ВІЙНА У ЦИФРОВОМУ ВИМІРІ ТА ПРАВА ЛЮДИНИ

Аналітичний звіт

за серпень 2022 р.

ГО «Платформа прав людини»

КИЇВ, 2022

24 лютого 2022 р. відбулося широкомасштабне вторгнення російської федерації в Україну. Цього ж дня Указом Президента України на всій території нашої держави було введено воєнний стан.

Вторгнення торкнулося не лише українських міст, сіл і селищ, а й українського кіберпростору. Ворожі хакери спрямували чимало зусиль на те, щоб поширити дезінформацію та порушити нормальну діяльність об'єктів критичної інфраструктури України, зокрема, в енергетичному та фінансовому секторах, а також у сфері надання державних послуг. Кожен день спеціалісти профільних державних органів разом з українськими кіберволонтерами та союзниками з усього світу ведуть запеклу боротьбу з окупантами та їхніми помічниками у віртуальному світі.

Описана ситуація не могла не позначитися на цифрових правах людини.

ГО "Платформа прав людини", після представлення двох звітів "Війна у цифровому вимірі та права людини", які охопили період з 24 лютого 30 квітня 2022 року та з 01 травня по 31 липня 2022 року, продовжує збирати і аналізувати через призму прав людини факти про події у кіберпросторі під час війни.

ЗМІСТ

КЛЮЧОВІ ПІДСУМКИ

Під час моніторингу подій, що відбувались у сфері цифрових прав у серпні 2022-го року, було виявлено наступні проблеми:

1. У серпні 2022 року Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) оприлюднила звіт "Війна в Україні. Пульс кіберзахисту", який охоплює період з 24 лютого по 24 серпня 2022 року. Кількість кібератак, про які йдеться в звіті, суттєво відрізняється від даних, які зафіксовано під час моніторингу загальнодоступних джерел інформації експертами ППЛ. З метою уточнення даних ГО "Платформа прав людини" було направлено запит з проханням надати відомості щодо кількості, напрямів, методів кібератак та переліку підприємств, які зазнали їх, в серпні 2022 року. І, якщо у відкритих джерелах нами було зафіксовано всього один такий випадок, Держспецзв'язку повідомила про **28 751 942** кібератак тільки протягом серпня місяця. В подальших звітах в частині кібератак ми будемо наводити дані як зібрані у відкритих джерелах, так і надані Держспецзв'язку. Отже, було зафіксовано:

– **28 751 942 кібератак,** про які, у відповідь на запит ППЛ повідомила Держспецзв'язку. Найчастіше зловмисниками здійснювався несанкціонований збір інформації, і таких спроб було 26 906 024; 1 575 507 раз ворог намагався розмістити шкідливий програмний код; 201 097 - спроби вторгнення з використанням вразливості мережі; 63 997 - намагання авторизації або входу в систему; 4277 - атаки на відмову в обслуговування (DoS/DDoS); 1040 випадків розсилки спаму та інших способів здійснення кібератак. У відкритих джерелах зафіксовано тільки **одне повідомлення** про кібератаку на офіційний сайт державного підприємства "Національна атомна енергогенеруюча компанія "Енергоатом".

2. **977 785 фішинг атак,** про які повідомила Держспецзв'язку, про **три з** яких писали інтернет-ЗМІ.

3. **133 випадки поширення дезінформації** шляхом розповсюдження неправдивих повідомлень. Основними темами дезінформаційних повідомлень були: ситуація на Запорізькій АЕС; звинувачення ЗСУ в обстрілах населених пунктів та цивільного населення; звинувачення США, ЄС та Великої Британії у війні проти окупантів; небажання українських військових воювати, дезертирство та здача позицій; санкції проти держави-окупанта виведуть з ладу економіку ЄС; захід втомився від України; маніпуляції пов'язані із постачанням газу; біолабораторії та проведення досліджень на українцях; ситуація в Оленівці; розколи в українських органах державної влади; вбивство Дугіної.

4. У звітному періоді хакери використовували різні шахрайські схеми для викрадення інформації або коштів. Зокрема, в серпні було виявлено **7 шахрайських схем** введення українців в оману. В умовах війни злочинці використовують нові способи та засоби для досягнення своїх цілей.

5. Здійснювались та продовжували діяти у звітному періоді позасудові блокування веб-ресурсів або інформації на веб-ресурсах, зокрема:

– продовжують діяти **854 блокування веб-ресурсів за ініціативи Національного центру оперативно-технічного управління мережами телекомунікацій (далі може бути - НЦУ) при Держспецзв'язку;**

- українські ІТ-волонтери заблокували або ускладнили роботу **1050 російських веб-ресурсів;**
- відбулось блокування **1003 повідомлень** платформами спільного доступу до інформації (соціальними мережами).

6. Без можливості користуватись українським зв'язком та інтернетом продовжували залишатись мешканці окупованих територій - Херсонської області, міст Бердянськ та Мелітополь. На окупованих територіях ворог заблокував доступ до українських ресурсів 30 травня 2022 року.[1]
7. Мала продовження практика притягнення до кримінальної відповідальності за частиною першою статті 111-1 КК України та призначення покарання у вигляді "позбавлення права обіймати певні посади або займатись певною діяльністю на строк від 10 до 15 років" непрацюючим особам. Тобто, особам, які в силу своїх соціальних статусів ніколи посад не займали і, відповідно, не несуть реального покарання за вчинені злочини. Проблема продовжує існувати, оскільки частина друга статті 111-1 КК України передбачає лише один безальтернативний вид покарання, який за своєю правовою природою є факультативним в інших складах злочинів.
8. Під час моніторингу судової практики було виявлено **93 рішення суду в кримінальних справах,** які безпосередньо стосуються питань свободи вираження поглядів. У **36 з них** є факти, що свідчать про можливе порушення цифрових прав:

- **17 рішень** не містять інформації, поширення якої стало підставою для притягнення до кримінальної відповідальності. Що, в свою чергу, не дає можливості оцінити її зміст та пропорційність застосованих державою санкцій;
- **11 рішень,** в яких не міститься інших способів аналізу поширеної інформації судом, крім посилань на висновки експертів-лінгвістів. Подібна судова практика свідчить про підміну ролі і повноважень суду практикою відповідних судових експертів;
- **8 рішень,** в яких поєднується, як відсутність інформації, поширення якої стало підставою для притягнення до кримінальної відповідальності, так і відсутність власної оцінки судом її змісту з посиланнями виключно на висновки експертів-лінгвістів;
- за наслідками розгляду цих кримінальних справ **три особи,** з числа тих, кого було визнано винними у вчинені злочинів, понесли реальне покарання. Абсолютну більшість засуджених було звільнено від відбування покарання на підставі статті 75 КК України.

9. Було виявлено **дві судові справи в цивільних справах, які порушують стандарти прав людини** в контексті застосування обмежень у сфері свободи вираження поглядів та в яких одночасно застосовано такі способи правового захисту, як спростування та видалення спірних відомостей без обґрунтування необхідності в цьому.
10. У серпні було виявлено **32 неправомірні відмови у наданні публічної інформації.** В своїх відмовах, розпорядники продовжували посилатись на воєнний стан, як на обставину непереборної сили (десять таких відповідей було виявлено у звітному періоді). В інших відповідях розпорядники відносили запитувану інформацію до інформації з обмеженим доступом (шість таких відповідей було надано у звітний період). Також, розпорядники вимагали від запитувача підписати запит електронним цифровим підписом, що не

[1] https://suspilne.media/245018-v-okupovanih-melitopoli-ta-berdansku-vidsutnij-ukrainskij-mobilnij-zvazok/

передбачено Законом України “Про доступ до публічної інформації” (три таких відмови було зафіксовано).

11. 01 серпня 2022 року Портал відкритих даних **Data.gov.ua** відновив роботу після вимушеної паузи через повномасштабне вторгнення рф в Україну.[2] Щодо відновлення роботи інших реєстрів, то у згаданий період **продовжував бути обмеженим доступ до 19 публічних електронних реєстрів.** Існують сумніви щодо необхідності закриття низки реєстрів і того наскільки такі дії є пропорційними та доцільними для досягнення мети – забезпечення захисту національної безпеки й оборони. Відповідно до вимог ч.3 ст.6 Закону України “Про доступ до публічної інформації” інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.
12. Під час звітного періоду було створено **два нові онлайн додатки та сервіси:** мобільний застосунок з мінної безпеки MineFree та чат-бот для пошуку інформації про військових, які потрапили у полон та зникли безвісти за особливих обставин. Введення воєнного стану в Україні стало додатковим поштовхом для цього процесу. Проте, крім допомоги у вирішенні тих чи інших питань, в тому числі, пов’язаних з війною, зазначені сервіси, потенційно, несуть ризики порушення прав користувачів на захист персональних даних. Відповідно, існує потреба у ефективному контролі за дотриманням вимог Закону України “Про захист персональних даних”.

Детальніше із зібраною та систематизованою під час моніторингу інформацією можна ознайомитись далі.

[2] https://zmina.info/news/portal-vidkrytyh-danyh-data-gov-ua-vidnovyv-robotu-minczyfry/

КІБЕР (ХАКЕРСЬКІ) АТАКИ

У серпні 2022 року ворожі хакери продовжували атакувати Україну. За інформацією, яку оприлюднила Державна служба спеціального зв'язку та захисту інформації в своєму звіті "Війна в Україні. Пульс кіберзахисту" основними об'єктами, на які найчастіше здійснював напади російський агресор, продовжували бути державні і місцеві органи влади та сектор безпеки. У звіті служба узагальнила і опублікувала інформацію, щодо кібератак, які були здійснені за період з 24 лютого 2022 року по 24 серпня 2022 року. Загальна кількість кількість кібератак, що відбулась в зазначений період, за інформацією Держспецзв'язку, становить - **1 123.**

Основними напрямами атак хакерів стали державні органи (260 атак) та структури сектору безпеки і оборони України (154). Відповідно, на комерційні організації припало 83 атаки, фінансову сферу — 72, а на об'єкти з інших секторів - 554.

Щодо мети кібератак, то в 306 випадках здійснювався несанкціонований збір інформації зловмисниками, у 267 — були спроби розмістити шкідливий програмний код, у 149 — спроби втручання у функціонування роботи ресурсів, інші різновиди атак — 401.

Перелік категорій кіберінцидентів відповідно до методів здійснення,[3] який розроблений Урядовою командою реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України - CERT-UA, виглядає наступним чином:

1. **Збір інформації зловмисником:**

– сканування - збір інформації про системи або мережі;

– сніфінг - несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку, несанкціонований моніторинг та зчитування мережевого трафіку;

– фішинг - спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти).

