

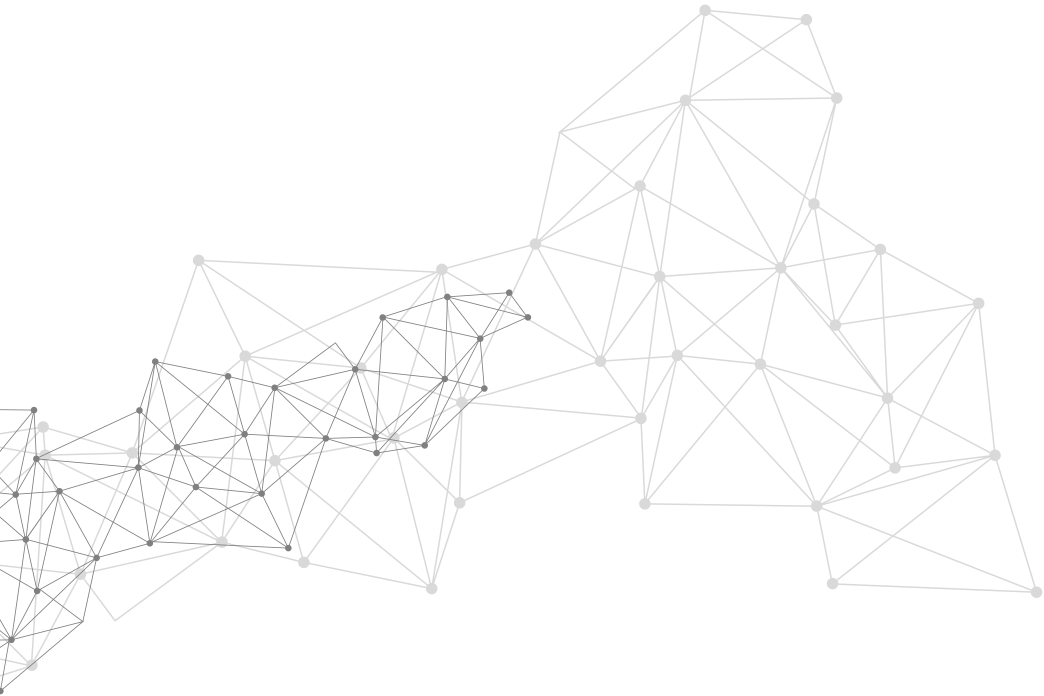


**ВІЙНА
У ЦИФРОВОМУ ВИМІРІ
ТА ПРАВА ЛЮДИНИ**

ПІДСУМКОВИЙ ЗВІТ

**із 24 лютого 2022 року
по 31 серпня 2023 року**

**ГО «Платформа прав людини»
Київ, 2023**



**ВІЙНА У ЦИФРОВОМУ ВИМІРІ ТА ПРАВА ЛЮДИНИ ПІДСУМКОВИЙ ЗВІТ
ІЗ 24 ЛЮТОГО 2022 РОКУ ПО 31 СЕРПНЯ 2023 РОКУ /** Вдовенко О., – Київ:
ГО «Платформа прав людини», 2023. – 84 с.

Це видання опубліковано в рамках проекту «Моніторинг ситуації з інтернет свободами в Україні», що реалізуються громадською організацією «Платформа прав людини» за фінансової підтримки Ініціативи з верховенства права Американської асоціації юристів (American Bar Association Rule of Law Initiative)

Всі права захищено.

Видано ГО «Платформа прав людини»

м. Київ, 2023

www.ppl.org.ua

© ГО «Платформа прав людини»



ПЛАТФОРМА
П Р А В Л Ю Д И Н И



AMERICAN BAR ASSOCIATION

Rule of Law Initiative

ЗМІСТ

Вступ	4
Ключові висновки	7
Кібератаки	14
Фішингатаки	22
Поширення дезінформації	28
Шахрайство в мережі	36
Блокування вебресурсів	40
Свобода вираження поглядів	47
Доступ до інформації	56
Зміни в законодавстві	63
Доступ до інтернету	78
Рекомендації	80

ВСТУП



Починаючи з 2019 року, Громадська організація “Платформа прав людини” (далі — ППЛ) здійснює моніторинг, який спрямовано на виявлення фактів порушення цифрових прав людини. Із 24 лютого 2022 року фокус цього дослідження було змінено на збір та аналіз інформації про загрози, які відбуваються у сфері цифрових прав людини під час повномасштабної війни.

Коригування мети, предмету та об’єкту моніторингу було пов’язано з початком нового етапу війни та запровадженням 24 лютого 2022 року Указом Президента України № 64/2022 на всій території України правового режиму воєнного стану. Під час його дії можливе тимчасове обмеження фундаментальних прав людини, серед яких і право на вільне вираження своїх поглядів і переконань, право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, право на особисте життя.

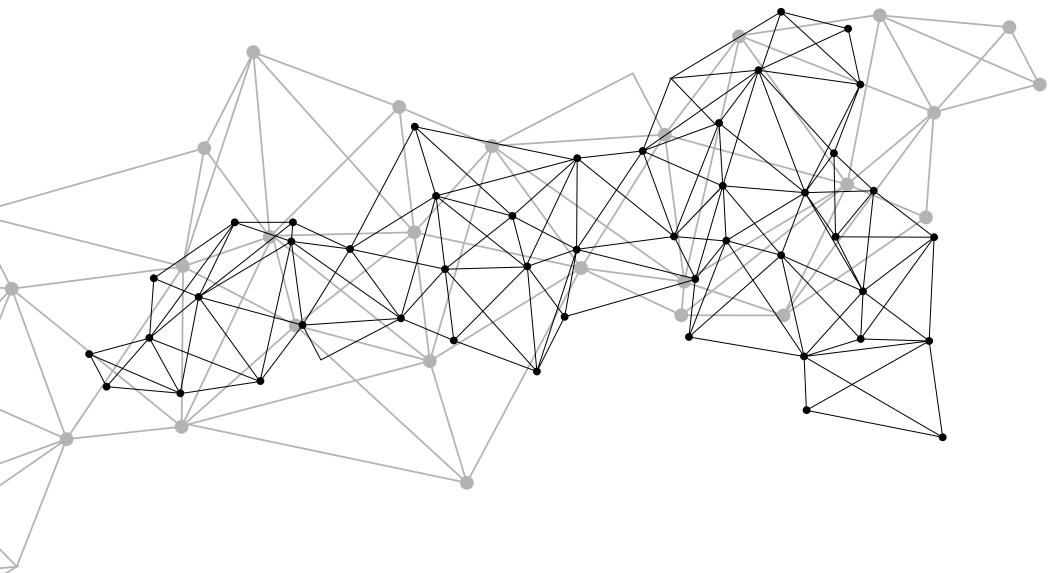
Законодавча рамка щодо обмежень прав людини під час воєнного стану є занадто загальною і передбачає прийняття відповідних рішень військовим командуванням для деталізації механізмів і підстав. У зв’язку з тим, що таких рішень було прийнято одиниці, класифікувати події, які відбувалися у сфері цифрових прав, як порушення стало достатньо проблематичним. Кожен випадок потребував детального вивчення всіх обставин і балансування інтересів національної безпеки та конкретного права чи свободи. Саме тому у цей період моніторингу ППЛ збирала, аналізувала, узагальнювала інформацію про загрози для цифрових прав людини, які тільки потенційно можуть бути визначені як порушення.

Під час моніторингу експерти ППЛ збирали та аналізували інформацію з відкритих джерел, а також з метою отримання відомостей направляли запити до відповідних державних органів. На підставі такої інформації було підготовлено та оприлюднено на сайті ППЛ¹ 14 звітів, які охопили період із 24 лютого 2022 року по 31 серпня 2023 року.

1. Моніторинг дотримання цифрових прав. Моніторинг 2019. URL: <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

Зокрема, завдяки дослідженню було зафіксовано значне збільшення кіберзлочинів, способів шахрайства в мережі, неправомірних відмов у наданні публічної інформації, порушення права на доступ до інтернету, виявлено низку проблем із правозастосуванням статей, введених на початку 2022 року до Кримінального кодексу України (далі — ККУ), а також у зв'язку із цим запропоновано відповідні зміни.

Підсумковий звіт з інформацією про загрози цифровим правам людини буде корисним юристам, науковцям, депутатам, представникам державних органів, органів місцевого самоврядування, представникам громадського сектору, іншим зацікавленим особам. Він посприє приверненню уваги з боку державних органів і громадськості до виявлених проблем у сфері цифрових прав людини та напрацюванню можливих рішень для їх вирішення.



КЛЮЧОВІ ВИСНОВКИ



Аналіз інформації, яка була зібрана під час моніторингу подій, що відбувалися у сфері цифрових прав за період із 24 лютого по 31 серпня 2023 року, дає змогу зробити такі висновки:

1. КІБЕРАТАКИ:

- з початком широкомасштабного вторгнення кількість кібератак на державний сектор збільшилася у 15 разів² (за період із 2019 по 2021 роки на державний сектор було здійснено 28 352 882 кібератаки, тоді як за період із січня 2022 року по 31 серпня 2023 року — 422 063 020 атаки), що свідчить про високий рівень загрози цифровим правам людини;
- інформування громадськості про масштаби кібервторгнення та кількість вчинених кіберзлочинів є низькою (у період із січня 2022 року по серпень 2023 року у медіа експерти виявили 83 повідомлення про кібератаки на державний і приватний сектори економіки, тоді як Державна служба спеціального зв'язку та захисту інформації України (далі — Держспецзв'язку) повідомляла про 422 063 020 кібератак на державний сектор, а Служба безпеки України (далі — СБУ) — про 7000 на державний і приватний сектори). Зазначене призводить до поганої обізнаності суспільства щодо ступеня загрози від кібератак, можливих засобів протидії та безпеки у зазначеній сфері;
- існує проблема повідомлення державних органів та реагування з їхнього боку на кібератаки, що здійснюються на приватний сектор. Приватні компанії не завжди повідомляють про здійснені на них атаки, а протидіяти таким загрозам Держспецзв'язку може тільки якщо до неї звернулися з таким проханням;
- протидія кібератакам, які здійснюються на державний сектор, є ефективною, бо всі кібератаки, за інформацією Держспецзв'язку, було припинено або заблоковано;
- національне законодавство є недосконалим із погляду притягнення до відповідальності за кібератаки. Передусім це пов'язано з тим, що кіберзлочини мають матеріальний склад (має бути встановлено настання конкретних наслідків) — витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації тощо.

2. Порівнювалася надана Держспецзв'язку інформація про кількість кібератак, які було здійснено на державний сектор за період із 2019 по 2021 роки та з 2022 по серпень 2023 року.

2. ФІШИНГАТАКИ:

- порівняння інформації про кількість фішингових атак за період із лютого 2022 по серпень 2023 року та їхньої кількості за період із 2019 року по 2021 рік свідчить, що їхня кількість збільшилася у півтора рази;
- протидія фішинговим атакам, які здійснюються на державний сектор, є ефективною, бо більшість таких атак, за інформацією Держспецзв'язку, було припинено або заблоковано за допомогою системи захищеного доступу державних органів до мережі Інтернет;
- існує проблема повідомлення державних органів та реагування з їхнього боку на фішингові атаки, що здійснюються на приватний сектор. Приватні компанії не завжди повідомляють про здійснені на них атаки, а протидіяти таким загрозам Держспецзв'язку може тільки якщо до неї звернулися з таким проханням;
- механізм притягнення до кримінальної відповідальності за фішинг недостатньо ефективний, бо національне законодавство є недосконалим із погляду кваліфікації фішингових атак за статтями 361, 361¹ та 363¹ ККУ;
- запроваджена в березні 2023 року система фільтрації фішингових доменів, за інформацією професійних інтернет-асоціацій, містить ризики для цифрових прав людини.

3. ДЕЗІНФОРМАЦІЯ:

- поширення дезінформації продовжувало бути одним із основних елементів гібридної війни, розпочатої проти України в 2014 році. Підтвердженням цього є збільшення вдвічі у 2023 році кількості дезінформаційних повідомлень, які було виявлено в медіа (**1454** таких повідомлення за період із січня по серпень 2023 року проти **742** за період із лютого по грудень 2022 року);
- дезінформація була і залишається одним із серйозних викликів, який постає перед урядами, громадянським суспільством і населенням країн. Огляд прикладів дезінформації підтверджує, що її вплив не можна недооцінювати: вона впливає на суспільну думку, безпеку держави і людей, здоров'я тощо;

- органи влади багатьох країн, міждержавні об'єднання намагаються розробити нові політики і рекомендації щодо протидії дезінформації, не порушивши при цьому право на вільне вираження поглядів;
- в Україні на законодавчому рівні наявні окремі елементи протидії дезінформації, але сам термін і системний механізм відсутні.

4. ШАХРАЙСТВО В МЕРЕЖІ:

- протягом звітного періоду шахраї активно використовували тему війни, щоб ошукувати українців. Найчастіше для заволодіння коштами застосовувались теми продажу неіснуючих товарів, збору коштів для Збройних Сил України (далі — ЗСУ), надання фінансової допомоги та необхідності лікування поранених.

5. БЛОКУВАННЯ ВЕБРЕСУРСІВ:

- кількість заблокованих у позасудовому порядку вебресурсів за період із лютого 2022 року по серпень 2023 року збільшилася у 50 разів, порівнюючи із кількістю таких блокувань, які були здійснені за період із травня 2019 року по січень 2022 року.

За період із лютого 2022 року по серпень 2023 року позасудові блокування вебресурсів здійснювалися на підставі:

- Закону України “Про санкції” — 114 блокувань;
- рекомендацій Національного центру оперативно-технічного управління мережами телекомунікацій (далі — НЦУ) — 11 754 блокування;
- розпорядження НЦУ “Про впровадження системи фільтрації фішингових доменів” — 23 096 блокувань;
- рішення Національної ради України з питань телебачення і радіомовлення (далі — Нацрада) — 2 блокування.

За період із травня 2019 року по січень 2022 року позасудові блокування вебресурсів здійснювалися на підставі Закону України “Про санкції” і загалом у цей період було заблоковано 697 сайтів;

- продовжувалася практика блокування сайтів на підставі Закону України “Про санкції”. Однак у загальному переліку видів санкцій він містить єдину підставу для блокування доступу до інформаційних ресурсів — заборона демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп), і не містить інших санкцій, що стосуються обмеження доступу до вебсайтів. І хоча перелік санкцій у цьому законі є відкритим, застосування таких “інших” санкцій має відповідати принципам, які Європейський суд з прав людини (даді — ЄСПЛ) виклав у низці своїх рішень щодо блокувань вебресурсів: прозорості, законності, відповідності меті, ефективності та об’єктивності;
- блокування вебресурсів на підставі рішень НЦУ та за допомогою системи фільтрації фішингових доменів мають ознаки порушення принципу законності, бо 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 нині законодавством не визначено. Окрім порушення принципу законності, практика блокувань вебресурсів містить ознаки втручання у право на свободу слова, або ознаки того, що таке втручання є непропорційним.

6. СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ:

- кількість ухвалених вироків під час дії правового режиму воєнного стану, що стосуються права на свободу вираження поглядів у мережі Інтернет, збільшилася втричі як порівняти з періодом із 2014 по 2021 роки (786 проти 247 відповідно)³;
- за період із лютого 2022 року по серпень 2023 року було виявлено та проаналізовано 786 вироків. Із них 633 (80,5 %) було ухвалено за статтями ККУ, які з’явилися вже після повномасштабного вторгнення, що свідчить про активне застосування правоохоронними органами та судами нових норм, спрямованих на протидію поширенню забороненого проросійського контенту;

3. Дослідження проводилося з метою виявлення тенденції щодо притягнення до відповідальності за поширення забороненого контенту під час правового режиму воєнного стану та до його введення. Було зіставлено кількісні показники ухвалених судами вироків за період із 2014 року по 2021 рік та за період із лютого 2022 року по серпень 2023 року.

- найчастіше суди застосовували покарання у вигляді позбавлення волі, але у 507 випадках із 786 (64,5 %) засуджених було звільнено від відбування покарання на підставі ст. 75 ККУ⁴ із призначенням іспитового строку;
- кількість осіб, які понесли реальне покарання за поширення забороненої інформації в інтернеті у вигляді позбавлення волі становить 122 осіб із 786 (15,5 %), а у вигляді штрафу — усього 12 осіб із 786 (1,5 %). Всі інші особи були звільнені від відбування покарання на підставі укладених угод із прокурором про визнання вини або визнання вини під час розгляду справи;
- у 137 із 786 (17,4 %) вироках не визначено інформацію, поширення якої стало підставою для притягнення особи до кримінальної відповідальності;
- у 227 із 786 (28,8 %) вироках не міститься інших способів аналізу поширеної інформації судом, крім посилань на висновки експертів-лінгвістів. У таких рішеннях вбачається ризик того, що судова практика є насправді повним відтворенням позиції і практикою відповідних судових експертів;
- у 79 із 786 вироків (10,05 %) 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;
- було виявлено 45 судових рішень у цивільних справах, які містять ознаки порушення цифрових прав людини у вигляді непропорційного обмеження права на свободу вираження поглядів;
- було зафіксовано 45 рішень у справах про захист честі, гідності і ділової репутації, в яких зміст спірної інформації прихований позначками «ІНФОРМАЦІЯ No_».

4. **Стаття 75.** Звільнення від відбування покарання з випробуванням

1. Якщо суд, крім випадків засудження за корупційне кримінальне правопорушення, кримінальне правопорушення, пов'язане з корупцією, порушення правил дорожнього руху або експлуатації транспорту особами, які керували транспортними засобами у стані алкогольного, наркотичного чи іншого сп'яніння або перебували під впливом лікарських препаратів, що знижують увагу та швидкість реакції, при призначенні покарання у виді виправних робіт, службового обмеження для військовослужбовців, обмеження волі, а також позбавлення волі на строк не більше п'яти років, враховуючи тяжкість кримінального правопорушення, особу винного та інші обставини справи, дійде висновку про можливість виправлення засудженого без відбування покарання, він може прийняти рішення про звільнення від відбування покарання з випробуванням.
2. Суд приймає рішення про звільнення від відбування покарання з випробуванням у випадку затвердження угоди про примирення або про визнання вини, якщо сторонами угоди узгоджено покарання у виді виправних робіт, службового обмеження для військовослужбовців, обмеження волі, позбавлення волі на строк не більше п'яти років, а також узгоджено звільнення від відбування покарання з випробуванням.

7. ДОСТУП ДО ІНФОРМАЦІЇ:

- було проаналізовано 3366 відповідей на запити, які розміщено у відкритому доступі на ресурсі “Доступ до правди”⁵, серед яких більшість були позитивними (81,96 % або 2759 відповідей);
- аналіз відмов у наданні публічної інформації свідчить про те, що майже 30 % є неправомірними, а найбільша кількість відмов була з посиланням на правовий режим воєнного стану та на те, що запитувана інформація є з обмеженим доступом без застосування трискладового тесту;
- залишається закритим доступ до 17 державних реєстрів, який виглядає непропорційним і суперечливим засобом для захисту національної безпеки, оскільки 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.

8. ЗМІНИ В ЗАКОНОДАВСТВІ:

- у період із 24 лютого по 31 серпня 2023 року українське законодавство зазнало багатьох кардинальних змін, пов’язаних із введенням та дією правового режиму воєнного стану в Україні. Загалом за звітний період було ухвалено 14 законів та нормативно-правових актів, які мають безпосередній вплив на цифрові права людини;
- наказ Головнокомандувача ЗСУ від 3 березня 2022 року № 73 “Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану” містить загрози надмірного втручання у свободу слова. Зокрема, перелік інформації, забороненої до поширення, містить дефініції, частина з яких чітко не визначена законодавством України;
- експерти ППЛА висловили низку зауважень до статей ККУ, які були додані в кодекс під час дії правового режиму воєнного стану. Детальний аналіз цих статей було представлено в аналітичному звіті “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”⁶.

5. Сайт “Доступ до правди”. URL: <https://dostup.ppravda.com.ua/>

6. Аналітичний звіт “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-A4-30-12-22.pdf>

КІБЕРАТАКИ



З початком широкомасштабного вторгнення Україна перебуває на першому місці в світі щодо кількості кібератак, що здійснюються на державний і приватний сектори⁷. Про це у травні 2023 року у своєму інтерв'ю повідомив заступник голови Держспецзв'язку з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктор Жора. Зі свого боку аналіз результатів моніторингу порушення цифрових прав за період із 24 лютого 2022 року по 31 серпня 2023 року, підготовлений експертами ППА, добре ілюструє ситуацію, яка склалася у сфері кібератак у зазначений період, та підтверджує те, що сучасна війна не обмежується землею, морем, повітрям, а також активно ведеться і у кіберпросторі.

За 18 місяців повномасштабної війни, із січня 2022 року, кількість втручань у роботу сайтів та реєстрів органів державної влади збільшилася у 15 разів проти трьох попередніх років. Зокрема, за період із 2019 по 2021 роки на державний сектор було здійснено **28 352 882** кібератак, тоді як за період із січня 2022 року по 31 серпня 2023 року — **422 063 020** кібератак.

Таблиця № 1. Інформація щодо кількості кібератак

	2019	2020	2021	2022	2023 (до 31 серпня 2023 року)
Кількість кібератак, здійснених на державний сектор (за інформацією Держспецзв'язку)	16 751 440	8 632 641	2 968 801	241 151 834	180 911 186
Кількість кібератак за результатами моніторингу, який здійснює СБУ	1080	800	1400	4500	2500
Кількість кібератак, виявлених у загальнодоступних джерелах	7	10	25	51	32

7. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї — заступник голови Держспецзв'язку. URL: <https://interfax.com.ua/news/interview/911979.html>

Варто зазначити, що відповідно до Закону України “Про основні засади забезпечення кібербезпеки України”⁸ **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 і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

- порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у 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.

Мета таких дій — викрадення або руйнування інформації в інформаційних системах і мережах, порушення їх нормальної роботи. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Незважаючи на вражаюче велику кількість кібератак, які було здійснено з початку широкомасштабного вторгнення, більшість із них, зокрема ті, які були здійснені на державний сектор, за інформацією Держспецзв’язку, було припинено або заблоковано⁹.

Крім зростання кількості атак у мережі, спеціалісти з моніторингу зробили висновок про те, що інформування громадськості про масштаби вторгнень у цифровому вимірі та кількість вчинених кіберзлочинів є дуже низькою. Зіставлення інформації, отриманої у відповідь на запити, які ППЛ направляла до Держспецзв’язку, СБУ, та тієї, яка була виявлена під час моніторингу загальнодоступних

8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

9. Відповідь Держспецзв’язку за результатами опрацювання вашого запиту на отримання публічної інформації від 12.06.2023. URL: <https://drive.google.com/file/d/1TkBVVlls0D3N0parmjDNzpbds7l1OKx/view?usp=sharing>

джерел, ілюструє неспівставно велику різницю між показниками. Наприклад, у період із січня 2022 року по серпень 2023 року у засобах масової інформації (далі — ЗМІ) експерти виявили **83** повідомлення про кібератаки на державний і приватний сектори економіки, тоді як Держспецзв'язку повідомляла про **422 063 020** кібератак на державний сектор, а СБУ — про **7000** на державний і приватний сектори, що в сумі становить **422 070 020** кібератак.

Аналіз даних щодо кібератак демонструє велику різницю між кількістю нападів на державний і приватний сектори. За інформацією Держспецзв'язку за звітний період, **на приватний сектор економіки було здійснено 156 071 кібератаку, тоді як на державний — 422 070 020, що в 2704 рази більше.**

При цьому слід враховувати, що основним завданням Держспецзв'язку є фіксація та протидія за допомогою системи захищеного доступу до мережі Інтернет кібератакам, які здійснюються саме на державний сектор. Відповідно, кількість кібератак на державний сектор є об'єктивно зафіксованою, натомість інформація про атаки на приватний сектор узагальнюється Держспецзв'язку на підставі повідомлень від приватних компаній. Враховуючи те, що приватні компанії не завжди повідомляють про атаки, їхня кількість насправді може бути значно більшою.

Про проблему повідомлення та реагування з боку державних органів на кібератаки, що здійснюються на приватний сектор, також повідомив заступник голови Держспецзв'язку України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктор Жора¹⁰. Він зазначив, що Держспецзв'язку отримує повідомлення про кіберзагрози з різних джерел: безпосередньо від жертв (різноманітними каналами зв'язку); від національної розвідки та від партнерів з інших країн, однак протидіяти таким загрозам Держспецзв'язку може тільки якщо приватна компанія звернулася з таким проханням.

10. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї — заступник голови Держспецзв'язку. URL: <https://interfax.com.ua/news/interview/911979.html>

Прагнучи більш глибоко дослідити та проаналізувати ситуацію щодо протидії кібератакам та притягнення до відповідальності винних у вчиненні кіберзлочинів, експерти ППА проаналізували норми національного законодавства, які передбачають притягнення до відповідальності за кібератаки.

Національне законодавство покладає на Національну поліцію України (далі — Нацполіція) та СБУ здійснення заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів. Розслідування та притягнення до відповідальності за кібератаки зазначеними органами можливе за умови їх класифікації за статтями ККУ. У чинному ККУ є розділ, який встановлює кримінальну відповідальність, зокрема і за кіберзлочини — розділ XVI “Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”, який складається із шести статей. Притягнення до відповідальності за кібератаки можливе на підставі двох статей із цього розділу:

- за ст. 361 — несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

За цією статтею ККУ притягнення до кримінальної відповідальності можливе лише при настанні конкретних наслідків — витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, при цьому нанесення шкоди у вигляді матеріальних втрат чи збитків не є обов’язковою;

- за ст. 363¹ — перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку.

За правовою конструкцією ст. 363¹ ККУ передбачає відповідальність за низку протиправних дій у мережі — від спаму електронних листів, розсилок смс-повідомлень до масових цілеспрямованих DDos-атак, які можуть паралізувати роботу майже будь-якого онлайн-ресурсу та завдати суттєвої шкоди.

Однак обов'язковою умовою для притягнення до відповідальності за цією статтею є настання наслідків у вигляді порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що має бути обов'язково зафіксовано під час досудового розслідування.

За інформацією Офісу Генерального Прокурора, упродовж 2019–2023 років правоохоронні органи відкрили таку кількість проваджень за зазначеними статтями (див. таблицю № 2)¹¹:

Таблиця № 2. Кількість кримінальних проваджень, що були відкриті за статтями 361 та 363¹ ККУ

	2019	2020	2021	2022	до 31.08.2023
За ст. 361 — несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж					
Зареєстровано кримінальних правопорушень у звітному періоді	1320	2708	1904	1676	859
Кримінальні правопорушення, у яких провадження закрито	141	212	230	275	49
Кримінальні правопорушення, за якими провадження направлені до суду	662	1492	1020	1403	356
За ст. 363¹ — перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку					
Зареєстровано кримінальних правопорушень у звітному періоді	6	4	3	5	3
Кримінальні правопорушення, у яких провадження закрито	4	1	0	0	0
Кримінальні правопорушення, за якими провадження направлені до суду	0	0	0	0	0

11. Відомості про зареєстровані упродовж 2019 року кримінальні правопорушення (провадження) у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України) та результати їх досудового розслідування. URL: https://docs.google.com/spreadsheets/d/1hOArvILBV_BTro03JvCPirdN9mKX91u-/edit?rtfpof=true#gid=1698507350

Аналіз статей ККУ, за якими може бути кваліфіковано дії як кібератаки, аналіз кількості зареєстрованих проваджень за цими статтями та зіставлення їхньої кількості з кількістю кібератак, які фіксує Держспецзв'язку, дає можливість зробити такі висновки:

- кількість зафіксованих кібератак є набагато більшою, ніж кількість відкритих проваджень за фактом їх вчинення;
- кількість зареєстрованих проваджень у більшості випадків є вдвічі більшою, ніж кількість кримінальних правопорушень, які направлено до суду (див. таблицю № 3).

Таблиця № 3. Порівняльна таблиця кількості зареєстрованих проваджень за статтями 361 та 363¹ ККУ та кількості кібератак, які були зафіксовані Держспецзв'язку та СБУ

	2019	2020	2021	2022	2023
Зареєстровано кримінальних правопорушень (за статтями 361 та 363¹ ККУ)	1326	2712	1907	1611	862
Зафіксовано кількість кібератак Держспецзв'язку на приватний сектор	32 654	122 577	155 230	841	
Зафіксовано кількість кібератак Держспецзв'язку на державний сектор	16 751 440	8 632 641	2 968 801	241 151 834	180 911 186
Кількість кібератак за результатами моніторингу, який здійснює СБУ	1080	800	1400	4500	2500

Це може свідчити про недосконалість законодавства у сфері притягнення до відповідальності за кібератаки. Наприклад, через те, що наведені вище статті ККУ, за якими може бути призначено покарання за кіберзлочини, мають матеріальний склад (має бути встановлено настання конкретних наслідків — витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації тощо, а не сам факт кібератаки) і це може бути однією з причин складнощів у кваліфікації та доведенні масових кібератак на приватний і державний сектори як відповідних злочинів.

На цю проблему також звертали увагу у своєму дослідженні “Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку”¹² науковці Т. Луцький та О. Пасека. Вони зазначили, що кількість кіберзлочинів є значно більшою проти кількості кримінальних проваджень і судових вироків із зазначених правопорушень. Серед проблем, які виникають під час кваліфікації кіберзлочинів, вони виділяють недосконалість вітчизняного законодавства, зокрема складність кваліфікації кіберзлочинів із погляду встановлення конкретних наслідків. Науковці Харківського національного університету внутрішніх справ А. Васильєв та Д. Пашнев у своїй статті “Особливості кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку”¹³ зазначали, що переважна більшість складів злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку є матеріальними, а тому виявляються за наслідками. Отже, під час кваліфікації цих злочинів та їх відмежування від суміжних складів злочинів необхідно оцінювати розмір і характер заподіяної шкоди з погляду характеристики її предмету.

