

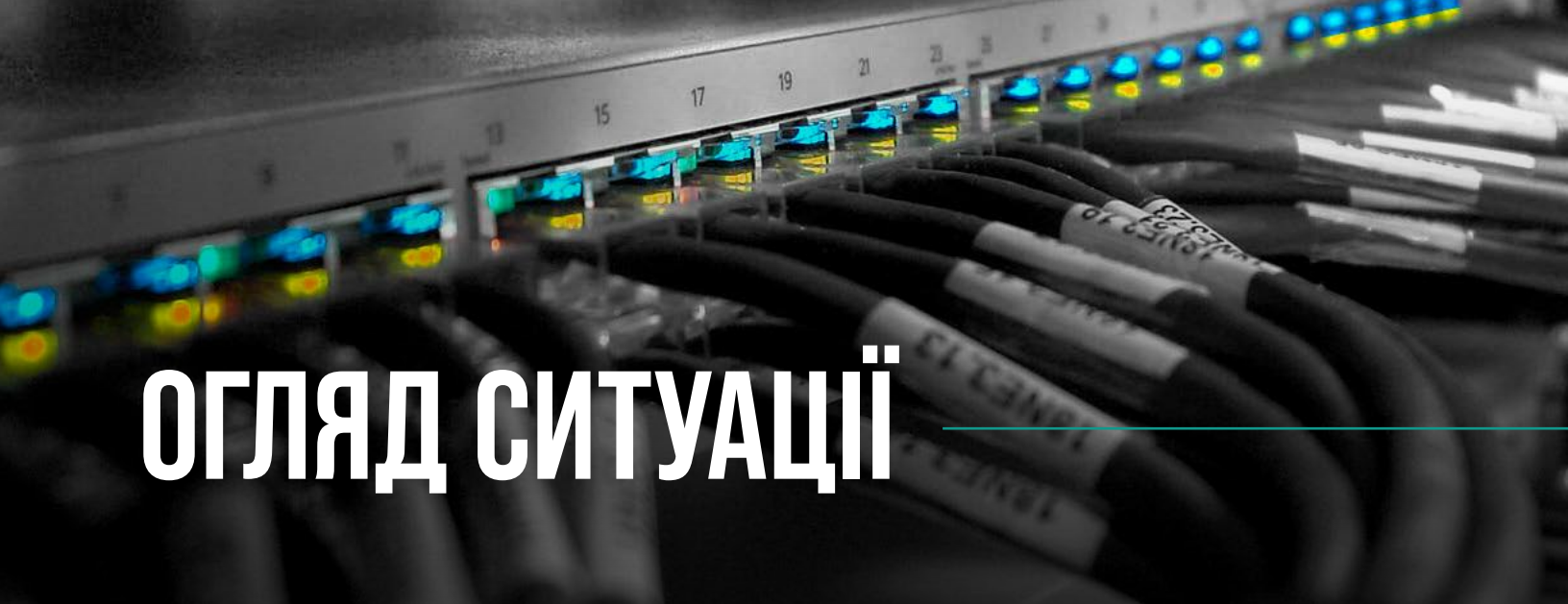
НАВЧАННЯ З ЦИФРОВОЇ БЕЗПЕКИ ДЛЯ УКРАЇНСЬКИХ ЖУРНАЛІСТІВ ТА ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