2. **Шкідливий програмний код:**

– зараження шкідливим програмним забезпеченням (далі – ШПЗ);

– розповсюдження ШПЗ, наприклад, шляхом розсилки повідомлень електронної пошти, що містять вкладення з шпз або посилання на його завантаження;

– командно-контрольний центр (С2) - система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами;

– шкідливе підключення - спроби з'єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад С2С або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі.

3. **Втручання:**

[3] https://cert.gov.ua/recommendation/16904

– компрометація облікового запису - фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора;

– компрометація системи - фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу.

4. **Відома вразливість:**

- вразливість - наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації;

– Некоректна конфігурація - недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо).

5. **Інше** - невизначений інцидент - недостатньо даних для обробки інциденту.

Варто зазначити, що кількість кібератак зі звіту Держспецзв'язку суттєво відрізняється від цифр, які було зафіксовано нами під час моніторингу загальнодоступних джерел інформації. З метою уточнення зазначеної інформації, ГО "Платформа прав людини" було направлено запит з проханням надати відомості щодо кількості, напрямів, методів кібератак та переліку підприємств, які їх зазнали в серпні 2022 року. Для порівняння: у лютому-квітні у відкритих джерелах було зафіксовано 32 кібератаки; у травні-липні - 12, а в серпні в мережі інтернет нами було зафіксовано всього один такий випадок, в той час як Держспецзв'язку нам повідомила про **28 751 942** кібератаки в тільки в серпні 2022 року.

У відповідь на запит Держспецзв'язку повідомила , що загальна кількість кібератак на державні інформаційні ресурси, кіберзахист яких відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" здійснює служба, за період з 01 по 31 серпня 2022 року, становить **28 751 942.** Найчастіше зловмисниками здійснювався несанкціонований збір інформації - 26 906 024; у 1 575 507 — були спроби розмістити шкідливий програмний код; 201 097 - спроби вторгнення з використанням вразливості мережі; 63 997 - спроб авторизації або входу в систему; 4277 - атак на відмову в обслуговування (DoS/DDoS); 1040 - розсилка спаму та інших способів здійснення кібератак.

Така вражаюча кількість кібератак в серпні 2022 року, про які було повідомлено у відповіді на запит, є неспівставна з кількістю, яка була виявлена нами під час моніторингу, ба більше, з тією, яка була наведена у звіті самої Держспецзв'язку за період з 24 лютого по 24 серпня 2022 року - **1123.** Аналізуючи та порівнюючи інформацію, наведу у зазначеному звіті та інформацію надану у відповідь на запит, можна зробити висновок, що Державною службою спеціального зв'язку були застосовані різні методи та критерії підрахунку кібератак.

В свою чергу, із інформації отриманої шляхом моніторингу загальнодоступних джерел, нами було зафіксовано повідомлення про те, що 16 серпня 2022 року відбулася найпотужніша від 24 лютого хакерська атака на офіційний сайт державного підприємства "Національна атомна енергогенеруюча компанія "Енергоатом". Його атакувала "російська група "народная киберармия", **використовуючи 7,25 млн бот-юзерів,** які впродовж трьох годин симулювали сотні мільйонів переглядів основної сторінки компанії". Напад хакерів вдалося відбити, і сайт продовжує роботу.[4]

Дана інформація дозволяє зробити припущення, що у звіті Держспецзвязку "Війна в Україні. Пульс кіберзахисту" наведено узагальнені цифри, які стосуються атак,

[4] https://t.me/energoatom_ua/8965

що здійснювали певні хакерські угруповання. В той час, як у відповіді на запит, було наведено кількість кібератак в розрізі втручання безпосереднім хакером.

В наступних звітних періодах ми будемо продовжувати дослідження і аналіз інформації щодо способів здійснення, кількості кібератак та об'єктів, на які вони націлені. Ми звернемось до Державної служби спеціального зв'язку та захисту інформації з проханням надати роз'яснення або методологію, згідно якої здійснюється аналіз інформації про кібератаки.

ФІШИНГ АТАКИ

Перелік категорій кіберінцидентів[5] відносить фішинг до методів збору інформації зловмисниками, який відбувається за допомогою методів соціальної інженерії (масової розсилки електронною поштою, спрямованої на збір даних, яка може містити посилання на фішингові сайти). У серпні 2022 року Державною служба спеціального зв'язку та захисту інформації було зафіксовано **977 785** фішинг атак. Про це Держспецзв'язку повідомила у відповідь на запит.

Також, під час моніторингу було зафіксовано повідомлення Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про розповсюдження фішингових листів 11 серпня 2022 року. Ці листи містили шкідливу програму AgentTesla. Завантаження програми призводило до інфікування всіх документів, які створюються на комп'ютері. Аналогічні розсилки також було зафіксовано 30 і 31 серпня 2022 року з темами “Технічне креслення" (“Technisches Zeichnen”).

ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ

У звітному періоді продовжувалась активні дезінформаційні атаки з боку російських пропагандистів, направлених на дискредитацію ЗСУ та української влади. Ворог щоденно знаходив приводи для інформаційного терору та залякування. 04 серпня 2022 р. Головне управління розвідки Міністерства оборони заявило, що держава-окупант почала новий етап спеціальних інформаційних операцій проти України. Його мета – посіяти панічні настрої серед населення. Агресор кожного дня поширював недостовірну інформацію та намагався маніпулювати суспільством, підштовхнути до дій, які можуть дестабілізувати країну в період війни.[6]

Поширення дезінформації у звітний період відбувалось в мережі Інтернет: на сайтах, в соціальних мережах, в месенджерах. Зокрема, дослідники нью-йоркської групи дослідників NewsGuard заявили 9 серпня 2022 року, що на початку серпня 2022 року виявили 250 вебсайтів, що поширюють дезінформацію, пов’язану з російсько-українською війною, проти 116 в березні. Зазвичай, вказані сайти уникають

[5] https://cert.gov.ua/recommendation/16904
[6] https://t.me/DIUkraine/1043

розголошення інформації про власників чи редакторів, але бездоказово стверджують, що є незалежними аналітичними центрами чи іншими неприбутковими організаціями.[7]

Служба безпеки України в серпні 2022 року знешкодила організоване угруповання, яке створило потужну ботоферму для масового поширення через інтернет дезінформації. Для "розгону" деструктивного контенту ділки адміністрували більше 1 млн. власних ботів, а також численні групи в соцмережах з аудиторією майже 400 тис. користувачів.[8]

В даному звіті проаналізовано повідомлення про інформаційні загрози, які було виявлено Центром протидії дезінформації (далі по тексту може бути - ЦПД) та, про які ЦПД повідомляв в своєму телеграм-каналі[9], а, також, було проаналізовано повідомлення про поширення дезінформації з інших джерел. Загалом, за звітний період було зафіксовано **133 випадки поширення дезінформації**.

Тематика дезінформаційних повідомлень, які ворог створив та поширював в серпні 2022 року була наступною:

1. Запорізька АЕС. Дезінформаційні повідомлення, які стосувались ситуації на Запорізькій АЕС найбільше поширювались у звітний період. Практично кожного дня ворог звинувачував українську владу в обстрілах Запорізької АЕС. Зокрема, представники посольства рф у США заявляли, що: "обстріли Запорізької АЕС формуваннями ЗСУ носять умисний характер, а для того, щоб дискредитувати рф, українська влада не гребує нічим, створюючи реальну загрозу ядерній безпеці не лише України, а й Європи".[10] Також, звинувачення поширювали колаборанти- "керівники" тимчасово окупованих територій Запорізької області: "влада України готує масштабну провокацію на Запорізькій АЕС, щоб шантажувати Європу загрозою ядерної катастрофи, а Київ навмисно намагається поцілити у сховище ядерних відходів на ЗАЕС, щоб спровокувати вибух "брудної бомби".[11] Окрім цього, постійний представник рф при ООН В.Небензя заявляв: "коли ЗСУ завдавали ударів по Запорізькій АЕС, катастрофи вдавалося уникнути лише завдяки самовідданій роботі російських військових та працівників станції".[12] Всього 28 повідомлень, в яких згадувалась ЗАЕС було поширено в серпні 2022 року.
2. Звинувачення ЗСУ в обстрілах населених пунктів та цивільного населення. З такою самою активністю, як і фейки про ЗАЕС, ворог поширював неправдиву інформацію, в якій звинувачував ЗСУ в розстрілах мирного населення, в ударах по цивільним обєктам та інших діях, до яких українські військові не мали відношення. Серед повідомлень, які були розповсюджені у звітний період були наступні: "поблизу н.п. Довгове націоналісти розстріляли автобус із мирними жителями, які евакуювалися на підконтрольні київській владі території, при цьому фото- та відеофіксацію нібито ударів військ рф по цивільному населенню здійснили ЗСУ";[13] "у Добропіллі Донецької області в приміщеннях пологового будинку зосереджено підрозділи ЗСУ, обладнано склади озброєння та боєприпасів, а медперсонал і жінки з новонародженими дітьми не евакуйовані та фактично використовуються, як "живий щит";[14] "вночі 30.07.2022 р. із житлових кварталів м.Оріхів здійснювався мінометний вогонь по позиціях

[7] https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/
[8] https://ssu.gov.ua/novyny/sbu-likviduvala-milionnu-botofermu-yaka-rozkhytuvala-obstanovku-v-ukraini-na-zamovlennia-odniiei-z-politsyl-video
[9] Дезінформація - інформація, яка є неправдивою та навмисно створена, щоб завдати шкоди людині, соціальній групі, організації чи країні (Звіт Ради Європи «Інформаційне безладдя: на шляху до міждисциплінарного підходу до досліджень та вироблення політик»).# Кембриджський словник називає дезінформацію "неправдивою інформацією, яка поширюється з метою введення в оману людей".
[10] https://t.me/CenterCounteringDisinformation/2285
[11] https://t.me/CenterCounteringDisinformation/2313
[12] https://t.me/CenterCounteringDisinformation/2314
[13] https://t.me/CenterCounteringDisinformation/2254
[14] https://t.me/CenterCounteringDisinformation/2262

військ рф. Підрозділи ЗСУ мали на меті спровокувати удари артилерії ЗС рф у відповідь для подальшої їх фіксації групою іноземних журналістів, однак ЗС рф, отримавши своєчасно інформацію про підготовку провокації, не допустили невиборних ударів";[15] "у Дніпропетровській області українські націоналісти замінували автомобільні мости через річки Гайчур та Ворона, які вони мають намір підірвати для звинувачення ЗС рф в руйнуванні об'єктів транспортної інфраструктури",[16] та інші повідомлення схожого змісту. Всього було поширено 28 повідомлень такого змісту.

