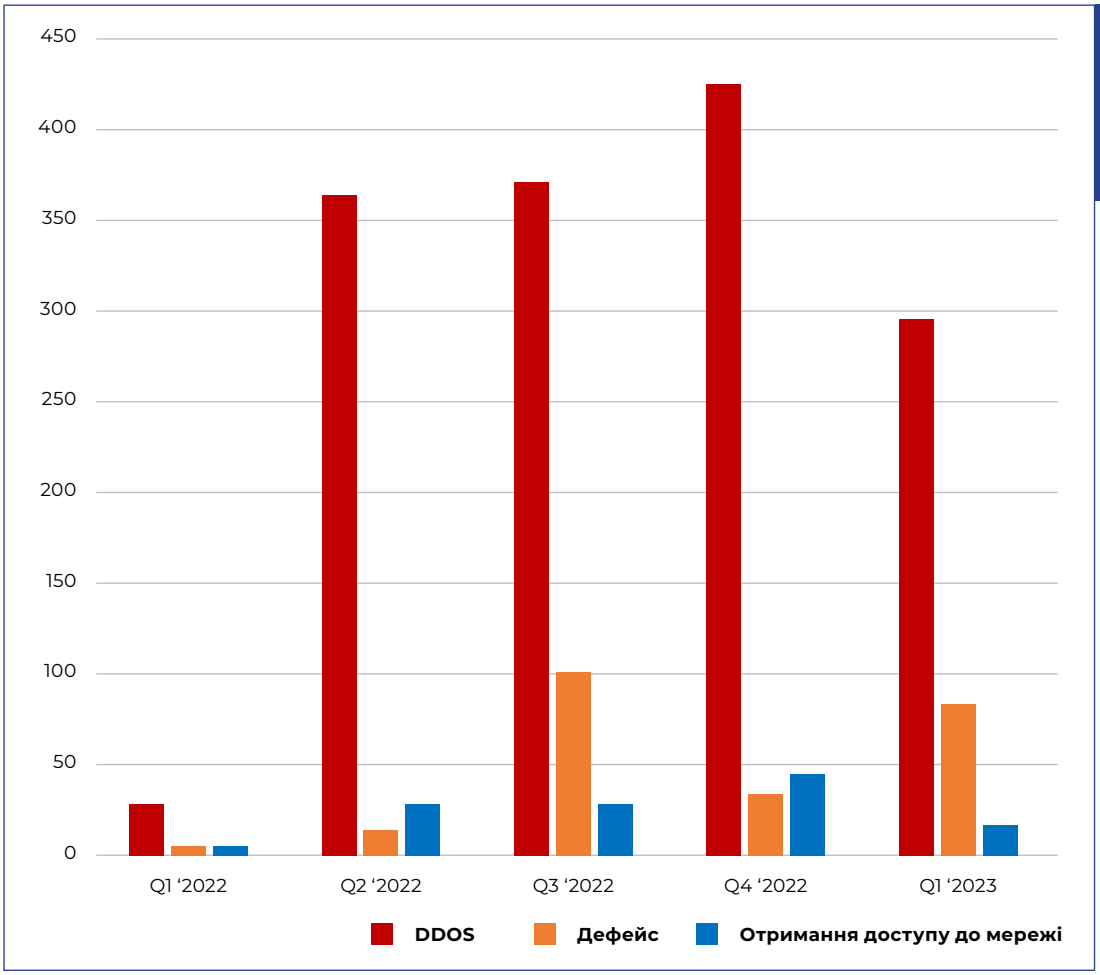


DDoS-атака на сайт «Української правди»

Джерело:
скриншот сайту «Української правди».

4.2. ДИНАМІКА DDOS-АТАК В УКРАЇНСЬКОМУ КІБЕРПРОСТОРІ

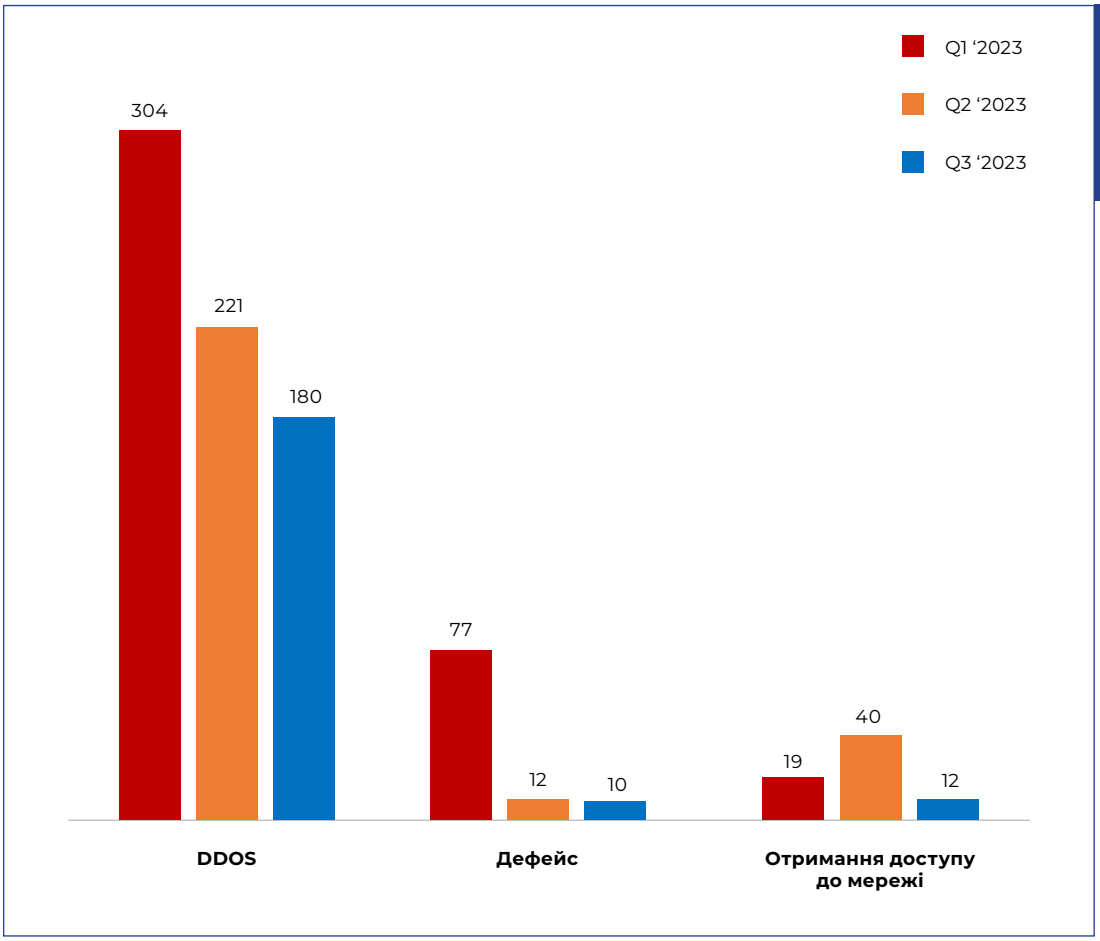
Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі — Держспецзв'язку) повідомляє про стрімке зростання DDoS-атак в українському кіберпросторі з боку (про)російських хакерських угруповань останніми роками. Якщо в I кварталі 2022 року кількість DDoS-атак становила менше ніж 50, то в II кварталі ця цифра збільшилася в кілька разів — понад 350 атак, до кінця 2022 року їх налічувалося більш як 400 за IV квартал.



Динаміка активності проросійських хакерських угруповань за типами атак, 2022-2023

Джерело:
Державний центр кіберзахисту Держспецзв'язку 2023 Q1.

Цікаво, що протягом 2023 року спостерігався тренд до зменшення як загальної кількості кібератак, так і DDoS-атак. З I до III кварталу 2023 року кількість DDoS-атак в українському кіберпросторі зменшилася з 304 до 180.



Динаміка активності проросійських хакерських угруповань за типами атак, 2023

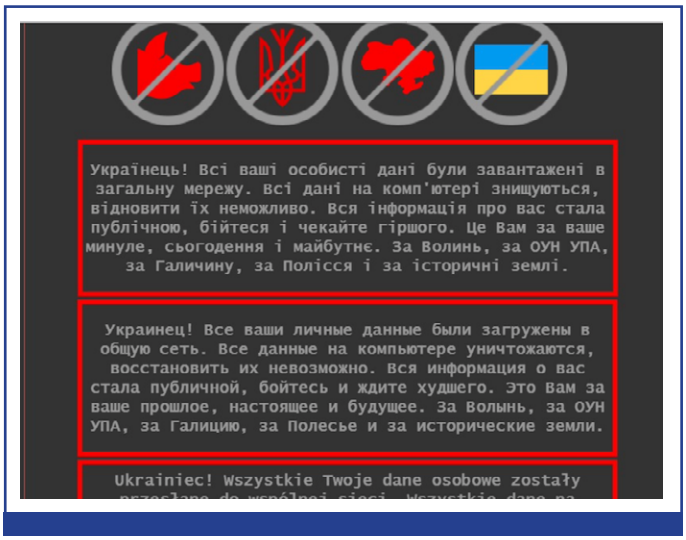
Джерело: Державний центр кіберзахисту Держспецзв'язку 2023 Q3.

4.3. КЕЙС-СТАДІ: МЕДІА ТА УСТАНОВИ, ЩО ПОСТРАЖДАЛИ ВІД DDOS-АТАК

З початку повномасштабного вторгнення низка українських медіа й громадських організацій потерпали від DDoS-атак: «Українська правда», «dev.ua», «Громадське радіо», «Цензор.НЕТ», «Детектор медіа», «Інститут Масової Інформації», освітня платформа «Prometheus» тощо.

Перепадало і сайтам державних установ. За день до повномасштабного вторгнення сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Національної поліції України тощо перестали відкриватися протягом певного часу. Ця тенденція продовжилася і в ході повномасштабного вторгнення.

Іноді, окрім ускладнення доступу до сайтів, зловмисники також залишали політично мотивовані погрози на екрані.



Погроза, опублікована хакерами на сайті Міністерства закордонних справ України в ході DDoS-атаки

Джерело: скриншот МЗС.

Зазвичай після DDoS-атак сайти стають недоступними на кілька годин, після чого їх функціонування, як правило, вдається відновити.

На перший погляд, недоступний сайт протягом кількох годин — невелика проблема, але разом з активними бойовими діями й масовими обстрілами це може бути небезпечно через ускладнений доступ до критичної інформації про перебіг вторгнення та рекомендацій щодо персональної безпеки.

4.4. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА / УСТАНОВ І КОРИСТУВАЧІВ ЩОДО ПРОТИДІЇ DDOS-АТАКАМ

4.4.1. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА / УСТАНОВ

- **Постійно відстежуйте свій мережевий трафік.** Так можна помітити незвичну активність, швидко ідентифікувати й реагувати на потенційні атаки.

- **Використовуйте хмарний DDoS-захист.** Багато хмарних сервісів пропонують вбудовані рішення для захисту від DDoS-атак, які можуть масштабуватися залежно від атаки й мінімізувати її вплив на доступність ресурсу. Приклади таких сервісів: «Project Shield», «Cloudflare» та «Deflect».

Окрім того, переконайтеся, що ваш хостинг-провайдер також використовує хмарні сервіси для захисту від DDoS-атак. Ви можете уточнити це безпосередньо в нього.

- **Зменште «поверхню атаки», щоб зменшити можливості для нападу.** Наприклад, ви можете дозволити трафік лише з певних місць за принципом геолокації. Тоді запити з певних регіонів або IP-адрес будуть блокуватися й не оброблятимуться. Це допоможе зменшити ризик DDoS-атак, обмеживши доступ лише до тих регіонів, звідки справді очікується трафік.

- **Збалансовуйте навантаження й рівномірно розподіляйте ваш мережевий трафік на багато серверів у різних місцях.** Таким чином, у випадку раптового сплеску трафіку його зможуть обробити декілька серверів, що зменшить ризик перевантаження.

- **Використовуйте метод кешування сайту.** У кеш-пам'яті зберігаються копії запитуваного контенту. Як наслідок, менше запитів повинні обслуговуватися вихідними серверами. Використання мережі доставки контенту (CDN) для кешування ресурсів може зменшити навантаження на сервери організації й ускладнити їх перевантаження як справжніми, так і фіктивними запитами.

- **Встановіть обмеження швидкості.** Це обмежить кількість трафіку з одного пристрою за певний час і допоможе запобігти перевантаженню серверів великою кількістю запитів одночасно, що є поширеною тактикою в DDoS-атаках.

- **Розробіть план реагування на DDoS-атаки.** Важливо мати детальний план реагування на інциденти. Визначте осіб, відповідальних за вжиття заходів, а також розробіть чіткі інструкції щодо дій під час і після атаки.

- **Регулярно навчайтеся й обмінюйтеся найкращими способами боротьби з DDoS-атаками.** Встановіть зв'язок із національними структурами у сфері кібербезпеки для обміну інформацією про поточні загрози та виявлені вразливості. Наприклад, Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) постійно відстежує й інформує про нові загрози в українському кіберпросторі, а також приймає релевантні запити за формою: https://cert.gov.ua/contact-us (див. у розділі 7.1 детальнішу інформацію про активності національних структур кібербезпеки).

- **Беріть участь у національних програмах кіберзахисту.** Долучайтеся до ініціатив, організованих державними структурами, таких як тренінги, семінари й симуляції, щоб підвищити свої знання та вміння у сфері кібербезпеки. Наприклад, Держспецзв'язку пропонує різноманітні освітні програми, можливості для професійної сертифікації й нові технічні рішення у сфері кібербезпеки (див. у розділі 7.1 детальнішу інформацію про активності Держспецзв'язку та інших національних структур кібербезпеки).

- **Співпраця з відповідальними органами.** Співпрацюйте з правоохоронними органами для розслідування та притягнення

до відповідальності зловмисників, що здійснюють DDoS-атаки. Зберіть всю доступну інформацію про вчинення DDoS-атаки та зверніться до кіберполіції: https://ticket.cyberpolice.gov.ua/ й Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA): https://cert.gov.ua/contact-us.

- **Використовуйте нові технологічні рішення й державні ресурси.** Скористайтеся доступними державними ресурсами й сервісами для підвищення захисту своїх мереж і систем. Так, для захисту держустанов від DDoS-атак Держспецзв'язку презентувала в червні 2024 року нові технічні рішення.

- **Інформуйте свою аудиторію.** Повідомляйте аудиторії про факт вчинення DDoS-атаки на ваш ресурс й альтернативні платформи споживання інформації.

4.4.2. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Використовуйте різноманітні платформи для отримання інформації.** Якщо основний сайт медіа впав, перевірте, чи воно має активні акаунти в соціальних мережах або на інших платформах, де може продовжувати публікувати новини. Багато медіа мають резервні канали на таких платформах, як Facebook, Instagram, X тощо, де вони можуть швидко публікувати важливі новини навіть у разі технічних проблем з основним сайтом і DDoS-атаки.

- **Виберіть кілька надійних джерел інформації.** Завжди корисно мати кілька перевірених і надійних джерел новин, яким ви довіряєте. Це стосується як традиційних медіа, так і онлайн-ресурсів. Таким чином, якщо один із ресурсів стане недоступним через DDoS-атаку чи інші причини, ви зможете звернутися до інших джерел й отримати актуальну інформацію.

- **Стежте за оновленнями безпосередньо від офіційних органів.** У випадку значущих подій або кризових ситуацій уряд та інші офіційні інституції часто публікують оновлення через свої офіційні канали або пресрелізи. Перевірка таких джерел може допомогти отримати важливу інформацію в період кризи.

- **Не натискайте на підозрілі посилання.** Не переходьте за підозрілими посиланнями, особливо якщо вони надійшли з невідомих джерел або електронних листів. Так вас можуть пробувати залучити до участі в DDoS-атаках без вашого відома.

5. ГЛУШІННЯ СУПУТНИКОВОГО СИГНАЛУ УКРАЇНСЬКИХ ТЕЛЕКАНАЛІВ

5.1. ЗАГАЛЬНА СХЕМА ПРОЦЕСУ ГЛУШІННЯ СУПУТНИКОВИХ СИГНАЛІВ

1. **Визначення цільових телеканалів і супутників, що їх транслюють.** Зловмисники визначають конкретні супутники, такі як «Astra4A» та «Hotbird13E», що передають сигнали для цільових українських телеканалів.

2. **Вибір необхідного обладнання.** Зловмисники використовують спеціальне обладнання, здатне відправляти потужніші сигнали на тих же частотах, на яких працюють цільові супутники. Це обладнання може бути стаціонарним або мобільним.

3. **Трансляція сильних сигналів / перешкод.** Обладнання відправляє шум або інший тип сигналів / перешкод на частоти супутника, які використовують українські канали. Ці перешкоди настільки сильні, що збивають оригінальний сигнал від супутника й ускладнюють його передачу та прийом.

4. **Моніторинг і коригування.** Зловмисники контролюють ефективність глушіння і вносять корективи в силу та характер перешкод, щоб продовжити деструктивний вплив і протидіяти будь-яким спробам оператора супутника обійти глушіння.

5. **Додаткові дії для транслювання пропаганди.** У деяких випадках зловмисники не лише глушать оригінальні сигнали, але й замінюють їх власним контентом, розповсюджуючи (про)російську дезінформацію або пропагандистські наративи.

Кожен із цих кроків передбачає використання складних технологій і потребує значних ресурсів. Та деякі держави (як-от Росія) вдаються до них як одного з інструментів боротьби в кіберпросторі.

5.2 КЕЙС-СТАДІ: УКРАЇНСЬКІ КАНАЛИ НА «ASTRA4A» ТА «HOTBIRD13E»

З початку березня 2024 року Росія активізувала процес глушіння супутникового сигналу українських телеканалів, що транслюються через супутники «Astra4A» та «Hotbird13E». Ці супутники належать європейським телекомунікаційним операторам «SES» та «Eutelsat».

Оператор супутникового мовлення «SES Astra» в березні надіслав листа телеканалам про факти умисного перешкоджання супутниковим трансляціям протягом місяця, зокрема глушіння сигналів телеканалів із використанням іншого потужного джерела.

Глобальний холдинг «SES» із мережею понад 70 супутників уживає належних заходів для визначення геолокації й документування джерел завад, щоб протидіяти їм.

Є підстави вважати, що глушіння сигналів супутникового зв'язку можуть бути спричинені стаціонарними або пересувними станціями супутникового зв'язку, розташованими на території ворожих сил. Служби моніторингу європейських операторів супутникового зв'язку вважають, що ідеться про локацію в Підмосков'ї.