ЗАХОДИ БЕЗПЕКИ ДЛЯ ПОТОЧНОГО КОНФЛІКТУ З РОСІЄЮ

НАТАЛІЯ АНТОНОВА

У ПАРТНЕРСТВІ ІЗ ІНСТИТУТОМ БЕЗПЕКИ ТА ТЕХНОЛОГІЙ

6 КВІТНЯ 2022 РОКУ



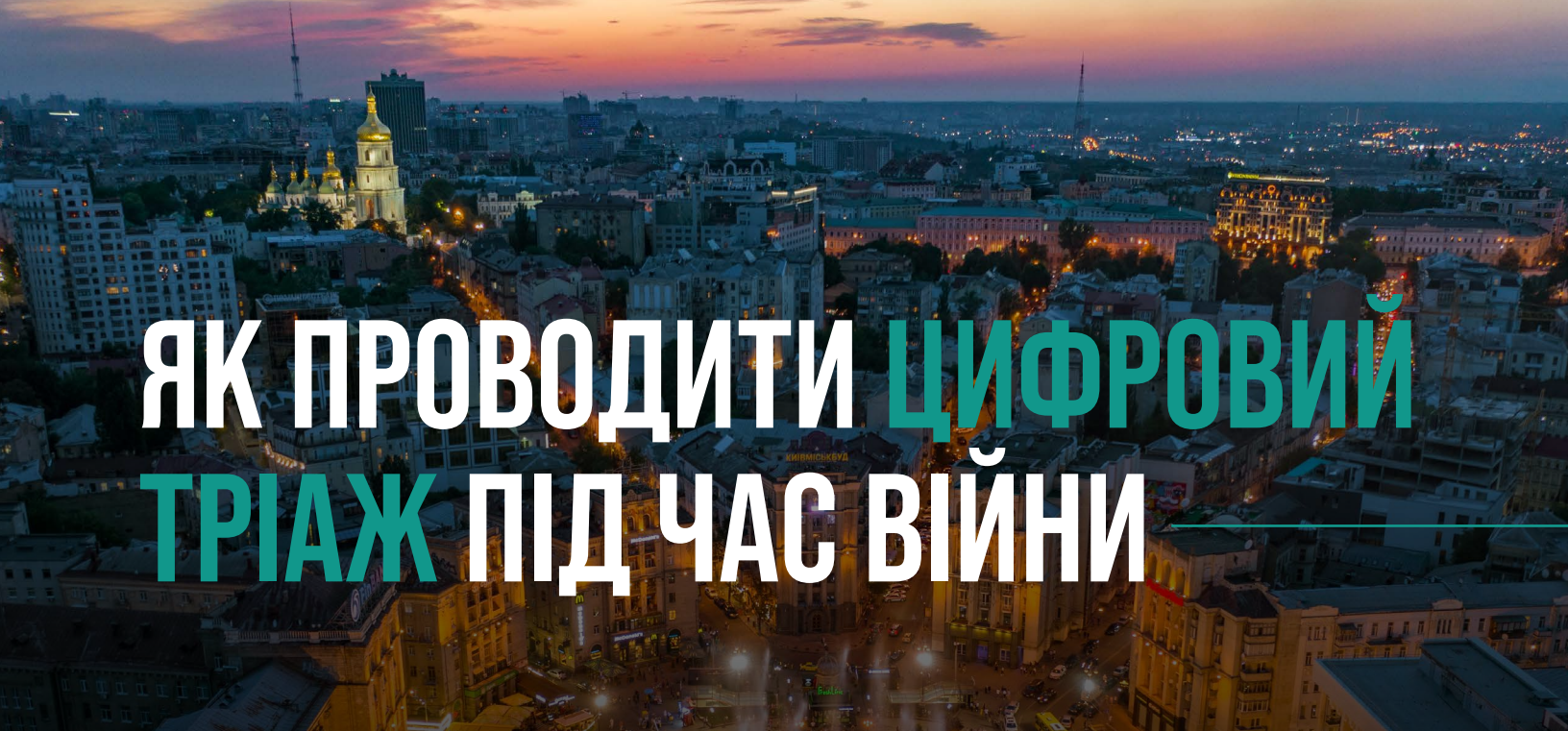
ОГЛЯД СИТУАЦІЇ

Вторгнення Росії до України спричиняє руйнування, смерть та втрату стабільності, справляючи глибоко руйнівну дію на українське суспільство. Кремль та його агенти активно використовують залякування, дезінформацію та пропаганду, цензуру, кібератаки, а також різноманітні інші засоби обмежити рух інформації в Україні, в Росії і на міжнародній арені та вплинути на нього.

В умовах постійного застосування подібних тактик всі українські громадяни, журналісти, правозахисники, а також урядові чиновники, що мають доступ до потенційно чутливої інформації—включаючи осіб, що контактують із групами ризику—мають проявляти підвищену пильність та обережність.

За інформацією Сполучених Штатів та урядів західних країн, Росія тримає списки ключових осіб, яких планує затримати і, потенційно, вбити на території України. Це означає, що захист ключової інформації є надзвичайно важливим питанням для опору російській загрозі.