3. Звинувачення США, ЄС та Великої Британії у війні проти рф. Не менш активно ворог використовував в інформаційній війні тематику звинувачення країн Європейського Союзу, США та Великої Британії у гібридній війні проти держави-окупанта. Зокрема, в посольстві рф у США повідомляли, що: "США продовжують діяти без огляду на безпеку та інтереси інших країн, що спричиняє підвищення ядерних ризиків. Кроки США із втягування в гібридне протистояння з рф у контексті української кризи загрожують ескалацією та прямим військовим зіткненням ядерних країн".[17] Також, російські ЗМІ з посиланням на видання Die Welt повідомляли, що: "всупереч публічним заявам про право Києва на самовизначення, саме президент США Джо Байден, канцлер ФРН Олаф Шольц та президент Франції Емманюель Макрон вирішують, що робити [Володимиру] Зеленському… насамперед, тому що без фінансової та військової допомоги з боку Заходу Україна була б абсолютно безпорадною".[18] Керівник МЗС рф С.Лавров заявляв: "США і Велика Британія [та] слухняна Європа [намагаються] змусити світ, змінити свою думку про рф, тому що більшість держав або вважають виправданим наше ставлення до ігнорування Заходом законних інтересів росії у сфері безпеки, або хочуть посідати нейтральну позицію".[19] Всього у звітному періоді було поширено 24 подібних фейки.

4. Звинувачення української влади. Ще однією темою дезінформаційних повідомлень було звинувачення української влади у проведені "каральних операцій" проти громадян з проросійськими поглядами. Прикладами таких фейків були наступні повідомлення, що були поширені: "київський режим направить до Харкова співробітників СБУ для проведення каральної операції з виявлення громадян з проросійськими поглядами, затриманим будуть погрожувати фізичною розправою над членами їхніх сімей, насильством та тортурами";[20] "багато жителів України не схвалили політику київської влади щодо реабілітації нацизму, в тому числі і жителі Донбасу, які не стали потурати правлячому режиму в його нацистських прагненнях, тоді проти них розгорнулася жорстока карательна операція".[21] В серпні було поширено 16 фейкових повідомлень подібного змісту.

5. Небажання українських військових воювати, дезертирство та здача позицій. Також активно поширювались фейки наступного змісту: "через великі безповоротні втрати в 93-й механізованій бригаді та 128-й гірсько-штурмовій бригаді відзначається масове залишення бойових позицій і дезертирство особового складу з'єднань у центральні та західні райони України";[22] "внаслідок знищення пунктів дислокації українських націоналістів, масових втрат та дезертирства втратило боєздатність нацформування "Кракен". Для термінового поповнення втрат командири нацистського формування марно намагаються

[15] https://t.me/CenterCounteringDisinformation/2275
[16] https://t.me/CenterCounteringDisinformation/2314
[17] https://t.me/CenterCounteringDisinformation/2343
[18] https://t.me/CenterCounteringDisinformation/2404
[19] https://t.me/CenterCounteringDisinformation/2464
[20] https://t.me/CenterCounteringDisinformation/2306
[21] https://t.me/CenterCounteringDisinformation/2386
[22] https://t.me/CenterCounteringDisinformation/2247

змусити вступати до нього жителів Харкова";[23] та інші неправдиві повідомлення, які дискредитували українських воїнів. Всього 11 подібних випадків було зафіксовано у серпні 2022 року.

6. Санкції проти держави-окупанта виведуть з ладу економіку ЄС. Прикладом такого повідомлення є інформація про те, що: "європейці влаштували флешмоб #againstSanctions проти антиросійських санкцій, під час якого публікують у Twitter фото порожніх тарілок, оскільки їжу "з'їли" санкції проти росії".[24] В період з 1 по 31 серпня було виявлено 9 фейків подібного змісту.
7. Захід втомився від України. ЗМІ держави-окупанта з посиланням на Bloomberg повідомляли, що: "Захід починає втомлюватися від України… у Європі від війни починають відверто втомлюватися, оскільки там на перший план виходять власні економічні проблеми, і це говорить лише про те, що "війна до останнього українця" триватиме доти, доки її ціна не стане надто великою".[25] 5 подібних неправдивих повідомлень було розповсюджено у серпні 2022 року.
8. Маніпуляції пов'язані із постачанням газу. Тема постачання газу в країни ЄС, також, активно використовувалась російськими пропагандистами під час створення та поширення дезінформаційних повідомлень. Серед повідомлень, які використовувались були наступні: "майбутня зима для мешканців та влади Німеччини – важливий тест, який покаже готовність країни пережити холод без російського газу… водночас експерти та місцеві підприємці прогнозують похмуре майбутнє промисловості та економіки ФРН";[26] "ми ніколи не нав'язували постачання, не намагалися вирішувати приписані нам вузькокон'юнктурні цілі… ми готові торгувати зі всіма, кому потрібні недорогі та високоякісні ресурси… проблеми із запуском "Північного потоку-2" почалися після запроваджених США санкцій".[27] Всього було зафіксовано 5 повідомлень в яких поширювалась така дезінформація.
9. Біолабораторії та проведення досліджень на українцях. У серпні 2022 року серед поширених фейків було зафіксовано й такі, в яких повідомлялось про проведення таємних досліджень, виготовлення біологічної зброї та функціонування біолабораторій на території України: "в Україні поблизу кордонів з рф розробляли компоненти біологічної зброї за участю США… Наявні конкретні приклади дозволяють констатувати, що США не збираються забезпечувати відкритість у питанні функціонування їх біолабораторій на території інших країн, зокрема на пострадянському просторі";[28] "у лабораторії медичного центру "Фармбіотест" (м.Рубіжне Луганської обл.), було виявлено документи, які підтверджують, що на українських громадянах здійснювалися клінічні випробування незареєстрованих фармпрепаратів американських та європейських компаній";[29] "у рамках реалізації в Україні американської військово-біологічної програми розроблялися компоненти біологічної зброї, відбувався збір та вивіз на територію США штамів небезпечних мікроорганізмів…, а дослідження підвищеної небезпеки проводилися таємно, за участю та під керівництвом фахівців із США".[30] Всього було виявлено 3 факти поширення аналогічних повідомлень.
10. Ситуація в Оленівці. В дезінформаційних повідомленнях, які поширювали російські ЗМІ мова йшла про те, що: "саме Київ наполіг на тому, щоб військовополонені були розміщені у СІЗО в Оленівці… таким чином Київ хотів

[23] https://t.me/CenterCounteringDisinformation/2291
[24] https://t.me/CenterCounteringDisinformation/2306
[25] https://t.me/CenterCounteringDisinformation/2403
[26] https://t.me/CenterCounteringDisinformation/2342
[27] https://t.me/CenterCounteringDisinformation/2358
[28] https://t.me/CenterCounteringDisinformation/2374
[29] https://t.me/CenterCounteringDisinformation/2269
[30] https://t.me/CenterCounteringDisinformation/2441

прибрати виконавців його злочинів проти власного народу, а удар по СІЗО було завдано після того, як полонені почали свідчити".[31] У серпні було зафіксовано поширення 2 повідомлень такого змісту.

11. Розколи в українських органах державної влади. Пропагандистські ЗМІ рф повідомляли, що всередині Служби безпеки України стався розкол: співробітників, які покинули підконтрольні державі-окупанту території, колеги звинувачують у втраті секретних архівів та переході на бік рф.[32] Також, російські ЗМІ з посиланням на "The Washington Post" повідомляли про "розкол між В.Зеленським та мерами великих міст України… Очільники міст підозрюють Київ у спробах відсунути регіони на другий план, зберегти контроль над мільярдами доларів міжнародної допомоги, а також послабити політичних опонентів".[33] Всього було зафіксовано 2 факти поширення подібної дезінформації.
12. Вбивство Дугіної. В своїй пропаганді росія використала також і тему звинувачення української влади у вбивстві Дарії Дугіної: "якщо версію про український слід у вбивстві Дарії Дугіної підтвердять компетентні органи, то варто говорити про політику державного тероризму Києва"; [34] "західні спецслужби допомагають українським диверсантам вбивати неугодних осіб… [водночас] росія закликає ООН рішуче засудити вбивство Києвом Дар'ї Дугіної"[35]. Таким був зміст двох дезінформаційних повідомлень, які було зафіксовано під час звітного періоду.

ШАХРАЙСТВО В МЕРЕЖІ

Протягом звітного періоду хакери, використовуючи війну, продовжували реалізовувати шахрайські схеми. Зокрема, в серпні було виявлено **7 схем** введення українців в оману:

- поширення в месенджерах інформації щодо перевезення громадян із тимчасово окупованих територій України у безпечні міста. Після перерахунку грошей за таку послугу зловмисники зникали; [36]
- розповсюдження фейкових оголошень про здачу помешкання для вимушених переселенців у безпечних областях України та про допомогу особам у виїзді за кордон або із зони бойових дій. Після отримання коштів шахрай одразу зникав;[37]
- розміщення оголошень про продаж військової амуніції;[38] Після отримання передоплати на банківську картку за тактичні плитоноски, зловмисник переставав виходити зі своїми клієнтами на зв'язок;[39]

[31] https://t.me/CenterCounteringDisinformation/2261
[32] https://t.me/CenterCounteringDisinformation/2248
[33] https://t.me/CenterCounteringDisinformation/2269
[34] https://t.me/CenterCounteringDisinformation/2392
[35] https://t.me/CenterCounteringDisinformation/2418
[36] https://cyberpolice.gov.ua/news/proponuvav-evakuacziyu-z-okupovanyx-terytorij-ukrayiny-kyyivski-pravooxoronczi-ta-kiberpoliczejski-vykryly-shaxraya-2531/
[37] https://cyberpolice.gov.ua/news/zdacha-kvartyr-pereselenczyam-ta-prodazh-vijskovoyi-amunicziyi-mykolayivski-policzejski-vykryly-onlajn-shaxraya-6623/
[38] https://cyberpolice.gov.ua/news/zdacha-kvartyr-pereselenczyam-ta-prodazh-vijskovoyi-amunicziyi-mykolayivski-policzejski-vykryly-onlajn-shaxraya-6623/
[39] https://cyberpolice.gov.ua/news/u-kyyevi-sud-pryznachyv-pokarannya-choloviku-za-prodazh-neisnuyuchogo-vijskovogo-sporyadzhennya-2199/