Так, 13 березня була зафіксована спроба заглушити сигнал супутникових телеканалів Суспільного мовлення, що транслюються через супутник «Astra», як-от: «Перший», «Суспільне Культура», «Суспільне Крим», «Суспільне Новини», «Суспільне Спорт», а також декілька радіостанцій. Суспільне мовлення повідомило, що сигнал глушили із центру космічного зв'язку «Ведмежі Озера» в Підмосков'ї. Канали вдалося заглушити на годину, що призвело до тимчасової

втрати сигналу радіо- і телеканалів. Мовлення згодом було відновлено.

Уже через місяць (17 квітня) трансляція 39 телеканалів на транспондері «Astra 4A 11766 H» була призупинена через спроби Росії заглушити супутникове мовлення України. Ці обмеження торкнулися, зокрема, таких каналів, як «1+1 Україна», «1+1 Марафон», «2+2», «ТЕТ», «24 канал», «Kvartal TV», «ПлюсПлюс», «X Sport», «ATR» та ін.

https://www.lyngsat.com/muxes/Astra-4A_Europe-BSS_11766-H.html

	Channel Name		Video	VPID	APID	Lang.	Audio Text	Encryption	Package
1+1 МАРАФОН	1+1 Marafon	S	MPEG-4 SD	1001	1002	Ukr	AAC		
1+1 УКРАЇНА	1+1 Ukraïna		MPEG-4 SD	1011	1012	Ukr	AAC		
KVARTAL TV	Kvartal TV		MPEG-4 SD	1081	1082 1083	Ukr Rus	AAC AAC	Verimatrix	Viasat Ukraina
ТЕТ	TET	S	MPEG-4 SD	1101	1102	Ukr	AAC		
ПЛЮС ПЛЮС	Plus Plus	S	MPEG-4 SD	1121	1122	Ukr	AAC		
Bigudi	Bigudi	S	MPEG-4 SD	1141	1142	Ukr	AAC		
KVARTAL TV	Kvartal TV International		MPEG-4 SD	1171	1172 1173	Ukr Rus	AAC AAC	Verimatrix	Viasat Ukraina

Вибрані українські канали, що транслюються на транспондері «Astra 4A 11766 H»

Джерело:
Детектор медіа.

Трапляються випадки, коли зловмисники не лише глушать супутниковий сигнал каналів, але й починають транслювати власний контент із пропагандистськими наративами держави-агресора.

Так, 9 травня кілька українських телеканалів зазнали хакерських атак, здійснених, імовірно, російськими угрупованнями з метою глушіння супутникового сигналу на супутнику «Astra». Серед постраждалих медіа були канали медіагруп «StarLight Media» та «Інтер», Суспільний мовник, канали «Дім» та «Апостроф ТВ». На декількох українських каналах запустили трансляцію параду на Червоній площі в Москві.

Трансляція параду 9 травня в Москві на одному з українських телеканалів після атаки шахраїв

Джерело:
Детектор медіа.

5.3. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА ТА КОРИСТУВАЧІВ ЩОДО ПРОТИДІЇ ГЛУШІННЮ КАНАЛІВ

5.3.1. РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

- **Постійно моніторте й реагуйте на інциденти глушіння.** Призначте відповідальну особу, яка в режимі реального часу буде відстежувати статус сигналів і зможе швидко реагувати на будь-які перебої. У разі виявлення ознак глушіння зверніться до Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA): https://cert.gov.ua/contact-us.

- **Зверніться до свого супутникового оператора.** У разі проблем із трансляцією медіа варто негайно зв'язатися зі своїм супутниковим оператором, таким як «SES» та «Eutelsat», для з'ясування причини перебоїв трансляції й обговорення шляхів розв'язання проблеми. Також варто проговорити з оператором потенційні заходи для запобігання подібним інцидентам у майбутньому.

- **Розробіть план дій на випадок глушіння каналів.** Важливо мати резервний план дій на випадок, якщо телеканал є основним каналом мовлення і його заглушили. План дій може передбачати використання альтернативних супутників, а також перехід на інтернет-трансляцію або цифровий ефір.

- **Диверсифікуйте платформи для мовлення.** Диверсифікуйте платформи для мовлення, щоб мінімізувати залежність від одного каналу розповсюдження інформації. Ви можете використовувати згадані інтернет-платформи, цифровий ефір тощо.

- **Співпрацюйте з правоохоронними органами.** Налагодьте співпрацю з правоохоронними органами для розслідування та притягнення до відповідальності зловмисників, що глушать канали. Зверніться до кіберполіції: https://ticket.cyberpolice.gov.ua/.

5.3.2. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

Щоб мінімізувати вплив глушіння супутникових сигналів українських каналів на споживання інформації, користувачі можуть дотримуватися таких рекомендацій:

- **Черпайте інформацію з різних джерел мовлення.** Це може бути цифрове ефірне телебачення (T2), кабельне/IPTV-телебачення, а також онлайн-платформи, такі як OTT (over-the-top) сервіси, офіційні сайти телеканалів та їхні YouTube-канали.

- **Стежте за сторінками медіа в соціальних мережах та інших офіційних каналах комунікації.** Офіційні сторінки телеканалів оновлюються в реальному часі та надають актуальну інформацію про стан мовлення й альтернативні джерела інформації у випадку глушіння каналу.

- **Дотримуйтеся інформаційної гігієни.** Критично ставтеся до інформації, яку отримуєте, особливо в періоди інформаційних атак. Перевіряйте новини в кількох надійних джерелах перш ніж ними ділитися.

6. ФІШИНГ ЯК ФОРМА ДЕЗІНФОРМАЦІЇ В УКРАЇНСЬКОМУ ЦИФРОВОМУ ПРОСТОРІ

ФІШИНГ — ЦЕ ФОРМА КІБЕРАТАКИ З ВИКОРИСТАННЯМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, У ХОДІ ЯКОЇ ЗЛОВМИСНИК МАСКУЄТЬСЯ ПІД НАДІЙНИЙ СУБ'ЄКТ І ВИМАНЮЄ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ, ЗМУШУЮЧИ ЖЕРТВУ ВИКОНАТИ ПЕВНУ ДІЮ (ЩОСЬ ВСТАНОВИТИ, НАПИСАТИ, УКАЗАТИ СВОЇ ДАНІ ТОЩО).

6.1. ЗАГАЛЬНА СХЕМА ФІШИНГУ

Загальна схема фішингу виглядає так:

Як працює фішинг

Джерело: «Cloudflare». Перекладено українською й відредаговано автором.

Спочатку зловмисник надсилає повідомлення жертві, спонукаючи її перейти за шкідливим посиланням. Це посилання веде на фішинговий сайт. Фішинговий сайт імітує справжній сайт упізнаваної установи чи сервісу й запитує конфіденційну інформацію: паролі, дані банківського рахунку тощо. Після введення й підтвердження передачі конфіденційної інформації ці дані стають доступними для зловмисника, який використовує їх для входу на справжній сайт установи чи сервісу — банку, щоб вкрасти гроші; соцмереж, щоб отримати несанкціонований доступ до акаунта жертви й просити друзів про грошову допомогу тощо.

Фішинг містить усі класичні елементи дезінформації, адже він є:

- неправдивим;
- шкідливим;
- поширеним свідомо.

Найпоширеніші фішингові атаки можна поділити на три категорії:

- викрадення аутентифікаційних даних (найчисленніша категорія);
- розповсюдження шкідливого вкладення (шкідливе програмне забезпечення);
- екстершен (вимога здійснити певні дії через погрози).

Окрім традиційних способів здійснення фішингових атак (надсилання жертві зловмисних імейлів чи повідомлень), останнім часом набирає обертів нова форма шахрайства — розповсюдження фішингових посилань через таргетовану рекламу в соцмережах. Про це йдеться в спільному дослідженні Центру стратегічних комунікацій та інформаційної безпеки і Центру демократії та верховенства права.

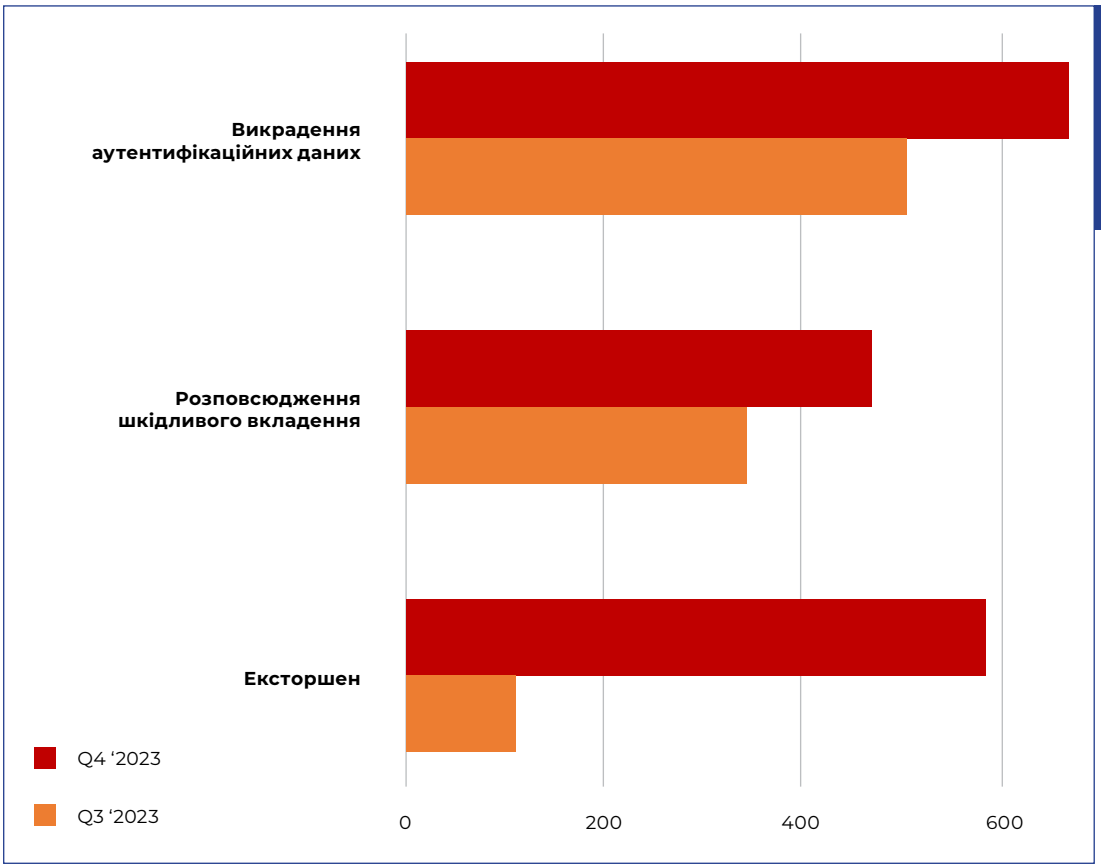
Схема працює так: спершу шахраї створюють масштабну мережу однотипних акаунтів у соцмережах за шаблоном. Наприклад, у певний період активно створювали сторінки, назва яких часто складалася зі слова, трьох-чотирьох літер і цифри, як-от ботмережі «Radiant qt6» або «Charming qrt5». Потім із цих фейкових сторінок (а також зі зламаних профілів справжніх користувачів) зловмисники поширювали фішингові посилання на користувачів соцмережі через таргетовану рекламу.

Реклама, яку запускають зловмисники, зазвичай стосується нібито соціальних виплат від українського уряду, «Дії» та навіть ООН, НАТО, Червоного Хреста тощо. Щоб отримати міфічну виплату, жертві пропонують перейти на шахрайський сайт, що імітує урядовий портал, інший офіційний ресурс або ж сайт, створений начебто для виплат. Далі вона потрапляє на сторінку, яка імітує вхід у банк, де потрібно або ввести повні реквізити картки, на яку буцімто має прийти зарахування, або телефон, пароль і пін-код (інтерфейси варіюють). Жертва вводить свої дані, підтверджує їх, і після цього шахраї отримують доступ до її картки і виводять кошти.

Основна причина успішності фішингу полягає в недостатній цифровій грамотності жертви або її вразливому психоемоційному стані, спричиненому різними обставинами: від завантаженості поточними справами до наслідків обстрілів із боку Росії.

6.2 ДИНАМІКА ФІШИНГОВИХ АТАК В УКРАЇНСЬКОМУ КІБЕРПРОСТОРІ

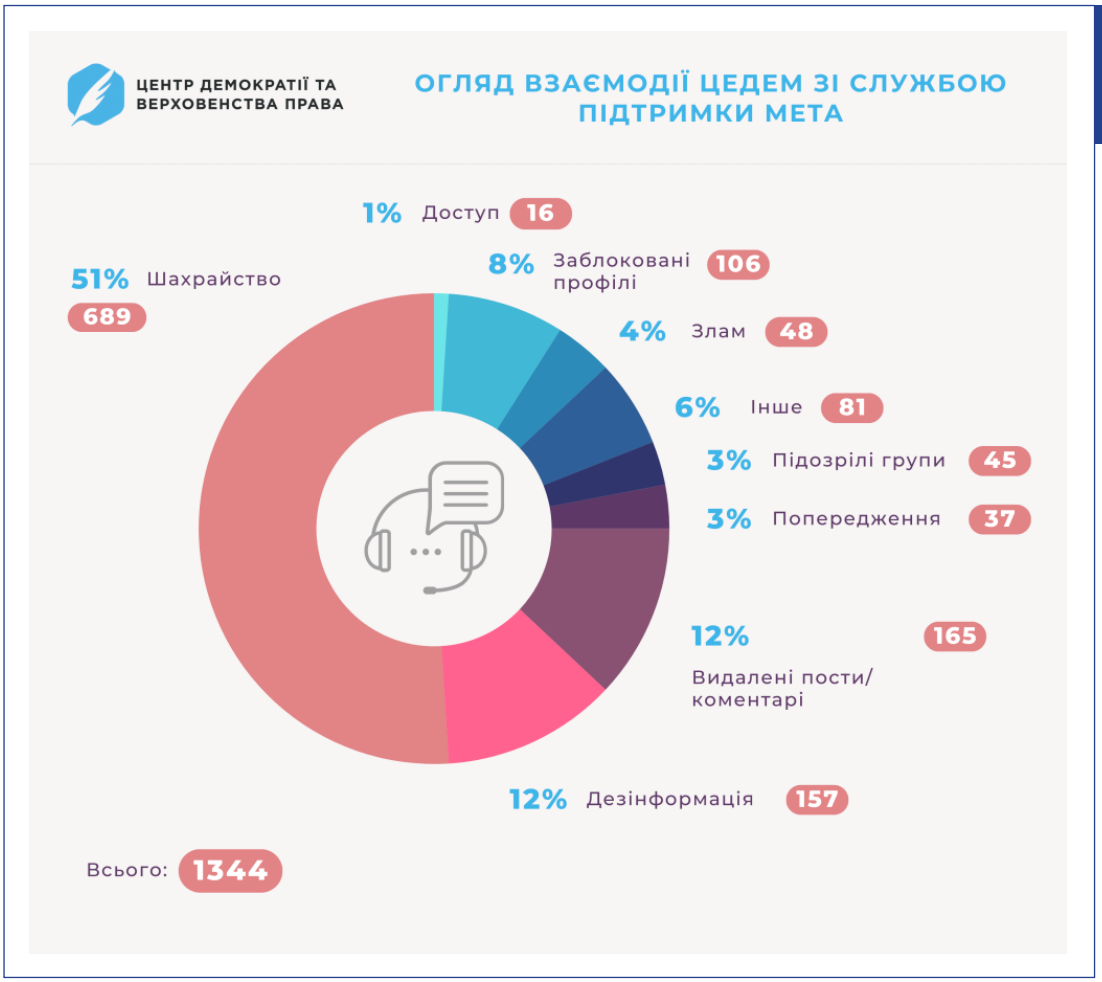
Хоча український кіберпростір потерпав від фішингу віддавна, кількість фішингових атак помітно зросла після повномасштабного російського вторгнення.
У другій половині 2023 року Державний центр кіберзахисту спостерігав суттєве збільшення кількості фішингових атак за категоріями загроз електронній пошті: з 955 зафіксованих атак у III кварталі 2023 року до 1731 атаки в IV кварталі 2023 року.



Розподіл кількості опрацьованих фішингових атак за категоріями загроз електронній пошті

Джерело: Державний центр кіберзахисту Держспецзв'язку Q4.

Підвищена активність зловмисників спостерігається в соціальних мережах. Центр демократії та верховенства права як довірений партнер «Meta» моніторить проблеми в українському сегменті соцмереж, як-от Facebook і Instagram. Від початку повномасштабного вторгнення експерти подали понад 1300 звернень до служби підтримки «Meta», більш ніж половина з них стосувалася шахрайства й фішингу.



Огляд взаємодії ЦЕДЕМ зі службою підтримки «Meta»

Джерело: ЦЕДЕМ.

«Meta» досить оперативно реагує на такі звернення: у середньому протягом дня. 99 % запитів Центру демократії та верховенства права було схвалено. Як наслідок, низку фішингових оголошень видалили, а акаунти, які їх поширювали, заблокували.

6.3. КЕЙС-СТАДІ: НАЙПОШИРЕНІШІ ТИПИ ФІШИНГОВИХ СХЕМ В УКРАЇНІ

При здійсненні фішингових атак зловмисники використовують низку схем. Нижче розглянемо найпоширеніші з них.

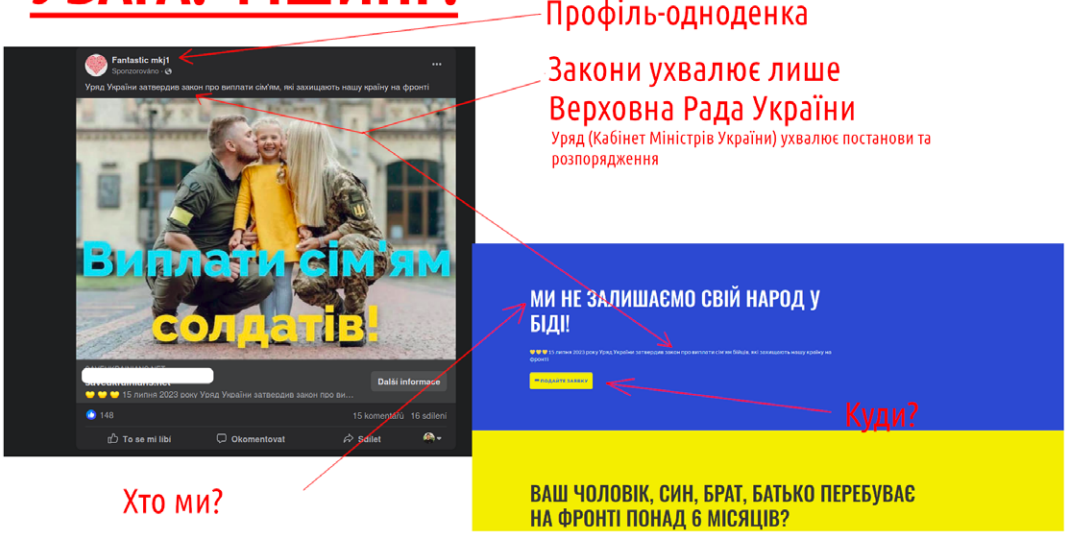
6.3.1. ОТРИМАННЯ ГРОШОВОЇ ДОПОМОГИ

Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) зафіксувала зростання кількості шахрайських сторінок у соціальних мережах (особливо Facebook). Вони часто поширюють рекламу, що стосується грошових компенсацій, платформи «єДопомога», а також фінансової допомоги від різних організацій і партнерів, таких як ООН, ЄС, Товариство Червоного Хреста тощо.