Цей посібник має на меті дати практичні поради для захисту вашої цифрової діяльності та покращення вашої цифрової гігієни. Для цілей цього посібника ми визначаємо поняття цифрова гігієна як комплекс регулярних практик з дотримання безпеки особистих цифрових активів і цифрового сліду.



ЯК ПРОВОДИТИ ЦИФРОВИЙ ТРІАЖ ПІД ЧАС ВІЙНИ

– **Цифровий тріаж:** пріоритетна увага до всіх завдань, які пов’язані з особистою кібер-гігієною.

Додаткову інформацію можна знайти на таких ресурсах: [The Totem Project](#) (Проект Тотем), [Committee to Protect Journalists](#) (Комітет захисту журналістів), the [PEN America Online Harassment Field Manual](#) (практичний посібник з онлайн-переслідувань від PEN America), and the [Global Cyber Alliance Cybersecurity Tool Kit for Journalists](#) (набір інструментів кібер-безпеки для журналістів від Глобального Кіберальянсу).

1. ПІКЛУЙТЕСЯ ПРО СЕБЕ

- Зменшіть свій рівень паніки. Точно так само, як при зустрічі з фізичною небезпекою—паніка, коли ви стикаєтеся з кібернетичною або цифровою загрозою, може бути небезпечною.
- Коли це потрібно, практикуйте “квадратне дихання”:
 - Вдихніть носом, повільно рахуючи до чотирьох.
 - Затримайте дихання, повільно рахуючи до чотирьох.
 - Видихніть ротом, повільно рахуючи до чотирьох.
 - В кінці видиху знову затримайте дихання, повільно рахуючи до чотирьох. За потребою повторіть цикл.



2. ДОТРИМУЙТЕСЯ БАЛАНСУ МІЖ ПИЛЬНІСТЮ ТА СПО- КОЄМ, КОЛИ ЦЕ МОЖЛИВО

- Ви можете відчувати, що це ваш обов'язок—публікувати загальнодоступний контент під час війни. Це нормально і зрозуміло! Просто намагайтеся тримати в голові можливі наслідки таких публікацій, щоб потім не мати справу з неприємними сюрпризами.
- Ми всі люди і через це всі ми вразливі у багатьох різних сферах. Пам'ятайте, ваша ціль не в тому, щоб бути супергероєм—мета в тому, щоб підтримувати та захищати ваші дані та дані вразливих людей, з якими ви підтримуєте зв'язок.
- Не забувайте, що серед ворогів теж немає супергероїв. Не давайте ворогу повного контролю над вашим життям, скільки б він не намагався вас залякати.
- Психологічна війна—звичайна тактика ведення бойових дій. Мета ворога полягає в тому, щоб тримати вас в постійному стані стресу, переляку. За можливості чиніть цій тактиці спротив.



3. ОЦІНІТЬ СТАН ВАШИХ ДАНИХ

- Тверезо та методично оцініть свій **цифровий слід та свою цифрову площу атаки**.
 - Ваш слід включає всі додатки, в яких є ідентифікація унікального користувача. Це включає: загальнодоступну та приватну інформацію в мережі—включаючи завантажені документи, списки контактів, бази даних (які часто повні дірок), акаунти (особисті облікові записи) в соціальних мережах, профілі в інтернет-магазинах та на сайтах хоббі, і так далі.
 - Площа атаки включає будь-які потенційні точки входу для зловмисників—включаючи програмне забезпечення, обладнання, зберігання даних, контент, де згадане ваше ім'я, контент, де ви відмічені, і так далі.
- Визначте найслабші ланки у своєму цифровому сліді. Чи ви звикли використовувати один і той самий пароль? Чи ви знаєте про скомпрометовані бази даних, в яких можуть бути ваші дані? Чи купляли ви товари через скомпрометовані сайти? Наскільки загальнодоступними є ваші публікації в соціальних мережах та фотографії?
- Не використовуйте публічні точки доступу wi-fi для пересилання, відправлення чи отримання чутливої інформації.