- псевдозбір грошей для дітей, які залишились без батьків;[40]
- створення шахрайських сторінок, які використовують тематику грошових компенсацій та фінансової допомоги від ООН, Європейського суду з прав людини, Товариства Червоного Хреста тощо. На цих сайтах користувачам пропонують отримати виплату за умови надання персональної інформації та здійснення додаткового платежу. Як результат, дані банківської картки будуть скомпрометовані.[41]

Також під час моніторингу було виявлено два судових рішення, які стосуються шахрайства в інтернеті:

1. Ухвала Білоцерківського міськрайонного суду Київської області щодо надання тимчасового доступу до речей у справі внесеному до ЄРДР № 12022116030001216 від 24.07.2022 року,[42] за ознаками кримінального правопорушення передбаченого ч.1 ст.190 КК України. Досудовим розслідуванням в даній справі було встановлено, що 12.07.2022 року потерпіла знайшла оголошення в інтернет-мережі “Facebook” про соціальні виплати на кожну родину 9000 гривень. Натиснувши на посилання, яке було під оголошенням (http:// next24.ie-pays.com/recv/6505913680) на екрані мобільного телефону висвітлився мобільний додаток. Ввівши свій логін, пароль номер телефону в подальшому ввела пін код від своєї банківської картки. Через хвилину почали надходити смс повідомлення про списання грошових коштів, які були на її кредитній картці. Таких транзакцій було 3 та загальна сума зняття грошових коштів становить 12000 гривень та 480 гривень комісії.
2. Ухвала Білоцерківського міськрайонного суду Київської області про тимчасовий доступ до інформації, яка містить охоронювану законом таємницю по кримінальному провадженню № 12022116030001199 від 22.07.2022 року.[43] В ході досудового розслідування встановлено, що 27.06.2022 року потерпілий, у додатку “Фейсбук” знайшов оголошення про продаж військової форми. Зв'язався із невідомим продавцем у “месенджері” та домовився про купівлю військової форми на суму 2600 гривень. Невідомий продавець скинув номер картки у “месенджер” та попросив потерпілого перерахувати йому суму 600 гривень завдатку за товар. Потерпілий кошти перерахував але товар не отримав, чим завдано матеріального збитку на суму 600 гривень.

БЛОКУВАННЯ ВЕБ-РЕСУРСІВ

I. Блокування веб-ресурсів за рішеннями державних органів

З початку дії в Україні правового режиму воєнного стану блокування вебресурсів здійснювалося у позасудовому порядку на підставі рекомендацій, які надавав постачальникам електронних комунікаційних мереж та/або послуг основних інтернет-ресурсів Національний центр оперативно-технічного управління електронними

[40] https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zhinku-na-psevdozbori-groshej-dlya-rodyny--richnogo-xlopczya-yakyj-iz-chotyrma-bratamy-ta-sestramy-cherez-vijnu-zalyshyvsya-bez-materi-949/
[41] https://www.imi.org.ua/news/u-facebook-aktyvizuvalysya-shahrayi-yaki-spekulyuyut-na-temi-groshovyh-vyplat-derzhspetszv-yazku-i47440
[42] https://reyestr.court.gov.ua/Review/105552247
[43] https://reyestr.court.gov.ua/Review/105791469

комунікаційними мережами України (далі – НЦУ). У звітному періоді НЦУ не надавав рекомендації щодо блокування вебресурсів, але продовжували діяти ті блокування, які НЦУ просив постачальників електронних комунікаційних мереж та/або послуг основних інтернет-ресурсів запровадити в перші місяці широкомасштабного вторгнення, зокрема:

Загалом, за рекомендацією НЦУ постачальниками електронних комунікаційних мереж та/або послуг було заблоковано **854 вебресурсів.**

II. Блокування веб-ресурсів окупантів українською ІТ-армією та іншими ІТ-волонтерами.

У перші дні повномасштабного російського вторгнення Міністр цифрової трансформації України Михайло Федоров у своєму телеграм-каналі запропонував створити українську ІТ-армію[44] з розробників, кіберспеціалістів, дизайнерів, копірайтерів, маркетологів, таргетологів тощо та запустити телеграм-канал IT ARMY of UKRAINE.

Основною ідеєю створення зазначеного телеграм-каналу було об'єднання зусиль ІТ-спеціалістів на волонтерських засадах з метою протидії окупантам на кібер- та інформаційному фронті. До ініціативи одразу долучилася велика кількість українських і міжнародних ІТ-фахівців.

Сьогодні українська "ІТ-армія" є самоорганізованим волонтерським рухом і відіграє велику роль у кіберзахисті України та особливу роль у цифровій війні. У серпні 2022 р. волонтери кібервійська долучалися до блокування роботи **1050 російських веб-ресурсів.** Міністерство цифрової трансформації України надало звіт про діяльність української ІТ-армії в серпні 2022 року. За даними міністерства, українська ІТ-армія заблокувала понад 600 ресурсів за два перших тижні серпня з 1 до 14 серпня[45] та вивела з ладу понад 450 російських онлайн-ресурсів[46] з 15 по 28 серпня 2022 року.

За даними відомства, українські айтівці блокували:

- центральний банк рф. Банку довелося відключати сервіси та обмін електронними документами. Це паралізувало роботу ЦБ з фінустановами та реєстрами й дестабілізувало роботу інших російських банків;
- політичну партію "Справедливая россия — патриоты — за правду". Всі ресурси партії, що поширюють пропаганду, були деякий час недоступні;
- популярні онлайн сервіси переказу грошей. ІТ-армія призупинила роботу російських аналогів банківських сервісів, через які росіяни досі могли оформляти міжнародні віртуальні карти і переказувати гроші;
- сервіс пошуку роботи. Російський сайт пошуку роботи SuperJob почав діяти в окупованих регіонах України. Це допомагало загарбникам швидко відкривати вакансії та працевлаштовувати "своїх". Атака ІТ-армії паралізувала ворожий сервіс;
- сайт рітейлера DNS. Компанія дозволяла росіянам безперешкодно незаконно імпортувати українські товари у рф. ІТ-армія зупинила головний сайт компанії, що реалізовував контрабанду;
- флагманські пропагандистські ЗМІ. Айтівці по черзі виводили з ладу великі пропагандистські російські медіа – ТАСС, РИА Новости, МК та їх окремі

[44] https://t.me/zedigital/1114
[45] https://t.me/mintsyfra/3324
[46] https://t.me/mintsyfra/3367

проєкти. За час простою ці ресурси загалом втратили понад мільйон потенційних споживачів пропаганди;

– сайти окупантів у Криму. 24 серпня на головних сторінках російських сайтів, які зараз діють у Криму, ІТ-армія розмістила привітання з Днем Незалежності України.

III. Блокування інформації платформами спільного доступу до інформації (соціальними мережами)

06 серпня 2022 року Компанія Meta оголосила, що **відключила понад тисячу фальшивих облікових записів,** з яких публікували численні коментарі на підтримку російського вторгнення в Україну. У своєму квартальному звіті Meta повідомила, що виявила "фізичну ферму тролів, яка працювала в офісній будівлі в Санкт-Петербурзі", відому як Cyber Front Z, через місяць після початку вторгнення в Україну. "Ферма" була націлена на користувачів на кількох платформах, включаючи Twitter і LinkedIn, а також Facebook і Instagram. "Cyber Front Z керував каналом Telegram, який закликав людей залишати проросійські коментарі до публікацій у соцмережах громадських діячів, журналістів, політиків, знаменитостей, таких як Анджеліна Джолі та Морган Фрімен", — заявив керівник відділу глобальної розвідки загроз Meta Бен Німмо.[47]

09 серпня 2022 року Інстаграм припинив доступ до сторінки Асоціації родин захисників "Азовсталі", де рідні військових, які боронили Маріуполь від росіян, повідомляли про все, що відбувається з ними після того, як вони потрапили в полон у травні 2022 року. Через добу після блокування Instagram повернула доступ до сторінки Асоціації родин захисників "Азовсталі"[48].

11 серпня 2022 року Ютуб видалив відео під назвою "Семинар резидентуры СВР рф для полиции Австрии об "украинских националистах". Про це повідомив його автор — медіаексперт, ексзаступник міністра інформаційної політики України Дмитро Золотухін на своїй сторінці у фейсбуку. Причиною санкцій з боку платформи стало "порушення авторських прав за скаргою Координаційної ради організацій російських співвітчизників в Австрії"[49].

14 серпня 2022 року Ютуб видалив черговий випуск програми "Вечір з Яніною Соколовою" за 12 серпня 2022 року, який було присвячено подіям в окупованому Криму. Це сталося через нібито "порушення політики щодо ворожих висловлювань. "Відео вийшло на каналі проєкту о 18-й годині, а вже о 20-й його видалили "через численні скарги московитів", - написала вона. Соколова уточнила, що у випуску порушували теми Криму, війни, брехні росіян щодо їхніх "успіхів" у війні, а також показали призерів нагородження конкурсу Z-культури в Москві[50]

Всього у звітний період зафіксовано **1003** випадки блокування постів платформами спільного доступу до інформації (соціальними мережами).

Таким чином, у звітний період зафіксовано наступні випадки блокувань веб-ресурсів або інформації на веб-ресурсах:

– продовжують діяти 854 блокування веб-ресурсів за ініціативи НЦУ;

– українські ІТ-волонтери заблокували або ускладнили роботу 1050 російських веб-ресурсів;

[47] https://zmina.info/news/kompaniya-meta-zablokuvala-fermu-troliv-yaka-poshyryuvala-rosijsku-propagandu/
[48] https://ms.detector.media/sotsmerezhi/post/30031/2022-08-10-instagram-vidnovyv-storinku-asotsiatsii-rodyn-zakhysnykiv-azovstali/
[49] https://www.facebook.com/dzolotukhin/posts/pfbid029RVU9MWWu4AYZXg7UmWZAKbUmpeeq5ntMRAspsn9AT9XKrWqrTW6cTPp1bEYfYiil
[50] https://www.facebook.com/yanina.sokolova/posts/pfbid02VzwacHT9KHBjk54kMwxfM6tPAQzkSZAr9JwQ2McxMpnh3dWm5V1Q2u8L3v9Wy6pHl

– відбулось блокування 1003 повідомлень платформами спільного доступу до інформації (соціальними мережами).