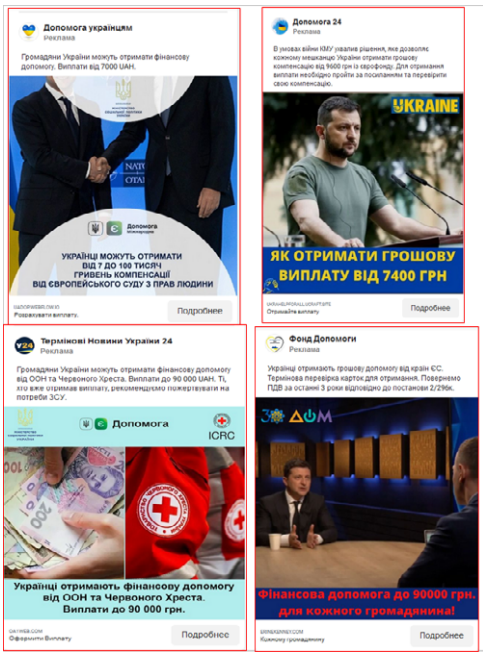
У рекламних оголошеннях користувачам пропонують перейти за посиланням, яке веде на фішингову сторінку, де вони нібито можуть отримати виплату. Для цього необхідно надати персональну інформацію та здійснити додатковий платіж. Як наслідок, шахраї дізнаються дані платіжної картки.

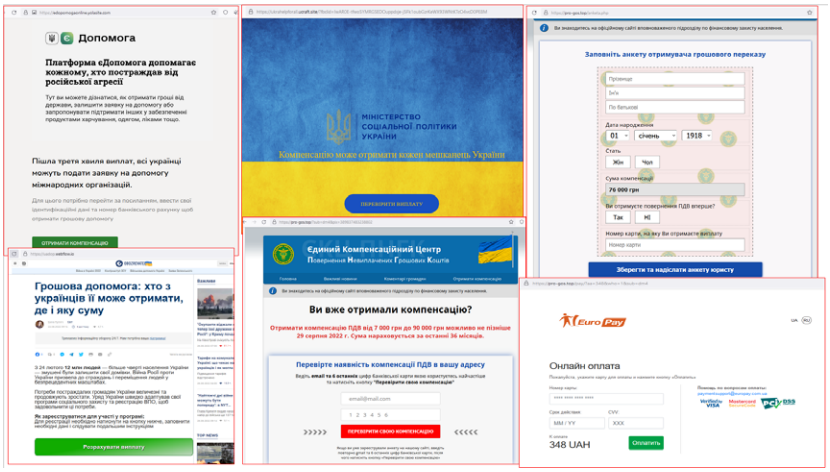
Нижче наведено приклади фішингу на тему отримання фінансової допомоги у Facebook:

УВАГА! ФІШИНГ!

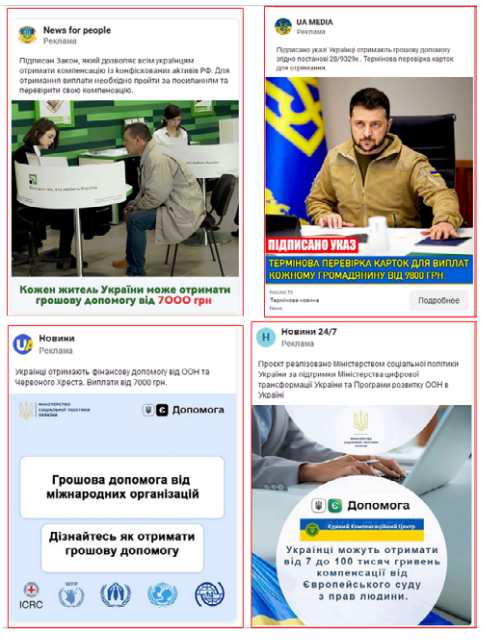


Джерело: інфографіка ЦЕДЕМ.

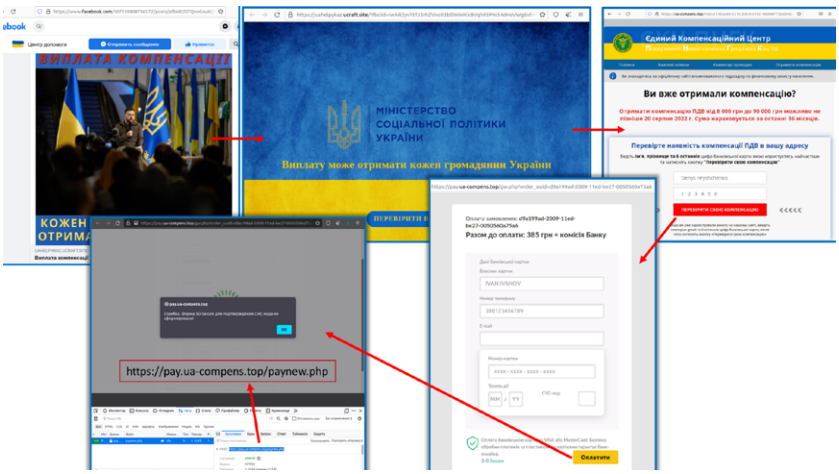




Джерело: CERT-UA.



Джерело: CERT-UA.



Джерело: CERT-UA.

Є підстави вважати, що деякі схеми (як оця) мають «російський слід».

6.3.2. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Подавайте запит на отримання грошової допомоги лише через офіційні сайти.** Користуйтеся офіційним сайтом платформи «єДопомога»: https://aid.edopomoga.gov.ua/. Наразі перший етап приймання заявок на виплату грошової допомоги від міжнародних організацій завершено. Якщо в майбутньому знову буде можливість отримати допомогу, скористайтеся для цього лише згаданим офіційним сайтом.

- **Стежте за інструкціями офіційних установ щодо виплат.** Ознайомтеся з відповідями Міністерства соціальної політики України на найпоширеніші запитання про виплати від міжнародних організацій. Скористайтеся основними порадами щодо платіжної безпеки від Національного банку України та не забувайте про основні правила кібергігієни.

- **Не вводьте персональні дані на неперевірених сайтах.** Ніколи не вводьте дані своєї платіжної картки на неперевірених і сумнівних вебсайтах. За жодних обставин не вводьте пін-код!

- **Моніторте свої транзакції, щоб оперативно реагувати в разі викрадення ваших даних.** Наприклад, можете активувати SMS-сповіщення про проведені транзакції та встановити ліміти на операції.

- **Заблокуйте скомпрометовану картку.** Якщо ви випадково ввели дані своєї картки на шахрайському сайті, негайно заблокуйте картку через мобільний додаток вашого банку, зателефонувавши на гарячу лінію (номер зазвичай указано на звороті картки) або через інтернет-банкінг.

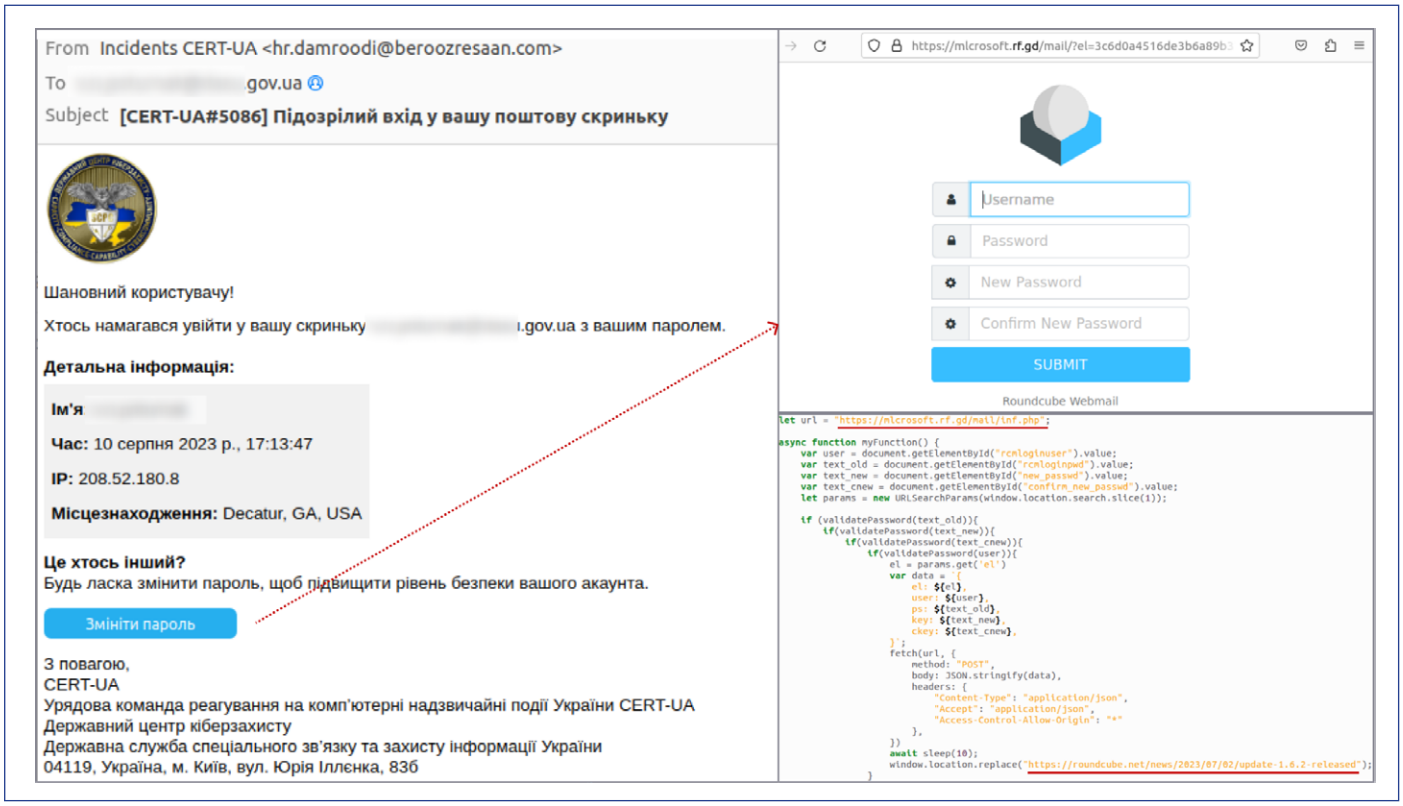
Як альтернативний варіант, тимчасово заблокуйте можливість здійснення оплат в інтернеті та вимкніть опцію оплат без підтвердження, щоб запобігти несанкціонованим транзакціям.

- **Встановіть ліміт для оплати товарів чи послуг в інтернеті.** Це допоможе запобігти великим втратам коштів у разі компрометації даних картки.

- **Зверніться до правоохоронних органів.** Повідомте кіберполіцію про випадок шахрайства: https://ticket.cyberpolice.gov.ua/.

6.3.3. ПІДОЗРІЛИЙ ВХІД У ВАШУ ПОШТОВУ СКРИНЬКУ

Шахраї розповсюджують фішингові листи з темою «Підозрілий вхід у вашу поштову скриньку». Іноді для цього використовують назву та символіку державних установ, як-от CERT-UA чи Державний центр кіберзахисту. Такі листи містять посилання на фішинговий сайт із закликом змінити пароль. Якщо ви перейдете за посиланням і введете логін та пароль, зловмисник отримає ці аутентифікаційні дані.



Джерело: CERT-UA.

6.3.4. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Перевірте джерело.** Перед тим, як клацати на будь-які посилання, ретельно перевірте електронну адресу відправника, щоб упевнитися, що вона відповідає офіційному домену заявленої організації. Шахрайські листи часто мають схожі, але трохи змінені адреси електронної пошти.

- **Не натискайте на посилання.** Уникайте натискань на будь-які посилання в листі. Якщо в листі наполягають на зміні пароля або перевірці облікового запису, перейдіть на офіційний сайт сервісу, де потрібно змінити пароль, але не використовуйте посилання в листі.

- **Використовуйте сервіси для перевірки посилань.** Якщо перейти за посиланням у листі таки треба, то для початку скористайтеся інструментами на кшталт «VirusTotal.com». Цей онлайн-інструмент дозволяє перевірити посилання на наявність шкідливого вмісту, щоб ви уникнули переходу на фішингові й інші небезпечні сайти.

Водночас варто наголосити, що навіть якщо сервіси на кшталт «VirusTotal» показують, що з посиланням усе гаразд, це необов'язково означає, що воно повністю безпечне. Бази даних цих сервісів не завжди вчасно оновлюють дані про нові загрози. Тому важливо додатково звертати увагу на інші ознаки фішингу.

- **Перевірте на наявність ознак фішингу.** Зверніть увагу на характерні ознаки фішингу, такі як граматичні та орфографічні помилки, використання закликів (наприклад, «Терміново потрібна допомога!!!»), загальні привітання (такі як «Шановний користувачу!») замість вашого справжнього імені тощо.

- **Прислухайтеся до порад із безпечної поведінки в інтернеті.** Ознайомтеся з порадами на ресурсі «StopFraud» від Національного банку України. Цей сайт містить важливу інформацію про запобігання фінансовим формам шахрайства і фішингу.

- **Використовуйте двофакторну аутентифікацію.** Увімкніть двофакторну аутентифікацію для всіх своїх акаунтів, де це можливо. Таким чином, навіть якщо ваш пароль буде скомпрометовано, зловмисник потребуватиме доступу до вашого другого фактора аутентифікації для входу в обліковий запис.

- **Повідомте про спробу фішингу.** Перешліть підозрілий лист на офіційну електронну пошту служби підтримки вашого поштового сервісу. Також зверніться в кіберполіцію: https://ticket.cyberpolice.gov.ua/.

- **Детальніше вивчіть особливості фішингу.** Ознайомтеся з тактиками, які використовують зловмисники. Часто корисну інформацію й поради можна знайти на сторінці безпеки вашого провайдера електронної пошти, сайтах державних установ із питань кібербезпеки тощо.

6.3.5. ГОЛОСУВАННЯ В МЕСЕНДЖЕРАХ

Останнім часом зростає кількість фішингових атак, спрямованих на отримання доступу до облікових записів популярних месенджерів, таких як Telegram і WhatsApp.

Через SMS і месенджери Telegram / WhatsApp шахраї розповсюджують повідомлення з проханням перейти за посиланням, авторизуватися й проголосувати за щось / когось. У разі сканування QR-коду або введення номера телефону й одноразового коду до облікового запису жертви додається сторонній пристрій, після чого акаунт стає скомпрометованим.

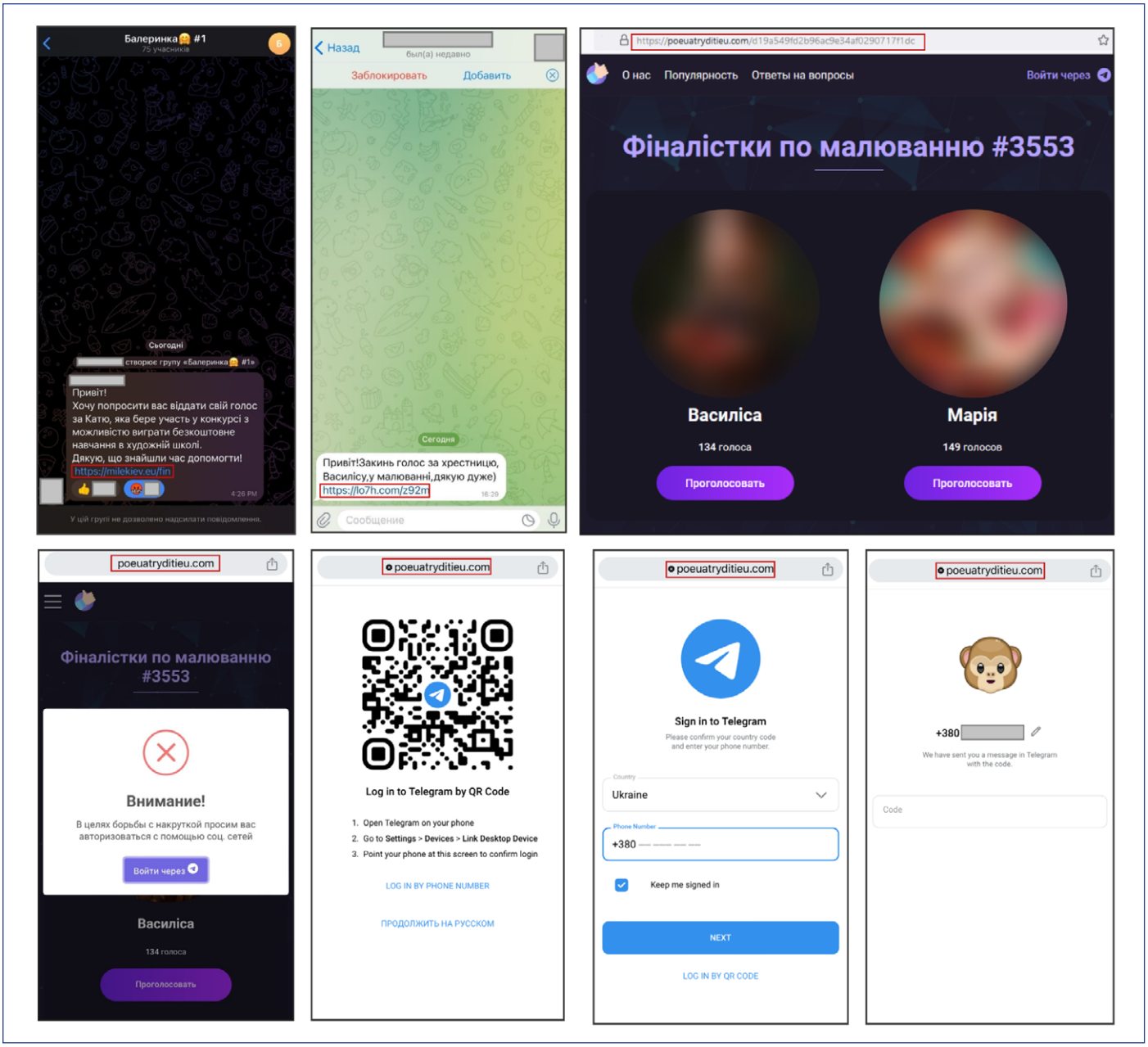
Після компрометації акаунта зловмисники використовують його для розповсюдження шкідливих повідомлень серед контактів жертви, зокрема шляхом створення нових груп у месенджерах.