4. ЗАСТОСУЙТЕ БАЗОВІ КРОКИ ДЛЯ ЗАХИСТУ СВОЇХ ДАНИХ

- Створіть сильні паролі, які ніхто не зможе зламати. Використовуйте літери, цифри, великі літери, особливі значки, а також фрази, які нелегко розпізнати.
 - Використовуйте менеджер паролів. Простий інструмент для паролів або для браузера може допомогти вам побачити скомпрометовані або повторювані паролі, що пов'язані з вашими адресами електронної пошти. Можливий варіант—LastPass.
 - Подальшу інформацію ви можете знайти тут: [Passwords for Journalism](#) (паролі для діяльності журналістів).
- Увімкніть 2-факторну аутентифікацію для всіх облікових записів, які передбачають таку можливість, включаючи: соціальні медіа та облікові записи електронної пошти—всюди, де це можливо. Те саме зробіть для банківських рахунків, рахунків комунальних послуг, сайтів, де ви щось купуєте, ігрових платформ, і так далі.
- Підключіть Програму [Посиленого Захисту Gmail](#).
 - Це потребує фізичного ключа безпеки, такого як *Google Titan* або *Yubikey*, але дає кращий захист, ніж 2-факторна аутентифікація.
- Пересвідчіться, що все ваше програмне забезпечення доповнене найсвіжішими доступними патчами, і використовуйте антивірусне програмне забезпечення.
- Якщо ви використовуєте роутер, переконайтеся, що він безпечний. Старі роутери мають особливо багато сильних вразливостей. Дешеві та куплені з рук роутери можуть мати “чорні ходи”, встановлені російською розвідкою—і ми протягом років бачили багато прикладів, коли це ставалося з українськими закладами. Розгляньте можливість від'єднання роутера від живлення на хвилину, щоб перевантажити його.
- Витріть будь-які рахунки, пов'язані з сайтами з російським хостінгом, наприклад *Одноклассники* та *ВКонтакте*, і ніколи не використовуйте паролі, які ви вживали на будь-якому з цих сайтів—а також перевірте, чи ваші списки френдів закриті для перегляду сторонніми особами, оскільки вони можуть потенційно використовуватися як точка входу для відслідковування людей з групи ризику.

- Там, де це можливо, зробіть свої списки френдів приватними.
 - Перегляньте свої списки френдів і видаліть з них всіх, кого ви не знаєте, а також всіх, чия поведінка викликає підозру.
- Зважте можливість того, щоб припинити використання авторизації за обличчям на ваших пристроях. Його легко обдурити.
- Використовуйте VPN, особливо якщо ви відвідуєте будь-які російські сайти.
 - Використовуйте захисний DNS для того, щоб не давати вашим комп'ютерам та приладам під'єднуватися до відомих фішингових сайтів та сайтів з шкідливим програмним забезпеченням.
- Не переходьте за підозрілими посиланнями та двічі перевіряйте будь-яке повідомлення та листи електронної пошти, якщо ви не впевнені в їх походженні.
- Не забувайте, що номери телефонів легко підробити. Не переходьте за дивними, неочікуваними посиланням, навіть якщо вони від когось, кому ви довіряєте.
 - Замість цього спитайте в цієї особи, "Це ти написав(ла) це повідомлення?"
 - Остерігайтеся "угону SIM-картки."
- Перегляньте та оновіть налаштування конфіденційності в соціальних мережах.
 - Подумайте про те, щоб зробити більшість ваших облікових записів у соцмережах приватними.
 - Ідеальним буде створення другого, публічного облікового запису для того, щоб ділитися новинами та відео не піддаючи ризику вашу інформацію.
- Передавайте важливу / чутливу інформацію каналами з шифруванням, влаштованими за принципом "рівний-рівному."
 - Не використовуйте прямі повідомлення (DM) з соцмереж Twitter чи Facebook, чи щось подібне!
 - Не використовуйте рації для передачі конфіденційної інформації
- Додайте опцію цифрового PIN-паролю до всіх ваших додатків для обміну повідомленнями з шифруванням. Додаток періодично запитуватиме ваш PIN.
 - WhatsApp, Signal та Telegram—вони всі підтримують функцію додання PIN-паролю.
- Періодично вимикайте свій телефон і потім знову його вмикайте, протримавши вимкненим мінімум хвилину.
- Не забувайте архівувати свої дані та увімкніть функцію автоматичного архівування на зовнішній диск, який не під'єднаний до вашого приладу.