Аналіз вищезазначеної інформації здебільшого свідчить про потенційну загрозу цифровим правам людини. Насамперед, це пов'язано з тим, що всупереч нормам національного законодавства, яке передбачає тільки судовий порядок, блокування здійснюються в позасудовому. Навіть, враховуючи той факт, що державні органи на період дії воєнного стану мають повноваження регулювати роботу постачальників електронних комунікаційних мереж та/або послуг, порядок такого регулювання та його межі, наразі, законодавством не визначено. По-друге, крім критерію "передбачено законом", практика Європейського суду з прав людини вимагає, щоб обмеження переслідувало "легітимну мету" та було "необхідним у демократичному суспільстві". На момент написання даного звіту немає можливості в повній мірі проаналізувати зазначені вимоги Конвенції про захист прав людини і основоположних свобод в контексті вищезазначених блокувань. Більшість повідомлень про факти обмежень, які були виявлені спеціалістами з моніторингу, містили лише загальну статистику без переліку чи посилань на самі ресурси, що було заблоковано. У випадках, коли ресурси ідентифіковано - до них вже обмежено доступ, що, в свою чергу, також, унеможливлює аналіз їх контенту.

ДОСТУП ДО ІНТЕРНЕТУ

У серпні 2022 року без можливості користуватись українським зв'язком та інтернетом продовжували залишались мешканці окупованих територій - Херсонської області, міст Бердянськ та Мелітополь. На окупованих територіях ворог заблокував доступ до українських ресурсів 30 травня 2022 року. [51]

ЗМІНИ В ЗАКОНОДАВСТВІ

У серпні 2022 року Указом Президента України було продовжено дію правового режиму воєнного стану. Указав № 573/2022 "Про продовження дії воєнного стану в Україні" [52]набув чинності 17 серпня 2022 року, після його затвердження Верховною Радою України відповідним законом. [53]

Кабінетом міністрів України у звітний період було прийнято дві постанови, які мають безпосередній вплив на цифрові права людини:

1. Постанова КМУ "Про затвердження Порядку надання електронних публічних послуг в автоматичному режимі" від 5 серпня 2022 р. № 868.[54] Цей Порядок визначає механізм надання електронних публічних послуг, що надаються в автоматичному режимі програмними засобами інформаційно-комунікаційних

[51] https://suspilne.media/245018-v-okupovanih-melitopoli-ta-berdansku-vidsutnij-ukrainskij-mobilnij-zvazok/
[52] https://zakon.rada.gov.ua/laws/show/573/2022#Text
[53] https://zakon.rada.gov.ua/laws/show/2500-20#Text
[54] https://zakon.rada.gov.ua/laws/show/868-2022-%D0%BF#Text

систем, без додаткового опрацювання суб'єктами надання електронних публічних послуг у режимі реального часу або з відкладеною умовою на підставі заяв (звернень, запитів) суб'єктів звернення, поданих в електронній формі з використанням засобів Єдиного державного веб-порталу електронних послуг.

2. Постанова КМУ "Деякі питання передачі персональних даних за межі України засобами Єдиного державного вебпорталу електронних послуг" від 16 серпня 2022 р. № 910.[55] Постанова визначає, що для забезпечення можливості використання громадянами України за їх бажанням електронного відображення інформації, що міститься у документах, передачі електронних копій відповідних документів, отримання публічних послуг за межами України персональні дані можуть передаватися за допомогою засобів Єдиного державного вебпорталу електронних послуг іноземним суб'єктам відносин, пов'язаних з персональними даними, держав, що забезпечують належний захист персональних даних та надає перелік держав, що забезпечують належний захист персональних даних. Також в постанові йдеться про те, що персональні дані не можуть передаватися іноземним суб'єктам, що зареєстровані у державі, визнаній Верховною Радою України державою-агресором чи державою-окупантом, державах, які входять до митних та воєнних союзів з такими державами, та/або кінцевим бенефіціарним власником, членом або учасником (акціонером) яких є зазначені держави, суб'єктам, діяльність яких підпадає під дію Закону України "Про санкції", щодо яких прийнято рішення про застосування санкцій в Україні.

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ

Введення воєнного стану в Україні у зв'язку з широкомасштабним вторгненням росії та необхідність захисту суверенітету і територіальної цілісності обумовили внесення змін до законодавства України в багатьох сферах, в тому числі й у інформаційній.

Зокрема, в серпні продовжував діяти правовий режим воєнного стану, який було введено Указом Президента України від 24 лютого 2022 р. № 64/2022 "Про введення воєнного стану в Україні"[56] та затверджено Законом України № 2102-IX "Про затвердження Указу Президента України "Про введення воєнного стану в Україні". Протягом березня–серпня 2022 р. строк дії правового режиму воєнного стану продовжувався чотири рази і нині він діятиме до 21 листопада 2022 р. Зазначеним Указом передбачена можливість обмеження ряду фундаментальних прав людини, зокрема, право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Також, продовжували дію нормативно-правові акти, більшість з яких було запроваджено в березні 2022 року на період дії правового режиму воєнного стану і які мають безпосередній вплив на свободу вираження поглядів. Серед них:

1) Закон України "Про правовий режим воєнного стану",[57] на підставі якого військове командування разом із військовими адміністраціями (у разі їх утворення) можуть самостійно або із залученням органів виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування регулювати у порядку, визначеному Кабінетом Міністрів України:

[55] https://zakon.rada.gov.ua/laws/show/910-2022-%D0%BF#Text
[56] https://www.president.gov.ua/documents/642022-41397
[57] https://zakon.rada.gov.ua/laws/show/389-19#Text

- роботу постачальників електронних комунікаційних мереж та/або послуг;
- роботу поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій і закладів культури та ЗМІ;
- використовувати місцеві радіостанції, телевізійні центри та друкарні для військових потреб і проведення роз'яснювальної роботи серед військ і населення.

2) Наказ Головнокомандувача ЗСУ від 3 березня 2022 р. № 73 "Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану" (далі – Наказ), яким окреслено перелік забороненої до поширення інформації.

Також, в березні 2022 року, Кримінальний кодекс України було доповнено новими статтями (ст.ст. 111^{-1}, 114^{-2}, 435^{-1}, 436^{-2}), практика застосування яких має безпосередній вплив на свободу вираження поглядів.

У серпні 2022 року судами було ухвалено 75 судових рішень за цими статтями КК України:

1. За **ч.1. ст.111^{-1} КК України,** яка передбачає відповідальність за заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України) - було ухвалено **20 вироків** із покаранням у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю строком від десяти до п'ятнадцяти років;
2. За **ч.2 ст.114^{-2} КК України,** яка передбачає відповідальність за поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, вчинене в умовах воєнного або надзвичайного стану) було ухвалено **19 судових рішень** - 2 (два) вироки із покаранням у виді позбавлення волі на строк 2 (два) роки 6 (шість) місяців та покарання у виді 5 (п`яти) років позбавлення волі та звільненням від призначеного покарання з іспитовим строком на 2 (два) роки; 17 (сімнадцять) ухвал про застосування запобіжних заходів у вигляді тримання під вартою або домашнього арешту;
3. За **ч. 3 ст. 114^{-2} КК України**, яка передбачає відповідальність за дії, передбачені частиною першою або другою цієї статті, вчинені за попередньою змовою групою осіб або з корисливих мотивів, або з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням, або якщо вони спричинили тяжкі наслідки, за відсутності ознак державної зради або шпигунства) - було прийнято **11 судових рішень -** 1 (один) вирок із покаранням у виді 9 (девяти) років позбавлення волі та 10 (десять) ухвал про застосування запобіжного заходу у вигляді тримання під вартою;

4. За **ч.1 ст.436-2 КК України**, яка передбачає відповідальність за виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії російської федерації проти України як внутрішнього громадянського конфлікту, виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України, а також глорифікація осіб, які здійснювали збройну агресію російської федерації проти України, розпочату у 2014 році, представників збройних формувань російської федерації, незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих російською федерацією, а також представників окупаційної адміністрації російської федерації, яку складають її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних російській федерації самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України) - судами було винесено **2 вироки** із покарання у вигляді 3 (трьох) років позбавлення волі та звільнення від відбуття призначеного покарання з випробуванням з іспитовим строком на 2 (два) роки та покарання у виді позбавлення волі на строк 1 (один) рік 6 (шість) місяців та звільнення від відбування призначеного покарання у виді позбавлення волі з іспитовим строком на три роки.
5. За **ч.2 ст. 436-2 КК України**, яка передбачає відповідальність за виготовлення, поширення матеріалів, у яких міститься виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії російської федерації проти України як внутрішнього громадянського конфлікту, виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України, а також глорифікація осіб, які здійснювали збройну агресію російської федерації проти України, розпочату у 2014 році, представників збройних формувань Російської Федерації, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих російською федерацією, а також представників окупаційної адміністрації російської федерації, яку складають її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних російській федерації самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України, - судами було винесено **19 судових рішеннь:**

– 16 вироків із покаранням від трьох до п'яти років позбавлення волі та звільнення від відбування покарання з іспитовим строком від одного до трьох років.

– три ухвали про застосування запобіжних заходів у вигляді тримання під вартою або домашнього арешту.

6. За **ч.3 ст.436-2 КК України**, яка містить відповідальність за дії, передбачені частиною першою або другою цієї статті, вчинені службовою особою, або вчинені повторно, або організованою групою, або з використанням засобів масової інформації судами було ухвалено **4 вироки** із покаранням у вигляді п'яти років позбавлення волі та звільнення від відбування покарання з іспитовим строком від двох до трьох років.

Крім ухвалення вироків за новими статтями Кримінального кодексу України, протягом звітного періоду судами було ухвалено досить велику кількість рішень, щодо притягнення до відповідальності за статтями 109, 110, 111, 436, 436-1 КК України. Зазначена практика також має вплив на цифрові права людини, оскільки передбачає

застосування кримінальної відповідальності в тому числі за поширення небезпечної інформації в інтернеті.

1. **За ч. 2 ст. 109 КК України,** яка передбачає відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій було винесено **шість судових рішень:**

– 3 вироки із покаранням у вигляді позбавлення волі від трьох до п'яти років та звільнення від відбування покарання з іспитовим строком від одного до трьох років на підставі ст. 75 Кримінального кодексу України;

– 1 вирок із покаранням у вигляді штрафу в розмірі 1000 неоподаткованих мінімумів доходів громадян, що становить 17 000 гривень із застосуванням ст. 69 КК України, яка передбачає призначення більш м'якого покарання, ніж передбачено законом;[58]

– 2 ухвали про застосування запобіжних заходів у вигляді тримання під вартою або особистого зобов'язання.