Викрадені акаунти можуть бути використані для різних шахрайських схем із метою монетизації. Зловмисники можуть розповсюджувати серед усіх контактів жертви прохання позичити гроші, перейти за посиланням і проголосувати за щось / когось (таким чином вони зламують ще більше акаунтів) тощо.

6.3.6. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Не авторизуйтеся на сайтах через месенджери.** Ніколи не авторизуйтеся на жодних сайтах через Telegram, Viber, WhatsApp (чи інші менеджери) за допомогою коду від Telegram, Viber, WhatsApp або QR-коду. Зловмисники можуть використовувати ці методи для крадіжки ваших облікових даних й отримання несанкціонованого доступу до ваших акаунтів.

- **Не переходьте за зовнішніми посиланнями.** Уникайте натискань на посилання в повідомленнях, навіть якщо отримали їх від людей, яких знаєте. Зловмисники можуть використовувати скомпрометовані акаунти ваших друзів / родичів для поширення фішингових посилань.



Джерело: CERT-UA.

■ **Використовуйте сервіси для перевірки посилань.** Якщо перейти за посиланням у листі таки треба, то перед тим, як це зробити, скористайтеся сервісами на кшталт «VirusTotal.com». Цей онлайн-інструмент дозволяє перевірити посилання на наявність шкідливого вмісту, щоб запобігти переходу на деякі фішингові та інші небезпечні сайти.

Водночас варто наголосити, що навіть якщо сервіси на кшталт «VirusTotal» показують, що з посиланням усе гаразд, це необов'язково означає, що воно повністю безпечне. Бази даних цих сервісів не завжди вчасно оновлюють дані про нові загрози. Тому важливо додатково звертати увагу на інші ознаки фішингу.

■ **Зателефонуйте другу чи родичу й перепитайте, чи справді він надсилав вам сумнівне повідомлення.** Якщо ви отримали підозріле посилання від свого друга чи родича, то можете перевірити справжність повідомлення, зв'язавшись із ними альтернативними каналами зв'язку. Зателефонуйте другу / родичу або скористайтеся відеодзвінком, щоб підтвердити справжність повідомлення. Це дозволить уникнути потенційних загроз, швидко й ефективно перевірити, чи справді вони надіслали вам це посилання.

■ **За потреби видаліть свій акаунт і повторно зареєструйте його.** Якщо несанкціонований доступ зловмисника до вашого акаунта триває більше ніж 24 години, він може завершити сесію в месенджері, і ви втрати-

те до нього доступ. У цьому випадку один із варіантів повернення облікового запису — видалити й повторно зареєструвати його.

- **Поінформуйте власника скомпрометованого акаунта.** Якщо ви отримали підозріле повідомлення, негайно повідомте власника акаунта через інший канал зв'язку.

- **Встановіть двофакторну аутентифікацію всюди, де це можливо.** Завжди налаштовуйте двофакторну аутентифікацію для додаткового рівня захисту вашого акаунта.

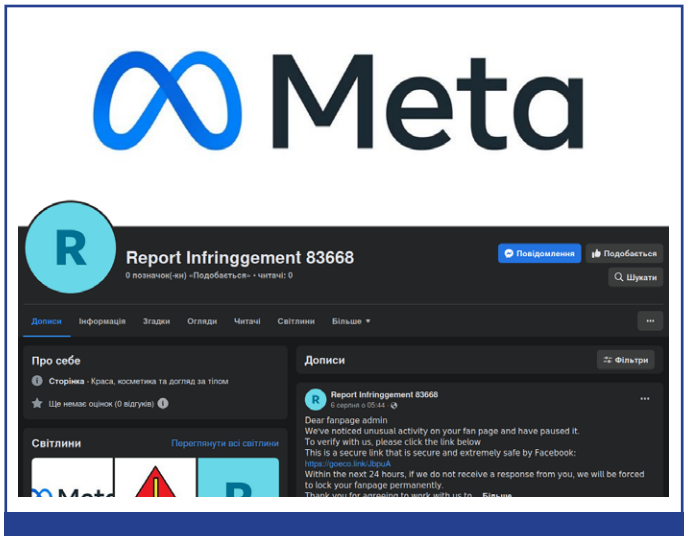
- **Перевіряйте активні сесії в налаштуваннях месенджера.** За потреби перегляньте активні сесії в налаштуваннях месенджера, щоб виявити невідомі пристрої чи сесії. Якщо ви виявили незнайомі пристрої / сесії, негайно завершіть їх у налаштуваннях месенджера.

6.3.7. ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ПРАВИЛ «META»

Через Instagram, Facebook Messenger, Business Manager, акаунти брендів чи електронну пошту зловмисники в особистих повідомленнях сповіщають жертву про буцімто «порушення правил спільноти». Іноді, окрім приватних повідомлень, шахраї масово тегають різні акаунти та сторінки і «попереджають», що їх буде деактивовано протягом 24/48 годин за «порушення правил» або підозрілу активність. Щоб уникнути блокування, зловмисники спонукають перейти за посиланням й «оскаржити» це рішення.

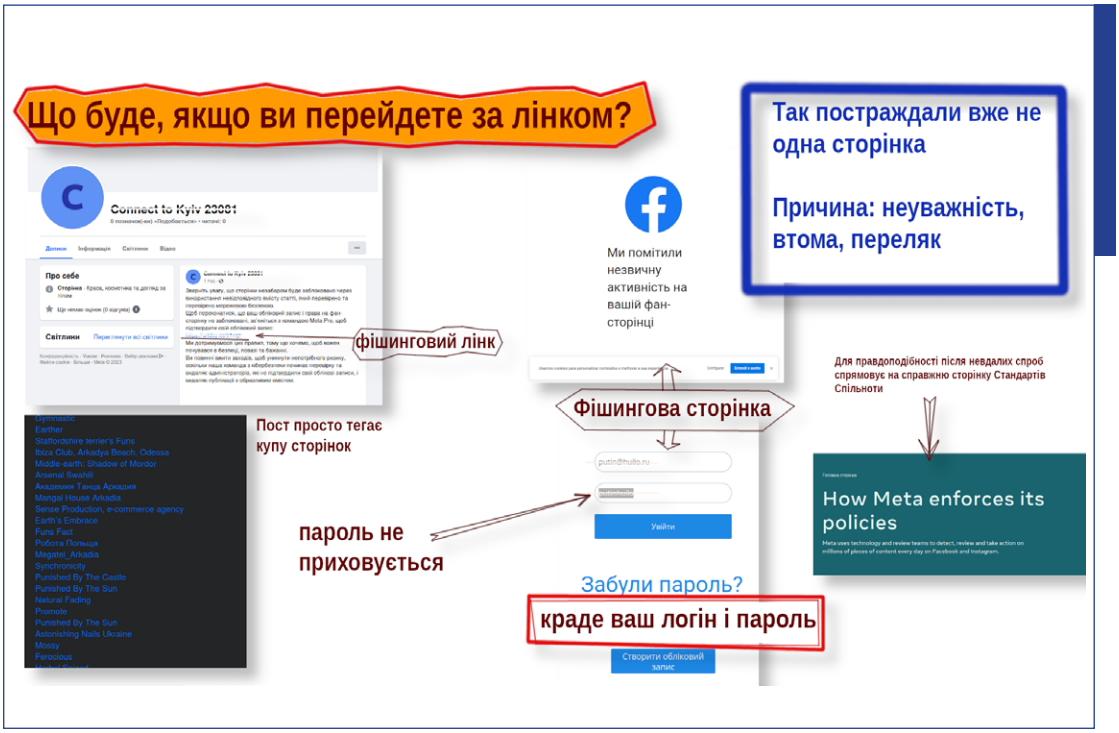
Посилання веде на фішинговий сайт, де повідомляється, що для «оскарження» треба спочатку ввійти в профіль і далі користувача перекине на сторінку, схожу на сторінку входу у Facebook або Instagram. Там йому потрібно ввести логін і пароль від свого акаунта. У такий спосіб шахраї отримують доступ до облікового запису.

Якщо за посиланням перейде адміністратор сторінки або бренду, шахраї можуть отримати доступ не лише до особистого облікового запису адміністратора, але й до сторінки, якою він керує.



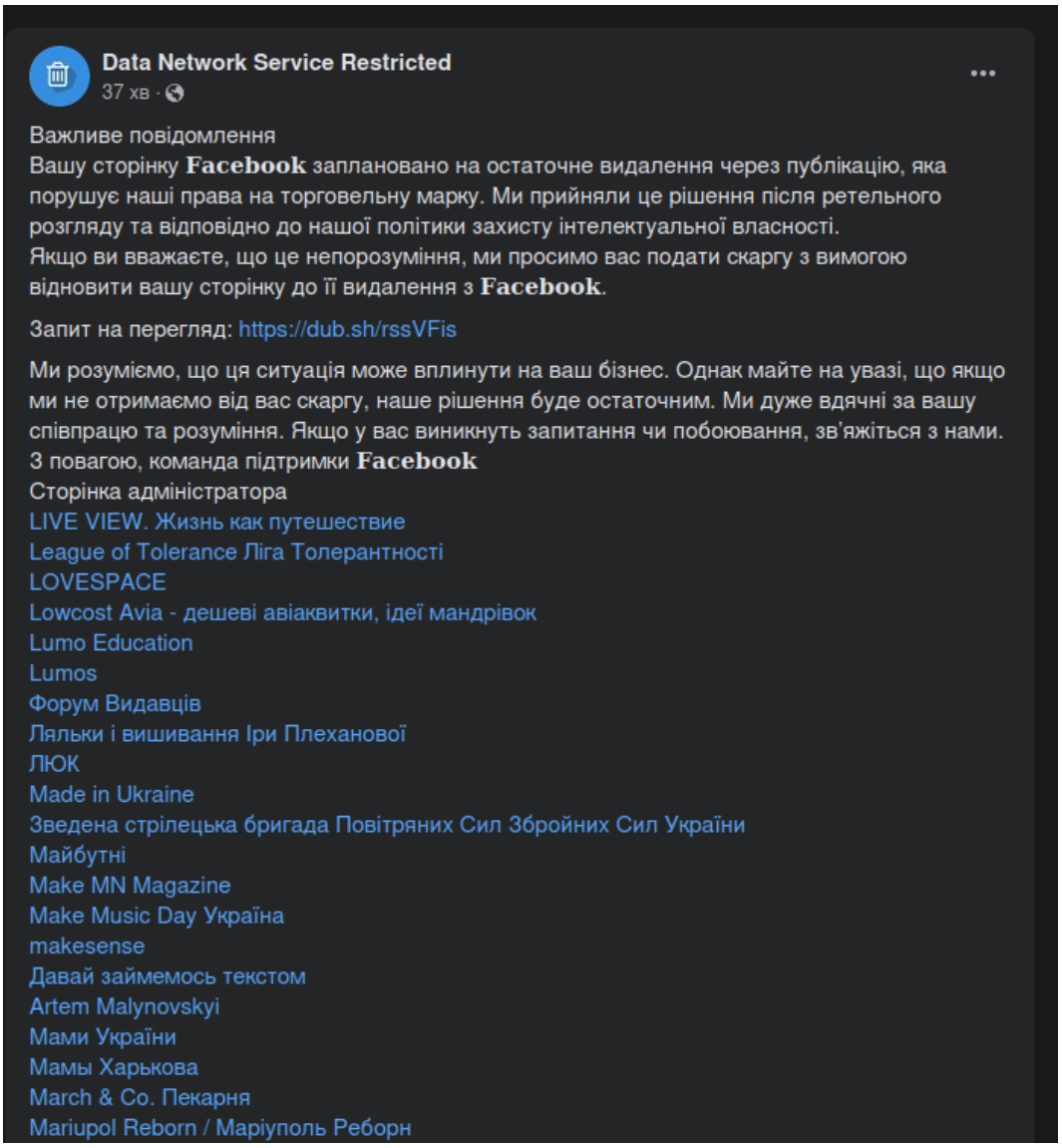
Приклад фейкової сторінки нібито служби підтримки «Meta», яка розповсюджує фішингові посилання

Джерело: скриншот ЦЕДЕМ.



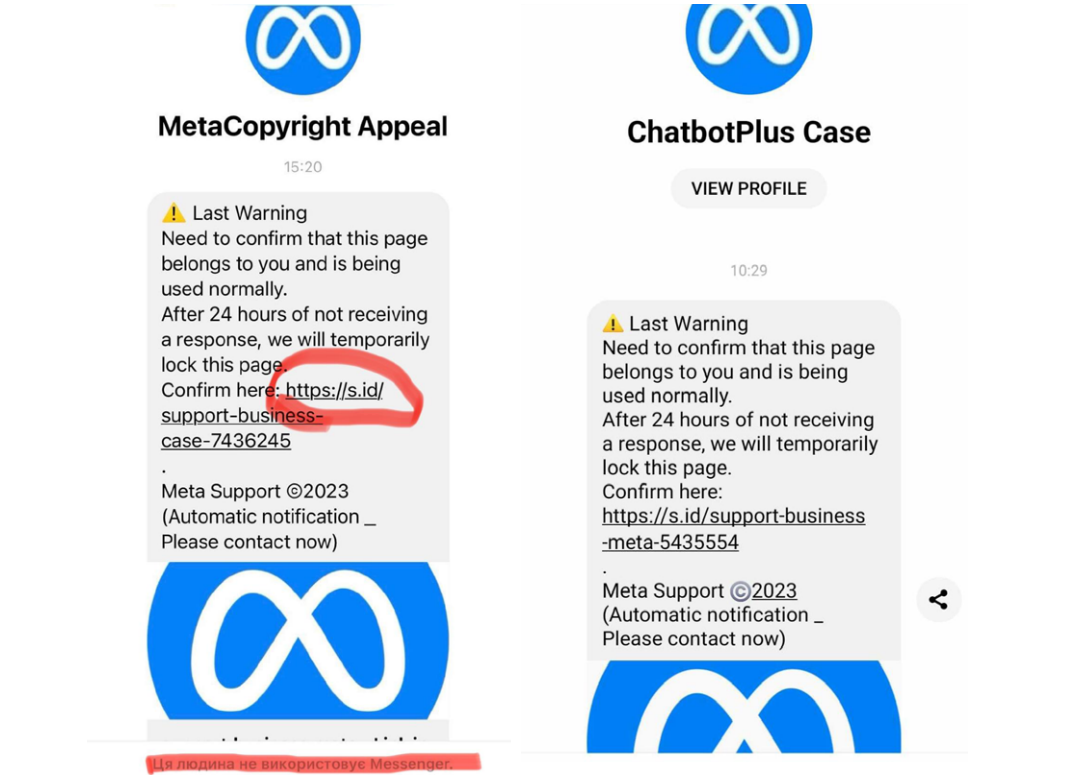
Приклади зловмисних повідомлень із фішинговими посиланнями нібито від служби підтримки «Meta»

Джерело: інфографіка ЦЕДЕМ.



Приклад масового тегання сторінок із фішинговим посиланням нібито від служби підтримки «Meta»

Джерело:
скриншот ЦЕДЕМ.



Приклад фішингового повідомлення нібито від служби підтримки «Meta»

Джерело:
скриншот ЦЕДЕМ.

6.3.8. РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

- **Ознайомтеся з можливими способами отримання повідомлень від «Meta».** Запам'ятайте, що «Meta» ніколи не повідомляє про скарги, репорти, блокування чи будь-що інше через репости або теги. Системи «Meta» можуть видавати таку інформацію у вікні, що спливає, сповіщеннях або ж листом на пошту (але будьте уважні, бо зловмисники можуть надсилати фішингові електронні листи від імені «Meta»).

- **Звертайте увагу на загальні ознаки фішингу.** Загальні ознаки фішингу: неперсоналізоване вітання на початку листа («Meta» завжди використовує для звернення ім'я, яке вказане в обліковому записі); наявність граматичних та орфографічних помилок; пошта відправника не збігається з поштою, яку використовують працівники «Meta» (як-от @facebookmail.com, @metamail.com) тощо.

- **Ознайомтеся зі способами перевірки отриманих повідомлень від «Meta».** Ви можете перевірити листи від «Meta», зробивши такі кроки: «Налаштування та конфіденційність» → «Налаштування» → «Допомога та підтримка» або «Безпека й авторизація» → «Повідомлення від служби підтримки» (для Facebook).

- **Встановіть двофакторну аутентифікацію всюди, де це можливо (зокрема, у Facebook та Instagram).** Завжди налаштовуйте двофакторну аутентифікацію для додаткового рівня захисту вашого акаунта.

- **Перевіряйте активні сесії в налаштуваннях безпеки.** За потреби переглядайте активні сесії в налаштуваннях безпеки, щоб виявити невідомі пристрої чи сесії. Якщо ви виявили незнайомі пристрої / сесії, негайно відключіть їх.

- **Налаштуйте отримання сповіщень про підозрілий вхід у ваш акаунт.** Якщо хтось увійде у ваш акаунт із невідомого пристрою, ви відразу дізнаєтеся про це.

7. ЗАХИСТ У ЦИФРОВОМУ ПРОСТОРІ: ЯК УКРАЇНА ПРОТИСТОЇТЬ КІБЕРАТАКАМ І ДЕЗІНФОРМАЦІЇ

7.1. РОЛЬ ДЕРЖАВНИХ ІНСТИТУЦІЙ У РЕАЛІЗАЦІЇ ПОЛІТИК КІБЕРБЕЗПЕКИ В УКРАЇНІ

Україна посідає 11 місце за національним індексом кібербезпеки в глобальному рейтингу, що вимірює готовність країн запобігати кіберзагрозам і реагувати на кіберінциденти.

Це стало можливим, зокрема, завдяки українській нормативно-правовій базі, яка комплексно регулює основні питання розвитку національних політик із кібербезпеки (див. розділ 1.2). Окрім того, інституційна структура для імплементації цих політик досить розгалужена.

Стаття 5 Закону України «Про основні засади забезпечення кібербезпеки України» визначає таких суб'єктів забезпечення кібербезпеки:

- **Президент України через очолювану ним Раду національної безпеки і оборони України** (далі — РНБО) здійснює координацію діяльності у сфері кібербезпеки як складової частини національної безпеки України.

Так, за рішенням РНБО від 14 травня 2021 року «Про Стратегію кібербезпеки України» указом Президента України було затверджено Стратегію кібербезпеки України — наріжний документ, що визначає пріоритети національних інтересів у сфері кібербезпеки, наявні й потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави.

