Марко Мельник

ТИ ПІД КОНТРОЛЕМ

Кібербезпека та цифрова гігієна під час війни

Київ

markobook

2025

УДК 004.056.5
М48

За загальною редакцією
Євгена Букета

Рецензент – IT-архітектор, розробник наноспутників України,
кандидат технічних наук, доцент
Євген Коваленко

М48 Мельник, Марко

Ти під контролем. Кібербезпека та цифрова гігієна під час війни / Марко Мельник; за заг. ред. Євгена Букета. — Київ : Видавництво Марка Мельника (ФОП Мельник М. Ю.), 2025. – 400 с.

Як нас «ведуть» через месенджери, хто і як розпоряджається нашими особистими даними, як за кожним з нас слідкують через камери і супутники та багато іншого. Книга пояснює, як не стати мішенню у світі тотального панування технологій і як від цифрової гігієни в прямому сенсі залежать життя військових та цивільних.

ISBN 978-617-7838-57-8

ЗМІСТ

ПЕРЕДМОВА

Ця книга народилася на стику розпалу війни і тотальної експансії технологій. Повномасштабне вторгнення змусило українців дивитися на інформацію інакше, ніж звикли: як на ресурс, що може врятувати життя, і як на поле бою, на якому ми щодня перебуваємо, навіть не усвідомлюючи цього.

Я поставив перед собою завдання створити посібник не для вузьких спеціалістів, а для всіх, хто живе у світі смартфонів, новинних стрічок і штучного інтелекту. Цивільних людей ця книга навчить, як захистити себе у цифровому просторі: які ризики приховують соціальні мережі, месенджери та мобільні оператори, чому варто уважно ставитися до паролів, камер і антивірусів, як правильно користуватися VPN і криптоактивами. Військовим вона дає інструменти для виживання у сучасному бою: що таке інформаційна гігієна на війні, як уникнути викриття через смартфон, як працюють засоби радіоелектронної боротьби і як діяти у світі, де кожен сигнал може бути перехоплений.

Це видання містить розділи про природу радіохвиль, історію інтернету від dial-up до супутникових систем, міфи навколо 5G, приклади катастроф через відключення мереж. Ми поговоримо про бази даних і їхній продаж, про глобальні інформаційні корпорації та навіть про таємничих гравців у сфері масового збору інформації про нас із вами. Окремо розглянемо вплив соціально-культурного середовища: коли російський контент діє як зброя, чому мова та інформація — це питання безпеки.

Я прагнув зробити цю книгу цілісною мапою інформаційного простору. Тут є все: від спаму й вебархівів до штучного інтелекту, OSINT і блокчейну. Але головне — тут є практичні висновки: що робити кожному, аби залишатися захищеним.

Моя мета — озброїти читача знаннями. В епоху, коли фронт проходить і в окопі, і у смартфоні, безпека починається з розуміння. Ця книга допоможе цивільним відчути

впевненість у цифровому вимірі свого життя, а військовим — зберегти життя і виконати завдання в умовах постійної боротьби за контроль над життєво-важливою інформацією.

На початку 2000-х, ще підлітком, я дуже мріяв про власний комп'ютер. Тоді їх мали одиниці, і в основному використовували їх у сфері бізнесу: комп'ютер у домашньому вжитку був рідкістю і фактично предметом розкоші. Я підробляв у свого батька в магазині, де продавалася електроніка для автомобілів, і якось ми поїхали купувати персональний комп'ютер на склад збанкрутілої фірми, яка за дешево розпродавала майно. Це був запилюжений комп'ютер із встановленою Windows 98.