2. **За ч. 1 ст. 110 КК України,** яка передбачає відповідальність за умисні дії, вчинені з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, а також публічні заклики чи розповсюдження матеріалів із закликами до вчинення таких дій - було винесено **п’ять вироків:**

– 4 вироки із покаранням у вигляді позбавлення волі від трьох до чотирьох років та звільнення від відбування покарання з іспитовим строком від одного до трьох років на підставі ст. 75 Кримінального кодексу України;

– 1 вирок із покарання у виді позбавлення волі на строк 3 (три) роки 6 (шість) місяців без конфіскації майна і без позбавлення права обіймати певні посади та займатися певною діяльністю та **без звільнення від відбування покарання.**

3. **За ч. 2 ст. 110 КК України,** яка передбачає відповідальність за ті самі дії, як і в частині першій статті 110 КК, але якщо їх вчинено особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднані з розпалюванням національної чи релігійної ворожнечі - було ухвалено **два судових рішення:**

– 1 вирок про призначення покарання із застосуванням ст. 69 КК України, яка передбачає призначення більш м'якого покарання, ніж передбачено законом у вигляді штрафу в розмірі 1000 неоподаткованих мінімумів доходів громадян, що становлять 17 000 гривень;

– 1 ухвала про застосування запобіжного заходу у виді тримання під вартою.

4. **За ч. 1 ст. 111 КК України,** яка передбачає відповідальність за державну зраду, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові,

[58] **Стаття ККУ 69.** Призначення більш м'якого покарання, ніж передбачено законом

1. За наявності кількох обставин, що пом'якшують покарання та істотно знижують ступінь тяжкості вчиненого кримінального правопорушення, з урахуванням особи винного суд, умотивувавши своє рішення, може, крім випадків засудження за корупційне кримінальне правопорушення, кримінальне правопорушення, пов’язане з корупцією, призначити основне покарання, нижче від найнижчої межі, встановленої в санкції статті (санкції частини статті) Особливої частини цього Кодексу, або перейти до іншого, більш м'якого виду основного покарання, не зазначеного в санкції статті (санкції частини статті) Особливої частини цього Кодексу за це кримінальне правопорушення. У цьому випадку суд не має права призначити покарання, нижче від найнижчої межі, встановленої для такого виду покарання в Загальній частині цього Кодексу. За вчинення кримінального правопорушення, за яке передбачене основне покарання у виді штрафу в розмірі понад три тисячі неоподатковуваних мінімумів доходів громадян, суд з підстав, передбачених цією частиною, може призначити основне покарання у виді штрафу, розмір якого не більше ніж на чверть нижчий від найнижчої межі, встановленої в санкції статті (санкції частини статті) Особливої частини цього Кодексу.

територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України - було винесено **один вирок** із покаранням у вигляді 5 (п`яти) років позбавлення волі без конфіскації майна із застосуванням ст. 69 КК України, **без звільнення від відбування покарання.**

5. **За ч.2 ст.111 КК України,** яка передбачає відповідальність за державну зраду, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України **в умовах воєнного стану** - було винесено **дві ухвали** про застосування запобіжного заходу у вигляді тримання під вартою.
6. **За ч. 1 ст. 436-1 КК України**, яка передбачає відповідальність за виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів - було винесено **два судові рішення:** один вирок з покаранням у вигляді позбавлення волі на два роки, на підставі ст. 75 КК України особу було звільнено від відбування призначеного покарання, встановлено іспитовий строк в 2 (два) роки та одну ухвалу про арешт майна (вилучення мобільного телефону).

Загалом за звітний період було судами було прийнято **93 рішень** за статтями Кримінального кодексу України, практика застосування яких має безпосередній вплив на свободу вираження поглядів в інтернеті. Це пов'язано з тим, що поширення інформації, яке стало підставою для застосування кримінальної відповідальності у всіх проаналізованих судових рішеннях, відбувалось в мережі Інтернет. В більшості випадків таке поширення відбувалось на платформах спільного доступу до інформації Фейсбук, ТікТок, Однокласники, Вконтакте та мессенджерах Телеграм, Вайбер, Вотсап, тощо.

Варто зазначити, що в даних рішеннях, досить часто мова йде про розповсюдження інформації шляхом репосту із написанням власних коментарів або шляхом поставлення “лайку” або “вважає класним”, а не поширення самостійно виготовлених матеріалів.

У серпні суди продовжували ухвалювати вироки за частиною першою статті 111-1 КК України із покаранням “позбавлення права обіймати певні посади або займатись певною діяльністю на строк від 10 до 15 років”, позбавляючи такого права непрацюючих або пенсіонерів. Загалом, в 10 з 20 вироків права обіймати посади позбавлялися саме такі групи населення. Така практика пов'язана з тим, що за ч. 1 ст. 111-1 КК України передбачено лише один, зазначений, безальтернативний вид покарання.

Окремо хотілось би звернути увагу та той факт, що відповідно до проаналізованих вироків **три особи,** яких було визнано винними у вчинені злочинів, понесли реальне покарання. Більшість від відбування покарання було звільнено на підставі статті 75 КК України (обвинувачені в переважній більшості визнавали свою провину). Реальні покарання у виді позбавлення волі було винесено за наступними справами:

1. Справа № №522/9616/22,[59] яку було розглянуто Приморським районним судом м. Одеса, і в якій громадянина російської федерації було визнано винуватим у вчиненні злочину, передбаченого **ч. 2 ст. 114-2 КК** України, та призначено

[59] https://reyestr.court.gov.ua/Review/105683797

покарання із застосуванням ст. 69 КК України, яка передбачає призначення більш м'якого покарання, ніж передбачено законом, у виді позбавлення волі на строк **2 (два) роки 6 (шість) місяців.**

2. Справа № 761/13295/22,[60] яку було розглянуто Шевченківським районним судом міста Києва, і в якій громадянина України було визнано винуватим за **ч. 3 ст. 114-2 КК** України і призначено покарання у виді **9 (дев`яти) років** позбавлення волі.
3. Справа № 279/1379/22,[61] яку було розглянуто Корольовським районним судом м. Житомира, і в якій громадянина України було визнано винним у вчиненні злочину, передбаченого **ч. 1 ст. 111 КК України** (в редакції 07.10.2014), та призначено йому покарання із застосуванням ст. 69 КК України у виді **5 (п`яти) років** позбавлення волі без конфіскації майна.

Варто зазначити, що серед трьох вироків, якими було призначено реальне покарання у виді позбавлення волі, два вироки було ухвалено за новою статтею ККУ 114-2 і такий вид покарання був застосований вперше, з моменту внесення до Кримінального кодексу України цієї статті.

Аналіз двох вироків, за якими було призначено покарання за ст. 114-2 КК України у вигляді позбавлення волі без звільнення від відбування покарання, дозволяє зробити висновки про існування проблеми неоднакового правозастосування - коли при аналогічних фабулах застосовується різна кваліфікація та суттєво різні санкції. Зокрема, цю ситуацію ілюструє порівняння цих вироків:

Справа	Справа № №522/9616/22[62]	Справа № 761/13295/22[63]
Суб'єкт	Уродженць м. Москва, російська федерація, громадянина російської федерації, одруженого, з вищою освітою, працюючий провідним інженером у Національному дослідницькому ядерному університеті «МІФІ» м. Москва, раніше не судимого	Уродженець м. Краматорськ, Донецької області, громадянин України, розлучений, освіта середньо-спеціальна, місце роботи: Краматорська ТЕЦ, охоронець
Суспільно небезпечного діяння, яке містить склад кримінального правопорушення	З метою реалізації злочинного умислу, в період часу з 24.02.2022 до 13.03.2022 (більш точний час досудовим розслідуванням не встановлено), перебуваючи за місцем свого проживання у, при невстановлених слідством обставинах, використовуючи хмарне сховище, доступ до якого, серед іншого, можливо здійснити через браузер Google Chrome, створив документ із	На виконання свого злочинного умислу, вступив у злочинну змову з користувачами додатку «Zello» - акаунт належить громадянину рф, співробітнику 9-го управління департаменту оперативної інформації 5-ї служби фсб рф, та іншими, та розуміючи, що вказані особи є представниками російської федерації та інших незаконних збройних формувань, погодився надавати останнім інформацію про переміщення, рух та розташування

[60] https://reyestr.court.gov.ua/Review/105914431
[61] https://reyestr.court.gov.ua/Review/105533952
[62] https://reyestr.court.gov.ua/Review/105683797
[63] https://reyestr.court.gov.ua/Review/105914431

	назвою «ІНФОРМАЦІЯ_3». Вказаний документ зберігався у вказаному хмарному сховищі та доступ до нього мали невстановлені особи, які знаходяться на території рф. Продовжуючи реалізацію свого вищевказаного злочинного умислу, у період часу з 24.02.2022 по 14 год. 04 хв. 06.06.2022 (більш точний час досудовим розслідуванням не встановлено), використовуючи наявні технічні засоби із доступом до мережі Інтернет, в документі із назвою «ІНФОРМАЦІЯ_3», до якого мають доступ невстановлені особи, які знаходяться на території рф, описував, чим навмисно та незаконно здійснював поширення інформації, про місця розміщення та розташування сил та засобів Збройних сил України чи інших утворених відповідно до законів України військових формувань у м. Одесі.	Збройних Сил України та інших утворених відповідно до законів України військових формувань, яка не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами. Так, у період часу з березня 2022 року до 26 квітня 2022 року передавав вказаним особам відомості щодо обстрілів у м. Краматорськ Донецької області. Після чого, у період часу з 26.04.2022 по 27.04.2022, більш точний час досудовим розслідуванням не встановлено, перебуваючи у м. Краматорськ Донецької області, через додаток «Zello» з акаунту «ІНФОРМАЦІЯ_3» повідомив ОСОБА_2 про те, що 27.04.2022 планує відвідати військову частину, яка знаходиться за адресою: АДРЕСА_2 , на що отримав від ОСОБА_2 завдавання щодо з`ясування розташування приміщень та військової техніки Збройних Сил України на території вказаної військової частини.  27.04.2022 ОСОБА_1 , знаходячись на території військової частини НОМЕР_2 , яка знаходиться за адресою: АДРЕСА_2 , на виконання свого злочинного умислу, запам`ятав розташування військової техніки, яка знаходилась на території військової частини НОМЕР_2 . Після чого, 27.04.2022 ОСОБА_1 , знаходячись за місцем свого проживання за адресою: АДРЕСА_1 , на виконання свого злочинного умислу направленого на надання інформації про розташування Збройних Сил України представникам Російської Федерації та іншим незаконним збройним формуванням, у своєму телефоні наніс на мапу військової частини НОМЕР_2 місця розташування військової техніки

		та передав зі свого акаунту «ІНФОРМАЦІЯ_3» у додатку «Zello» фотознімок ОСОБА_2 шляхом надсилання особистого повідомлення у акаунт «ІНФОРМАЦІЯ_4» додатку «Zello».
Кваліфікація	Діяння обвинуваченого кваліфіковано **за ч. 2 ст. 114-2 КК** України, як: поширення інформації про переміщення, рух та розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, вчинене в умовах воєнного стану.	Вчинив поширення інформації про переміщення, рух та розташування Збройних Сил України та інших утворених відповідно до законів України військових формувань, їх ідентифікація на місцевості, яка не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, вчинене в умовах воєнного стану, з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам або іншим незаконним збройним формуванням, тобто кримінальне правопорушення, передбачене **ч. 3 ст. 114-2 КК України.**
Визнання провини	Визнав	Визнав
Покарання	Визнано винуватим у вчиненні злочину, передбаченого **ч. 2 ст. 114-2 КК України** та призначено покарання, із застосуванням ст. 69 КК України, **у виді позбавлення волі на строк 2 (два) роки 6 (шість) місяців.**	Визнано винуватим за **ч. 3 ст. 114-2 КК України** і призначено покарання у **виді 9 (дев`яти) років позбавлення волі.**

Крім правозастосовчих проблем, під час моніторингу було виявлено факти, які свідчать про потенційне порушення цифрових прав та полягають в наступному:

1. У **17** ухвалених рішеннях не визначено інформацію, поширення якої стало підставою для притягнення особи до кримінальної відповідальності, що не дає можливості оцінити зміст поширеної інформації та пропорційність застосування до особи заходів або санкцій.