- **Національний координаційний центр кібербезпеки як робочий орган РНБО** (далі — НКЦК) здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

У червні 2024 року НКЦК спільно з Міністерством цифрової трансформації України та Держспецзв'язку презентував інструмент для автоматичного моніторингу виконання Стратегії кібербезпеки України — «CyberTracker». Він дозволяє автоматизувати процес моніторингу, краще виявляти слабкі та сильні сторони імплементації стратегії, а також ефективніше інформувати і звітувати про прогрес її виконання.

Окрім того, для підвищення цифрової грамотності в Україні НКЦК сприяв організації понад 100 тренінгів, семінарів і змагань для більш як 5000 технічних спеціалістів і керівників із кібербезпеки державних органів, об'єктів критичної інфраструктури, приватних компаній.

- **Кабінет Міністрів України** відповідає за розроблення та впровадження державної політики у сфері кібербезпеки, боротьбу з кіберзлочинністю, захист прав і свобод людини, а також національних інтересів України в кіберпросторі. Також він організовує й забезпечує роботу національної системи кібербезпеки, встановлює вимоги й контролює систему аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Приклад діяльності Кабінету Міністрів України в цьому напрямі — розпорядження від 19 грудня 2023 року № 1163-р «Про затверджен-

ня плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України». План визначає чіткі завдання для міністерств та інших органів виконавчої влади з реалізації стратегії, налагоджує процес моніторингу й подання звітів про прогрес тощо.

Кабінет Міністрів України також ухвалив постанову від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж». Порядок дає можливість кіберспеціалістам за винагороду легально тестувати мережі на наявність вразливостей і в разі виявлення — усувати їх, щоб підвищити рівень кіберзахисту своїх систем. Такий підхід поширений у багатьох інших країнах під назвою Bug Bounty.

Активну діяльність для підвищення кіберстійкості України здійснює Міністерство цифрової трансформації України. Наприклад, у березні 2023 року за його підтримки стартувала програма «re/start in cyber» — тримісячне безоплатне навчання з теоретичних і практичних основ кібербезпеки для українців, які прагнуть реалізувати себе у сфері кібербезпеки. У липні 2024 року міністерство запустило Програму з кіберді-агностики бізнесу, яка повинна допомогти 500 українським компаніям безоплатно перевірити своє підприємство на вразливість до кібератак і вжити заходів для посилення кіберзахисту. Загальний фонд програми — 1,5 мільйона доларів.

- **Суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки:** міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні й контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Серед основних суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, варто виділити такі:

- **Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку):**
  - забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів, активної протидії агресії в кіберпросторі;
  - координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту;
  - забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;
  - проводить заходи для запобігання, виявлення й реагування на кіберінциденти та кібератаки;
  - інформує про кіберзагрози та відповідні методи захисту від них;
  - впроваджує аудит інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів і проводить їх атестацію;
  - координує, організовує й проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;
  - забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії в кіберпросторі, Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA).

Приклади діяльності Держспецзв'язку для зміцнення кіберстійкості:

- Освітні програми з кібербезпеки для держслужбовців. Так, у травні та червні 2024 року експерти Держспецзв'язку провели навчання з кібербезпеки для близько 200 працівників Міністерства оборони України, Секретаріату Кабінету Міністрів України, Верховного Суду та Державної служби України з питань праці. Учасники дізналися про основні ознаки кібератак і навчилися розпізнавати, запобігати й нейтралізувати їх наслідки.

- Кваліфікаційний центр інформаційних технологій та кібербезпеки. У червні 2024 року Держспецзв'язку відкрила перший Кваліфікаційний центр інформаційних технологій та кібербезпеки, мета якого — запровадити сучасну систему професійної сертифікації фахівців із кібербезпеки з урахуванням найкращих світових практик. Наразі кіберфахівці можуть підтвердити свої навички та компетенції за двома новими напрямами — «Розробник безпеки інформаційних систем» та «Адміністратор безпеки мережі та систем». Надалі акредитаційний перелік заплановано розширити ще на дев'ять кваліфікацій.

- Нові технічні рішення для захисту держустанов від DDoS-атак. Співробітники Держспецзв'язку продемонстрували сучасні можливості для аналізу трафіку, ефективного моніторингу, виявлення й блокування різних типів кіберзагроз за допомогою програмної продукції та сервісної підтримки компаній «Radware» й «Akamai Technologies».

- **Державний центр кіберзахисту забезпечує створення та функціонування основних складових частин:**

  - системи захищеного доступу державних органів до мережі Інтернет;

  - системи антивірусного захисту національних інформаційних ресурсів;

  - аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури;

  - системи виявлення вразливостей і реагування на кіберінциденти та кібератаки на об'єкти кіберзахисту;

  - системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки.

  Окрім того, він розробляє сценарії реагування на кіберзагрози, заходи з протидії таким загрозам, програми й методики проведення кібернавчань.

  Приклади діяльності Державного центру кіберзахисту для зміцнення кіберстійкості:

  - Розширення технічних спроможностей Національного центру резервування державних інформаційних ресурсів. Так, Державний центр кіберзахисту передав, зокрема, серверне обладнання для розширення обсягу сховища системи післяаварійного відновлення національних електронних інформаційних ресурсів. Це має підвищити рівень захисту об'єктів критичної інформаційної інфраструктури від потенційних кіберзагроз.

  - Дослідження розповсюдження шкідливого програмного забезпечення в Україні. У грудні 2023 року Державний центр кіберзахисту опублікував результати дослідження розповсюдження шкідливого програмного забезпечення «SmokeLoader» в Україні з травня по листопад 2023 року, проведеного спільно з командою дослідників «Unit 42» компанії «Palo Alto Networks». Фахівці проаналізували, зокрема, 23 хвилі фішингових атак, деякі з яких мають російське походження.

  - Регулярні звіти про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Ці звіти містять результати цілодобового програмного моніторингу, вивчення та передачі телеметричної інформації про кіберінциденти й кібератаки, що трапляються на об'єктах кіберзахисту в Україні.

- **Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA)** виконує такі завдання:

  - накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

  - надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

  - організація та проведення практичних семінарів із питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

  - підготовка й розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак і кіберзагроз;

  - взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

  - взаємодія з іноземними та міжнародними організаціями з питань реагуван-

ня на кіберінциденти, зокрема в межах участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків;

- взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами й організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

- опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

- сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України в розв'язанні питань кіберзахисту та протидії кіберзагрозам.

Приклади діяльності CERT-UA для зміцнення кіберстійкості:

- Практичні семінари для кіберфахівців. Спеціалісти CERT-UA ініціювали проведення семінару для кіберфахівців-практиків з органів державної влади, місцевого самоврядування, військових формувань, державних установ і підприємств із метою обговорення кіберзагроз й обміну досвідом реагування на них.

- Інформаційно-консультаційні та практичні матеріали з кібербезпеки. Так, фахівці CERT-UA підготували покрокові інструкції (разом зі скриншотами) для підвищення безпеки акаунтів шляхом налаштування двофакторної аутентифікації для деяких месенджерів та інформаційних систем, зокрема Telegram, Signal, WhatsApp, Viber, Ukr.net, Google, Facebook.

- Регулярне відстеження кібератак в українському цифровому просторі, пояснення специфіки їх здійснення та надання рекомендацій для захисту від них. Так, експерти CERT-UA проаналізували, зокрема, нові способи викрадення акаунтів через буцімто «голосування» в месенджерах, фішингові атаки для отримання аутентифікаційних даних до публічних поштових сервісів, онлайн-шахрайство з використанням тематики «грошових виплат», розсилання SMS-повідомлень із темою судових повісток, цільові атаки проти українських військовослужбовців із використанням тематики рекрутингу до 3-ї окремої штурмової бригади та Армії оборони Ізраїлю тощо.

- **Національна поліція України:**

  - забезпечує захист прав і свобод людини і громадянина, інтересів суспільства й держави від кримінально протиправних посягань у кіберпросторі;

  - здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Для реалізації державної політики у сфері протидії кіберзлочинності, завчасного інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів і реагування на запити закордонних партнерів було створено Департамент кіберполіції Національної поліції України (кіберполіцію). Одна з головних цілей діяльності кіберполіції — створення безпечного цифрового середовища для користувачів інтернету.

Отримати онлайн-допомогу й надати дані для оперативного реагування на кіберінциденти можна в системі подання електронних звернень громадян за посиланням: https://ticket.cyberpolice.gov.ua/. Інформацію буде опрацьовано відповідно до Закону України «Про звернення громадян».

Приклади діяльності кіберполіції:

- У 2022 році кіберполіцейські супроводжували 5 тисяч кримінальних правопорушень, виявили 2,3 тисячі кіберзлочинів, повідомили про підозру 1 тисячі осіб у вчиненні 2,3 тисячі кримінальних правопорушень; затримали понад 100 кіберзлочинців і скерували 2,7 тисячі кримінальних правопорушень за обвинуваченням 840 осіб до суду з обвинувальними актами.

- У 2023 році показники кіберполіцейських суттєво зросли: вони супроводжували понад 6,4 тисячі кримінальних правопорушень, виявили 3,6 тисячі кіберзлочинів, повідомили про підозру 1,7 тисячі осіб за вчинення 3,7 тисячі кримінальних правопорушень. Окрім того,

кіберполіцейські скерували до суду з обвинувальними актами 4 тисячі кримінальних правопорушень за обвинуваченням 1,3 тисячі осіб.

- За даними, озвученими в березні 2024 року, до кіберполіції за рік надходить у середньому близько 40 тисяч звернень громадян. 80 % із них стосуються шахрайства (зокрема, фішингу). Окрім розслідування випадків онлайн-шахрайства, кіберполіція також регулярно інформує про його нові прояви й надає рекомендації, як не потрапити на гачок шахраїв.

7.2. ІНСТИТУЦІЙНА СТРУКТУРА ДЛЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

До основних установ та ініціатив, спрямованих на боротьбу з дезінформацією в Україні, належать такі:

- **Центр протидії дезінформації (ЦПД)** — робочий орган РНБО, утворений відповідно до рішення РНБО від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію указом Президента України від 19 березня 2021 року № 106.

Варто наголосити, що ЦПД не має статусу виконавчого органу влади або права проводити перевірки чи застосовувати санкції. Його основна роль полягає в координуванні дій із боротьби з дезінформацією та формуванні політик у цій сфері, насамперед:

- проведення аналізу й моніторингу подій, явищ і загроз в інформаційному просторі України, стану інформаційної безпеки й присутності України у світовому інформаційному просторі;

- забезпечення РНБО, секретаря РНБО інформаційно-аналітичними матеріалами й пропозиціями щодо питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

- участь у розбудові системи стратегічних комунікацій, організації та координації заходів із її розвитку;

- участь у розробленні й реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефективності заходів із протидії дезінформації;

- участь у створенні інтегрованої системи оцінювання інформаційних загроз й оперативного реагування на них;

- розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру;

- сприяння взаємодії держави та інституцій громадянського суспільства для протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційно-просвітницьких заходах із питань підвищення медіаграмотності суспільства;

- вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій із протидії дезінформації та підготовка пропозицій щодо його використання в Україні.

Приклади діяльності ЦПД для підвищення інформаційної безпеки:

- Спростування. ЦПД регулярно спростовує та пояснює мотивацію поширення російської дезінформації та маніпуляцій. Приклади розвінчання неправдивої інформації: нібито мінування берегів річки Тиса, щоб запобігти втечі чоловіків мобілізаційного віку за кордон; блокування українськими військовими евакуації цивільних із Вовчанська, щоб використовувати їх як «живий щит»; пояснення російської маніпуляції про відсутність оборонних рубежів на Харківщині тощо.

- Статті. Фахівці ЦПД готують статті, які торкаються важливих суспільно-політичних питань, зокрема у сфері протидії дезінформації. Наприклад, «Як ЄС буде протидіяти російській дезінформації», «Навіщо Росія звинувачує в теракті [у концертному залі «Крокус Сіті Хол»] Україну» тощо.

- Подкасти. У форматі подкасту «ДезінFAKEція» спеціалісти ЦПД періодично обговорюють основні події інформаційної частини російсько-української війни, як-от фейки та маніпуляції про відклю-

чення електроенергії, провокації щодо оновлення українцями даних у ТЦК, залякування світу ядерною зброєю Росії тощо.

- Виявлені загрози. ЦПД постійно моніторить й аналізує загрози, які несе російська дезінформація, та описує їх. Наприклад, фахівці визначили, як Росія використовує «молодіжні форуми» для поширення пропаганди на тимчасово окупованих територіях, як Росія просуває свою пропаганду в ООН під виглядом захисту прав людини, які проросійські наративи просуваються в медіа Глобального Півдня (Близький Схід) тощо.

- Звіти. Фахівці ЦПД регулярно публікують аналітичні звіти, у яких висвітлюють різні аспекти дезінформаційних кампаній Росії. Опубліковані звіти стосувалися таких тем, як дискредитація українських біженців, канали поширення ворожої пропаганди в соцмережі X і TikTok, інформаційний вплив Росії в Німеччині тощо.

- **Центр стратегічних комунікацій та інформаційної безпеки** (далі — ЦСКІБ) — державний механізм протидії дезінформації, створений у березні 2021 року при Міністерстві культури та інформаційної політики України (далі — МКІП).

ЦСКІБ працює за трьома напрямами:

- розбудова стратегічних комунікацій — напрацювання наративів для зміцнення позицій України з тем, які найбільше таргетує агресор; розроблення меседжів для скоординованої державної комунікації; об'єднання зусиль держави й громадського сектору для скоординованої протидії дезінформації;

- протидія дезінформації та формування стійкості до неї — створення онлайн-ресурсу, який забезпечує реагування на інформаційні загрози, єдину базу інформаційної присутності агресора, доступ до інструментів із формування стійкості, підтримку українських наративів; проведення інформаційних кампаній; формування публічного майданчика для обговорення проблем і розроблення рішень із протидії дезінформації;

- об'єднання зусиль зі світом — регулярне інформування про гібридну агресію РФ; розбудова співпраці з країнами, що мають однакові з Україною інформаційні загрози; розроблення механізмів протидії дезінформації спільно з партнерами.

Приклади діяльності ЦСКІБ для підвищення інформаційної безпеки:

- «Школа протидії дезінформації». У створеній при ЦСКІБ школі державні службовці вивчають стратегічні комунікації, кризові комунікації та протидію дезінформації. У межах активностей школи відбулося понад 100 тренінгів, участь у яких узяло більш як 1000 осіб.

- Спростування фейків. ЦСКІБ веде активну діяльність у сфері протидії російській дезінформації та спростування фейків, поширюваних в умовах російської агресії. Так, були спростовані такі російські фейки: «Українські спецслужби причетні до замаху на Дональда Трампа», «Київ влаштував постановку із закривавленим лікарем "Охматдиту"», «Зеленський обкрадає фронт і вводить в оману Захід» тощо.

- Посібник з основних аспектів протидії російській дезінформації. Команда ЦСКІБ спільно із Центром демократії та верховенства права створила посібник «Гібридна війна Росії проти України. Як перемогти на інформаційному фронті».

- Дослідження. Фахівці ЦСКІБ регулярно проводять дослідження у сфері інформаційної безпеки, наприклад «"Київ за три дні", "брудна бомба" і "другий Сталінград": як змінювалася російська пропаганда за два роки повномасштабної війни». Ще один приклад — спільне дослідження ЦСКІБ і Центру демократії та верховенства права про російську дезінформацію в соцмережах «Як Росія атакує Україну дезінформацією через рекламу в Facebook».

- Моніторинги й розслідування. У межах моніторингу російської дезінформації і пропагандистських наративів ЦСКІБ публікує щоденні дайджести ворожої пропаганди. Окрім того, фахівці вивчають методи і способи поширення російської пропаганди й пояснюють їх у своїх матеріалах: «Про що ворожать російські тарологи під час війни», «Реальні фото і фейкові новини: як російська пропаганда вигадала "жіночий батальйон "Білосніжка"» тощо.

- **Національний проєкт із медіаграмотності «Фільтр».** Це проєкт МКІП, створений у 2021 році для підвищення медіаграмотності громадян. Його мета — згуртувати зусилля

державних установ, громадського сектору, міжнародних організацій і медіаспільноти для поліпшення знань українців у сфері медіаграмотності.

Приклади активностей «Фільтра» для підвищення інформаційної безпеки:

- Каталог матеріалів для медіаосвіти. На сайті «Фільтра» створено окремий розділ, що класифікує доступні посібники, відеозаписи, комікси та інші інтерактивні матеріали з підвищення рівня інформаційної грамотності для різних категорій населення: учителів та учнів, батьків, викладачів та студентів, журналістів, а також загальної аудиторії — для всіх.

- Карта перевірених джерел інформації. У межах активностей «Фільтра» розроблено спеціальний ресурс, що містить широкий перелік перевірених медіа — як загальнонаціональних, так і місцевих — у різних областях України.

- Стратегія медіаграмотності. У червні 2024 року «Фільтр» разом із МКІП презентував Стратегію Міністерства культури та інформаційної політики України з розвитку медіаграмотності на період до 2026 року. Цей документ має стати стратегічним і концептуальним орієнтиром на майбутнє. Його мета — збільшення стійкості українського суспільства в умовах дезінформації, забезпечення відповідального використання медійного контенту, а також підвищення рівня критичного мислення та загального добробуту громадян через здатність ухвалювати обдумані рішення.

Важливо, що в стратегії окремими блоками йдуть питання інформаційної / медіаграмотності та цифрової грамотності. Цифрова грамотність передбачає використання правил цифрової гігієни в повсякденному житті й розвиває такі компетенції:

- здатність захищати персональні дані й приватність;
- розуміння впливу алгоритмів соціальних мереж і налаштувань браузерів на підбір інформації, яку споживає людина;
- уміння розрізняти безпечні медіасервіси та середовища;
- уміння захистити себе від шахрайств і зловживань в інтернеті;
- розуміння роботи штучного інтелекту, можливостей і загроз, які він становить;
- уміння застосовувати цифрові технології для участі в житті суспільства;
- застосування цифрового етикету під час користування медіасервісами.

8. МІЖНАРОДНИЙ ВИМІР ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТА ІНФОРМАЦІЙНОЇ СТІЙКОСТІ УКРАЇНИ

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ ПРИДІЛЯЄ ПІДВИЩЕНУ УВАГУ НАПРЯМУ ЗОВНІШНЬОПОЛІТИЧНОЇ ДІЯЛЬНОСТІ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ. МЕТА УКРАЇНИ — ПОГЛИБЛЕННЯ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ ШЛЯХОМ УНІФІКАЦІЇ ПІДХОДІВ, МЕТОДІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ З УСТАЛЕНИМИ ПРАКТИКАМИ ЄС І НАТО, ВЖИТТЯ ІНШИХ УЗГОДЖЕНИХ ІЗ КЛЮЧОВИМИ ІНОЗЕМНИМИ ПАРТНЕРАМИ ЗАХОДІВ, СПРЯМОВАНИХ НА ПОСИЛЕННЯ КІБЕРСТІЙКОСТІ УКРАЇНИ, РОЗВИТОК СПРОМОЖНОСТЕЙ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ У КІБЕРПРОСТОРІ.