І ось він в офісі. Настав час знайомитись з ним. Я почав захоплено клацати кожне вікно і кожне повідомлення, яке випадало на моніторі. Разом із системним адміністратором мого батька Вовою ми розбиралися в усіх нюансах встановлення нової операційної системи Windows 2000. Це був цікавий та захоплюючий процес. А вже за кілька днів встановив перші комп'ютерні ігри і весь вільний від роботи час проводив за робочим комп'ютером. Мені було цікаво все — від ігор до програми Microsoft Office і системних налаштувань операційної системи. Батько помітив мою зацікавленість і виписав журнал «Хакер». Це був гарний кольоровий глянцевий російськомовний журнал, де в деталях і нюансах розповідалися різні вразливості та небезпеки, пов'язані з керуванням і володінням комп'ютером. Вже невдовзі я почав писати перші BAT-скрипти для налаштування різних системних параметрів операційної системи.

За деякий час ми зібралися всім колективом, щоб розібратися із встановленням модему і вийти в мережу інтернет. Після численних невдач і поразок ми все ж це зробили, і я побачив приголомшливу картину віртуального світу, безмежного, як океан. Тоді ще не був поширений Google, і ми користувалися браузером Netscape. Я не знав, що шукати в інтернеті, тому шукав усе, що приходило в голову, завантажував картинки (що для тогочасного інтернету вже було надскладним завданням), читав різні статті та новини. Освоївши деякі

команди командного рядка Windows, почав створювати програми для оптимізації функцій операційної системи і, за аналогією до поширеного тоді російського антивірусу «Доктор Веб», підписував свої програмні творіння dr.zip. Не можу пояснити логіку такого неймінгу, але створені мною програми вантажив на різні каталоги програм і спостерігав, як перші користувачі завантажували їх. І почувався справжнім програмістом!

Згодом набули популярності мобільні телефони, а з часом вони почали підтримувати так звану поліфонію. На них можна було завантажувати примітивні мелодії. Якраз тоді батько почав продавати у своєму магазині мобільну техніку. Коли з'явилися перші телефони з кольоровим екраном, вони здавалися дивом техніки, майже фантастикою. Насправді ж їхні дисплеї були примітивними, маленькими, низької роздільної здатності та тьмяні. Та попри це, моделі від Motorola, Sagem і Mitsubishi на той час вважалися вершиною інженерного цифрового мистецтва. Тому я придбав на свої кишенькові заощадження data-кабелі, завантажив програмне забезпечення і створив на базі батькового бізнесу власний бізнес із платного завантаження на телефони клієнтів картинок, мелодій та Java-ігор. У нас саме з'явився струменевий кольоровий принтер, і я роздрукував товстелезні каталоги картинок, списки мелодій та Java-ігор, які були доступними для завантаження на деякі моделі мобільних телефонів. З появою MP3 у широкому вжитку мій бізнес набув розмаху. Я міг заробити 100 грн лише за один день, що на початок 2000-х були шалені кошти, особливо для підлітка. Всі ці гроші я витрачав зазвичай на подарунки своїм колегам та родичам і почувався успішним бізнесменом та Святим Миколаєм одночасно.

Але одного Нового року, коли я вчергове приготував усім подарунки, мене спіткало розчарування: я довго мріяв про власний комп'ютер удома і всім завжди про це казав, а натомість отримав під ялинку саму лише мишку. Я тоді навіть плакав. Моє розчарування батько зрозумів і вже невдовзі придбав мені власний комп'ютер, який був у кілька разів потужнішим за наш робочий в офісі і мав цілих 256 МБ

оперативної пам'яті, плоский монітор та процесор 1,5 ГГц. Це зараз здається смішним, але тоді це була монстр-машина. На додачу до комп'ютера я отримав модем і одразу був готовий досліджувати інтернет значно масштабніше. Спочатку я завантажував компактні флеш-мультфільми «Масяня», а вже невдовзі розширив спектр свого контент-архіву до MP3. На той час завантажити одну композицію було цілою пригодою: зв'язок з інтернетом через модем увесь час обривався, і часом доводилось витратити всю ніч, завантажуючи одну композицію. Але це було того варте — на зміну касетам прийшов цифровий формат з беззаперечною якістю і, головне, майже безкоштовно (вираховуючи вартість prepaid-карток для доступу в інтернет).