Прикладом такого рішення може бути вирок, ухвалений Київським районним судом м. Харкова у справі № 953/4226/22, в якому наступним чином описано кримінальне правопорушення:[64] *"З метою реалізації свого злочинного умислу, ОСОБА_2 в період часу з 17.03.2022 по 27.03.2022, перебуваючи за адресою проживання: АДРЕСА_1 , використовуючи свій мобільний телефон, з використанням власної сторінки « ОСОБА_3 » у соціальній мережі «Одноклассники», здійснював перегляд сторінок окремих осіб та груп (« ІНФОРМАЦІЯ_2 », « ІНФОРМАЦІЯ_6 », «ІНФОРМАЦІЯ_5», « ІНФОРМАЦІЯ_3 », « ІНФОРМАЦІЯ_7 », « ІНФОРМАЦІЯ_4 »), що поширювали інформацію в якій містилось виправдовування, визнання правомірною збройної агресії рф проти України, та як наслідок тимчасову окупацію територій України, а також глорифікація дій осіб, які причетні до вказаної збройної агресії, та осіб, які були учасниками іррегулярних збройних формувань контрольованих рф, діяльність яких була направлена на тимчасову окупацію територій України, розпочату у 2014 році.*

Продовжуючи реалізацію свого злочинного умислу, ОСОБА_2 , в період часу з 17.03.2022 по 27.03.2022, перебуваючи за вказаною адресою, в ході огляду зазначених сторінок та груп у соціальній мережі «Одноклассники», виокремив окремі публікації, які відповідають його ідейним і політичним поглядам та доводячи свій злочинний умисел до кінця, шляхом натиснення на клавішу «вподобати», що розміщувалась внизу кожної публікації, які містили вищевказану інформацію, здійснив поширення даних публікацій на власній сторінці, у зв`язку з чим вони стали доступні для ознайомлення та прочитання невизначеній кількості людей.

Таким чином, ОСОБА_2 вчинив поширення матеріалів в яких міститься виправдовування, визнання правомірною збройної агресії рф проти України, заперечення тимчасової окупації частини території України, глорифікація осіб, які здійснюють збройну агресію з боку російської федерації проти України, а також глорифікація осіб, які були учасниками іррегулярних збройних формувань контрольованих рф, діяльність яких була направлена на тимчасову окупацію територій України, розпочату у 2014 році, тобто кримінальне правопорушення - злочин, передбачений ч. 2 ст. 436-2 КК України."

Варто зазначити, що приховування від громадськості обставин справи не дає можливості зрозуміти суть правопорушення, встановленого судом, а також мотиви суду при ухваленні рішення. Відтак, публікація подібних неповних текстів судових рішень із приховуванням значної частини інформації, важливої для громадського контролю, має ознаки порушення принципу гласності та публічності судових процесів та, зокрема, публічності судових рішень, а також права громадян на інформацію про діяльність судової влади.

2. **11 рішень,** в яких не міститься інших способів аналізу поширеної інформації судом, крім посилань на висновки експертів-лінгвістів. В таких рішеннях вбачається ризик того, що судова практика є, насправді, повним відтворенням позиції і практикою відповідних судових експертів. Прикладом такого рішення може бути вирок, ухвалений Солом'янським районним судом м. Києва у справі № 760/7425/22.[65]

3. **8 рішень,** в яких поєднується, як відсутність інформації, поширення якої стало підставою для притягнення до кримінальної відповідальності так і відсутність власної оцінки судом її змісту з виключно посиланнями на висновки експертів-лінгвістів. Прикладом такого судового рішення є вирок ухвалений Жмеринським міськрайонним судом Вінницької області у справі № 1-кп/130/296/2022.[66]

Також, під час моніторингу було виявлено **два судові рішення у цивільних справах,** які містять порушення цифрових прав людини у вигляді непропорційного обмеження права на свободу вираження поглядів:

[64] https://reyestr.court.gov.ua/Review/104469905
[65] https://reyestr.court.gov.ua/Review/105596225
[66] https://reyestr.court.gov.ua/Review/105679231

Одночасне застосування таких способів правового захисту, як спростування та видалення спірних відомостей без обґрунтування необхідності в цьому; невмотивованість рішень про видалення спірної інформації, що порушує європейські стандарти у галузі свободи слова.

Як зазначалось в попередніх звітах про результати моніторингу цифрових прав, в Україні активно розвивається судова практика, відповідно до якої суди зобов'язують не лише спростовувати ту чи іншу інформацію, визнану недостовірною, але й видаляти спірні відомості. При цьому, такі судові рішення, як правило, належним чином не мотивуються. Детальніше зазначену проблему описано в аналітичному звіті "Судова практика у справах про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики"[67].

У серпні 2022 року під час моніторингу виявлено 2 (два) рішення про спростування та видалення спірних відомостей без належного обґрунтування необхідності в цьому, а саме: рішення Господарського суду м. Києва у справах № 910/15276/21[68] та № 910/19527/21[69].

Окремо варто зауважити, що в Єдиному державному реєстрі судових рішень продовжують з'являтися рішення у справах про захист честі, гідності і ділової репутації, а також вироки судів в яких зміст спірної інформації прихований позначками "ІНФОРМАЦІЯ No_", що унеможливлює ознайомлення з відомостями, щодо яких заявлено позовні вимоги (подано заяву про встановлення фактів, що мають юридичне значення, постановлено вирок). Прикладом такої практики є рішення Господарського суду м. Києва у справі № 910/15276/21[70]

ДОСТУП ДО ІНФОРМАЦІЇ

Відповідно до пункту 3 Указу Президента України № 64/2022 "Про введення воєнного стану в Україні" (затверджено Законом України "Про затвердження Указу Президента України "Про введення воєнного стану в Україні", реєстраційний № 2102-IX від 24 лютого 2022 р.) у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, передбачено можливість обмеження, в тому числі, права вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Негативна практика, яка була зафіксована в лютому-липні 2022 року щодо практики застосування Закону України "Про доступ до публічної інформації" та стосувалась відмови у наданні відповідей на запити, неоприлюднення інформації на офіційних вебсайтах органів державної влади та обмеженням чи повним припиненням доступу до інформації в публічних реєстрах, зменшилась у звітний період, але все ще мала місце.

[67] https://www.ppl.org.ua/wp-content/uploads/2020/08/Судова-практика-у-справах-поширення-інформації-в-інтернеті.pdf
[68] https://reyestr.court.gov.ua/Review/105702063
[69] https://reyestr.court.gov.ua/Review/105782760
[70] https://reyestr.court.gov.ua/Review/105702063

I. Щодо надання інформації на запити

У серпні 2022 року було проаналізовано **257 (двісті п'ятдесят сім) запитів**, які були направлені за допомогою веб ресурсу "Доступ до правди"[71]

Серед проаналізованих запитів щодо надання інформації було виявлено:

- 177 (сто сімдесят сім) запитів, на які розпорядники вчасно та в повній мірі надали свої відповіді;
- 48 (сорок вісім) запитів, на які розпорядники не надали відповідь;
- 32 (тридцять два) запити, на які було відмовлено в наданні публічної інформації.

Варто зазначити, що **із 32 відмов у наданні інформації 19 є неправомірними.** Надаючи неправомірні відмови у наданні доступу до публічної інформації, розпорядники посилались на наступні підстави:

1) Відстрочка у зв'язку із дією правового режиму воєнного стану.

10 (десять) відповідей, в яких розпорядник посилається на воєнний стан як на обставину непереборної сили було виявлено під час моніторингу. І серед розпорядників, які надавали такі відповіді були:

- Секретаріат Конституційного суду України;[72]
- Департамент охорони здоров'я та реабілітації Міністерства внутрішніх справ України;[73]
- Дніпровська міська рада (3 відповіді);[74];[75];[76]
- Дніпропетровська обласна військова адміністрація (2 відповіді);[77];[78]
- Черкаська міська рада;[79]
- Полтавська міська рада;[80]
- Івано-Франківська обласна прокуратура;[81]

В попередніх звітах ми, неодноразово, звертали увагу на те, і ще раз зазначаємо, що відстрочка розгляду запиту на отримання публічної інформації має відбуватись лише тоді, коли надання відповіді у визначені законодавством терміни є об'єктивно неможливим. Тобто, введення та дія воєнного стану самі собою не є достатньою підставою для відстрочення розгляду запиту, а тому в діях розпорядників інформації, які посилаються тільки на цей факт, спостерігається зловживання цією нормою.

2) Віднесення запитуваної інформації до інформації з обмеженим доступом.