СТРАТЕГІЯ ПЕРЕДБАЧАЄ, ЩО УКРАЇНА СПІВПРАЦЮВАТИМЕ З МІЖНАРОДНИМИ ПАРТНЕРАМИ, ОРГАНІЗАЦІЯМИ Й ІНШИМИ ЗАІНТЕРЕСОВАНИМИ СТОРОНАМИ, ЯКІ ПОДІЛЯЮТЬ СПІЛЬНЕ БАЧЕННЯ МАЙБУТНЬОГО КІБЕРПРОСТОРУ ЯК ГЛОБАЛЬНОГО, ВІДКРИТОГО, ВІЛЬНОГО, СТАБІЛЬНОГО ТА БЕЗПЕЧНОГО, В ОСНОВІ ЯКОГО ДОТРИМАННЯ ПРАВ ЛЮДИНИ, ОСНОВНИХ СВОБОД І ДЕМОКРАТИЧНИХ ЦІННОСТЕЙ, ЩО Є ЗАПОРУКОЮ СОЦІАЛЬНО-ЕКОНОМІЧНОГО ТА ПОЛІТИЧНОГО РОЗВИТКУ УКРАЇНИ.

УКРАЇНА ЗОБОВ'ЯЗУЄТЬСЯ НАДАЛІ ПІДТРИМУВАТИ АКТИВНУ УЧАСТЬ У МІЖНАРОДНОМУ ДІАЛОЗІ З ПИТАНЬ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ ДЕРЖАВ У КІБЕРПРОСТОРІ НА ОСНОВІ ДОТРИМАННЯ ПРИНЦИПІВ МІЖНАРОДНОГО ПРАВА, СТАТУТУ ООН, А ТАКОЖ НОРМ, ПРАВИЛ І ПРИНЦИПІВ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ ДЕРЖАВИ.

8.1. КООПЕРАЦІЯ З МІЖНАРОДНИМИ ПАРТНЕРАМИ У СФЕРІ КІБЕРБЕЗПЕКИ

8.1.1. СПІВПРАЦЯ З ЄС ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ

Кібердіалоги. З 2021 року Україна і ЄС спільно провели три раунди кібердіалогу з метою поглиблення кооперації у сфері забезпечення кібербезпеки й адаптації законодавства України до законодавства ЄС:

- Перший раунд (червень 2021). Україна та ЄС обмінялися інформацією про інституційну структуру й повноваження органів у сфері кіберпростору. Сторони також обговорили оновлення Директиви ЄС про безпеку мережевих та інформаційних систем (Директива NIS) і зусилля України в розробленні політик і законодавства у сфері кібербезпеки, узгоджених із правовою та інституційною базами ЄС.
- Другий раунд (вересень 2022). На тлі повномасштабної російської агресії учасники діалогу підкреслили важливість подальшої співпраці для нарощування стійкості до кіберзагроз. ЄС виділив Україні 29 мільйонів євро для посилення її кіберстійкості. Сторони продовжили діалог про гармонізацію українського законодавства про кібербезпеку з відповідними стандартами ЄС (зокрема, оновленнями Директиви NIS).
- Третій раунд (липень 2024). Учасники діалогу обмінялися інформацією про досвід та виклики у сфері кібербезпеки, а також продовжили ділитися новинами про узгодження законодавства України з нормативно-правовою базою ЄС, зокрема Директивою NIS 2. Директива набрала чинності в січні 2023 року, і країни

ЄС повинні імплементувати її до жовтня 2024 року. Вона передбачає імплементацію правових заходів для підвищення загального рівня кібербезпеки в ЄС, як-от: створення спеціальної групи реагування на інциденти комп'ютерної безпеки (CSIRT) і компетентного національного органу з мережевих та інформаційних систем (NIS); гармонізація національних стратегій кібербезпеки, вимог до безпеки і звітування; посилення співпраці між державами-членами ЄС для управління кібербезпекою (EU-CyCLONe); запровадження більшої кількості стандартів кібербезпеки для об'єктів критичної інфраструктури й приватних компаній, які підпадають під сферу дії директиви; посилення співпраці між державами й приватним сектором у сфері кібербезпеки тощо.

Україні потрібно буде оновити законодавство відповідно до підходів NIS 2, зокрема вимоги кібербезпеки до об'єктів критичної інфраструктури та окремих приватних компаній, механізмів звітування та обміну інформацією, поглибленої співпраці з державами ЄС тощо.

Співпраця з ENISA. У листопаді 2023 року Національний координаційний центр кібербезпеки та Адміністрація Держспецзв'язку уклали Угоду про співпрацю з Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA). Укладена угода спрямована на обмін найкращими практиками, підвищення рівня обізнаності про загрози в кіберпросторі й розбудову спроможностей.

Угода з ENISA — додатковий компонент підтримки України в посиленні її кіберстійкості та захисті від російських кібератак. Вона є довгостроковою та передбачає співпрацю за такими напрямами:

- підвищення обізнаності й розбудова потенціалу для зміцнення кіберстійкості: навчання та тренінги з кібербезпеки на рівні ЄС, обмін засобами й програмами для підвищення обізнаності у сфері кібербезпеки;
- обмін найкращими практиками для гармонізації українського законодавства зі стандартами ЄС, як-от вищезгаданою Директивою NIS 2;
- систематичний обмін знаннями та інформацією для підвищення загальної обізнаності про ландшафт кіберзагроз.

Створення кіберлабораторії та кіберкласу. ЄС через Європейський фонд миру підтримує зміцнення кібербезпекового потенціалу Збройних Сил України. Так, ЄС виділив 3 мільйони євро для створення кіберлабораторії та кіберкласу:

- кіберлабораторія дозволяє створити реалістичне онлайн-середовище для навчання, проведення тренінгів і досліджень, щоб військові Збройних Сил України могли відпрацьовувати навички реагування на кібератаки в режимі реального часу;
- кіберклас надає 15 робочих місць і необхідне програмне й апаратне забезпечення для проведення навчань і виконання вправ із кіберзахисту.

Проєкт очолює Академія електронного управління (eGA), а кіберлабораторія та навчання з кібербезпеки були реалізовані у співпраці з компанією «CybExer Technologies».

8.1.2. СПІВПРАЦЯ З НАТО ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ

Об'єднаний центр передових технологій із кібероборони НАТО (NATO CCDCOE). Заснований у 2008 році зі штаб-квартирою в Таллінні, один із провідних центрів НАТО координує різноманітні ініціативи, навчальні та освітні рішення, спрямовані на захист інформаційних систем у кіберпросторі. CCDCOE також розробив Талліннський посібник (його кілька разів переглядали й оновлювали) — провідну академічну працю, у якій досліджені питання застосування міжнародного права до кібернетичних війн.

До CCDCOE входять як окремі країни-члени НАТО, так і держави поза Альянсом, які поділяють спільні принципи й бачення гарантування кібербезпеки.

Україна стала учасником-контрибутором CCDCOE в березні 2022 року, а вже через рік — у травні 2023 — офіційно приєдналася до нього на правах повноцінного учасника. Це дозволяє проводити спільні дослідження, навчання й обмінюватися досвідом і найкращими практиками в царині кібербезпеки.

Так, у квітні 2024 року стало відомо, що Україна вперше стане учасником найбільших у світі навчань із кібербезпеки «Locked Shields 2024», що проводяться під егідою CCDCOE. У цьогорічних навчаннях візьмуть участь близько 4000 експертів із понад 40 країн, перед якими стоятиме завдання захистити інфраструктуру вигаданої країни в умовах, наближених до реальних. Участь у цих навчаннях — важливий крок для України й демонструє її прагнення до міжнародної співпраці у сфері кібербезпеки.

Перевірка систем кібербезпеки за стандартами, які використовуються в країнах НАТО. У липні 2024 року Міністерство оборони України повідомило, що вперше в історії України військова система «DELTA» успішно пройшла діагностику кібербезпеки за стандартами рівня НАТО. «DELTA» — це військова система, що дає змогу планувати операції й спостерігати за подіями на полі бою в режимі реального часу. Вона забезпечує обмін інформацією в межах підрозділу, бригади, угруповання, а за потреби також із союзниками.

Сертифікація системи «DELTA» проходила півтора місяця. У процесі було проаналізовано 162 заходи захисту інформації, використані в ній. Встановлено, що система побудована на сучасних технологіях і відповідає стандартам НАТО щодо кіберзахисту.

Візити до штаб-квартир та органів НАТО для посилення кооперації з кібербезпеки. Делегації українських установ, що займаються кібербезпекою, періодично здійснюють візити до органів НАТО з метою обміну інформацією та досвідом.

Так, у липні 2023 року делегація представників основних суб'єктів забезпечення кібербезпеки України відвідала штаб-квартиру НАТО, Командування НАТО з операцій та Агенцію НАТО зі зв'язку та інформації в межах проєкту з обміну знаннями С4 Трастового фонду Комплексного пакета допомоги НАТО-Україна.

До складу делегації ввійшли представники НКЦК, Служби безпеки України, Держспецзв'язку, Міністерства оборони України, Збройних Сил України, Департаменту кіберполіції Національної поліції України та Офісу Генерального прокурора.

За сприяння Управління нових викликів безпеці штаб-квартири НАТО та Місії України при НАТО делегація мала нагоду познайомитися зі структурами НАТО, що займаються кібербезпекою. Українські учасники виступили з оглядовою презентацією про систему кібербезпеки України та уроки, отримані під час тривалої кібервійни з Росією. Також було представлено пропозиції щодо поглиблення майбутньої співпраці з НАТО у сфері кібербезпеки.

8.1.3. МІЖДЕРЖАВНА СПІВПРАЦЯ ЗАДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

З огляду на значну кількість фішингових атак та інших кіберзлочинів в українському кіберпросторі (частина яких здійснюється не з території України або ж торкається кількох країн) доцільно розглянути кооперацію України з іншими державами для протидії цим та іншим загрозам.

Для посилення боротьби з кіберзлочинністю Україна ратифікувала Конвенцію про кіберзлочинність — перший подібний міжнародний договір для боротьби зі злочинністю на просторах інтернету. Цей документ, початково відкритий для підписання у 2001 році, набрав чинності в Україні у 2006 році.

Цього ж року Україна ратифікувала Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, учинених через комп'ютерні системи (набрав чинності у 2007 році). А у 2022 році Україна підписала (але ще не ратифікувала) Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленого співробітництва та розкриття електронних доказів.

8.2. КООПЕРАЦІЯ З МІЖНАРОДНИМИ ПАРТНЕРАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

8.2.1. СПІВПРАЦЯ З ЄС ДЛЯ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ

EUvsDisinfo. У ЄС віддавна активно борються з дезінформацією, зокрема російською. Один із провідних європейських проєктів для протидії дезінформації — «EUvsDisinfo». Його розпочали у 2015 році для виявлення, аналізу й підвищення обізнаності про різні форми дезінформації — насамперед російської. Схожою діяльністю займаються українські ЦСКІБ, ЦПД та деякі інші установи.

«EUvsDisinfo» разом із Міністерством закордонних справ Естонської Республіки та МКІП, Міністерством закордонних справ України та ГО «BRAND UKRAINE» ініціювали кампанію «Nations Against Disinformation». Вона спрямована на підвищення рівня обізнаності про небезпеку та негативні наслідки для суспільства, які несе дезінформація, зокрема російська. У межах цієї активності партнери також обмінюються найкращими практиками протидії дезінформації на спільних між-

народних заходах, конференціях, вебінарах і майстер-класах.

Конференції, форуми. Одним із важливих кроків у розвитку спільного бачення важелів і способів протидії дезінформації є обговорення актуальних проблем, пов'язаних із розповсюдженням дезінформації, під час публічних заходів, конференцій і форумів.

Так, у грудні 2022 року в Брюсселі пройшла конференція «Протидія російським фальшивим наративам — Форум Україна-ЄС з протидії дезінформації». Вона мала на меті привернути увагу європейських політиків, науковців, експертів та ЗМІ до інформаційної війни Росії проти України та Європи. Іншим важливим аспектом стало обговорення найкращих практик протидії російській дезінформації та вироблення плану спільних дій. До заходу долучилися, зокрема, представники Оперативної робочої групи зі стратегічних комунікацій, що вивчають поширення російської дезінформації.

Домовленості з окремими країнами-членами ЄС. У жовтні 2023 року медіарегулятори Латвії, Литви, Польщі, Румунії та України підписали спільну декларацію про співпрацю і взаємну підтримку в питаннях протидії дезінформації.

Країни-учасники домовилися надавати одна одній підтримку у сфері аналізу та стримування розповсюдження багатовимірної дезінформації, зокрема російської, на національному, регіональному й міжнародному рівнях. Вони намагатимуться розробити спільні позиції й оцінки у сфері протидії дезінформації.

Декларація також передбачає організацію спільних заходів для навчання громадян, як виявити, реагувати й запобігати дезінформації. Це робитиметься через освітні кампанії, тренінги, семінари та співпрацю європейських і національних платформ фактчекінгу.

Схожі домовленості щодо об'єднання зусиль для боротьби з пропагандою й зміцнення інформаційної безпеки містяться в багатьох нещодавно укладених двосторонніх угодах про співпрацю у сфері безпеки між Україною та іншими державами-членами ЄС, наприклад Німеччиною та Польщею.

8.2.2. СПІВПРАЦЯ З НАТО ДЛЯ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ

Комітет з питань стратегічних комунікацій Ради Україна-НАТО. Активізація співпраці у сфері стратегічних комунікацій між Україною і НАТО вийшла на якісно новий рівень у березні 2024 року. Тоді у штаб-квартирі НАТО в Брюсселі пройшло установче засідання Комітету з питань стратегічних комунікацій Ради Україна-НАТО.

Під час засідання представники української делегації розповіли про роботу України у сфері забезпечення інформаційної безпеки, боротьби з російською дезінформацією та пропагандою. Підвищену увагу приділили механізмам донесення правдивої інформації до населення на тимчасово окупованих територіях.

Союзники НАТО підтвердили свою готовність підтримувати Україну, зокрема в боротьбі з російською дезінформацією та пропагандою. Ця співпраця є взаємовигідною, адже Україна може ділитися з державами-учасниками НАТО своїм унікальним досвідом у веденні успішних комунікацій і протидії дезінформації під час війни.

Співпраця та партнерство у сфері стратегічних комунікацій з НАТО важливі для України, адже це допоможе:

- ефективніше протидіяти російській дезінформації та пропаганді, краще захищати власну інформаційну безпеку;
- підвищити обізнаність про Україну та НАТО й посилити до них довіру на міжнародній арені;
- укотре підтримати євроатлантичні прагнення України.

Платформа НАТО-Україна з протидії гібридній війні. Один із пріоритетів діяльності НАТО — протидія гібридним загрозам, зокрема дезінформації та пропаганді. Щоб сприяти обміну досвідом у цій сфері, на саміті НАТО у Варшаві 2016 року започаткували платформу НАТО-Україна з протидії гібридній війні. Цей майданчик для зустрічей покликаний поглиблювати співпрацю у сфері виявлення і протидії гібридним загрозам, як-от дезінформації, задля підвищення стійкості.

У межах активностей платформи періодично організовуються експертні зустрічі, коли фахівці обох сторін обмінюються досвідом і найкращими практиками протидії різним гібридним загрозам. Одна з таких експертних зустрічей відбулася у листопаді 2023 року в Молдові. Серед питань для обговорення були виклики, пов'язані з ефективною організацією стратегічних комунікацій і протидією дезінформації.

8.3. РЕКОМЕНДАЦІЇ ДЛЯ ВДОСКОНАЛЕННЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА У СФЕРІ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ Й ДЕЗІНФОРМАЦІЇ

8.3.1. РЕКОМЕНДАЦІЇ ДЛЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Українському законодавству у сфері кібербезпеки наразі бракує ефективності в координації зусиль між різними державними органами. Не вистачає чітко визначеної й систематизованої державної політики.

Зокрема, це проявляється таким чином:

- **Брак системного підходу.** Незважаючи на наявність багатьох нормативно-правових інструментів, які визначають повноваження й компетенції різних установ у сфері кібербезпеки, наразі бракує більш цілісної, ефективної системи управління і взаємодії між державними органами. Іноді їхні повноваження перетинаються. За певних обставин це може призводити до проблем у координуванні їхніх дій та ускладнювати розроблення і реалізацію спільних заходів для протидії кіберзагрозам.

- **Брак регламентації партнерства між державою й приватним сектором.** В Україні ще не сформовано чіткої системи співпраці між державним і приватним сектором для обміну інформацією, спільного планування та реалізації захисних проєктів.

- **Недостатня відповідність українського законодавства про кібербезпеку положенням Директиви NIS 2**. Хоча це відносно нова директива і навіть держави-члени ЄС мають час ще до жовтня 2024 року, щоб її повністю імплементувати, узгодження національної нормативно-правової бази України з Директивою NIS 2 — важливий крок у контексті євроінтеграційних прагнень України.

Для вдосконалення ситуації можна запропонувати такі кроки:

- **Внесення змін до законодавства про кібербезпеку.** Оновлення наявних нормативно-правових документів для забезпечення чіткої, узгодженої політики й зміцнення міжвідомчої координації.

- **Активізація партнерства між державою й приватним сектором.** Розроблення прозорих та ефективних процедур для залучення приватного сектору до стратегій національної кібербезпеки, включно з підтримкою інновацій та обміном даними.

- **Гармонізація національного законодавства з підходами NIS 2.** Ідеться, зокрема, про кібербезпекові вимоги до об'єктів критичної інфраструктури та окремих приватних компаній, механізмів звітування та обміну інформацією, поглибленої співпраці з державами ЄС тощо.

8.3.2. ПОТЕНЦІЙНІ КРОКИ ДЛЯ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ НА ДЕРЖАВНОМУ РІВНІ

Для ефективної боротьби з дезінформацією важливо мати певне розуміння цього явища в законодавстві з урахуванням захисту свободи слова і захисту від цензури. Оскільки наразі не існує єдиного підходу до інтерпретації дезінформації ані в Україні, ані на міжнародній арені, можна розпочати з визначення критеріїв дезінформації, адже без цього її іноді важко ефективно ідентифікувати та протидіяти їй.

Викладені нижче рекомендації можуть сприяти вдосконаленню підходів України в цій галузі:

- **Юридичне визначення критеріїв дезінформації.** Важливо закріпити в законодавстві критерії дезінформації з огляду на міжнародні стандарти в цій галузі.