12. Луцький Т. М., Пасека О. Ф. Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. URL: <http://journal-app.uzhnu.edu.ua/article/view/260148/256522>

13. Васильєв А. А., Пашнев Д. В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/79f9c3d4-4a69-4cff-a559-60b25a1f0767/content>

ФІШИНГАКИ



На момент підготовки звіту українське законодавство не містило визначення, що таке “фішинг”. Однак перелік категорій кіберінцидентів, який розробила Держспецзв’язку¹⁴, відносить фішинг до методів збору інформації зловмисниками, який відбувається за допомогою методів соціальної інженерії, яка може містити посилання на фішингові сайти і спрямована на збір даних.

Фішингові атаки здійснюють зловмисники, які маскуються під надійні джерела, щоб отримати легкий доступ до будь-якого типу даних. Існують різні типи фішингу, та найпоширенішим є фішинг в електронних листах. Зловмисники в електронному листі надсилають шкідливі гіперпосилання або вкладення, після відкриття яких запускається шкідлива програма, яка надає доступ до даних або навіть може паралізувати цілі ІТ-системи. Зазвичай такі посилання та вкладення видають за безпечні на перший погляд файли, наприклад, резюме або банківська виписка тощо¹⁵.

З метою виявлення тенденцій, які відбуваються у сфері фішингових атак, ми порівняли результати проведеного моніторингу за період із 24 лютого 2022 року по 31 серпня 2023 року з результатами моніторингів, які проводилися у період із 2019 по 2021 роки, а також з інформацією, яку одержали від Держспецзв’язку. Аналіз інформації щодо кількості здійснених фішингових атак свідчить про те, що з початком широкомасштабного вторгнення кількість фішингових атак збільшилась у півтора рази.

Таблиця № 4. Кількість фішингових атак

	2019	2020	2021	2022	2023
Кількість фішингових атак, здійснених на державний сектор (за інформацією Держспецзв’язку)	1 276 283	4 641 791	678 814	9 549 384	433 160
Кількість фішингових атак, виявлених у загальнодоступних джерелах	8	7	10	15	17

14. ПЕРЕЛІК категорій кіберінцидентів.URL: <https://cert.gov.ua/recommendation/16904>

15. Різні види фішингових атак. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing>

Департамент кіберполіції Нацполіції повідомляв, що фішингові кампанії були добре сплановані та мали масовий характер. Цей вид атак загрожував не тільки працівникам цільових організацій (держслужбовцям, працівникам підприємств критичної інфраструктури), а й кожному громадянину. За допомогою фішингу російські спецслужби намагалися зібрати про українців усю можливу інформацію. За період із січня по травень 2023 року Департамент кіберполіції Нацполіції отримав понад 15 000 звернень від громадян, які постраждали від фішингових атак¹⁶.

Протидію фішинговим атакам на державний сектор здійснює Держспецзв'язку і за її інформацією всі фішингові атаки за період із 24 лютого 2022 року по 31 серпня 2023 року було припинено або заблоковано.

Щодо протидії та притягненню до відповідальності за фішингові атаки, які здійснюються на приватний сектор або на громадян, то розслідування таких злочинів здійснює Департамент кіберполіції Нацполіції.

ККУ містить три статті, за якими можливе притягнення до відповідальності та покарання за фішинг:

- **за ст. 361 ККУ** — несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;
- **за ст. 361¹ ККУ** — створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;
- **за ст. 363¹ ККУ** — перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Щодо кваліфікації фішингових атак за статтями 361 та 363¹, існує та сама проблема, що й із кваліфікацією інших видів кіберзлочинів, яка часто полягає в неможливості встановлення факту витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації тощо.

16. Від початку року кіберполіція отримала більш як 15 тисяч звернень щодо фішингових атак. URL: <https://zmina.info/news/vid-pochatku-roku-kiberpolicziya-otrimala-bilsh-yak-15-tysyach-zvernenn-shhodo-fishyngovyh-atak/>

Щодо ст. 361¹ ККУ, яка передбачає відповідальність за створення з метою використання, розповсюдження або збуту, а також за розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, то для кваліфікації фішингової атаки за цією статтею необхідно встановити факт створення або розповсюдження саме шкідливих програм. Окрім цього, під час кваліфікації злочину за цією статтею надзвичайно важливим є визначити призначення досліджуваної програми, а саме створення її для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Зазначене свідчить, що фішингові атаки часто складно кваліфікувати за зазначеними статтями ККУ, а у випадку, коли відповідна кваліфікація відбулася, доведення вини під час досудового і судового слідства може бути також складним процесом. Підтвердженням цього висновку може бути порівняння кількості виявлених фішингових атак із кількістю відкритих проваджень за наведеними вище статтями ККУ.

Таблиця № 5. Порівняння кількості зафіксованих фішингових атак із кількістю відкритих проваджень за статтями ККУ

	2019	2020	2021	2022	2023
Зареєстровано кримінальних правопорушень за ст. 361	1320	2708	1904	1676	859
Зареєстровано кримінальних правопорушень за ст. 361¹	203	121	43	285	25
Зареєстровано кримінальних правопорушень за ст. 363¹	6	4	3	5	3
Зафіксовано кількість фішингових атак за інформацією Держспецзв'язку на державний сектор	1 276 283	4 641 791	678 814	9 549 384	433 160
Кількість фішингових атак, виявлених у загальнодоступних джерелах	8	7	10	15	17

Різниця між кількістю здійснених фішингових атак, про які повідомляла Держспецзв'язку, із кількістю відкритих кримінальних проваджень є неспівставно великою, що, знову ж таки, може свідчити про недосконалість правового регулювання притягнення до відповідальності за фішинг.

Варто зазначити, що з метою протидії фішинговим атакам НЦУ — орган, відповідальний за телекомунікації в країні під час війни, у січні 2023 року видав Розпорядження щодо системи фільтрації фішингових доменів¹⁷. На підставі цього розпорядження з 2 березня 2023 року в Україні почала працювати нова автоматизована система блокування інтернет-доменів в українському сегменті мережі Інтернет.

Робота антифішингової системи працює таким чином: фахівці Центру кіберзахисту Національного банку України (далі — НБУ) моніторять інтернет і соцмережі та виявляють сайти шахраїв. Далі шкідливі ресурси додаються до бази, а провайдери обмежують переходи користувачів на них. Користувачів же переспрямовують зі шкідливого сайту на сторінку з попередженням, що вказаний сайт створений зловмисниками і може призвести до втрати грошей.

У травні 2023 року директор департаменту платіжних систем та інноваційного розвитку НБУ Андрій Поддєрьогін заявив, що проєкт *Protective DNS* допоміг уникнути 2,5 млн переходів на шахрайські ресурси протягом трьох місяців функціонування системи¹⁸.

Однак оператори електронних комунікацій вважають, що система фільтрації фішингових сайтів несе загрози інформаційній безпеці України. У квітні 2023 року Інтернет Асоціація України (далі — ІнаУ) провела опитування щодо ризиків Системи фільтрації фішингових сайтів, яка була впроваджена Розпорядженням НЦУ. В опитуванні взяли участь 78 керівників підприємств, які представляють більшість операторів електронних комунікацій серед членів ІнаУ.

17. Розпорядження Держспецзв'язку про впровадження системи фільтрації фішингових доменів від 30 січня 2023 р. № 67/850. URL: https://nkrzi.gov.ua/images/news/11/2580/67_30012023.pdf

18. Що не так із законопроектами проти фішингу або як НБУ намагається контролювати інтернет. URL: <https://ua.news/ua/technologies/chto-ne-tak-s-zakonoproektamy-protiv-fyshynga-ily-kak-nbu-pytaetsya-kontrolyrovat-ynternet>

Результати опитування показали таке:

- 62 % опитаних операторів вважають, що впроваджена Розпорядженням система блокування доменів несе загрози для інформаційної безпеки України;
- 72 % опитаних вважають, що використання “транзитного” сервера Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (далі — НКЦК РНБО) для передачі провайдерам переліку фішингових сайтів, сформованих командою CSIRT НБУ, створює додаткові суттєві ризики.

З моменту оприлюднення Розпорядження ІнАУ пропонувала терміново змінити систему фільтрації. Згідно з експертизою Асоціації централізована автоматична система має стратегічні технологічні вразливості, які ставлять під загрозу весь сегмент українського інтернету та створюють загрози національній безпеці. У військовий час такі вразливості дають змогу на суттєвий час заблокувати доступ до інтернету в зоні .ua. Транзитний сервер РНБО, на який передається інформація, є дублюванням функцій та знижує рівень захисту системи.

ІнАУ направила відповідним державним інституціям пропозиції постатейних змін до “Регламенту взаємодії сторін в процесі фільтрації фішингових доменів”, які дадуть змогу:

- виключити заподіяння шкоди інформаційній безпеці України системою фільтрації фішингових доменів;
- унеможливити незаконний збір і використання персональних даних користувачів;
- знизити ризики позасудового блокування сайтів, які не є фішинговими¹⁹.

19. Оператори вважають, що Система фільтрації фішингових сайтів несе загрози інформаційній безпеці України.
URL: <https://inau.ua/news/novyny-inau/operatory-vvazhayut-shcho-systema-filtratsiyi-fishynhovyykh-saytiv-nese-zahrozy>

ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ



Національне законодавство не містить визначення терміна “дезінформація”, а Кембриджський словник називає її “неправдивою інформацією, яка поширюється з метою введення в оману людей”. У Звіті Ради Європи “Інформаційне безладдя: на шляху до міждисциплінарного підходу до досліджень та вироблення політик” дезінформацією називають інформацію, яка є неправдивою та навмисно створеною, щоб завдати шкоди людині, соціальній групі, організації чи країні²⁰.

Збір та аналіз дезінформаційних повідомлень є важливою частиною цього моніторингу, бо дає можливість не тільки зафіксувати факт їх поширення, а й показати системність і мету поширення неправдивої інформації, що є однією з її ключових ознак. Щомісячні звіти, які підготувала ППА, укотре засвідчили: розповсюдження певних повідомлень є спланованими дезінформаційними кампаніями, що тривають протягом декількох років. Серед прикладів таких кампаній, починаючи з 2019 року, можна назвати поширення неправдивих повідомлень з метою дискредитації Президента України та загалом влади в Україні²¹, ЗСУ²², створення та роботи на території України біологічних лабораторій²³, звинувачення США, Європейського Союзу (далі — ЄС) та Великої Британії у війні проти російської федерації (далі — рф) тощо.

рф активно застосовувала і продовжує застосовувати дезінформацію як інструмент ведення війни проти України. Це підтверджують дані. Удвічі зросла кількість дезінформаційних повідомлень, які було виявлено в медіа за період із січня 2023 року по серпень 2023 року (**1454** повідомлення), тоді як за період із лютого 2022 року по грудень 2022 року — **742**. При цьому в період із 2019 року по 2021 рік було виявлено всього **71** дезінформаційне повідомлення у загальнодоступних джерелах, що ілюструє як зростання хвилі дезінформації після повномасштабного вторгнення, так і кількість проєктів в Україні, спрямованих на виявлення і протидію їй.

20. INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making. URL: <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>

21. Obozrevatel заявив, що російські пропагандисти поширюють фейки від його імені. URL: <https://ms.detector.media/manipulyatsii/post/23058/2019-06-19-obozrevatel-zayavyv-shcho-rosiyski-propagandysty-poshyruyut-fejky-vid-yogo-imeni/>

22. Alexander Kovalenko. URL: https://www.facebook.com/story.php?story_fbid=2564767997162438&id=100008877886960

23. У СБУ спростовують фейк про існування «американських біологічних лабораторій» в Україні. URL: <https://ms.detector.media/manipulyatsii/post/24645/2020-05-08-u-sbu-sprostovuyut-feyk-pro-isnuvannya-amerykanskykh-biologichnykh-laboratoriy-v-ukraini/>

Теми дезінформаційних повідомлень у розрізі років були такі:

- 1.** У 2019 році російські пропагандисти поширювали фейкові повідомлення щодо дискредитації Президента України. Для цього вони використовували начебто скрини видання *Obozrevatel*, які вони поширювали на своїх ресурсах і в соцмережі *Facebook*²⁴.
- 2.** У 2020 році більшість дезінформаційних повідомлень стосувалися теми коронавірусу, виборів. У медіа та соцмережах вперше почали з'являтися повідомлення про нібито діяльність на території України американських військових біологічних лабораторій²⁵ та звинувачення у загибелі дітей від обстрілів української армії²⁶. Варто зазначити, що ці дві теми є найстійкішими для створення фейків, і ворог протягом трьох років продовжує транслювати неправдиву інформацію про біологічну зброю та вбивства дітей українськими військовими, не надаючи жодних достовірних доказів.
- 3.** У 2021 році значна кількість дезінформації стосувалася, знову ж таки, коронавірусу. Проросійські ЗМІ продовжували дискредитувати ЗСУ та поширювали неправдиву інформацію про те, що в Олександрівці на околиці Донецька внаслідок дій ЗСУ загинула дитина²⁷. Окрім цього, розповсюджували інформацію про те, що з румунської території нібито переправляють зброю та війська до кордонів України з аеродрому в Отопени²⁸ та про те, що у Карпати ввозять військову техніку²⁹.
- 4.** У 2022–2023 роках росія розгорнула масштабну інформаційну війну проти України, використовуючи для своїх цілей різноманітні інформаційні ресурси та залучаючи до цього величезну кількість людей. Головними завданнями інформаційних операцій, які проводив ворог, було поширення в українському суспільстві зневіри та “підігрівання” бажання завершити війну чи, принаймні, зупинити обстріли інфраструктури, віддавши агресору те, що він хоче, створення якомога більшої кількості “розломів” у суспільстві,

24. Obozrevatel заявив, що російські пропагандисти поширюють фейки від його імені. URL: <https://ms.detector.media/manipulyatsii/post/23058/2019-06-19-obozrevatel-zayavyv-shcho-rosiyski-propagandysty-poshyryuyut-fejky-vid-yogo-imeni/>

25. У СБУ спростовують фейк про існування “американських біологічних лабораторій” в Україні. URL: <https://ms.detector.media/manipulyatsii/post/24645/2020-05-08-u-sbu-sprostovuyut-feyk-pro-itsnuvannya-amerykanskykh-biologichnykh-laboratoriy-v-ukraini/>

26. Російський дипломат розповсюдив фейк про війну на Донбасі. URL: <https://ms.detector.media/manipulyatsii/post/24839/2020-06-10-rosiysky-dyplomats-rozpovsyudyv-feyk-pro-vynnu-na-donbasi/>

27. Alexander Kovalenko. URL: https://www.facebook.com/story.php?story_fbid=2564767997162438&id=100008877886960

28. В соцмережах Румунії поширюють фейк про перекидання літаками озброєння в Україну. URL: <https://www.eurointegration.com.ua/news/2021/04/13/7122057/>

29. ФЕЙК: У Карпатах перевозять американську військову техніку. URL: <https://voxukraine.org/uk/fejku-karpatah-perevozyat-amerikansku-vijskovu-tehniku/>

збільшення невдоволення українців центральною владою, місцевим самоврядуванням, мешканцями інших регіонів і навіть власними сусідами, яким дістається більше світла, а також створення негативного фону навколо “українського питання” для зниження рівня підтримки України по всьому світу. Прагнучи досягти поставленої мети, ворог активно розповсюджував у різних джерелах дезінформаційні повідомлення. Узагальнюючи дезінформаційні повідомлення, які були виявлені під час моніторингу в 2022 році, можна зробити висновок, що найчастіше ворог використовував для створення фейків такі теми:

- звинувачення ЗСУ в обстрілах цивільного населення, обстрілах Запорізької атомної електростанції, використання гуманітарних коридорів для ведення боїв, здачі позицій та інших злочинах;
- звинувачення ЄС, Великої Британії та США у веденні війни проти росії та постачанні зброї Україні;
- звинувачення української влади у небажанні йти на переговори;
- Україна — це нацистська країна;
- санкції проти рф;
- погрози використати ядерну зброю;
- геноцид проти російськомовних в Україні;
- функціонування американських біологічних лабораторій на території України;
- каральні заходи на деокупованих територіях;
- енергетична криза.