Але мене цікавив не тільки контент. Вичитавши в журналі «Хакер» про експлойти, я почав досліджувати цю тему на громіздких форумах і вже невдовзі був готовий до хакерської діяльності. Інтернет тоді не був цілодобовим, і основну кількість часу я проводив у локальній мережі, яка об'єднувала наш район, була швидкою і цілодобово доступною. Там були мої сусіди, однокласники та інші люди з району. Ми сиділи в чатах, переписувалися, обмінювалися файлами, які завантажували вночі через dial-up connection за нічним тарифом. Я налаштував експлойт і через командний рядок, як справжній хакер, проник у файлову систему хлопця з паралельного класу. Моєму захопленню не було меж: я несанкціоновано дістав доступ до файлової системи іншого комп'ютера, який був у кварталі від мене. Я не очікував там знайти нічого цінного, тому завантажив його колекцію музичних композицій у MP3 та якісь зображення і, звісно ж, розповів про це у чаті. Щасливий, я ліг спати, а вже на ранок мене чекала несподіванка.

Ми жили вдвох із мамою. Коли зранку у двері хтось загрюкав, мама, подивившись у вічко, чомусь відкрила двері двом незнайомим людям: один — солідний, низького зросту, і ще один — амбал, схожий на тілоохоронця. Це справді був тілоохоронець бізнесмена, яким був батько хлопчика, чий комп'ютер я вчора зламав. Чоловіки мовчки зайшли в квартиру і попросили маму зайти в кімнату та сісти на диван,

а мене — стати поруч. Вони пояснили, що я зробив, і сказали, що я завантажив їхню фінансову документацію. За це мене чекало покарання — зламані пальці, оскільки документація була цінною, вони мали впевнитися, що я більше ніколи не зможу нікого зламувати. Мама була шокована, а я поруч тремтів від напруження. Після довгої паузи бізнесмен сказав, що знає мого батька та веде з ним справи, тому цього разу мені пощастило, але я маю припинити робити подібне.

Звісно, я пообіцяв припинити, мама заприсяглася, що проконтролює мене, але вже за кілька днів я почав писати свій найбільший хакерський проєкт — зловмисну програму, яка паралізує роботу системи через флеш-накопичувач та дає мені віддалений доступ до файлової системи. Задум був простий — викрасти ігрову карту Counter-Strike в інтернет-клубі, куди ходили практично всі мої однокласники після школи, щоб пограти в комп'ютерні ігри. Коли я завершив своє зловмисне творіння, я зібрав декількох приятелів, які вже мали комп'ютери вдома і теж хотіли роздобути цю карту. Один із них імітував гру на комп'ютері, а я серед інших стояв навколо, імітуючи захоплення від цієї гри. Ще один наш друг стояв біля жінки-адміністратора комп'ютерного клубу та відволікав її увагу. Я вставив флешку — і програма запустилася. Операція була проведена блискуче, і вже наступного дня я зі своїми товаришами вдома грав у Counter-Strike на дуже рідкісній карті, яка була раніше тільки в одному комп'ютерному клубі.

У мене було ще кілька хакерських проєктів, але про них я розповідати не буду, бо мені соромно: це були програми-вимагачі та фальшиві інтерфейси соціальних мереж, які крали паролі. Нічого корисного з цієї інформації я не отримував та вже усвідомлював ризики, тому переключився на інший вид діяльності. Мене дуже захоплювали такі програми, як Adobe Photoshop, які тоді тільки з'являлися. Я цілком поринув у світ комп'ютерної графіки, модифікував скіни для ігор, розробляв карти, одного разу навіть на основі популярної тоді гри створив свою: її суть полягала в тому, що з-за кущів виринали качки, яких треба було відстрілювати. Замість качок я поставив зображення ненависних учителів зі школи, і після

поширення цієї гри у локальній мережі закономірно до мене виникли питання, тож я знову повернувся в русло мирного графічного дизайну.