5. ОБИРАЙТЕ РОЗВАЖЛИВО ІНФОРМАЦІЮ, ЯКУ ПУБЛІКУЄТЕ

- Добре думайте про те, чим ділитесь. Під час війни важливо отримувати інформацію про звірства та інші події, які варто вмістити в новини. Тим не менше, зважте на те, що одночасно з цим ви можете розповсюджувати і компрометуючу інформацію.
- Завжди питайте дозволу про те, чи можна тегнути когось /ідентифікувати когось в загальнодоступній публікації. У час миру це просто ввічливо. А у час війни—це може врятувати життя.
- Не забувайте, що геолокація навіть випадкового фото або відео може бути швидко визначена.
 - Щоб не дати визначити геолокацію, не треба ділитися фотографіями, зробленими перед вашим будинкомчи, з його вікон, або інших місць, де ви часто буваєте.
 - Якщо ви все ж хочете публікувати подібний контент, подумайте про те, щоб робити це тільки через приватний рахунок, або ж на альтернативному загальнодоступному рахунку.
- Коли ви робите доступним контент, пов'язаний з військовими, не видавайте руху українських військ.
 - Редагуйте фотографії таким чином, щоб приховати ключові деталі—обличчя та/або номери, коли це можливо, та військові нашивки, коли ця інформація є чутливою.
 - Особливо стережіться, щоб не видати сили спеціальних операцій, оскільки вони є мішенями номер один.
 - Можна просто опублікувати повідомлення пізніше—таким чином також можна запобігти тому, аби видати місцезнаходження таких сил.



6. ВЖИВАЙТЕ ПРАКТИЧНИХ ПЕРЕСТОРОГ

- Уважно стежте за оточенням. Якщо ви гадаєте, що за вами можуть стежити вдома, залиште маленьку ниточку на порозі або маленьку пушинку в себе на переносному комп'ютері. Ці непомітні трюки можуть допомогти встановити факт стеження, і вони не видадуть вас так, як, наприклад, встановлення камери спостереження.
- Якщо ви мандруєте ворожою територією, подумайте про те, щоб взяти з собою якомога більше приладів. Ось факт: ніякий звичайний солдат на блок-посту не захоче перевіряти всі ваші приналежності. Поміняйте імена важливих контактних осіб у вашій системі. Ви маєте зв'язок з мером вашого міста? Краще запишіть його як “сантехнік Петро”, а не “мер Петро”. Ця проста хитрість може врятувати життя.
- Зважайте на те, кому ви даєте номер свого телефону. Вже існує технологія, яка може поставити у небезпеку ваші дані, якщо хтось має ваш номер—навіть якщо ви нічого не робитимете.
- Зважайте на те, що відбувається навколо. Це давно стало банальною істиною, але у стін є вуха—особливо під час війни.
- Завжди самі спакуйте свої сумки. Не забувайте: прилади для стеження, навіть такі безневинні на вигляд, як *AirTags*, можна модифікувати, а отже, їх можуть використати особи з нечистими намірами.



7. СТЕЖТЕ ЗА ЗАГРОЗАМИ, ЩО ВИНИКАЮТЬ

- Уважно стежте за пересуваннями ворожих військ у місці вашого розташування.
- Не обманюйтеся—навіть місця, які утримують українці, місця в ЄС та взагалі у світі можуть бути під наглядом російської розвідки. Не треба почуватися у цілковитій безпеці навіть тоді, коли ви впевнені, що навколо лише свої
 - Обережно ставтеся до нових друзів та знайомих під час війни і намагайтеся помічати все незвичайне, що відбувається у місці вашого розташування.
- Старайтеся уважно стежити за тактикою дезінформації росіян.
 - Чи ви впевнені, що новини походять з загальновідомих веб-сайтів та джерел, які можна перевірити? Складіть для себе список вебсайтів, контактних осіб та рахунків, яким ви довіряєте, і остерігайтеся фальшивих рахунків, тролів та ботів.
 - Обережно ставтеся до “кричущих” заголовків з сенсаціями і думайте, перш ніж клацнути на посилання. Іншими словами, критично мисліть про походження інформації, яку ви споживаєте, і діліться зі своєю мережею.



ІНСТИТУТ БЕЗПЕКИ ТА ТЕХНОЛОГІЙ
www.securityandtechnology.org

counterdisinfo@securityandtechnology.org

Copyright 2022, The Institute for Security and Technology