Отже, війна стала повномасштабною не тільки на полі бою, а й в інформаційному, цифровому просторі і триває багато років.

Щодо притягнення до відповідальності за поширення дезінформації, то це можливо лише в тому випадку, якщо повідомлення містить інформацію, поширення якої заборонено законодавством. В Україні такий контент визначається як на рівні кримінального закону, так і законів України “Про медіа”, “Про інформацію”, Кодексу України про адміністративні правопорушення.

Зокрема, ККУ містить 15 статей, які забороняють поширення інформації:

- 1)** що містить публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ст. 109 ККУ);
- 2)** що містить публічні заклики до зміни меж території або державного кордону України або порушення порядку, встановленого Конституцією України (ст. 110 ККУ);
- 3)** що шкодить 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 (ст. 111 ККУ);
- 4)** що перешкоджає законній діяльності Збройних Сил України та інших військових формувань в особливий період (ст. 114¹ ККУ);
- 5)** поширення якої спрямоване на розпалювання національної, регіональної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образу почуттів громадян у зв'язку з їхніми релігійними переконаннями, а також пряме чи непряме обмеження прав або встановлення прямих чи непрямих привілеїв громадян за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками (ст. 161 ККУ);
- 6)** що містить публічні заклики до вчинення терористичного акту (ст. 258² ККУ);
- 7)** що містить публічні заклики до погромів, підпалів, знищення майна, захоплення будівель чи споруд, насильницького виселення громадян, що загрожують громадському порядку (ст. 295 ККУ);
- 8)** що містить публічні заклики до агресивної війни або до розв'язування воєнного конфлікту (ст. 436 ККУ);
- 9)** інформації з використанням символіки комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів (ст. ККУ 436¹).
- 10)** що містить публічні заклики до геноциду (ст. 442 ККУ);

11) що містить публічне 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 (ч. 1 ст. 111¹ ККУ);

12) інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, у тому числі про їх переміщення територією України, якщо така інформація не розміщувалася (не поширювалася) у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України, Головним управлінням розвідки Міністерства оборони України чи Службою безпеки України або в офіційних джерелах країн-партнерів, вчинене в умовах воєнного або надзвичайного стану (ч. 1 ст. 114² ККУ);

13) 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 (ч. 1 ст. 114² ККУ);

14) що містить образу честі і гідності, погроза вбивством, насильством або знищенням чи пошкодженням майна військовослужбовцю, який здійснює заходи із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації, його близьким родичам чи членам сім'ї (ст. 435¹ ККУ);

15) що містить 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 (ст. 436² ККУ).

Натомість ст. 36 Закону України “Про медіа” містить перелік інформації, що заборонено поширювати:

- 1)** заклики до насильницької зміни, повалення конституційного ладу, розв’язування або ведення агресивної війни або воєнного конфлікту, порушення територіальної цілісності України, ліквідації незалежності України, інформацію, яка виправдовує чи пропагує такі дії;
- 2)** висловлювання, що розпалюють ненависть, ворожнечу чи жорстокість до окремих осіб чи груп осіб за ознакою етнічного чи соціального походження, громадянства, національності, раси, релігії та вірувань, віку, статі, сексуальної орієнтації, гендерної ідентичності, інвалідності;
- 3)** висловлювання, що підбурюють до дискримінації чи утисків стосовно окремих осіб чи груп осіб за ознакою етнічного чи соціального походження, громадянства, національності, раси, релігії та вірувань, віку, статі, сексуальної орієнтації, гендерної ідентичності, інвалідності або за іншими ознаками;
- 4)** пропаганду або заклики до тероризму та терористичних актів, інформацію, що виправдовує чи схвалює такі дії;
- 5)** фільми, розповідження та демонстрування яких заборонено відповідно до Закону України “Про кінематографію”;
- 6)** порнографічні матеріали, а також матеріали, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у видовищних заходах сексуального чи еротичного характеру;
- 7)** пропаганду вживання наркотичних засобів, психотропних речовин;
- 8)** пропаганду жорстокого поводження з тваринами;
- 9)** інструкції або поради щодо виготовлення, придбання або використання вибухових, наркотичних чи психотропних речовин;

- 10)** інформацію, що заперечує або виправдовує злочинний характер комуністичного тоталітарного режиму 1917–1991 років в Україні, злочинний характер націонал-соціалістичного (нацистського) тоталітарного режиму, створює позитивний образ осіб, які обіймали керівні посади у комуністичній партії (посаду секретаря районного комітету і вище), вищих органах влади та управління СРСР, УРСР (УСРР), інших союзних та автономних радянських республік (крім випадків, пов'язаних з розвитком української науки та культури), працівників радянських органів державної безпеки, виправдовує діяльність радянських органів державної безпеки, встановлення радянської влади на території України або в окремих адміністративно-територіальних одиницях, переслідування учасників боротьби за незалежність України у ХХ столітті;
- 11)** інформацію, що містить символіку комуністичного або націонал-соціалістичного (нацистського) тоталітарного режиму;
- 12)** інформацію, що містить пропаганду російського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, а також символіку воєнного вторгнення російського тоталітарного режиму;
- 13)** інформацію, що принижує або зневажає державну мову;
- 14)** інформацію, що заперечує або ставить під сумнів існування українського народу (нації) та/або української державності та/або української мови.

Із зазначеного вище вбачається, що в українському законодавстві існують обмеження щодо поширення певних видів інформації на рівні законодавства, зокрема і для протидії дезінформації. Однак вони не завжди дають змогу ефективно зупинити поширення ворожих наративів. Передусім через відсутність на рівні законодавства термінологічної бази і спеціальних механізмів, адже «деза» часто створюється за допомогою різноманітних маніпуляцій з інформацією, змішування правди та брехні, неточних перекладів з однієї мови на іншу і т. д.

Для підсилення боротьби з дезінформацією, протидії поширенню російських наративів Рішенням РНБО³⁰ було створено Центр протидії дезінформації (далі — ЦПД) як робочий орган РНБО. Одним з його основних завдань є виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, прогнозування, та оцінювання наслідків для безпеки національних інтересів України. ЦПД не є виконавчим органом влади, не має повноважень із проведення перевірок, притягнення до відповідальності, він лише координує роботу щодо протидії дезінформації та розробляє відповідні політики.

30. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/n0015525-21#Text>

**ШАХРАЙСТВО
В МЕРЕЖІ**



Протягом звітного періоду шахраї системно використовували вразливий емоційний стан та довіру громадян на фоні повномасштабної війни³¹. Для ошукування жертв вони використовували теми надання вигаданої фінансової допомоги, продаж неіснуючих товарів, прохання надати безпідставну фінансову допомогу на лікування та інші, які наведено нижче у таблиці.

Таблиця № 6. Кількість повідомлень про шахрайство в мережі

№	Опис теми і способу отримання коштів або персональних даних	Кількість повідомлень, які були виявлені під час моніторингу
1	Продаж неіснуючих товарів	43
2	Збір коштів для ЗСУ	33
3	Створення шахрайських сторінок, які використовують тематику грошових компенсацій та фінансової допомоги, на яких потрібно залишати дані платіжних карток, включаючи секретні коди	29
4	Продаж військової амуніції	15
5	Збір коштів на лікування	8
6	Збір коштів на пошук зниклих безвісти військовослужбовців ЗСУ	6
7	Інвестиції у псевдоприбуткові проєкти	5
8	Організація перевезень із “гарячих точок” за передоплатою	5
9	Отримання доступу до профілів користувачів соцмереж з метою направлення їхнім друзям повідомлення з проханням дати кошти в борг	5
10	Розповсюдження фейкових оголошень про здачу неіснуючих помешкань для вимушених переселенців у безпечних областях України за передоплатою	5

31. У кіберполіції розповіли про найпоширеніші шахрайські схеми заволодіння персональними даними.
URL: <https://ms.detector.media/internet/post/32589/2023-08-02-u-kiberpolitsii-rozpovily-pro-nayposhyrenishi-shakhrayski-skhemy-zavolodinnya-personalnymy-danyamy/>

11	Працевлаштування за кордоном за передоплатою	4
12	Виготовлення документів щодо перетину кордону в період дії правового режиму воєнного стану	2
13	Збір грошей для дітей, які залишилися без батьків	2
	Всього повідомлень	162

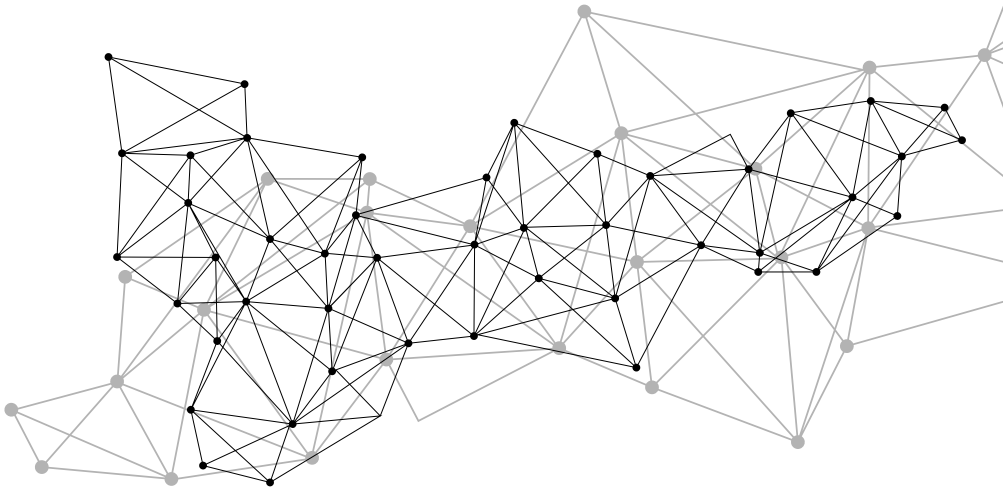
Більшість із наведених способів незаконного отримання коштів полягає в тому, що зловмисники розміщують оголошення в інтернеті про продаж, оренду, надання послуг тощо і просять здійснити передоплату. Наприклад, одна зі схем кібершахрайства, від якої постраждали тисячі українців (особливо на сході нашої країни) — імітація перевезення до безпечних міст і допомога в розміщенні. Злодії розміщують у мережі Інтернет оголошення, пропонуючи усім бажаючим швидко та безпечно виїхати на захід України чи навіть за кордон. Під час спілкування шахраї намагаються виманити передоплату за свої послуги, посилаючись на небезпеку, необхідність резервування місць тощо. Отримавши передоплату, шахраї зникають і перестають виходити на зв'язок.

Ще одна схема злочинів, яка поширилася з початком воєнних дій — діяльність фейкових благодійних і волонтерських організацій. Під виглядом збору грошей на благодійність аферисти створюють фіктивні сайти, сторінки в соціальних мережах, телеграм-канали та привласнюють кошти громадян. Великого поширення набула схема зі збору коштів нібито на лікування дітей, які постраждали від військової агресії.

Також злочинці масово розповсюджують повідомлення різноманітними інформаційними каналами — у соціальних мережах і месенджерах — про можливість отримання грошової допомоги, зокрема, ніби в межах програм “єПідтримка”, “Дія”, допомоги від ЄС, від представників Організації Об'єднаних Націй (далі — ООН), різних програм міжнародних організацій та благодійних фондів. У розсилці шахраї пропонують перейти за посиланнями, які спрямовують на шахрайські сайти-приманки, схожі на справжні сайти державних органів, міжнародних організацій, благодійних фондів. На таких сайтах-приманках розміщені посилання на фішингові ресурси, стилізовані під сторінки відомих українських банків, де необхідно авторизуватися та ввести мобільний номер телефону, пін-код, пароль до інтернет-банкінгу, смс-код від банку. Коли громадяни вводять усі дані, вони автоматично стають відомі шахраям.

Перераховані вище варіанти інтернет-шахрайства є найпоширенішими, але не єдиними. З кожним днем з'являються нові види шахрайства в інтернеті. Для того щоб не втрапити у пастки шахраїв, варто під час здійснення операцій в інтернеті дотримуватися таких правил:

- 1.** Не вказувати власні персональні дані на неперевірених сайтах.
- 2.** Нікому не повідомляти термін дії банківської карти та CVV-код.
- 3.** Перевіряти гіперпосилання та наповнення сайту на відповідність офіційним даним компаній.
- 4.** У разі отримання спірних листів чи повідомлень не здійснювати ніяких оплат до встановлення обставин ситуації, що виникла.
- 5.** Не робити передоплат у неперевірених інтернет-магазинах.
- 6.** Не користуватися неперевіреними оголошеннями щодо роботи, яка обіцяє швидкий зарібок за внесення завдатку.



БЛОКУВАННЯ ВЕБРЕСУРСІВ



З початком широкомасштабного вторгнення блокування вебресурсів, які здійснювали державні органи, стало одним зі способів боротьби з кіберзлочинністю та поширенням ворожого контенту. Однак, незважаючи на основну позитивну мету таких заходів, як захист національної безпеки та прав людини, способи, за допомогою яких реалізовувалося блокування, не завжди були пропорційними до права на вільне вираження поглядів.

За весь період проведення моніторингу порушення цифрових прав людей експерти ППЛ неодноразово у своїх звітах і рекомендаціях наголошували на тому, що більшість способів блокувань, які здійснювалися до та після початку широкомасштабного вторгнення, не відповідають нормам національного законодавства та яскраво демонструють відхилення від стандартів, напрацьованих ЄСПЛ³².

Передусім це пов'язано з тим, що до 24 лютого 2022 року можливість блокування вебресурсів чи певного незаконного контенту була визначена двома нормативно-правовими актами: Законом України “Про електронні комунікації”, який передбачає обов'язок обмежувати доступ до сайтів, які поширюють дитячу порнографію (за рішенням суду)³³, та Законом України “Про авторське право і суміжні права”³⁴, яким передбачені певні можливості для обмеження поширення незаконного контенту, також за рішенням суду.