У 13 років я зробив обкладинку для першої книжки — це була збірка поезій батькового друга. Вона була низької естетичної привабливості, але відтоді я почав довгу історію роботи з книжками. За кілька років навіть працював віддалено в одній студії маркетингу і малював для них листівки. До естетики листівок у роботодавців були критичні зауваження, мене критика ображала, тому довелося звільнитися, та й професійний рівень необхідно було підвищити перед тим, як братися за таку серйозну роботу. Практикувався на дизайні та верстці шкільної газети, написанні статей, тому невдовзі мені довірили стати її головним редактором. У студентські роки займався тим самим у студентській газеті. Таким чином я плавно перейшов у цифровій сфері до мирної діяльності, паралельно вивчаючи різні аспекти: віруси, антивіруси, експлойти та інше програмне забезпечення.

За програмою Work and Travel 2008 року вперше потрапив до Сполучених Штатів, будучи першокурсником інституту. Саме тоді натрапив на публікацію про нову перспективну технологію — блокчейн. Зацікавившись, швидко розібрався з біткоїном і зареєстрував гаманець. Інтерфейси тоді були ще складні та незручні, але існував сайт, де кількома кліками можна було отримувати Bitcoin, і програма, яка використовувала потужності мого нетбука для його добування. Незабаром на рахунку мого криптогаманця почали з'являтися якісь цифри— соті чи десяті долі біткоїна (вже згадати важко). Тепер це були б десятки тисяч доларів, якби я тоді зберіг ключі доступу. Але нині це вже не має значення.

Технології останніми роками зробили такий ривок, що більшість нашого життєвого простору тепер залежить від них. Рівень цифрової освіченості у Сполучених Штатах мене відверто засмучував: у 2009 році, коли я вдруге потрапив до США, там досі користувалися dial-up модемами, у той час як в Україні вже набирав поширення публічний Wi-Fi.

Зараз я пишу цю книгу, надиктовуючи текст штучному інтелекту на телефоні з гнучким розкладним екраном, який у десятки разів потужніший за мій перший комп'ютер. Завантаження гігабайтних файлів тепер займає хвилини, а роздільну здатність і якість камер мобільних пристроїв не порівняти з професійною апаратурою часів, коли я починав опановувати цифровий світ. Ми маємо у вільному доступі інструменти на основі штучного інтелекту, які дозволяють нам створювати фільми, книжки та складне програмне забезпечення, сидячи в кафе або в шанцях. Кількість сфер життя, пов'язаних із цифровими технологіями, зараз збільшилася експоненціально. Розмаїття доступних цифрових інструментів вражає, і вони інтегруються в життя кожного — навіть тих, хто відмежовується від цифрових технологій.

Звідси й виникли численні загрози, від ігнорування яких може постраждати як звичайна людина, так і військовий, який виконує важливе завдання і ризикує втратити цінну інформацію на користь ворога або навіть піддати себе чи побратимів смертельній загрозі. Саме тому ми маємо бути свідомими всього потенціалу та загроз цифрового світу, який став невід'ємною частиною нашого життя. Тому й виникла ідея написати цю книжку. Приємного читання.

ВСТУП

Коли ворожі ракети б'ють по електростанціях та інших інфраструктурних об'єктах, у небі працює ППО, а підрозділи Військ зв'язку та кібербезпеки ЗСУ тримають фронт цифрової інфраструктури, будь-яка недбалість із даними та «кліком не туди» вже не просто помилка. Це те, що може зірвати оповіщення про тривогу, покласти мобільний зв'язок, поставити під удар банківські рахунки, документи та інші персональні дані. В російсько-українській війні, війні за Незалежність, інформаційна гігієна — це достеменно дисципліна виживання.

Україна в останні півтора десятиліття стала полігоном для російських кібератак. Часто саме на українських системах ворог відпрацьовував те, що пізніше намагався застосовувати й проти інших країн. Експерти з кібербезпеки ще в 2009–2010 роках фіксували спрямовані фішингові кампанії проти українських держструктур. Але це була радше розвідка.