- **Програми медіаграмотності з елементами кібербезпеки.** Потрібно розширити освітні програми для різних груп населення, зокрема обов'язкові курси для держслужбовців, співробітників критичної інфраструктури тощо. У програми медіаграмотності слід обов'язково закладати елементи цифрової безпеки.

- **Активізація партнерства між державою й приватним сектором.** Варто сприяти новим спільним ініціативам державно-приватного партнерства у сфері кібербезпеки та боротьби з дезінформацією.

Ці рекомендації допоможуть краще розвинути нормативно-правову базу й підходи до регулювання та протидії дезінформації крізь призму кібербезпеки.

ВИСНОВКИ

НА ТЛІ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ РОСІЯ СИНХРОНІЗУЄ КОНВЕНЦІЙНІ БОЙОВІ ДІЇ З КІБЕРАТАКАМИ ТА ДЕЗІНФОРМАЦІЙНИМИ КАМПАНІЯМИ, ЩОБ ЗАБЕЗПЕЧИТИ ЯКНАЙБІЛЬШ ДЕСТРУКТИВНИЙ ВПЛИВ НА ЦИФРОВИЙ ТА ІНФОРМАЦІЙНИЙ ПРОСТОРИ УКРАЇНИ. У ЦЬОМУ ДОСЛІДЖЕННІ ВИСВІТЛЕНА СКЛАДНА Й БАГАТОГРАННА ПРИРОДА ТАКИХ ВИКЛИКІВ.

Проаналізувавши широкий спектр кібератак крізь призму дезінформації, ми дійшли висновку, що захист від таких загроз вимагає інтегрованих зусиль, які охоплюють технічні, правові та освітні аспекти.

Вивчення кіберзагроз крізь призму дезінформації, зокрема зламу і клонування сайтів, фішингу, DDoS-атак та глушіння супутникових сигналів, показало, що такі атаки можуть мати серйозний вплив на цифрову та інформаційну екосистеми України, особливо в умовах перманентної агресії з боку Росії. Виявлення та аналіз методів, які використовують зловмисники, мають ключове значення для розроблення ефективних стратегій захисту та відповідей на ці загрози.

Основні рекомендації для протидії кіберзагрозам і дезінформації:

- удосконалювати державні процеси регулювання кібербезпеки для налагодження ефективніших механізмів співпраці між держустановами, відповідальними за гарантування кібербезпеки;
- покращувати механізми взаємодії між державним і приватним секторами для обміну інформацією і найкращими практиками з протидії кіберзагрозам і дезінформації;
- запроваджувати сучасні технологічні рішення для захисту кібернетичних та інформаційних систем;
- гармонізувати національне законодавство з кібербезпеки зі стандартами ЄС у цій сфері, зокрема Директивою NIS 2;
- затвердити юридично визначені критерії поняття «дезінформація»;
- підвищувати рівень цифрової та медіаграмотності населення.

Зрештою, забезпечення кібербезпеки та боротьба з дезінформацією — це постійний процес, який вимагає перманентної активної участі всіх зацікавлених сторін. Тільки спільними зусиллями можна досягти стійкості цифрового й інформаційного просторів і захистити суспільство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Європейська правда, 2023. Україна домовилася з чотирма країнами ЄС разом боротися з дезінформацією. URL: https://www.eurointegration.com.ua/news/2023/10/5/7170826/

2. Інститут масової інформації, 2022. Російські хакери атакували сайт «Детектора медіа». URL: https://imi.org.ua/news/rosijski-hakery-atakuvaly-sajt-detektora-media-i49301

3. Інститут масової інформації, 2023. РБК-Україна звернувся до кіберполіції через підробку сайту та фейкову статтю з критикою Залужного. URL: https://imi.org.ua/news/rbk-ukrayina-zvernuvsya-do-kiberpolitsiyi-cherez-pidrobku-sajtu-ta-fejkovu-stattyu-z-krytykoyu-i51458

4. Інститут масової інформації, 2023. Сайт IMI зазнав DDoS-атаки. URL: https://imi.org.ua/news/sajt-imi-zaznav-ddos-ataky-i55175

5. Інститут масової інформації, 2023. У мережі з'явився фейковий сайт УП з вигаданою колонкою Казаріна. URL: https://imi.org.ua/news/u-merezhi-z-yavyvsya-fejkovyj-sajt-up-z-vygadanoyu-kolonkoyu-kazarina-i52050

6. Інститут масової інформації, 2024. Білий список: 11 медіа, що стали найякіснішими. URL: https://imi.org.ua/news/bilyj-spysok-11-media-shho-staly-najyakisnishymy-i60964

7. Інститут масової інформації, 2024. УП заявила про DDoS-атаку, але сайт вже працює. URL: https://imi.org.ua/news/up-zayavyla-pro-ddos-ataku-ale-sajt-vzhe-pratsyuye-i58722

8. Інститут масової інформації, 2024. Хакери атакували сайт Цензор.Нет щонайменше шість годин. URL: https://imi.org.ua/news/hakery-atakuvaly-sajt-tsenzor-net-shhonajmenshe-shist-godyn-i58432

9. Ірина Гамалій, 2023. Наразі відбувається кібератака на державні ресурси України. URL: https://lb.ua/society/2023/03/17/549163_narazi_vidbuvaietsya_kiberataka.html

10. Ірина Лисогор, 2022. Хакери атакували сайти уряду та «Дію». URL: https://lb.ua/society/2022/01/14/503059_hakeri_atakuvali_sayti_uryadu_diyu.html

11. Аніта Прасад, 2024. Росія атакувала супутникове мовлення України, трансляцію кількох десятків каналів призупинено. URL: https://forbes.ua/news/rosiya-atakuvala-suputnikove-movlennya-ukraini-translyatsiya-kilkokh-desyatkiv-kanaliv-prizupinena-17042024-20616

12. Богдан Миколайчук, 2023. Епідемія дезінформації: чому фейки стали частиною нашого життя і як «вакцинуватися». URL: https://cedem.org.ua/analytics/epidemiya-dezinformatsiyi/

13. Володимир Зеленський (zelenskyy_official). Пост в Instagram. URL: https://www.instagram.com/p/CgRjvSHoty1/

14. Віра Олійник, 2024. Сайт dev.ua зазнав потужної DDoS-атаки. URL: https://ain.ua/2024/05/15/sajt-dev-ua-zaznav-ddos-ataky/

15. Департамент кіберполіції Національної поліції України, 2023. Звіт про результати роботи Департаменту кіберполіції у 2022 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/

16. Департамент кіберполіції Національної поліції України, 2024. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/

17. Департамент кіберполіції Національної поліції України. Система електронного звернення громадян. URL: https://ticket.cyberpolice.gov.ua/

18. Державний центр кіберзахисту Держспецзв'язку, 2024. Державний центр кіберзахисту збільшує технічні спроможності Національного центру резервування державних інформаційних ресурсів. URL: https://scpc.gov.ua/uk/articles/362

19. Держспецзв'язку, 2022. Україна стане учасником-контрибутором Об'єднаного центру передових технологій з кібероборони НАТО (ОЦПТКО НАТО). URL: https://cip.gov.ua/ua/news/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe

20. Держспецзв'язку, 2022. Україна та ЄС провели другий раунд діалогу з питань кібербезпеки. URL: https://cip.gov.ua/ua/news/ukrayina-ta-yes-proveli-drugii-raund-dialogu-z-pitan-kiberbezpeki

21. Держспецзв'язку, 2023. Протидія спільним загрозам: представник Держспецзв'язку взяв участь в експертній зустрічі в межах Платформи Україна-НАТО. URL: https://cip.gov.ua/ua/news/protidiya-spilnim-zagrozam-predstavnik-derzhspeczv-yazku-vzyav-uchast-v-ekspertnii-zustrichi-v-mezhakh-platformi-ukrayina-nato

22. Держспецзв'язку, 2023. Українські фахівці з кібербезпеки здійснили візит до штаб-квартири та низки органів НАТО. URL: https://cip.gov.ua/ua/news/ukrayinski-fakhivci-z-kiberbezpeki-zdiisnili-vizit-do-shtab-kvartiri-ta-nizki-organiv-nato

23. Держспецзв'язку, 2023. Уряд ухвалив Порядок проведення Bug Bounty. URL: https://www.kmu.gov.ua/news/uriad-ukhvalyv-rozroblenyi-fakhivtsiamy-derzhspetszviazku-poriadok-provedennia-bug-bounty

24. Держспецзв'язку, 2024. Держспецзв'язку презентувала нові технічні рішення для захисту держустанов від DDoS-атак. URL: https://cip.gov.ua/ua/news/ssscip-presents-new-technical-solutions-to-protect-ukrainian-institutions-from-ddos-attacks

25. Держспецзв'язку, 2024. Держспецзв'язку презентувала нові технічні рішення для захисту держустанов від DDoS-атак. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-prezentuvala-novi-tekhnichni-rishennia-dlia-zakhystu-derzhustanov-vid-ddos-atak

26. Держспецзв'язку, 2024. Держспецзв'язку провела навчання з кібербезпеки для Міноборони та інших державних структур. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-provela-navchannya-z-kiberbezpeki-dlya-minoboroni-ta-inshikh-derzhavnikh-struktur

27. Держспецзв'язку, 2024. Держспецзв'язку та НКЦК презентували CyberTracker — інструмент для автоматичного моніторингу виконання Стратегії кібербезпеки України. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-ta-nkck-prezentuvali-cybertracker-instrument-dlya-avtomatichnogo-monitoringu-vikonannya-strategiyi-kiberbezpeki-ukrayini

28. Держспецзв'язку, 2024. Перший в Україні Кваліфікаційний центр інформаційних технологій та кібербезпеки розпочав сертифікацію спеціалістів. URL: https://cip.gov.ua/ua/news/the-first-information-technology-and-cybersecurity-qualification-center-in-ukraine-has-started-operations

29. Держспецзв'язку, 2024. Стратегія кібербезпеки України. URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini

30. Держспецзв'язку. Що таке DDoS-атака? URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka

31. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

32. Еспресо, 2024. Супутникові трансляції Еспресо атакують: в чому причина. URL: https://espreso.tv/espresotv-suputnikovi-translyatsii-espreso-atakuyut-v-chomu-prichina

33. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2022. Онлайн-шахрайство з використанням тематики «грошових виплат» (CERT-UA#5239). URL: https://cert.gov.ua/article/1545776

34. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2023. «Змініть пароль до Roundcube»: чергова фішингова атака з використанням атрибутів CERT-UA та символіки ДЦКЗ Держспецзв'язку (CERT-UA#7223). URL: https://cert.gov.ua/article/5455833

35. 35. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2023. Розсилання SMS-повідомлень з темою судових повісток з використанням шахрайського альфа-імені «SUDpovistka» (CERT-UA#6804). URL: https://cert.gov.ua/article/4789582

36. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2024. UAC-0184: Цільові атаки у відношенні українських військовослужбовців з використанням тематики рекрутингу до 3 ОШБр та ЦАХАЛ (CERT-UA#8386). URL: https://cert.gov.ua/article/6276988

37. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2024. АНОНС: Практичний семінар для кіберфахівців. URL: https://cert.gov.ua/article/6277896

38. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2018. Основні правила кібергігієни. URL: https://cert.gov.ua/recommendation/31

39. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2023. Фішингові атаки групи APT28 (UAC-0028) з метою отримання автентифікаційних даних до публічних поштових сервісів (CERT-UA#6975). URL: https://cert.gov.ua/article/5105791

40. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2024. Тематика голосування в месенджерах — новий спосіб викрадення акаунтів набирає обертів (CERT-UA#9688). URL: https://cert.gov.ua/article/6279491

41. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2024. Фактор кібербезпеки. URL: https://cert.gov.ua/article/6278274

42. Команда реагування на комп'ютерні надзвичайні події України CERT-UA, 2024. Щодо обстановки в сфері кібер на 23–24 лютого 2024 року. URL: https://cert.gov.ua/article/6277822

43. Команда реагування на комп'ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua/contact-us

44. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). URL: https://zakon.rada.gov.ua/laws/show/995_004

45. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575

46. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

47. Лабораторія цифрової безпеки, 2022. «Порушення правил фейсбука». URL: https://yak.dslua.org/phishing/porushennia-pravyl-feysbuka/

48. Лабораторія цифрової безпеки, 2023. Повідомлення «від підтримки Meta». URL: https://yak.dslua.org/phishing/povidomlennia-vid-pidtrymky-meta/

49. Міністерство оборони України, 2024. В Україні вперше перевірили кібербезпеку бойової системи за стандартами рівня НАТО. URL: https://www.mil.gov.ua/news/2024/07/17/v-ukraini-vpershe-perevirili-kiberbezpeku-bojovoi-sistemi-za-standartami-rivnya-nato/

50. Міністерство внутрішніх справ України, 2024. Кіберполіція застерігає: Як не стати жертвою онлайн-шахраїв. URL: https://www.kmu.gov.ua/news/kiberpolitsiia-zasterihaie-iak-ne-staty-zhertvoiu-onlain-shakhraiv

51. Міністерство закордонних справ України, 2021. Україна та ЄС започаткували Кібердіалог. URL: https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog

52. Міністерство культури та інформаційної політики України, 2021. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki

53. Міністерство культури та інформаційної політики України, 2024. Україна та НАТО працюватимуть над поглибленням співпраці у сфері стратегічних комунікацій. URL: https://www.kmu.gov.ua/news/ukraina-ta-nato-pratsiuvatymut-nad-pohlyblenniam-spivpratsi-u-sferi-stratehichnykh-komunikatsii

54. Міністерство культури та інформаційної політики України і Фільтр. Стратегія Міністерства культури та інформаційної політики України з розвитку медіаграмотності на період до 2026 року. URL: https://filter.mkip.gov.ua/wp-content/uploads/2024/06/the-strategy-of-the-ministry-of-culture-and-information-policy-of-ukraine-for-media-literacy-development-until-2026.pdf

55. Міністерство розвитку громад, територій та інфраструктури України. Законодавство у сфері кіберзахисту об'єктів критичної інформаційної інфраструктури. URL: https://mtu.gov.ua/content/zakonodavstvo-u-sferi-kiberzahistu-obektiv-kritichnoi-informaciynoi-infrastrukturi.html

56. Міністерство соціальної політики України, 2022. Відповіді на найпоширеніші запитання щодо виплат від міжнародних організацій. URL: https://www.msp.gov.ua/news/22077.html

57. Міністерство цифрової трансформації України, 2024. Мінцифри: Долучайтесь до Програми з кібердіагностики бізнесу, щоб безоплатно перевірити підприємство на вразливості до кібератак. URL: https://www.kmu.gov.ua/news/mintsyfry-doluchaites-do-prohramy-z-kiberdiahnostyky-biznesu-shchob-bezoplatno-pereviryty-pidpryiemstvo-na-vrazlyvosti-do-kiberatak

58. Надія Собенко, 2023. Хакери атакували сайти Суспільного. Атаку розслідує Держспецзв'язку. URL: https://suspilne.media/507837-hakeri-atakuvali-sajti-suspilnogo/

59. Наталія Данькова, 2024. Через атаку ворога призупинена трансляція каналів «1+1» та інших на супутнику Astra. URL: https://detector.media/rinok/article/225578/2024-04-17-cherez-ataku-voroga-pryzupynena-translyatsiya-kanaliv-1-1-ta-inshykh-na-suputnyku-astra/

60. Національний банк України та Департамент кіберполіції Національної поліції України. Проєкт #ШахрайГудбай. URL: https://promo.bank.gov.ua/stopfraud/

61. Національний координаційний центр кібербезпеки, 2023. Пост у Facebook. URL: https://www.facebook.com/ncsccUA/posts/pfbid0go6r1ZgFzq6qmBXEG7AXN2DLQbtT2KjuAjcXQWJnDuhzZovWYT5JdBy3BokDCHaSl

62. Олег Павлюк, 2024. Україна вперше візьме участь у найбільших навчаннях НАТО з кібербезпеки. URL: https://www.eurointegration.com.ua/news/2024/04/17/7184044/

63. Олена Ребрик, 2024. Громадське радіо продовжує відбиватися від потужних DDoS-атак. URL: https://hromadske.radio/news/2024/05/14/hromadske-radio-prodovzhuie-vidbyvatysia-vid-potuzhnykh-ddos-atak

64. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, 2021. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки — Звіт про роботу 2021. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf

65. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, 2022. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки — Звіт про роботу 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf

66. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, 2023. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки — Звіт про роботу 2023. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

67. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, 2023. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки — Звіт про роботу 2023 Q4. URL: https://scpc.gov.ua/api/files/3d552013-d5f6-4c75-9ea3-9e77b429d7a7

68. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, 2023. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки — Звіт про роботу 2023 Q1. URL: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710

69. Платформа прав людини, 2022. Війна у цифровому вимірі та права людини. URL: https://ppl.org.ua/wp-content/uploads/2022/11/Жовтень-2022-рік.pdf

70. Платформа прав людини, 2023. Війна у цифровому вимірі та права людини. URL: https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf

71. Платформа єДопомога. URL: https://aid.edopomoga.gov.ua /

72. Представництво Європейського Союзу в Україні, 2024. Європейський Союз посилює кіберзахист України. URL: https://www.eeas.europa.eu/delegations/ukraine/європейський-союз-посилює-кіберзахист-у-україні_uk?s=232

73. Представництво України при Європейському Союзі, 2022. Україна та ЄС синхронізують боротьбу з дезінформацією. URL: https://ukraine-eu.mfa.gov.ua/news/ukrayina-ta-yes-sinhronizuyut-borotbu-z-dezinformaciyeyu

74. Пресофіс Міністерства цифрової трансформації, 2023. За підтримки Мінцифри стартує програма безоплатного навчання спеціалістів з кібербезпеки. URL: https://thedigital.gov.ua/news/za-pidtrimki-mintsifri-startue-programa-bezoplatnogo-navchannya-spetsialistiv-z-kiberbezpeki

75. Про Концепцію боротьби з тероризмом в Україні. URL: https://zakon.rada.gov.ua/laws/show/53/2019

76. Про Центр протидії дезінформації. URL: https://zakon.rada.gov.ua/laws/show/187/2021

77. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

78. Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163

79. Про звернення громадян. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text

80. Про медіа. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

81. Про національну безпеку України. URL: https://zakon.rada.gov.ua/laws/show/2469-19

82. Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

83. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації». URL: https://zakon.rada.gov.ua/laws/show/106/2021

84. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

85. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/447/2021

86. Про створення Центру протидії дезінформації. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21

87. Про схвалення Концепції розвитку штучного інтелекту в Україні. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80/conv#Text

88. Про утворення територіального органу Національної поліції. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

89. Про інформацію. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

90. Прямий, 2024. Телеканал «Прямий» зазнав російської хакерської атаки. URL: https://prm.ua/telekanal-priamyy-zaznav-rosiyskoi-khakerskoi-ataky/

91. Рада економічної безпеки України і Держспецзв'язку, 2023. Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi

92. Рада національної безпеки і оборони України, 2023. Україна посилює співпрацю з ЄС у сфері кібербезпеки: НКЦК підписав Угоду про співпрацю з ENISA. URL: https://www.rnbo.gov.ua/ua/Diialnist/6706.htm |

93. Copyscape. URL: https://www.copyscape.com/

94. Служба безпеки України, 2023. СБУ зібрала докази державної зради ексведучої телеканалів Медведчука Діани Панченко, їй повідомлено про нову підозру. URL: https://ssu.gov.ua/novyny/sbu-zibrala-dokazy-derzhavnoi-zrady-eksveduchoi-telekanaliv-medvedchuka-diany-panchenko-yii-povidomleno-pro-novu-pidozru

95. Станіслав Погорілов, 2023. В мережі невідомі поширюють фейкові публікації від імені «Української правди»: УП звертається в СБУ. URL: https://www.pravda.com.ua/news/2023/04/10/7397275/

96. Суспільне, 2024. З росії намагались глушити сигнал Суспільного на супутнику. URL: https://corp.suspilne.media/newsdetails/9400

97. ТАВР Медіа — TAVR Media. Пост у Facebook. URL: https://www.facebook.com/tavrmedia/posts/pfbid0voE4Ft6pfrDKKQ5iyrkk11ydPtBYcZJsMAW3VW27HQQy3nn6cRyLUSLZysqsSNyHl

98. Угода про співробітництво у сфері безпеки між Україною та Республікою Польща. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-92009

99. Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною та Федеративною Республікою Німеччина. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-88985

100. Українська правда, 2022. Хакери атакували українське радіо і запустили фейк про госпіталізацію Зеленського. URL: https://x.com/ukrpravda_news/status/1550085098099380224?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1550085098099380224%7Ctwgr%5Ecfc4a7c4074eb9776b3e8beee7aaf2d4679084e2%7Ctwcon%5Es1_&ref_url=URL%3A+https%3A%2F%2Fwww.pravda.com.ua%2Fnews%2F2022%2F07%2F21%2F7359395%2F

101. Укрінформ, 2023. Україна офіційно приєдналася до Центру кіберзахисту НАТО. URL: https://www.ukrinform.ua/rubric-technology/3710022-ukraina-oficijno-priednalasa-do-centru-kiberzahistu-nato.html

102. Фільтр. Мапа перевірених джерел новин. URL: https://filter.mkip.gov.ua/mapa/

103. Фільтр. Медіаосвіта. URL: https://filter.mkip.gov.ua/#mediaosvita_yak

104. ЦЕДЕМ, 2024. Масштаб проблеми блокування соцмережами українських медіа, блогерів та користувачів (дані співпраці ЦЕДЕМ з Meta, 24 лютого 2022 — 5 травня 2024). URL: https://cedem.org.ua/library/meta-blokuvannya/

105. Центральне міжрегіональне управління Міністерства юстиції, 2024. Спільний фронт України та НАТО у боротьбі за правду. URL: https://centraljust.gov.ua/news/info/spilniy-front-ukraini-ta-nato-u-borotbi-za-pravdu

106. Центр протидії дезінформації, 2024. «ДезінFAKEція» (19 випуск). URL: https://cpd.gov.ua/announcement/dezinfakecziya-19-vypusk /

107. Центр протидії дезінформації, 2024. «ДезінFAKEція» (20 випуск). URL: https://cpd.gov.ua/announcement/dezinfakecziya-20-vypusk/

108. Центр протидії дезінформації, 2024. «ДезінFAKEція» (21 випуск). URL: https://cpd.gov.ua/announcement/dezinfakecziya-21-vypusk/

109. Центр протидії дезінформації, 2024. «ДезінFAKEція» (27 випуск). URL: https://cpd.gov.ua/announcement/dezinfakecziya-27-vypusk/

110. Центр протидії дезінформації, 2024. Аналітичний звіт «Інформаційний вплив рф у Німеччині». URL: https://cpd.gov.ua/reports/analitychnyj-zvitinformaczijnyj-vplyv-rf-u-nimechchyni/

111. Центр протидії дезінформації, 2024. Аналітичний звіт «Дискредитація українських біженців». URL: https://cpd.gov.ua/reports/analitychnyj-zvit-dyskredytacziya-ukrayinskyh-bizhenczіv/

112. Центр протидії дезінформації, 2024. Навіщо росія звинувачує в теракті Україну. URL: https://cpd.gov.ua/main/navishho-rosiya-zvynuvachuye-v-terakti-ukrayinu/

113. Центр протидії дезінформації, 2024. Пропаганда розповсюджує фейк, що Президент України став власником одного з найбільших казино в Європі. URL: https://cpd.gov.ua/warnin/propaganda-rozpovsyudzhuye-fejk-shho-prezydent-ukrayiny-stav-vlasnykom-odnogo-z-najbilshyh-kazyno-v-yevropi/

114. Центр протидії дезінформації, 2024. Список TikTok-каналів поширення ворожої пропаганди. URL: https://cpd.gov.ua/reports/spysok-tiktok-kanaliv-poshyrennya-vorozhoyi-propagandy/

115. Центр протидії дезінформації, 2024. Список каналів поширення ворожої пропаганди в соцмережі X. URL: https://cpd.gov.ua/reports/spysok-kanaliv-poshyrennya-vorozhoyi-propagandy-v-soczmerezhi-h/

116. Центр протидії дезінформації, 2024. Фейк про блокаду евакуації цивільних з Вовчанська. URL: https://cpd.gov.ua/warnin/fejk-pro-blokadu-evakuacziyi-czyvilnyh-z-vovchanska/

117. Центр протидії дезінформації, 2024. Фейк про мінування берегів річки Тиса. URL: https://cpd.gov.ua/warnin/fejk-pro-minuvannya-beregiv-richky-tysa/

118. Центр протидії дезінформації, 2024. Як ЄС буде протидіяти російській дезінформації. URL: https://cpd.gov.ua/main/yak-yes-bude-protydiyaty-rosijskij-dezinformacziyi/

119. Центр протидії дезінформації, 2024. Як росія використовує «молодіжні форуми» для пропаганди на ТОТ. URL: https://cpd.gov.ua/result/yak-rosiya-vykorystovuye-molodizhni-forumy-dlya-propagandy-na-tot/

120. Центр протидії дезінформації, 2024. Як росія просуває свою пропаганду в ООН під виглядом захисту прав людини. URL: https://cpd.gov.ua/result/yak-rosiya-prosuvaye-svoyu-propagandu-v-oon-pid-vyglyadom-zahystu-prav-lyudyny/

121. Центр протидії дезінформації, 2024. Які проросійські наративи просуваються в медіа Глобального Півдня: Близький Схід. URL: https://cpd.gov.ua/result/yaki-prorosijski-naratyvy-prosuvayutsya-v-media-globalnogo-pivdnya-blyzkyj-shid/

122. Центр протидії дезінформації. Виявлені загрози. URL: https://cpd.gov.ua/category/result/

123. Центр протидії дезінформації. Звіти. URL: https://cpd.gov.ua/category/reports/

124. Центр протидії дезінформації. Спростування. URL: https://cpd.gov.ua/category/warnin/

125. Центр протидії дезінформації. Статті. URL: https://cpd.gov.ua/category/articles/

126. Центр стратегічних комунікацій та інформаційної безпеки, 2023. Про що ворожать російські тарологи під час війни. URL: https://spravdi.gov.ua/pro-shho-vorozhat-rosijski-tarology-pid-chas-vijny/

127. Центр стратегічних комунікацій та інформаційної безпеки, 2023. Росіяни запустили нову ІПСО, прикрившись клоном українського медіа. Що вигадали пропагандисти? URL: https://spravdi.gov.ua/rosiyany-zapustyly-novu-ipso-prykryvshys-klonom-ukrayinskogo-media-shho-vygadaly-propagandysty/

128. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Наркобарони не допомагають американським ПВК в Україні: дайджест пропаганди за 11 липня. URL: https://spravdi.gov.ua/narkobarony-ne-dopomagayut-amerykanskym-pvk-v-ukrayini-dajdzhest-propagandy-za-11-lypnya/

129. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Путін спалить гроші росіян у трубі війни: дайджест пропаганди за 10 липня. URL: https://spravdi.gov.ua/putin-spalyt-groshi-rosiyan-u-trubi-vijny-dajdzhest-propagandy-za-10-lypnya/

130. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Реальні фото і фейкові новини: як російська пропаганда вигадала «жіночий батальйон «Білосніжка». URL: https://spravdi.gov.ua/realni-foto-i-fejkovi-novyny-yak-rosijska-propaganda-vygadala-zhinochyj-bataljon-bilosnizhka/

131. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Російська «антиракетна» брехня почалась з Сирії: дайджест пропаганди за 9 липня. URL: https://spravdi.gov.ua/rosijska-antyraketna-brehnya-pochalas-z-syriyi-dajdzhest-propagandy-za-9-lypnya/

132. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Росіяни вчинили масштабну атаку на українські телеканали. URL: https://spravdi.gov.ua/rosiyany-vchynyly-masshtabnu-ataku-na-ukrayinski-telekanaly/?__cf_chl_tk=IzsgdSZhQBfRhDPBHw.6MrBnbvq9UBJOroeLl1JvK8Q-1720152349-0.0.1.1-4372

133. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Фейк: «Зеленський обкрадає фронт і вводить в оману Захід». URL: https://spravdi.gov.ua/fejk-zelenskyj-obkradaye-front-i-vvodyt-v-omanu-zahid/

134. Центр стратегічних комунікацій та інформаційної безпеки, 2024. Фейк: «Київ влаштував постановку із закривавленим лікарем «Охматдиту». URL: https://spravdi.gov.ua/fejk-kyyiv-vlashtuvav-postanovku-iz-zakryvavlenym-likarem-ohmatdytu/

135. Центр стратегічних комунікацій та інформаційної безпеки, 2024. «Київ за три дні», «брудна бомба» і «другий Сталінград»: як змінювалася російська пропаганда за два роки повномасштабної війни. URL: https://spravdi.gov.ua/kyyiv-za-try-dni-brudna-bomba-i-drugyj-stalingrad-yak-zminyuvalasya-rosijska-propaganda-za-dva-roky-povnomasshtabnoyi-vijny/

136. Центр стратегічних комунікацій та інформаційної безпеки, 2024. «Мирний план» Кремля вдарив по «Охматдиту»: дайджест пропаганди за 8 липня. URL: https://spravdi.gov.ua/myrnyj-plan-kremlya-vdaryv-po-ohmatdytu-dajdzhest-propagandy-za-8-lypnya/

137. Центр стратегічних комунікацій та інформаційної безпеки, 2024. «Українські спецслужби причетні до замаху на Дональда Трампа». Це — ворожа маячня. URL: https://spravdi.gov.ua/ukrayinski-speczsluzhby-prychetni-do-zamahu-na-donalda-trampa-cze-vorozha-mayachnya/

138. Центр стратегічних комунікацій та інформаційної безпеки. Антифейк. URL: https://spravdi.gov.ua/sprostuvannya-fejkiv/

139. Центр стратегічних комунікацій та інформаційної безпеки. Дослідження. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/vsi-doslidzhennia/

140. Центр стратегічних комунікацій та інформаційної безпеки. Моніторинг. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/monitoryng/

141. Центр стратегічних комунікацій та інформаційної безпеки. Про центр. URL: https://spravdi.gov.ua/pro-nas/

142. Центр стратегічних комунікацій та інформаційної безпеки. Розслідування. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/investigation/

143. Центр стратегічних комунікацій та інформаційної безпеки. Школа протидії дезінформації. URL: https://spravdi.gov.ua/treningy-dlya-derzhsluzhbovcziv/

144. Центр стратегічних комунікацій та інформаційної безпеки і Центр демократії та верховенства права, 2023. Гібридна війна Росії проти України. Як перемогти на інформаційному фронті (посібник). URL: https://drive.google.com/file/d/1AEUYRLeYOx7kBbNPJL1XzwHXstCNJaJW/view

145. Центр стратегічних комунікацій та інформаційної безпеки і Центр демократії та верховенства права, 2024. Інформаційні атаки в соцмережах: дослідження впливу російської дезінформації через рекламу в Facebook. URL: https://cedem.org.ua/wp-content/uploads/2024/05/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf

146. Balázs Kárász, 2020. Social Aspects of Reliability and Security Issues of Authentication Solutions. URL: https://real.mtak.hu/123491/1/HSZ_2020_2_9_Karasz_111-127.pdf

147. BBC News Україна, 2022. Нова масштабна кібератака: ключові урядові сайти знову «лягли». URL: https://www.bbc.com/ukrainian/news-60497679

148. CDN Finder. URL: https://www.cdnplanet.com/tools/cdnfinder/

149. Certificate Search. URL: http://crt.sh

150. Chart of signatures and ratifications of Treaty 224. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

151. Cloudflare. How to prevent DDoS attacks | Methods and tools. URL: https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

152. Cloudflare. URL: https://www.cloudflare.com/

153. Cloudflare. What is a phishing attack? URL: https://www.cloudflare.com/learning/access-management/phishing-attack/

154. Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) Text with EEA relevance. URL: https://eur-lex.europa.eu/eli/dir/2022/2555

155. Council of Europe report DGI(2017)09. Information disorder: Toward an interdisciplinary framework for research and policy making. URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

156. Cyber Diia, 2024. A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience. URL: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

157. Cyberpeace Institute, 2023. Impact & Harm How do cyberattacks and operations impact civilians? URL: https://cyberconflicts.cyberpeaceinstitute.org/impact

158. David Gilbert, 2024. A Russian Influence Campaign Is Exploiting College Campus Protests. URL: https://www.wired.com/story/russian-influence-campaign-exploiting-college-campus-protests/

159. Deflect. URL: https://deflect.ca/ua/

160. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148

161. ESET. Розподілена атака на відмову в обслуговуванні (DDoS). URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/distributed-denial-of-service/

162. ESET. Фішинг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/

163. EU Neighbours East, 2024. Співпраця у сфері кібербезпеки: третій раунд діалогу Україна-ЄС відбувся у Брюсселі. URL: https://euneighbourseast.eu/uk/news/latest-news/cpivpraczya-u-sferi-kiberbezpeky-tretij-raund-dialogu-ukrayina-yes-vidbuvsya-u-bryusseli/

164. European Parliamentary Research Service, 2023. The NIS2 Directive: A high common level of cybersecurity in the EU. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

165. EUvsDisinfo. URL: https://euvsdisinfo.eu/ua/

166. Fortra. Spotting Cloned Websites. URL: https://support.alertlogic.com/hc/en-us/articles/360057785872-Spotting-Cloned-Websites

167. Google Security Issues report. URL: https://support.google.com/webmasters/answer/9044101?hl=en

168. Google Безпечний перегляд: статус сайту. URL: https://transparencyreport.google.com/safe-browsing/search

169. Google Сповіщення. URL: https://www.google.com/alerts

170. HOSTiQ. Що таке SSL-сертифікат. URL: https://hostiq.ua/ukr/info/what-is-ssl/

171. IMATAG. URL: https://www.imatag.com/

172. Irene Khan, 2021. Disinformation and freedom of opinion and expression : report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan. URL: https://digitallibrary.un.org/record/3925306?v=pdf&ln=es

173. Juliana Suess, 2022. Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine. URL: https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine

174. Kerstin Zettl-Schabath and Sebastian Harnisch, 2023. One Year of Hostilities in Ukraine: Nine Notes on Cyber Operations. URL: https://eurepoc.eu/wp-content/uploads/2023/06/One_Year_of_Hostilities_in_Ukraine_EuRepoC.pdf

175. Meta Sharing Debugger. URL: https://developers.facebook.com/tools/debug/

176. National Cyber Security Index — Ukraine, 2024. URL: https://ncsi.ega.ee/country/ua/

177. Nations Against Disinformation Initiative. URL: https://ua.nationsagainstdisinformation.org/

178. North Atlantic Treaty Organization, 2024. Countering hybrid threats. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm

179. NV, 2024. Втручання хакерів у роботу сайту NV: зловмисники розмістили контент, до якого редакція не має стосунку. URL: https://nv.ua/ukr/ukraine/events/sayt-nv-bulo-zlamano-24-lyutogo-2024-roku-robotu-vzhe-vidnovleno-novini-ukrajini-50395661.html

180. Obozrevatel, 2023. Розганяють «зраду»: у мережі поширюють фейки від імені OBOZREVATEL з проплаченою рекламою у FB, видання звернулося в СБУ. URL: https://news.obozrevatel.com/ukr/society/rozganyayut-zradu-u-merezhi-poshiryuyut-fejki-vid-imeni-obozrevatel-z-proplachenoyu-reklamoyu-u-fb-vidannya-zvernulosya-v-sbu.htm

181. Project Shield. URL: https://projectshield.withgoogle.com/landing

182. Prometheus. Пост у Facebook. URL: https://www.facebook.com/prometheusmooc/posts/624107749747669

183. Red Points, 2023. Website cloning: How to identify, prevent, and respond. URL: https://www.redpoints.com/blog/website-cloning/

184. Resisting Russia's False Narrative — EU-Ukraine Forum on Countering Disinformation. Conference programme. URL: https://drive.google.com/file/d/15ga0cCvuqs_-NUDQ5dQo34Tc7Twt2WvG/view

185. The NATO Cooperative Cyber Defence Centre of Excellence. About us. URL: https://ccdcoe.org/about-us/

186. The NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual. URL: https://ccdcoe.org/research/tallinn-manual/

187. The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2023. Semi-Annual Chronicles of UAC-0006 Operations. URL: https://scpc.gov.ua/api/files/8e300d33-6257-4d7f-8f72-457224268343

188. UN. Secretary-General, 2022. Countering disinformation for the promotion and protection of human rights and fundamental freedoms : report of the Secretary-General. URL: https://digitallibrary.un.org/record/3987886?ln=ru&v=pdf

189. United Nations High Commissioner for Refugees, 2022. Factsheet 4: Types of Misinformation and Disinformation. URL: https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf

190. VirusTotal. URL: https://www.virustotal.com/gui/home/url

191. Vitalii Zubok, Andrii Davydiuk, and T. M. Klymenko, 2023. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555. URL: https://www.researchgate.net/publication/375323482_Cybersecurity_of_Critical_Infrastructure_in_Ukrainian_Legislation_and_in_Directive_EU_20222555

192. Who is hosting this. URL: https://www.whoishostingthis.com/

193. WHOIS Search, Domain Name, Website, and IP Tools. URL: https://who.is/

194. Zmina, 2023. Росіяни створили низку фейкових сторінок українських медіа для поширення власної пропаганди. URL: https://zmina.info/news/rosiyany-stvoryly-nyzku-fejkovyh-storinok-ukrayinskyh-media-dlya-poshyrennya-vlasnoyi-propagandy/