Однак, незважаючи на те, що національне законодавство не містило інших, позасудових підстав, механізмів та способів блокування вебресурсів, ніж зазначені вище, доступ до сайтів обмежувався на підставі Закону України “Про санкції”. Загалом до початку широкомасштабного вторгнення у такий спосіб було заблоковано 697 вебресурсів³⁵ і така практика застосування санкцій для блокувань сайтів продовжується і під час воєнного стану. Указом Президента України від 19 жовтня 2022 року № 726/2022³⁶ було продовжено практику використання санкційних указів для

32. Юридичний аналіз указу президента про блокування сайтів. URL: <https://www.ppl.org.ua/yuridichniy-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

33. Про електронні комунікації: Закон України від 16 грудня 2020 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

34. Про авторське право і суміжні права: Закон України від 1 грудня 2022 р. № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#n855>

35. Моніторинг порушення цифрових прав в Україні. Аналітичний звіт Період моніторингу – СІЧЕНЬ 2022 року. URL: <https://www.ppl.org.ua/wp-content/uploads/2022/02/%D0%86%D0%BD%D0%B4%D0%B5%D0%BA%D1%81-%D0%B7%D0%B0-%D1%81%D1%96%D1%87%D0%B5%D0%BD%D1%8C-2022-%D1%80%D0%BE%D0%BA%D1%83.pdf>

36. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ № 726/2022. URL: <https://www.president.gov.ua/documents/7262022-44481?fbclid=IwAR02ROVTV4QVJadgI9Q-LCFqzWgeNhMK6uTrKAuaMY5NfT-22093CfI31-E>

обмеження доступу до різноманітних вебсайтів. Безпосередньо цим указом продовжено блокування 114 сайтів, що належать компанії “Яндекс”, сайтів адміністрацій та органів так званих Луганської народної республіки та Донецької народної республіки, а також їхніх новинних порталів.

Найбільшою проблемою застосування цієї санкції є її невідповідність ані вимогам Закону України “Про санкції”, ані міжнародним стандартам захисту прав людини. Це пов’язано з тим, що Закон України “Про санкції” містить у загальному переліку видів санкцій єдину підставу для блокування доступу до інформаційних ресурсів — заборона демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп), і не містить інших санкцій, що стосуються обмеження доступу до вебсайтів. І хоча перелік санкцій у цьому законі є відкритим, застосування таких “інших” санкцій має відповідати принципам, які ЄСПЛ виклав у низці своїх рішень щодо блокувань вебресурсів: прозорості, законності, відповідності меті, ефективності та об’єктивності;

Окрім зазначеного вище способу блокувань вебресурсів, з початку дії в Україні правового режиму воєнного стану національне законодавство було доповнено низкою норм, які визначають нові механізми обмеження доступу до вебресурсів:

1. На підставі рекомендацій НЦУ.

У травні 2022 року Закон України “Про електронні комунікації” було доповнено нормою, яка вимагає від операторів телекомунікаційних мереж виконувати розпорядження НЦУ в умовах надзвичайного або воєнного стану і ці розпорядження можуть стосуватися блокувань вебресурсів, бо відповідно до п. 14 “Порядку оперативнотехнічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного чи воєнного стану” НЦУ та центри управління мережами за погодженням із Адміністрацією Держспецзв’язку відповідно до законодавства можуть допускати деяке зниження якості послуг та встановлювати тимчасові обмеження щодо їх надання до ліквідації надзвичайних ситуацій, скасування надзвичайного та воєнного стану³⁷.

37. Деякі питання оперативнотехнічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану: Постанова Кабінету Міністрів України від 29 червня 2004 р. N 812. URL: <https://zakon.rada.gov.ua/laws/show/812-2004-%D0%BF#Text>

Варто зазначити, що блокування вебресурсів на підставі таких рекомендацій НЦУ почало застосовуватись у перші дні широкомасштабного вторгнення в лютому 2022 року, ще до внесення відповідних змін до Закону України “Про електронні комунікації”.

2. Згідно з розпорядженням НЦУ № 67/850 “Про впровадження системи фільтрації фішингових доменів”³⁸.

Як зазначалося вище, Закон України “Про електронні комунікації” надає НЦУ повноваження видавати розпорядження щодо оперативно-технічного управління електронними комунікаційними мережами, які є обов’язковими для виконання постачальниками електронних комунікаційних мереж та/або послуг, серед яких можуть бути розпорядження про блокування вебресурсів.

Окрім розпоряджень про безпосереднє блокування сайтів, 30 січня 2023 року НЦУ прийняв рішення та затвердив розпорядження № 67/850 “Про впровадження системи фільтрації фішингових доменів”³⁹, на підставі якого на українських інтернет-провайдерів було покладено обов’язок встановити систему блокування, яка кожні 15 хвилин автоматично завантажує перелік адрес, доступ до яких має бути заблокований. Перелік таких адрес створює команда реагування на кіберінциденти в банківській системі України, що входить до складу Центру кіберзахисту НБУ. Метою запровадження такої системи блокування є протидія фішингу та захист користувачів інтернету від шахрайства, яке відбувається у банківській сфері, бо одним із найпоширеніших видів шахрайства є створення фішингових ресурсів, які використовуються для викрадення персональних даних і доступу до банківських рахунків.

Варто зазначити, що оператори електронних комунікацій вважають, що система фільтрації фішингових сайтів несе загрози інформаційній безпеці України. З моменту оприлюднення Розпорядження ІнАУ пропонувала терміново змінити систему фільтрації. Згідно з експертизою Асоціації централізована автоматична система має стратегічні технологічні вразливості, які ставлять під загрозу весь

38. Розпорядження НЦУ від 30.01.2023 № 67/850 про впровадження системи фільтрації фішингових доменів.
URL: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2580&language=uk>

39. Розпорядження НЦУ від 30.01.2023 № 67/850 про впровадження системи фільтрації фішингових доменів.
URL: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2580&language=uk>

сегмент українського інтернету та створюють загрози національній безпеці. У військовий час такі вразливості дають змогу на суттєвий час заблокувати доступ до інтернету в зоні .ua. Транзитний сервер РНБО, на який передається інформація, є дублюванням функцій та знижує рівень захисту системи⁴⁰.

3. За рішенням Нацради або за рішенням суду відповідно до Закону України “Про медіа”⁴¹.

31 березня 2023 року набув чинності Закон України “Про медіа”, який містить норми, що дозволяють Нацраді своїм рішенням або в судовому порядку заблокувати доступ до вебресурсів. Зокрема, ст. 36 встановлює для медіа та платформ спільного доступу до відео заборону поширювати певні види інформації (заклики до насильницької зміни, повалення конституційного ладу, розв’язування або ведення агресивної війни або воєнного конфлікту, порушення територіальної цілісності України, ліквідації незалежності України, інформацію, яка виправдовує чи пропагує такі дії тощо).

Також ст. 119 встановлює обмеження щодо змісту інформації у медіа, пов’язані зі збройною агресією (інформацію, що висвітлює збройну агресію проти України як внутрішній конфлікт, громадянський конфлікт чи громадянську війну, якщо наслідком цього є розпалювання ворожнечі чи ненависті або заклики до насильницької зміни, повалення конституційного ладу чи порушення територіальної цілісності тощо).

Окрім цього, ст. 120 встановлює обмеження щодо структури власності та фінансування медіа під час збройної агресії, а ст. 123 визначає підстави для заборони поширення аудіовізуальних медіасервісів на замовлення та сервісів провайдерів аудіовізуальних сервісів держави-агресора на території України.

За порушення зазначених вище заборон онлайн-медіа може бути заблоковано за рішенням Нацради або в судовому порядку.

40. Оператори вважають, що Система фільтрації фішингових сайтів несе загрози інформаційній безпеці України. URL: <https://inau.ua/news/novyny-inau/operatory-vvazhayut-shcho-systema-filtratsiyi-fishynhovyykh-saytiv-nese-zahrozy>

41. Про медіа: Закон України від 13 грудня 2022 р. № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#n2071>

Аналіз способів блокування вебресурсів здебільшого свідчить про потенційну загрозу цифровим правам людини. Насамперед це пов'язано з тим, що способи блокувань не відповідають європейським стандартам, які ЄСПЛ виклав у низці своїх рішень:

- будь-які формулювання, навіть розроблені національними судами або іншими незалежними органами, з яких випливає блокування, повинні мати належне підґрунтя у законодавстві;
- чіткість визначення категорій протиправного контенту, за поширення якого сайт може підлягати блокуванню;
- наявність запобіжників. Незалежно від того, яким чином відбувалося блокування ресурсу, власників сайтів повинні повідомляти про такий захід. Їм необхідно надати можливість висловити власні аргументи щодо підстав блокування, залучивши їх до процесу;
- необхідність проведення оцінки впливу заходів із блокування до його впровадження. Варто як зважати на розмежування між законним і протиправним контентом, так і розуміти, що окремі види блокувань (наприклад, усього сайту, а не окремої сторінки, що містить протиправний контент, блокування за IP-адресою, де розміщено кілька сайтів) будуть апріорі свавільними;
- використання судовими або іншими незалежними органами, які мають розглядати справи про блокування, практики ЄСПЛ та балансування ними інтересів власників, користувачів і держави при ухваленні відповідного рішення про блокування;
- оцінка протиправності контенту та оцінка правомірності блокування має проводитися окремо і відповідно до практики ЄСПЛ з цих питань.

Якщо звернутися до української практики блокування вебресурсів, то можна побачити, що нині вона не повною мірою відповідає названим принципам.

Окремо варто зазначити, що на момент написання цього звіту немає можливості повною мірою проаналізувати зазначені вимоги Конвенції про захист прав людини і основоположних свобод у контексті зазначених вище блокувань, тому що обмеження доступу до цих ресурсів унеможливорює аналіз їхнього контенту.

Щодо кількісних показників блокувань вебресурсів, то кількість заблокованих вебресурсів, здійснених на підставі Закону України "Про санкції", на підставі рекомендацій НЦУ та за рішеннями Нацради за період із лютого 2022 року по серпень 2023 року збільшилась у 50 разів проти кількості блокувань, які здійснювалися на підставі Закону України "Про санкції" за період із травня 2019 року по січень 2022 року.

Таблиця № 7. Кількість блокувань вебресурсів, які було зафіксовано під час моніторингу

Спосіб блокувань	Кількість заблокованих вебресурсів за період із травня 2019 року по січень 2022 року	Кількість заблокованих вебресурсів за період із лютого 2022 року по серпень 2023 року
На підставі Закону України "Про санкції"	697	114
На підставі рекомендацій НЦУ	-	11 754
Згідно з розпорядженням НЦУ "Про впровадження системи фільтрації фішингових доменів"	-	23 096
За рішенням Нацради	-	2
РАЗОМ	697	34 966

**СВОБОДА ВИРАЖЕННЯ
ПОГЛЯДІВ**



У межах цього дослідження експерти ППЛ здійснювали моніторинг судових рішень, які стосуються права на свободу вираження поглядів у мережі Інтернет. Фокус дослідження з метою виявлення потенційних порушень права на свободу думки і слова, на вільне вираження своїх поглядів і переконань, передусім був направлений на застосування статей ККУ, які містять заборону поширення певних видів інформації, а також рішення, які суд ухвалює у справах про захист честі, гідності та ділової репутації.

Варто зазначити, що до березня 2022 року ККУ містив дев'ять статей, які передбачали кримінальну відповідальність за поширення певних видів інформації, зокрема і в інтернеті:

- 1)** інформації, що містить публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ст. 109 ККУ);
- 2)** інформації, що містить публічні заклики до зміни меж території або державного кордону України або порушення порядку, встановленого Конституцією України (ст. 110 ККУ);
- 3)** інформації, що шкодить 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 (ст. 111 ККУ);
- 4)** інформації, що перешкоджає законній діяльності Збройних сил України та інших військових формувань в особливий період (ст. 114¹ ККУ);
- 5)** інформації, поширення якої спрямоване на розпалювання національної, регіональної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образу почуттів громадян у зв'язку з їхніми релігійними переконаннями, а також пряме чи непряме обмеження прав або встановлення прямих чи непрямих привілеїв громадян за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками (ст. 161 ККУ);

- 6)** інформації, що містить публічні заклики до вчинення терористичного акту (ст. 258² ККУ);
- 7)** інформації, що містить публічні заклики до погромів, підпалів, знищення майна, захоплення будівель чи споруд, насильницького виселення громадян, що загрожують громадському порядку (ст. 295 ККУ);
- 8)** інформації, що містить публічні заклики до агресивної війни або до розв’язування воєнного конфлікту (ст. 436 ККУ);
- 9)** інформації з використанням символіки комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436¹ ККУ).

За період із березня 2022 року по 30 вересня 2022 року ККУ було доповнено ще чотирма статтями, які, зокрема, стосуються поширення інформації в інтернеті:

- 1)** 15 березня 2022 року набув чинності Закон України “Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність”⁴². Він доповнив ККУ новою ст. 111¹ — “Колабораційна діяльність”;
- 2)** 16 березня 2022 року набув чинності Закон України “Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції”⁴³. Він доповнив ККУ двома новими статтями: 435¹ — “Образа честі і гідності військовослужбовця, погроза військовослужбовцю” та 436² — “Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників”;

42. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України від 3 березня 2022 р. № 2108-IX. URL: <https://zakon.rada.gov.ua/laws/show/2108-20#n6>

43. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 3 березня 2022 р. № 2110-IX. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text>

3) 27 березня 2022 року набув чинності Закон України “Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану”⁴⁴. Він доповнив ККУ новою ст. 114² — “Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану”. 1 квітня 2022 року законодавці, з метою додаткового удосконалення складу цього кримінального правопорушення, внесли у ст. 114² зміни⁴⁵.

За результатами пошуку в Єдиному державному реєстрі судових рішень, які стосуються поширення забороненої інформації в інтернеті, за період із лютого 2022 року по серпень 2023 року **було виявлено та проаналізовано 786 вироків**. Із них 633 було ухвалено за новими статтями ККУ, що становить 80,5 % з усіх вироків за окреслений період. Це свідчить про те, що внесення до ККУ нових статей дає змогу більш системно реагувати на поширення забороненого проросійського контенту. Окрім цього, варто зазначити, **що кількість вироків, які ухвалили під час правового режиму воєнного стану та які стосуються права на свободу вираження поглядів у мережі Інтернет, збільшилася втричі проти періоду з 2014 по 2021 роки**. У зазначений період було ухвалено 247 вироків у таких справах⁴⁶.

44. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 р. № 2160-IX. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#n6>

45. Про внесення змін до статті 114² Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 1 квітня 2022 р. № 2178-IX. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-30-12-22.pdf>

46. Аналітичний звіт “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-30-12-22.pdf>

Таблиця № 8. Кількість вироків у кримінальних справах

	109	110	111	111 ¹	114 ¹	114 ²	161	258 ²	295	435 ¹	436	436 ¹	436 ²
Травень-липень	16	18	-	9	-	6	-	-	-	1	1	1	49
Серпень	4	6	1	23	-	2	-	-	-	-	-	1	22
Вересень	2	3	1	14	-	4	-	-	-	-	1	-	25
Жовтень	-	-	-	-	-	-	-	-	-	-	-	-	-
Листопад	-	-	1	1	-	-	-	-	-	-	-	-	4
Грудень	-	-	1	5	-	10	-	-	-	-	-	-	15
Січень	-	1	1	12	-	3	-	-	-	-	-	-	20
Лютий	2	6	4	11	-	8	-	-	-	1	-	-	32
Березень	7	3	3	12	-	3	-	-	-	-	-	-	55
Квітень	2	3	5	8	-	6	-	-	-	-	-	-	31
Травень	2	10	8	13	-	4	-	-	-	-	-	-	59
Червень	1	6	3	12	-	3	1	-	-	-	-	-	49
Липень	1	6	3	13	-	11	-	-	-	-	-	2	33
Серпень	1	3	2	12	-	5	-	-	-	-	-	8	29
РАЗОМ	38	65	33	145	0	65	1	0	0	2	2	12	423
ВСЬОГО	786												

Відповідно до проведеного аналізу судових рішень за період із лютого 2022 року по серпень 2023 року було встановлено, що найчастіше суди застосовували покарання у вигляді позбавлення волі, однак у 507 випадках із 786 (64,5 %) засуджених було звільнено від відбування покарання у вигляді позбавлення волі на підставі ст. 75 ККУ з призначенням іспитового строку.