Хакерське угруповання Gamaredon, пов'язане з ФСБ РФ, починає активно діяти з 2013 року. Воно спеціалізувалося на збиранні інформації з комп'ютерів українських держслужбовців та військових через заражені документи (Word, Excel із макросами). Це вважають першою довготривалою російською кібершпигунською кампанією проти України.

У травні 2014 року перед президентськими виборами ЦВК зазнала потужних кібератак. Шкідливе ПЗ мало змінити результати голосування, але атака була вчасно виявлена й знешкоджена. Ця перша масштабна політична кібератака на Україну мала на меті підірвати довіру до державних інституцій. У 2019-му російські хакери намагалися знову атакувати виборчу інфраструктуру, але, на щастя, знов безрезультатно.

23 грудня 2015 року внаслідок зараження шкідливим ПЗ *BlackEnergy* були атаковані три обленерго (Прикарпаттяобленерго, Київобленерго та Чернівціобленерго). Понад 230 тис. абонентів залишалися без світла від 1 до 6 годин. Це був перший у світі підтверджений випадок успішної кібератаки

енергосистеми, яке здійснила хакерська група Sandworm, пов'язана з ГРУ РФ.

17 грудня 2016 року Київобленерго знову зазнало атаки, цього разу з використанням нового шкідливого ПЗ Industroyer. Було знеструмлено п'яту частину столиці, без світла опинилися десятки тисяч абонентів. Industroyer — це модульне шкідливе програмне забезпечення, що вміло безпосередньо працювати з промисловими протоколами, які керують обладнанням енергосистем.

27 червня 2017 року шкідливе ПЗ NotPetya поширилося через оновлення української бухгалтерської програми M. E. Doc. Були паралізовані банки, урядові органи, транспорт, медіа. Вірус вийшов за межі України й завдав збитків світовій економіці на понад $10 млрд (найбільша кібератака за масштабами збитків на той час). Хоча вірус і виглядав як «вимагач», насамперед він мав на меті знищення даних.

Уночі з 13 на 14 січня 2022 року хакери Ghostwriter/UNC1151, пов'язані з Міністерством оборони РБ, здійснили глобальну атаку на сайти Кабінету Міністрів та окремих міністерств. Також тимчасово поклали сайт держпослуг «Дія».

Серед інших, були атаковані сайти Кабміну, МЗС, ДСНС, Міносвіти, Мінспорту, Міненерго, Мінагрополітики, Мінветеранів, Мінзахисту довкілля та Держказначейства. На них можна було побачити повідомлення: «Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі». Це була підготовка до великої війни.

24 лютого 2022-го, майже синхронно з початком вторгнення, противник вивів із ладу тисячі супутникових модемів ViaSat у Європі, у тому числі в Україні. Зв'язок «посипався» навіть у німецьких вітроелектростанцій. Щонайменше 27 тисяч

користувачів відчули масштаб «бокової шкоди» від кібератаки, що вдарила по військових і цивільних одночасно.

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, зареєструвала та дослідила протягом 2022 року 2100 інцидентів та кібератак, з них понад 1500 мали місце під час повномасштабного воєнного вторгнення Росії в Україну.

«Зламали Дію!» — коли паніку сіють навмисно

Ще до повномасштабної війни, на тлі січневої атаки 2022-го, зловмисники розмістили в даркнеті для подальшого продажу нібито дані 13,5 мільйонів користувачів порталу «Дія». Кіберполіція й Мінцифри це спростували: йшлося про компіляцію старих витоків з інших сервісів, яку видали за «злам державного порталу», аби посіяти паніку. Для ворога, коли він запускає ІПСО (інформаційно-психологічну спецоперацію) різниці між справжнім зламом і майстерно упакованим фейком немає — важливий негативний суспільний резонанс. До теми «зламу Дії» ворог під час війни повертався ще кілька разів, але щоразу за гучними заявами були ті самі файли, що фігурували ще в січні 2022 року.

Висновок простий: коли «друзі з чатиків» приносять «100% підтверджений» дамп «із Дії» — це майже завжди частина інформаційно-психологічної операції. Перевіряйте першоджерела, дивіться на дати й офіційні коментарі інституцій, що адмініструють сервіси.