6 (шість) відповідей, які містять посилання на інформацію з обмеженим доступом і серед розпорядників, які використали таку підставу:

- Рада національної безпеки та оборони;[82]

[71] https://dostup.pravda.com.ua
[72] https://dostup.pravda.com.ua/request/103050/response/361999/attach/2/2781..pdf?cookie_passthrough=1
[73] https://dostup.pravda.com.ua/request/103614/response/362640/attach/2/DLRKS907599 0AXUCF2NT.pdf?cookie
[74] https://dostup.pravda.com.ua/request/102336/response/361731/attach/3/.pdf?cookie_passthrough=1
[75] https://dostup.pravda.com.ua/request/102338/response/361365/attach/3/.pdf?cookie_passthrough=1
[76] https://dostup.pravda.com.ua/request/100190/response/361724/attach/3/.pdf?cookie_passthrough=1
[77] https://dostup.pravda.com.ua/request/103149/response/361997/attach/3/SendFile5828021.pdf?cookie_passthrough
[78] https://dostup.pravda.com.ua/request/103149/response/361997/attach/3/SendFile5828021.pdf?cookie_passthrough
[79] https://dostup.pravda.com.ua/request/103332/response/362373/attach/3/6706 2 17.08.2022.jpg?cookie_
[80] https://dostup.pravda.com.ua/request/103321/response/362615/attach/2/.jpg?cookie_passthrough=1
[81] https://dostup.pravda.com.ua/request/103058/response/361817/attach/3/.pdf?cookie_passthrough=1
[82] https://dostup.pravda.com.ua/request/103344/response/362388/attach/2/378.pdf?cookie_passthrough=1

- Головне управління розвідки Міністерства оборони України;[83]
- Чернігівська обласна прокуратура (2 відповіді);[84]; [85]
- Сумська міська рада;[86]
- Деснянська районна у місті Києві державна адміністрація.[87]

Обмеження доступу до інформації та віднесення її до інформації з обмеженим доступом має здійснюватись розпорядником інформації на підставі проведення "трискладового тесту" згідно Закону України "Про доступ до публічної інформації". У відповідях, які були проаналізовані в серпні 2022 року, розпорядники надавали відмови просто зазначаючи, що запитувана інформація є з обмеженим доступом без обгрунтування та застосування "трискладового тесту".

3) Відсутність на запиті електронного цифрового підпису.

3 (три) ідентичні відповіді із посиланням на те, що запит має підписаний електронним цифровим підписом надала у звітний період Самбірська міська рада.[88]

Щодо правомірності такої відмови варто зазначити, що Закон України "Про доступ до публічної інформації" містить вичерпні підстави для надання відмови на запит та правила оформлення запиту, які не містять вимоги накладення електронного цифрового підпису.

II. Щодо закриття публічного доступу до державних реєстрів

Гарною новиною у звітний період стало те, що 01 серпня 2022 року Портал відкритих даних Data.gov.ua відновив роботу після вимушеної паузи через повномасштабне вторгнення рф в Україну.[89] Щодо відновлення роботи інших реєстрів, то у згаданий період **продовжував бути обмеженим доступ до 19** публічних електронних **реєстрів, серед яких:**

1. Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань.
2. Єдиний реєстр громадських формувань.
3. Реєстр громадських об'єднань.
4. Реєстр повідомлень суддів про втручання у здійснення правосуддя. На сайті міститься повідомлення про тимчасове обмеження роботи реєстру.
5. Державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності.
6. Реєстр декларацій родинних зв'язків та доброчесності.
7. Державний реєстр атестованих судових експертів.
8. Реєстр методик проведення судових експертиз.
9. Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство.
10. Єдиний реєстр арбітражних керуючих України.
11. Реєстр суднозаходів.

[83] https://dostup.pravda.com.ua/request/103447/response/362671/attach/3/..pdf?cookie_passthrough=1
[84] https://dostup.pravda.com.ua/request/103059/response/362042/attach/1/08.08.2022.pdf?cookie_passthrough=1
[85] https://dostup.pravda.com.ua/request/103059/response/362042/attach/1/08.08.2022.pdf?cookie_passthrough=1
[86] https://dostup.pravda.com.ua/request/103201/response/362233/attach/3/121%200001.pdf?cookie_passthrough=1
[87] https://dostup.pravda.com.ua/request/103201/response/362233/attach/3/121%200001.pdf?cookie_passthrough=1
[88] https://dostup.pravda.com.ua/request/103238/response/362235/attach/3/238.pdf?cookie_passthrough=1
[89] https://zmina.info/news/portal-vidkrytyh-danyh-data-gov-ua-vidnovyv-robotu-minczyfry/

12. Реєстр морських портів.
13. Реєстр гідротехнічних споруд морських портів України.
14. Реєстр суб'єктів господарювання, що провадять свою господарську діяльність у сферах енергетики та комунальних послуг, діяльність яких регулюється НКРЕКП.
15. Реєстр операторів, провайдерів телекомунікацій.
16. Єдиний державний реєстр операторів поштового зв'язку.
17. Реєстр виданих ліцензій на користування радіочастотним ресурсом України.
18. Реєстр платників акцизного податку з реалізації пального та спирту етилового.
19. Реєстр альтернативних видів палива.

Після запровадження в Україні правового режиму воєнного стану та набрання чинності Постановою Кабінету Міністрів України від 12 березня 2022 р. № 263 "Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану"[90] відбулося закриття доступу до низки публічних реєстрів, а також до вебпорталів, які містять набори відкритих даних.

Зазначена Постанова надала можливість міністерствам, іншим центральним і місцевим органам виконавчої влади, державним і комунальним підприємствам, установам, організаціям, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких вони є, та захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, під час дії правового режиму воєнного стану зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

Закриття деяких реєстрів порталу відкритих даних і публічних реєстрів не виглядає пропорційним і доцільним засобом для захисту національної безпеки. Відповідно до вимог ч.3 ст.6 Закону України "Про доступ до публічної інформації", інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

Окрім закриття реєстрів, ненадання публічної інформації за запитами, негативна динаміка прослідковувалась і в частині зобов'язань розпорядників публічної інформації щодо її оприлюднення. Незважаючи на вимогу Закону України "Про доступ до публічної інформації" щодо невідкладного оприлюдненню інформації про факти, що загрожують життю, здоров'ю та/або майну осіб, і про заходи, які застосовуються у зв'язку з цим, така інформація не публікувалася.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

[90] https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263

Після введення воєнного стану в Україні з'явилося чимало додатків та інших онлайн-сервісів, спрямованих на розв'язання різних питань, пов'язаних із війною, користування якими може впливати на захист персональних даних особи.

Зокрема, під час під час моніторингу у звітний період було виявлено інформацію про застосунки, які з'явилися:

1. 09 серпня 2022 року в Україні створили мобільний застосунок з мінної безпеки MineFree. Він дозволяє користувачам повідомити про виявлення підозрілих предметів, а також отримати сповіщення про наближення до небезпечного об'єкта. Що може зробити користувач, встановивши цю програму на телефон:

- переглянути мапу, на якій позначено потенційно небезпечні території згідно з даними ДСНС;
- отримати сповіщення в разі наближення до небезпечного об'єкта;
- ознайомитися з довідником ДСНС, у якому є фото та опис вибухонебезпечних предметів;
- повідомити про виявлення вибухонебезпечних або підозрілих предметів.

Функцію сповіщення про небезпеку можна налаштувати через іконку дзвіночка в правому верхньому куті на головному екрані. Сповіщення працює в разі використання мапи в розділі "Переглянути мапу". Застосунок автоматично сповіщає користувача, якщо відстань до небезпеки стає менш ніж 500 метрів.[91]

2. Кіберполіція попереджає про небезпеку використання мобільних застосунків, розроблених спецслужбами рф. Через застосунки ворог у формі гри отримує від користувачів інформацію про розташування військових об'єктів, критичної інфраструктури або схиляє громадян несвідомо допомагати окупантам. Насамперед, користувача має насторожити, якщо у додатку пропонується здійснювати фотофіксацію місцевості, ділитися геолокацією чи нанести "малюнок" на асфальті. Для безпечного користування онлайн-застосунками кіберполіція рекомендує завантажувати їх лише з офіційних джерел – App Store, Google Play, Galaxy Store, AppGallery та ін., перевірити усі доступні дані, такі як інформація про розробників, доступи, які додаток вимагає при встановленні, відгуки користувачів[92].

Окрім застосунків, у зазначений період було створено чат-бот для пошуку інформації про військових, які потрапили у полон та зникли безвісти за особливих обставин. Чат-бот створили Національне інформаційне бюро спільно з фахівцями Координаційного штабу з питань поводження з військовополоненими ГУР. За допомогою цього інструмента рідні та близькі зможуть здійснити швидкий пошук даних про оборонців України, які потрапили в полон або зникли безвісти за особливих обставин. Чат-бот полегшує і пришвидшує взаємодію родичів та близьких із державними органами. Для визначення статусу розшукуваної особи слід подати ідентифікаційний код, ПІБ, номер телефону та дату народження особи, яка розшукує, а також ПІБ, дату народження та ідентифікаційний номер розшукуваної особи.[93]

Варто зазначити, що зазначені застосунки окрім допомоги у вирішенні певних питань, пов'язаних із війною, потенційно несуть у собі ризики порушення прав користувачів на захист їхніх персональних даних.

Мобільний застосунок з мінної безпеки MineFree оприлюднив політику конфіденційності, яка не містять інформацію про місцезнаходження персональних даних, які збирають дані застосунки. Також в політиці конфіденційності додатку

[91] https://t.me/dsns_telegram/8816
[92] https://www.facebook.com/photo?fbid=370145578629682&set=a.234579145519660
[93] https://t.me/DIUkraine/1074

MineFree міститься інформація про те, що власник застосунку залишає за собою право розкрити персональну інформацію покупцеві (або потенційному покупцеві) будь-якого бізнесу або активів, які він продає (або збирається продати), що не відповідає меті їх обробки. Відповідно, існує потреба у посиленні контролю за дотриманням ними вимог Закону України “Про захист персональних даних”.

ІНШІ ПОРУШЕННЯ ЦИФРОВИХ ПРАВ

Окрім безпосередніх атак, протягом серпня продожували надходити погрози на адресу ЗМІ. Так, 15 серпня 2022 року на адресу інтернет видання "Волинь Online" надішов 20-й лист з початку широкомаштабного вторгнення із вимогами "не поширювати фейків про росію" та погрозами у покаранні.[94]

29 серпня 2022 року Запорізькому онлайн-медіа inform.zp.ua після тривалої перерви знову надійшли погрози з росії, пов'язані з професійною діяльністю сайту. В листі співробітникам редакції погрожують допитами й ув'язненням через підтримку “неонацистського режиму Зеленського”.[95]

[94] https://imi.org.ua/news/sajt-volyn-online-otrymav-novi-pogrozy-z-rosiyi-pro-banderivsku-huntu-i47210
[95] https://www.imi.org.ua/news/rosiyany-znovu-pogrozhuyut-uv-yaznennyam-zaporizkomu-media-inform-zp-ua-i47380