У 145 із 786 вироків (18,64 %), які було ухвалено за ч. 1 ст. 111¹ ККУ, призначено покарання у вигляді позбавленням права обіймати певні посади або займатися певною діяльністю на строк від десяти до п'ятнадцяти років. Варто зазначити, що часто ця міра покарання у більшості випадків застосовувалася до пенсіонерів або непрацюючих осіб.

У 12 із 786 (1,5 %) вироків засуджені отримали покарання у вигляді штрафу.

У 122 із 786 вироків (15,5 %) засудженим було призначено покарання у вигляді позбавлення волі, без звільнення від його відбування.

Тобто тенденція непризначення судами реального покарання за поширення незаконної інформації в інтернеті спостерігається протягом усього періоду дослідження і вона залишається сталою.

Таблиця № 9. Кількісні показники щодо застосованих судами покарань

Стаття ККУ	Звільнено від відбування покарання	Штраф	Позбавлення волі	Позбавлення права обіймати посади	Всього
109	28	1	10	-	39
110	46	2	16	-	64
111	-	-	33	-	33
114 ¹	-	-	-	-	0
161	1	-	-	-	1
258 ²	-	-	-	-	0

295	-	-	-	-	0
436	-	-	2	-	2
436 ¹	11	1	-	-	12
111 ¹	-	-	-	145	145
114 ²	34	2	29	-	65
436 ²	386	5	32	-	423
435 ¹	1	1	-	-	2
РАЗОМ	507	12	122	145	786

Кількість осіб, які понесли реальне покарання за поширення забороненої інформації в інтернеті у вигляді позбавлення волі, становить 15,5 %, а у вигляді штрафу — всього 1,5 %. Усі інші особи були звільнені від відбування покарання у зв'язку з укладенням угоди з прокурором про визнання вини або визнання вини під час розгляду справи. Уникнення реальної відповідальності особами, які вчинили кримінально карані злочини, що стосуються поширення інформації, у більшості випадків відбувається у зв'язку з тим, що суди застосовують ст. 75 ККУ. Остання передбачає звільнення від відбування покарання з випробуванням у випадку затвердження угоди про примирення або про визнання вини. Обвинувачені здебільшого визнавали свою вину та уклали угоду про примирення.

Суди застосовують такий спосіб призначення покарання, бо доволі часто позбавлення або обмеження волі — саме ті санкції, які містять більшість аналізованих статей, є непропорційними щодо шкоди, яка була завдана поширенням забороненої інформації. Однак у випадку поширення інформації, яка завдає суттєвої шкоди суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України, мають застосовуватися такі суворі покарання, як обмеження або позбавлення волі.

Також під час аналізу вироків було виявлено **проблему в кваліфікації однотипних дій та, відповідно, застосування різних видів покарання до осіб, які здійснювали поширення інформації в той самий спосіб та схожого змісту.** Розглянемо детально:

1) частина 1 ст. 111¹ та ст. 436² ККУ є колізійними і щомісячний аналіз судової практики за цими статтями підтверджує цю проблему застосування різних видів покарань за однотипні діяння;

2) кваліфікації та призначення покарання за поширення інформації про рух та розташування підрозділів ЗСУ відбувалися за різними статтями ККУ — за ч. 2 ст. 111 ККУ та ч. 3 ст. 114² ККУ, які є конкуруючими і передбачають відповідальність за однотипні діяння, які складно кваліфікувати.

Окремо варто звернути увагу на те, що значна частина вироків не містять тексту інформації, поширення якої стало підставою для притягнення особи до кримінальної відповідальності, що не дає можливості оцінити її зміст і пропорційність застосування до особи покарання. **У 137 з 786 (17,4 %) ухвалених вироків не визначено інформацію,** поширення якої стало підставою для притягнення особи до кримінальної відповідальності.

Національні суди досить часто **не проводять самостійного аналізу** тексту та змісту відео- чи фотоповідомлень, які стали підставою для обвинувачень у порушенні норм ККУ. У більшості випадків наявність/ відсутність вини особи встановлюється за допомогою проведення судової експертизи (комплексної, семантико-текстуальної експертизи писемного мовлення, судово-лінгвістичної експертизи тощо). Отже, у таких справах факт вчинення злочину встановлюється скоріше не судом, а судовим експертом, який надає оцінку змісту поширеного повідомлення. Роль суду найчастіше зводиться лише до констатації факту наявності кримінального правопорушення, підтвердженого висновком експерта, та призначення міри покарання. **У 227 із 786 (28,8 %) вироків,** які були проаналізовані під час цього моніторингу, не міститься інших способів аналізу поширеної інформації судом, крім посилань на висновки експертів-лінгвістів. У таких рішеннях вбачається ризик того, що судова практика є насправді повним відтворенням позиції та практикою відповідних судових експертів.

У 79 із 786 (10,05 %) вироків 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.

Варто зазначити, що всі висновки, які стосуються практики розгляду судами справ про поширення забороненої інформації, ґрунтовно розписані в аналітичному звіті “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”⁴⁷. Також у цьому звіті надано вичерпні рекомендації щодо покращення ситуації у цій галузі та на підставі рекомендацій група експертів підготувала пропозиції щодо внесення змін до ККУ. На момент написання звіту ППЛ веде переговори з народними депутатами України щодо реєстрації та просування відповідного законопроекту.

Щодо моніторингу судових рішень у справах про захист честі, гідності та ділової репутації. Під час моніторингу було виявлено **45 рішень у цій категорії справ**, які містять ознаки порушення цифрових прав людини у вигляді непропорційного обмеження права на свободу вираження поглядів — *одночасного застосування таких способів правового захисту, як спростування та видалення спірних відомостей без обґрунтування необхідності у цьому, невмотивованість рішень про видалення спірної інформації, що порушує європейські стандарти у галузі свободи слова.*

Як зазначалося у попередніх звітах про результати моніторингу цифрових прав, в Україні активно розвивається судова практика, відповідно до якої суди зобов'язують не лише спростувати ту чи іншу інформацію, визнану недостовірною, а 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”⁴⁸.

Окремо варто зауважити, що в Єдиному державному реєстрі судових рішень продовжували з'являтися рішення у справах про захист честі, гідності і ділової репутації, а також вирoki судів, у яких зміст спірної інформації прихований позначками “ІНФОРМАЦІЯ No_”, що унеможлиблює ознайомлення з відомостями, щодо яких заявлено позовні вимоги. Під час звітного періоду **було виявлено 5 таких рішень.**

47. Аналітичний звіт “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-A4-30-12-22.pdf>

48. Бурмагін О., Опришко А. Судова практика про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики. URL: <https://www.ppl.org.ua/wp-content/uploads/2020/08/Судова-практика-у-справах-поширення-інформації-в-інтернеті.pdf>

**ДОСТУП
ДО ІНФОРМАЦІЇ**



Право на доступ до публічної інформації є одним із прав людини, яке в сучасному світі все більше знаходить реалізацію у цифровому вимірі. Велику кількість інформації ми можемо отримувати з мережі Інтернет на загальнодоступних офіційних онлайн-ресурсах — офіційних вебсайтах, на єдиному державному вебпорталі відкритих даних, із публічних електронних реєстрів. Це право гарантовано статтями 34, 50 Конституції України, Конвенцією Ради Європи про доступ до офіційних документів, Конвенцією про захист прав людини і основоположних свобод, Законом України “Про доступ до публічної інформації” та іншими законами. Право на доступ до публічної інформації може бути обмежене виключно законом для захисту інтересів національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням.

Відповідно до п. 3 Указу Президента України № 64/2022 “Про введення воєнного стану в Україні” у зв’язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, передбачено можливість обмеження, зокрема, права вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір.

Варто зазначити, що крім Закону України “Про доступ до публічної інформації”, яким визначено види інформації, доступ до якої може бути обмежено та механізм такого обмеження, у травні 2022 року до Закону України “Про правовий режим воєнного стану” було додано норми ч. 10 ст. 9, яка дозволила органам місцевого самоврядування, військово-цивільним адміністраціям та військовим адміністраціям:

- не оприлюднювати перелік та умови отримання послуг, що надаються цими органами, форми і зразки документів, правила їх заповнення;
- оприлюднювати з порушенням строку проекти нормативно-правових актів, рішень органів місцевого самоврядування, розроблені відповідними розпорядниками;
- не оприлюднювати інформацію, яку розпорядники повинні оприлюднювати згідно з Законом України “Про засади державної регуляторної політики у сфері господарської діяльності” та Законом України “Про державну допомогу суб’єктам господарювання”.

Та це не означає, що доступ до такої інформації обмежено. Ці заходи стосуються лише оприлюднення інформації на сайті.

Окрім цього, у березні 2022 року було прийнято Постанову Кабінету Міністрів України № 263 “Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану”, яка 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**. Після затвердження цієї постанови відбулося закриття доступу до низки державних публічних реєстрів, а також до вебпорталів, які містять набори відкритих даних.

З метою виявлення проблем у сфері доступу до публічної інформації під час правового режиму воєнного стану експерти ППА здійснювали моніторинг та аналіз відповідей на запити на сайті “Доступ до правди”⁴⁹. Окрім цього, експерти щомісячно відслідковували роботу публічних реєстрів, перевіряючи їхню доступність і відкритість, бо доступ до низки державних реєстрів був обмежений певний період, а частина залишається закритою і станом на момент написання цього звіту.

Щодо моніторингу відповідей на запити

Під час моніторингу було проаналізовано **3366** відповідей на запити, які розміщені у відкритому доступі на ресурсі “Доступ до правди”. У більшості випадків розпорядники вчасно та повною мірою надали інформацію у відповідь на запити (2759 запитів, що відсотково становить 81,96 %).

Щодо відмов у наданні публічної інформації варто зазначити, що майже 30 % відмов у наданні публічної інформації є неправомірними, а найбільша кількість відмов на запити протягом року була з

49. Як надіслати запит. URL: <https://dostup.pravda.com.ua/>

посиланням на правовий режим воєнного стану та на те, що запитувана інформація є з обмеженим доступом, без застосування трискладового тесту.

Також дуже розповсюдженою підставою для відмов у наданні публічної інформації було посилання на те, що інформація не створена, тоді як розпорядник володів такою інформацією. Часто ця інформація стосувалася використання бюджетних коштів.

І ще однією підставою, яку розпорядники використовували для відмов, було віднесення запиту до такого, що не відповідає встановленій формі. Наприклад, посилання на те, що запит не містить підпису, або навіть електронного підпису.

Щодо кількісних показників, то вони наведені у таблицях нижче:

Таблиця № 10. Порівняльна таблиця загальної кількості запитів та кількості відмов, включаючи неправомірні відмови

Період моніторингу	Загальна кількість запитів, які були проаналізовані	Кількість відмов	Кількість неправомірних відмов	Кількість неправомірних відмов у відсотках
Серпень 2022	257	32	19	59,3 %
Вересень 2022	257	54	19	35,1 %
Жовтень 2022	212	46	4	8,6 %
Листопад 2022	314	63	22	34,9 %
Грудень 2022	221	62	21	33,8 %
Січень 2023	133	23	9	39,1 %
Лютий 2023	359	51	16	31,3 %

Березень 2023	197	30	5	16,6 %
Квітень 2023	352	69	19	27,5 %
Травень 2023	276	43	14	32,5 %
Червень 2023	271	49	7	14,2 %
Липень 2023	257	43	9	20,9 %
Серпень 2023	260	43	12	27 %
ВСЬОГО	3366	608	176	28,9 %

Таблиця № 11. Порівняльна таблиця загальної кількості за підставами відмов

Період моніторингу	Всього відмов	Відмова з посиланням на правовий режим воєнного стану	Віднесення до інформації з обмеженим доступом	Неправомірні зауваження до форми запиту	Відсутність інформації	Інші підстави для відмов
Серпень 2022	19	10	6	3	-	-
Вересень 2022	19	6	3	-	10	-
Жовтень 2022	4	2	-	-	2	-
Листопад 2022	22	7	1	11	3	-
Грудень 2022	21	14	3	1	2	1⁵⁰
Січень 2023	9	1	2	-	3	3
Лютий 2023	16	4	4	4	2	2
Березень 2023	5	2	2	1	-	-
Квітень 2023	19	2	9	3	3	2

50. Підставою для надання відмов у відповідь на запит було посилання на те, що запитувана інформація опублікована на сайті або її можна отримати під час особистого візиту безпосередньо у розпорядника.

Травень 2023	14	2	7	3	2	-
Червень 2023	7	1	3	2	1	-
Липень 2023	9	-	6	3	-	-
Серпень 2023	12	-	5	2	2	2
ВСЬОГО	176	51	51	33	30	10

Аналіз кількісних показників відмов у наданні публічної інформації ще раз підкреслює, що їхня кількість є достатньо великою. І хоча періодично спостерігається позитивна тенденція щодо надання відповідей на запити, розпорядники продовжують зловживати правовим режимом воєнного стану та приховувати суспільно важливу інформацію.

Щодо закриття публічного доступу до державних реєстрів

Як зазначалося вище, у березні 2022 року на підставі Постанови Кабінету Міністрів України № 263 було обмежено доступ до низки державних реєстрів. Як повідомляла Державна судова адміністрація, доступ до Єдиного державного реєстру судових рішень та сервісів “Стан розгляду справ” і “Список справ, призначених до розгляду” було обмежено з метою запобігання загрози життю та здоров’ю суддів та учасників судового процесу в умовах воєнного стану, а також забезпечення інформаційної безпеки⁵¹.

Загалом під час моніторингу, проведеного ППА із 24 лютого 2022 року по 31 серпня 2022 рік, було виявлено обмеження доступу до таких реєстрів:

Обмеженими на певний період були:

- 1.** Єдиний державний реєстр судових рішень (із березня 2022 року по 20 червня 2022 року).
- 2.** Реєстр повідомлень суддів про втручання у здійснення правосуддя (з березня 2022 року по 20 червня 2022 року).
- 3.** Єдиний державний реєстр юридичних осіб, фізичних осіб — підприємців та громадських формувань (із березня по грудень 2022 року).
- 4.** Реєстр операторів, провайдерів телекомунікацій (із березня 2022 по грудень 2022 року).