Фішинг «під державу» та кібершпигунство «під повістку»

CERT-UA регулярно фіксує кампанії, де противник маскує шкідливі вкладення під «судові повістки», «накази», «перевірки безпеки», а інколи навіть видає себе за саму CERT-UA, просячи «дозволити віддалене підключення». Це націлено на держслужбовців, військових і оборонні компанії — тобто на тих, від кого сьогодні залежить стійкість тилу.

Наймодніша обгортка таких атак — файли, що імітують урядові документи, й повідомлення в закритих месенджерах. Наприклад, упродовж березня 2025 року у месенджері

Signal виявлено факти розповсюдження повідомлень з архівами, в яких, нібито, містився звіт з результатами наради, що стосувався БПЛА, засобів РЕБ тощо. При цьому в деяких випадках, для підвищення довіри, відправлення повідомлень здійснювалося від осіб зі списку існуючих контактів, чиї облікові записи було заздалегідь зламано. Як правило, згадані архіви містили файл з розширенням «.pdf», а також файл «.exe», класифікований як вірус DarkTortilla.

Як бачимо, звичка «відкрити та подивитися, що там» під час війни може коштувати надто дорого.

Діпфейк як зброя: «Зеленський капітулює»

Діпфейк походить від англійських слів deep learning (глибоке навчання) та fake (підробка). Просто кажучи, це майстерна підробка за спеціальною методикою синтезу зображення і голосу з використанням штучного інтелекту. Її використовують для поєднання і накладення одних зображень та відео на інші.

Уперше про них почули ще восени 2017 року, коли анонімний користувач Reddit під псевдонімом Deepfakes опублікував в Інтернеті кілька порнографічних відео з відомими акторками. Сцени були настільки реальними, що мало не спричинили грандіозний скандал.

У березні 2022 року з'явилося підроблене відео із заявою про капітуляцію від Володимира Зеленського. Його швидко викрили, прибрали із соцмереж, але залишився важливий урок: доступна штучна «картинка» може на хвилини-години посіяти розгубленість. Наступного разу діпфейк може бути якіснішим і з'явитися в потрібну мить — під час обстрілів чи великої військової операції. Саме тому верифікація джерела є базовою навичкою самооборони.

Кібератаки, що торкнулися кожного

12 грудня 2023 року відбулася атака на Kyivstar. Зв'язок зник для мільйонів, місцями, як от на Сумщині, «підглухли» сирени. Українська розвідка та профільні структури називали серед підозрюваних Sandworm / Solntsepek (підрозділ ГРУ), а сама

компанія потім витратила $90 млн на ліквідацію наслідків і посилення захисту. Цей кейс показав: удар по телеком-ядру миттєво стає проблемою безпеки людей, а не «питанням IT».

Ця сама хакерська група раніше (серпень 2023) запускала мобільного шкідника «Infamous Chisel», орієнтованого на Android-пристрої, якими користувалися українські військові. Він був призначений для збору інформації: повідомлень, 2FA-даних, VPN-налаштувань, інформації з месенджерів тощо.

У січні 2024 року росіянами була атакована комунальна енергетична компанія Львівтеплоенерго, через що на короткий термін були знеструмлені понад 600 будинків у Львові під час морозів.

А в грудні того самого року російські кібервійська здійснили масштабну атаку на українські державні реєстри, які перебувають у компетенції Міністерства юстиції України, через що було тимчасово зупинено низку сервісів.

«Зливи даних русні»: удар повертається рикошетом

Парадокс, але саме російські громадяни живуть у режимі тотального витоку: за оцінками топ-менеджера Сбербанку, персональні дані близько 90% дорослого населення РФ вже гуляють у публічному доступі. 2023 рік став піком витоків у російських фінансових установах — сотні мільйонів записів. Для українців це важлива ремарка: ворог сам загруз у «чорних базах», а отже активніше експлуатує соціальну інженерію — дзвінки, фішингові СМС, підроблені «держсервіси».