51. На період війни призупинили доступ до реєстру судових рішень. URL: <https://sudreporter.org/na-period-vijny-pruzupynyly-dostup-do-reyestru-sudovyh-rishen/>

Залишаються закритими на момент написання цього звіту:

1. Єдиний реєстр громадських формувань.
2. Реєстр громадських об'єднань.
3. Реєстр суб'єктів у сфері медіа.
4. Реєстр декларацій родинних зв'язків та добросовісності.
5. Державний реєстр атестованих судових експертів.
6. Реєстр методик проведення судових експертиз.
7. Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство.
8. Єдиний реєстр арбітражних керуючих України.
9. Реєстр суднозаходів.
10. Реєстр морських портів України.
11. Реєстр гідротехнічних споруд морських портів України.
12. Реєстр суб'єктів господарювання, що провадять свою господарську діяльність у сферах енергетики та комунальних послуг, діяльність яких регулює Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг.
13. Єдиний державний реєстр операторів поштового зв'язку.
14. Реєстр виданих ліцензій на користування радіочастотним ресурсом України.
15. Реєстр платників акцизного податку з реалізації пального та спирту етилового.
16. Реєстр альтернативних видів палива.

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.

**ЗМІНИ
В ЗАКОНОДАВСТВІ**



У період із 24 лютого по 31 серпня 2023 року українське законодавство зазнало багатьох кардинальних змін, які пов’язані із введенням та дією правового режиму воєнного стану в Україні. Загалом за звітний період було ухвалено 14 законів та нормативно-правових актів, які мають безпосередній вплив на цифрові права людини.

1. Першим нормативно-правовим актом, який розділив життя кожного українця на “до” та “після” був Указ Президента України від 24 лютого 2022 року № 64/2022 “Про введення воєнного стану в Україні” у зв’язку з військовою агресією рф проти України. Невідкладно, цього ж дня, Верховна Рада України ухвалила Закон України № 2102-IX “Про затвердження Указу Президента України “Про введення воєнного стану в Україні”. У результаті їх ухвалення на всій території України було введено воєнний стан із 05 години 30 хвилин 24 лютого 2022 року. Протягом березня 2022 — серпня 2023 року строк дії правового режиму воєнного стану продовжувався вісім разів. У липні 2023 року його було продовжено, На момент написання цього звіту він діє до 15 листопада 2023 року. Указом передбачено можливість обмеження низки фундаментальних прав людини, зокрема: на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

2. Введення воєнного стану в Україні дало можливість застосовувати норми Закону України “Про правовий режим воєнного стану”.

Закон визначає зміст правового режиму воєнного стану, порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб.

Стаття 1 визначає воєнний стан як особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози

небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Отже, зазначений закон дозволяє під час дії воєнного стану обмежувати права і свободи людини. З огляду на це Указом Президента України від 24 лютого 2022 року № 64/2022 "Про введення воєнного стану в Україні" передбачена можливість обмеження прав людини, гарантованих такими нормами Конституції України, як:

- ст. 30 ("Кожному гарантується недоторканність житла");
- ст. 31 ("Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції");
- ст. 32 ("Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України");
- ст. 33 ("Кожному, хто на законних підставах перебуває на території України, гарантується свобода пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом");
- ст. 34 ("Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань");
- ст. 38 ("Громадяни мають право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування");
- ст. 39 ("Громадяни мають право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації, про проведення яких завчасно сповіщаються органи виконавчої влади чи органи місцевого самоврядування");
- ст. 41 ("Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності");
- ст. 42 ("Кожен має право на підприємницьку діяльність, яка не заборонена законом");

- ст. 43 (“Кожен має право на працю, що включає можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується”);
- ст. 44 (“Ті, хто працює, мають право на страйк для захисту своїх економічних і соціальних інтересів”);
- ст. 53 (“Кожен має право на освіту”).

Варто також звернути увагу на те, що з введенням воєнного стану Україна частково відступила від своїх міжнародних зобов'язань у сфері захисту прав людини. Зокрема, відбулася дерогація зобов'язань за Конвенцією про захист прав людини і основоположних свобод, про що Уряд України сповістив Раду Європи. Межі відступу відповідають приписам Указу Президента України № 64/2022 “Про введення воєнного стану в Україні”⁵² і наступним указам про продовження дії воєнного стану⁵³.

Як бачимо, введення воєнного стану в Україні має суттєвий вплив на низку фундаментальних прав людини, зокрема і тих із них, які в сучасному світі тісно пов'язані з цифровим виміром, а саме на:

- право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції в інтернеті;
- право на приватність і захист даних;
- право на свободу думки і слова, на вільне вираження своїх поглядів і переконань;
- право на мирні збори та освіту в інтернеті тощо.

Перелік заходів, які можуть запроваджувати та здійснювати військові адміністрації (у разі їх утворення) самостійно або із залученням органів виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування, у межах тимчасових обмежень конституційних прав і свобод людини і громадянина під час воєнного стану міститься у Законі України “Про правовий

52. Note Verbale. URL: <https://rm.coe.int/0900001680a5b0b0>

53. Див., зокрема: Notification of Communication. URL: <https://rm.coe.int/0900001680a6ccc2>

режим воєнного стану”. Зокрема, п. 11 ст. 8 дозволяє регулювати у порядку, визначеному Кабінетом Міністрів України:

- 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;
- забороняти роботу приймально-передавальних радіостанцій особистого і колективного користування та передачу інформації через комп’ютерні мережі.

Таким чином, закон не забороняє відповідним органам влади під час воєнного стану вводити необхідні обмеження чи покладати додаткові обов’язки на осіб, які здійснюють діяльність у наведених сферах. Утім, такі обмеження прав повинні відбуватися у порядку, визначеному Кабінетом Міністрів України.

3. На виконання вимог Закону України “Про правовий режим воєнного стану” Кабінетом Міністрів України 12 березня 2022 року було прийнято Постанову № 263 “Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану”⁵⁴. Постанова надала право на період дії воєнного стану міністерствам, іншим центральним і місцевим органам виконавчої влади, державним та 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, зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

54. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12 березня 2022 р. № 263. URL: <https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text>

4. Нормативно-правовим актом, що окреслив перелік забороненої до поширення інформації, став 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”. З метою оптимізації процесу акредитації, а також покращення взаємодії з представниками ЗМІ під час роботи в районах бойових дій, 27 лютого 2023 року до нього було внесено зміни.

Ухвалення наказу мотивовано, зокрема, метою забезпечення об’єктивного висвітлення подій, інформування населення та світової спільноти про воєнні злочини, які вчиняє РФ під час широкомасштабної збройної агресії проти України, розпочатої 24 лютого 2022 року. Водночас він став інструментом контролю за поширенням інформації. У преамбулі зазначається, що він спрямований на попередження витоку інформації з обмеженим доступом, запобігання поширенню представниками засобів масової інформації (у тому числі іноземними) та публічними особами, до думки яких прислуховується громадськість (лідери думок, блогери тощо) відомостей, розголошення яких може призвести до обізнаності противника про дії ЗСУ та інших складових сил оборони, негативно вплинути на хід виконання завдань за призначенням під час дії правового режиму воєнного стану.

Зокрема, визначено перелік інформації, розголошення якої може призвести до обізнаності противника про дії ЗСУ, інших складових сил оборони, негативно вплинути на хід виконання завдань за призначенням під час дії правового режиму воєнного стану. До такої інформації віднесено:

- 1.** Найменування військових частин (підрозділів) та інших військових об’єктів в районах виконання бойових (спеціальних) завдань, географічні координати місць їх розташування.
- 2.** Чисельність особового складу військових частин (підрозділів).
- 3.** Кількість озброєння та бойової техніки, матеріально-технічних засобів, їх стан та місця зберігання.
- 4.** Описи, зображення та умовні позначки, які ідентифікують або можуть ідентифікувати об’єкти.
- 5.** Інформація щодо операцій (бойових дій), які проводяться або плануються.

- 6.** Інформація щодо системи охорони та оборони військових об'єктів і засобів захисту особового складу, озброєння та військової техніки, які використовуються (крім тих, які видимі або очевидно виражені).
- 7.** Порядок залучення сил та засобів до виконання бойових (спеціальних) завдань.
- 8.** Інформація про збір розвідувальних даних (способи, методи, сили та засоби, що залучаються).
- 9.** Інформація про переміщення та розгортання своїх військ (найменування, кількість, місця, райони, маршрути руху).
- 10.** Інформація про військові частини (підрозділи), форми, методи, тактику їхніх дій та способи застосування за призначенням.
- 11.** Інформація про проведення унікальних операцій із зазначенням прийомів та способів, що використовувалися.
- 12.** Інформація про ефективність сил і засобів радіоелектронної боротьби противника.
- 13.** Інформація про відкладені або скасовані операції.
- 14.** Інформація про зниклий або збитий літак, літальний апарат, зникле судно та пошуково-рятувальні операції, які плануються або проводяться.
- 15.** Інформація про планування та проведення заходів забезпечення безпеки застосування військ (дезінформація, імітація, демонстративні дії, маскування, протидія технічним розвідкам і захист інформації).
- 16.** Відомості про проведені інформаційно-психологічні операції, ті, що проводяться, а також плануються.
- 17.** Інформація, яка має на меті пропаганду або виправдання широкомасштабної збройної агресії Російської Федерації проти України.
- 18.** Інформація, яка може призвести до обізнаності противника про результати ракетних ударів по військових об'єктах (пунктах), якщо така інформація не розміщувалась у відкритому доступі Генеральним штабом або іншими органами військового управління Збройних сил України.

19. Інформація, яка може призвести до обізнаності противника про результати ракетних ударів по об'єктах критичної інфраструктури держави, якщо така інформація не розміщувалася органами державної влади України.

20. Інформація про скерування, переміщення зброї, озброєння та бойових припасів в Україну, зокрема про їхнє переміщення територією України, якщо така інформація не розміщувалась у відкритому доступі Генеральним штабом Збройних сил України чи Міністерством оборони України або в офіційних джерелах відповідних відомств країн-партнерів.

21. Інформація про переміщення, рух або розташування Збройних сил України чи інших утворених відповідно до законів України військових формувань, за можливості їхньої ідентифікації на місцевості, якщо така інформація не розміщувалась у відкритому доступі Генеральним штабом Збройних сил України.

22. Інформація, яка може дозволити противнику встановити конкретне місце розміщення сил і засобів підрозділів протиповітряної оборони.

23. Реєстраційні номери, прапори або інші позначки на озброєнні та військовій техніці іноземного виробництва, що надавалась у межах матеріально-технічної допомоги від країн-партнерів, які безпосередньо можуть свідчити про країну походження зразка озброєння та військової техніки.

24. Фото- або відеоматеріали зі знищеними (ураженими, пошкодженими) зразками озброєння та військової техніки іноземного виробництва, які надавалися в межах матеріально-технічної допомоги від країн-партнерів.

Не оспорюючи необхідності обмеження поширення певної інформації в умовах дії правового режиму воєнного стану в інтересах національної безпеки, вважаємо за необхідне висловити низку зауважень, які можуть вказувати на існування загрози надмірного втручання у свободу слова.

Перелік інформації, забороненої до поширення, містить дефініції, частина з яких чітко не визначена законодавством України. До прикладу:

- у п. 4 йдеться про заборону поширювати описи, зображення та умовні позначки, які ідентифікують або можуть ідентифікувати об’єкти. Які об’єкти мається на увазі — військові чи цивільні — залишається незрозумілим і дає підстави для широкого тлумачення заборони;
- п. 11 – інформація про проведення унікальних операцій із зазначенням прийомів та способів, що використовувались. Які операції слід вважати унікальними також чітко не визначено, а тому в умовах воєнного часу ймовірніше за все поширення будь-якої інформації про проведення операцій буде обмежуватись, що не завжди може бути виправданим;
- п. 12 — інформація про ефективність сил і засобів радіоелектронної боротьби противника. Зміст поняття “радіоелектронна боротьба противника” також є недостатньо зрозумілим і невизначеним у законодавстві України, а тому застосування цього обмеження може викликати труднощі практичного характеру.

З огляду на викладене, на нашу думку, доцільним було б Міністерству оборони України та/або Генеральному штабу ЗСУ оприлюднити на своєму офіційному вебсайті словник термінів, які застосовано в наказі Головнокомандувача ЗСУ від 3 березня 2022 року № 73 “Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану”, надавши відповідні роз’яснення вживаним у ньому поняттям, зокрема, таким як “унікальна операція”, “сили і засоби радіоелектронної боротьби противника”, “інформаційні операції”, “психологічні операції” тощо.

5. Ухвалено 5 травня 2022 року Закон України “Про внесення змін до Закону України ‘Про електронні комунікації’ щодо підвищення ефективності організації роботи постачальників електронних комунікаційних мереж та/або послуг в умовах воєнного стану”, який набув чинності 27 травня 2022 року⁵⁵.

55. Про внесення змін до Закону України “Про електронні комунікації” щодо підвищення ефективності організації роботи постачальників електронних комунікаційних мереж та/або послуг в умовах воєнного стану: Закон України від 3 травня 2022 р. № 2240-IX. URL: <https://zakon.rada.gov.ua/laws/show/2240-20#Text>

Основною його новелою є надання Національному центру оперативнотехнічного управління електронними комунікаційними мережами повноважень щодо видання в умовах надзвичайного або воєнного стану обов'язкових для виконання розпоряджень постачальникам електронних комунікаційних мереж та/або послуг.

6. 22 травня 2022 року Верховна Рада України ухвалила Закон України № 2265-IX “Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну” (далі — Закон № 2265-IX), який набув чинності 12 червня 2022 року⁵⁶.

Законодавці визначили декілька типів інформації, поширення якої вважатиметься пропагандою російського режиму, який описується як нацистський і тоталітарний:

- підтримка або виправдання злочинного характеру діяльності Російської Федерації та її органів, що діють проти України;
- публічне заперечення злочинного характеру збройної агресії Російської Федерації проти України;
- публічне використання символіки воєнного вторгнення російського режиму в Україну;
- поширення продукції, що містить таку символіку, в Україні та за кордоном.

Варто зазначити, що частина із цих заборон вже містилася у подібних формулюваннях у змінах до ККУ та профільного медійного законодавства, прийнятих у березні. Тож змістовно новою для Закону № 2265-IX є деталізація заборони на використання символіки вторгнення.

56. Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну: Закон України від 22 травня 2022 р. № 2265-IX.
URL: <https://zakon.rada.gov.ua/laws/show/2265-IX#Text>

Законом № 2265-IX використання символіки російського воєнного вторгнення в Україну визнається окремим видом пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України та вносяться зміни, зокрема, до Закону України “Про боротьбу з тероризмом”. Відповідно до них пропаганда російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України визнається терористичною діяльністю.

Кримінальна відповідальність за вчинення терористичного акту та іншої терористичної діяльності настає за правовими підставами, викладеними у низці статей розділу IX ККУ “Кримінальні правопорушення проти громадської безпеки”. Поруч із цим ст. 436² ККУ України встановлює спеціальну відповідальність за “Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників”. Отже, ухвалення Закону № 2265-IX, який включив використання певних символів, поширення іншого забороненого ним **та іншими, попередніми законами** контенту до терористичної діяльності може призвести до колізій і формування суперечливої практики засудження осіб.

За таких умов необхідно ретельно стежити за судовою практикою щодо притягнення осіб до відповідальності за використання символіки російського вторгнення.

7. За період із 24 лютого 2022 року по 31 серпня 2023 року набули чинності п’ять законів, якими було внесено зміни до ККУ, які стосуються поширення інформації в інтернеті:

- 1)** 7 березня 2022 року набув чинності Закон України “Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану”⁵⁷. Він вніс зміни до **ст. 111 ККУ** — “Державна зрада”;

57. Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану: Закон України від 3 березня 2022 р. № 2113-IX. URL: <https://zakon.rada.gov.ua/laws/show/2113-20#n2>

- 2) 15 березня 2022 року набув чинності Закон України “Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність”⁵⁸. Він доповнив ККУ новою **ст. 111¹** — “Колабораційна діяльність”;
- 3) 16 березня 2022 року набув чинності Закон України “Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції”⁵⁹. Він вніс зміни до **ст. 161 ККУ** — “Порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками” та доповнено ККУ двома новими статтями: **435¹** — “Образа честі і гідності військовослужбовця, погроза військовослужбовцю”; **436²** — “Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників”;
- 4) 27 березня 2022 року набув чинності Закон України “Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану”⁶⁰. Він доповнив ККУ новою **ст. 114²** — “Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану”;
- 5) 1 квітня 2022 року законодавці, з метою додаткового удосконалення складів цього кримінального правопорушення, внесли Законом України “Про внесення змін до статті **114²**

58. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України від 3 березня 2022 р. № 2108-IX. URL: <https://zakon.rada.gov.ua/laws/show/2108-20#n6>

59. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 3 березня 2022 р. № 2110-IX. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Tex>

60. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 р. № 2160-IX. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#n6>

Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації”⁶¹ зміни до **ст. 114²**.

Таким чином, з початку широкомасштабного вторгнення ККУ було доповнено чотирма новими статтями, які передбачають кримінальну відповідальність за поширення інформації в інтернеті, та до двох статей ККУ було внесено зміни.

Детальний аналіз нових статей ККУ було представлено експертами ППА в аналітичному звіті “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”⁶².

8. Закон України “Про медіа” було ухвалено 13 грудня 2022 року. Він набрав чинності 31 березня 2023 року. Основною зміною, яка стосується цифрових прав людини, є регулювання онлайн-медіа. Зазначене регулювання поєднує ліберальні підходи (реєструються добровільно) з відповідальністю за порушення контентних обмежень (незалежно від того, зареєстроване медіа чи ні). При реєстрації онлайн-медіа отримуватимуть “бонуси”: офіційний статус медіа, журналістів, підтвердження спеціальних професійних прав редакцій та журналістів, захист професійної діяльності на рівні ККУ, зменшені санкції проти незареєстрованих та анонімних онлайн-медіа. Також закон передбачає регулювання OTT-платформ, платформ спільного доступу до відео відповідно до стандартів Директиви ЄС про аудіовізуальні медіапослуги та надає можливість регулятору (Нацраді) комунікувати, укладати меморандуми і договори про співпрацю з платформами спільного доступу до інформації (соцмережами).

9. Верховна Рада України 1 грудня 2022 року ухвалила Закон “Про взаємне визнання кваліфікованих електронних довірчих послуг та імплементацію законодавства Європейського Союзу у сфері електронної ідентифікації”. Основною ідеєю закону є інтеграція України до Єдиного цифрового ринку ЄС. Національне законодавство у сферах електронної ідентифікації та електронних довірчих послуг буде максимально наближене до європейських вимог. Це стане фундаментом для підписання у майбутньому

61. Про внесення змін до статті 1142 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 1 квітня 2022 р. № 2178-IX. URL: <https://zakon.rada.gov.ua/laws/show/2178-20#n2>

62. Аналітичний звіт “Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року”. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-A4-30-12-22.pdf>

Угоди між Україною та ЄС щодо взаємного визнання електронних довірчих послуг. Подібну Угоду ЄС не укладав із жодною третьою країною⁶³.

Для українців, які перебувають у країнах ЄС, та для України загалом він відкриває нові можливості у сфері електронної ідентифікації й електронних довірчих послуг:

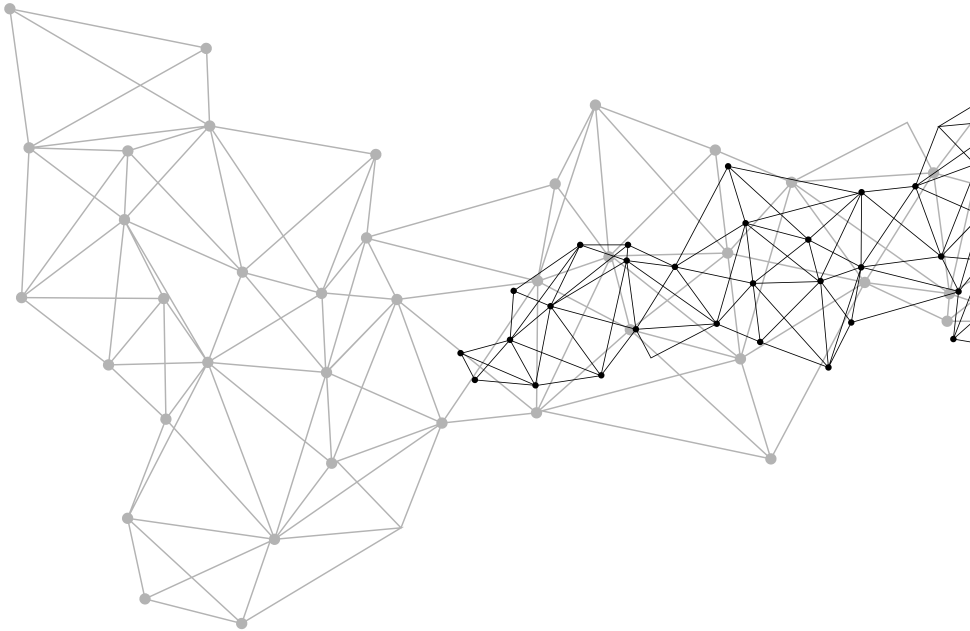
- можливість отримати кваліфікований електронний підпис (далі — КЕП) дистанційно;
- широкий асортимент засобів е-ідентифікації всіх рівнів довіри;
- можливість користуватися е-довірчими послугами навіть тоді, коли їх надавач припинить діяльність;
- доступ до українських онлайн-послуг із-за кордону;
- подати документи для отримання електронного підпису можна буде у нотаріусів та в центрах надання адміністративних послуг (ЦНАП);
- безпека даних в інформаційних системах, де використовують засоби е-ідентифікації за європейськими стандартами;
- можливість проходження процедури оцінки відповідності в іноземному органі з оцінки відповідності;
- правові основи для визнання та використання гаманців із цифровою ідентифікацією.

Це означає, що Україна визнаватиме КЕП ЄС. Зі свого боку в ЄС зможуть тимчасово визнавати український КЕП як удосконалений до укладення Угоди з ЄС, а після — як КЕП. Також в Україні будуть визнавати засоби електронної ідентифікації ЄС, оскільки вони відрізняються від вже встановлених у нашій країні.

Це важливий крок у розбудову цифрового майбутнього України та отримання цифрового “безвізу” з ЄС.

63. На крок ближче до цифрового безвізу з ЄС: Верховна Рада прийняла законопроект про е-ідентифікацію та е-довірчі послуги. URL: <https://thedigital.gov.ua/news/na-krok-blizhche-do-tsirovogo-bezvizu-z-es-verkhovna-rada-priynyala-zakonoproekt-pro-e-identifikatsiyu-ta-e-dovirchi-poslugi>

10. НЦУ 30 січня 2023 року прийняла рішення та затвердила розпорядження № 67/850 «Про впровадження системи фільтрації фішингових доменів»⁶⁴. На його підставі на українських інтернет-провайдерів було покладено обов'язок встановити систему блокування, яка кожні 15 хвилин автоматично завантажує перелік адрес, доступ до яких має бути заблокований. Перелік таких адрес створює команда реагування на кіберінциденти в банківській системі України, що входить до складу Центру кіберзахисту НБУ. Метою запровадження такої системи блокування є протидія фішингу та захист користувачів інтернету від шахрайства, яке відбувається у банківській сфері, бо одним із найпоширеніших видів шахрайства є створення фішингових ресурсів, які створюються для викрадення персональних даних та доступу до банківських рахунків.



64. Розпорядження НЦУ від 30.01.2023 № 67/850 про впровадження системи фільтрації фішингових доменів.
URL: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2580&language=uk>

**ДОСТУП
ДО ІНТЕРНЕТУ**



У сучасному світі доступ до інтернету є дуже важливою умовою для реалізації багатьох прав людини. Сьогодні нам важко уявити право на свободу вираження поглядів, право на освіту, на охорону здоров'я, на зібрання, на особисте життя та інші права без використання інтернету. Інтернет створює можливість простого, вільного та швидкого інформаційного обміну. Він є цінністю для людини, держави та людства загалом. Поряд із міжнародними документами, які визнають право на доступ до інтернету як одну з передумов реалізації прав людини, Закон України «Про електронні комунікації» гарантує доступ до інтернету, зокрема до універсальних електронних комунікаційних послуг широкосмутового доступу до мережі Інтернет у фіксованому місці на всій території України.

Після широкомасштабного вторгнення право на доступ до інтернету зазнало особливого втручання. Спостерігалися численні спроби порушити нормальну роботу електронних комунікаційних мереж України, здійснити відключення інтернету на її території, заблокувати доступ до вебресурсів органів державної влади та військового управління України, банків, ЗМІ, впливових громадських організацій тощо.

За оцінкою Світового банку, збитки телекомунікаційного ринку в Україні за рік повномасштабної війни сягнули 2,3 млрд дол. Незважаючи на таку фантастичну суму втрат для одного лише сектора економіки, зв'язок не зник, і це є наслідком його децентралізації та наявності, крім великих операторів, кількох тисяч провайдерів, які діють локально й терміново лагодять свої мережі. Тому мільйони абонентів залишаються на зв'язку й оперативно отримують доступ до мережі Інтернет. А ще після масових знеструмлень обладнання оператори встановили генератори та батареї безперебійного живлення, щоб і ця проблема не заважала залишатися на зв'язку⁶⁵.

Значну роль відіграло своєчасне підключення України до системи супутникового зв'язку *Starlink* від американської компанії *SpaceX*. Швидко постачалися тисячі терміналів *Starlink*, які використовувалися не лише для потреб армії, а й для відновлення зв'язку в постраждалих районах. Перша партія станцій супутникового інтернету *Starlink* прибула до України вже 1 березня 2022 року, тобто через чотири дні повномасштабної війни. Україна стала місцем тестування найновітніших технологій.

Підсумовуючи зазначене, можна зробити висновок, що попри варварські дії окупантів, які свідомо руйнували телекомунікаційні мережі, українські оператори зв'язку та інтернет-провайдери швидко відновлювали мобільний зв'язок та інтернет на деокупованих територіях і після руйнувань, заподіяних агресивним російським режимом.

65. Досвід війни: оператори навчилися швидко відновлювати й створювати надійний зв'язок. URL: <https://zn.ua/ukr/TECHNOLOGIES/dosvid-vijni-operatori-navchilisja-shvidko-vidnovljuvati-j-stvorjuvati-nadijnij-zvjazok.html>

РЕКОМЕНДАЦІЇ



Для покращення ситуації у сферах, які були досліджені під час цього моніторингу, можна надати такі рекомендації:

1. Кібератаки (хакерські атаки):

- підвищувати рівень обізнаності суспільства щодо кіберзагроз і кіберзахисту, розвивати культуру безпечного поведіння у кіберпросторі, адже кібератаки спрямовані не тільки на урядові та державні установи, а й на звичайних українців. Високий рівень цифрової грамотності населення є елементом ефективної протидії кібератакам;
- забезпечити на всіх рівнях взаємодію між державним і приватним сектором для обміну інформацією про кіберзагрози. Швидкість та обсяг взаємодії мають вирішальне значення для кіберстійкості країни;
- внести зміни до ККУ, які дадуть змогу більш ефективно реагувати на вчинення правопорушень у кіберпросторі.

2. Фішингатаки:

- внести зміни до ККУ, які нададуть можливість правоохоронним органам притягати до відповідальності за фішингові атаки;
- удосконалити систему фільтрації фішингових доменів;
- підвищувати рівень обізнаності суспільства про фішингові атаки.

3. Поширення дезінформації:

- дезінформація як явище потребує юридичного визначення в українському законодавстві. Для ефективної протидії цьому явищу потрібне законодавство, яке визначатиме чіткі механізми боротьби, відповідальність за поширення дезінформації та порядок притягнення до неї;
- медіаграмотність має бути запроваджена на всіх рівнях освіти, просвіти тощо, адже вона є важливою складовою протидії дезінформації. На це вказує і міжнародна спільнота і громадський сектор в Україні. Споживач інформації повинен мати знання і вміння із перевірки інформації, виявлення сумнівної або очевидно фейкової інформації. Він має ретельно ставитися до надання доступу до персональних даних тощо.

■ **4. Шахрайство в мережі.** Для того щоб не втрапити у пастки шахраїв, варто під час здійснення операцій в інтернеті дотримуватись таких правил:

- не вказувати власні персональні дані на неперевірених сайтах;
- нікому не повідомляти термін дії банківської карти та CVV-код;
- перевіряти гіперпосилання та наповнення сайту на відповідність офіційним даним компаній;
- у разі отримання спірних листів чи повідомлень не здійснювати ніяких оплат до встановлення обставин ситуації, що виникла;
- не робити передоплат у неперевірених інтернет-магазинах;
- не користуватися неперевіреними оголошеннями щодо роботи, яка обіцяє швидкий зарібок за внесення завдатку.

■ **5. Блокування вебресурсів:**

- внести зміни до чинного законодавства, які будуть чітко визначати механізми здійснення блокувань вебресурсів з урахуванням принципу пропорційності та міжнародних стандартів у сфері захисту свободи вираження поглядів.

■ **6. Свобода вираження поглядів:**

- вирішення проблеми різної кваліфікації однотипних діянь можливе через внесення змін до відповідних статей ККУ;
- змінити ситуацію щодо призначення реального покарання за поширення забороненої інформації можливо за допомогою внесення змін до досліджуваних статей ККУ альтернативних видів покарання у вигляді суттєвих штрафів, громадських або виправних робіт, про що також зазначалося в аналітичному звіті;
- судам варто не обмежуватись лише посиланням на факти, встановлені зазначеними експертними висновками, а й самостійно аналізувати зміст поширених обвинуваченими повідомлень та оцінювати його на предмет наявності чи відсутності складу відповідного кримінального правопорушення;
- звернути увагу судів на те, що у зазначеній категорії справ необхідно оприлюднювати зміст інформації, яка була поширена таким чином, щоб існувала можливість оцінити її зміст і пропорційність застосування до особи покарання.

7. Доступ до інформації:

- необхідно проводити роз'яснювальну роботу із розпорядниками публічної інформації щодо застосування норм Закону України "Про доступ до публічної інформації" в умовах воєнного стану.

8. Зміни в законодавстві:

- Міністерству оборони України та/або Генеральному штабу ЗСУ було б доцільно оприлюднити на своєму офіційному вебсайті словник термінів, які застосовано в наказі Головнокомандувача ЗСУ від 3 березня 2022 року № 73 "Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану", надавши відповідні роз'яснення вживаним у ньому поняттям, зокрема, таким як "унікальна операція", "сили і засоби радіоелектронної боротьби противника", "інформаційні операції", "психологічні операції" тощо.