Окремий кейс — масштабний витік даних соцмережі «ВКонтакте» (390+ млн акаунтів). Навіть якщо це «не банк», масове поєднання імен, номерів, локацій і фото — золота жила для шахраїв, які будують таргетовані атаки й легенди під конкретні родини, використовуючи їхні контакти, вподобання, страхи.

Чимало кібератак з витоком чи руйнуванням даних у РФ, були здійснені українськими хакерами або за підтримки України

після 24 лютого 2022 року. Серед найважливіших: злам Центрального банку РФ (~27 000 документів, 2.6 ТБ файлів), витік бази Альфа-Банк (38 млн клієнтів, 115 млн записів), витік з Роскомнадзору (~800 ГБ), витік з Міністерства праці та соцзахисту РФ (>100 ТБ), атака на Росводоканал (понад 50 ТБ знищено), злам російського космічного центру (~2 РВ даних знищено), злам Міноборони РФ (отримано документи 2000 структурних підрозділів), витік внутрішньої технічної документації з розробника безпілотників Альбатрос (~100 ГБ креслень та описів дронів, що могли використовуватися у війні), витік даних з авіабудівної корпорації Туполев (4,4 ГБ документів, що стосуються стратегічних бомбардувальників), атака на авіакомпанію «Аерофлот» тощо. Це все послаблює ворога і робить сильнішими нас.

ЧОМУ ІНФОРМАЦІЙНА ГІГІЄНА СТАЛА ПИТАННЯМ ВИЖИВАННЯ

1. *Від неї залежить життя*: атака на телеком — мінус зв'язок і сирени; фішинг на робочій пошті — мінус безпека підрозділу чи підприємства; поширення фейку — мінус довіра в тилу.

2. *Це б'є по гаманцю*: витоки даних — пальне для шахрайства. У 2024-му в РФ рекордні крадіжки з рахунків через соціальну інженерію — той самий інструментарій противник застосовує і проти українців.

3. *Це б'є по волі до спротиву*: Діпфейки у відповідальний момент породжують сумнів і страх.

Мінімальний набір правил інформаційної гігієни, які вже рятували тисячі людей:

• *Перевіряйте джерело й дату.* Будь-який «злив» державних даних без офіційного підтвердження сприймайте як ІПСО, поки інше не доведено. Дивіться офіційні коментарі Кіберполіції, Держспецзв'язку, СБУ.

• *Не відкривайте «повістки/накази/судові виклики» з пошти невідомого походження.* Про підозрілі листи чи повідомлення із вкладеннями повідомляйте одразу у свій підрозділ безпеки.

• *Не давайте віддалений доступ «службам підтримки» з повідомлень/дзвінків, не повідомляйте по телефону свої персональні дані.*

• *Сумніваєтесь у відео/заяві — чекайте підтверджень із кількох надійних медіа.* Пам'ятайте кейс із «капітуляцією» — він був знешкоджений завдяки пильності користувачів і швидкій реакції держави та інтернет-платформ.

Ця війна навчила: кожен із нас — вузол критичної інфраструктури. Наші телефони, акаунти, реакції — це поверхня атаки. Дбайливе поводження з інформацією так само важливе, як перебування у бомбосховищі під час атаки з повітря чи тримання вдома тривожної валізи. Інформаційна гігієна — це звичка, що тримає вас, ваших рідних і країну в живих.

ІНФОРМАЦІЙНА ВІЙНА ЯК СКЛАДОВА СУЧАСНОЇ ВІЙНИ

Сучасні війни вже неможливо уявити без фронту інформаційного. Поруч зі зброєю на полі бою працюють аналітики, журналісти-розслідувачі, кібервійська, волонтери-осінтери та цілі армії цифрових добровольців. Кожен смартфон, кожна публікація у соціальних мережах стає джерелом розвідданих. Тому інформаційна війна перетворилася на ключову складову збройних конфліктів XXI століття.