

Д. Волошин, мол. наук. співроб., НЮБ НБУВ

Фінансове шахрайство під час війни: актуальні схеми та методи захисту

Сучасні виклики національній безпеці вимагають переосмислення методів боротьби із фінансовими злочинами, які набули нових масштабів у період воєнного стану. Російська агресія проти України спричинила зростання нелегальних фінансових потоків і посилила загрози фінансовій безпеці. Війна продовжує підривати глобальну фінансову стабільність, посилює вразливість населення та ускладнює фінансовий моніторинг, створюючи сприятливе середовище для приховування злочинних доходів, розширення тіньової економіки та обходу санкцій. У зв'язку з цим актуалізовано дослідження, що розкриває ключові механізми функціонування сучасних шахрайських схем та методів легалізації коштів³⁰. А саме розкриття юридичних аспектів відповідальності за шахрайство, дослідження актуальних схем залучення громадян до протиправної діяльності та аналіз алгоритмів захисту, що дозволяють мінімізувати ризики як для окремих осіб, так і для фінансової системи держави в цілому.

Фундаментом для розуміння природи цих злочинів є чітке розмежування їхніх видів у правовому полі. Адже залежно від об'єкта посягання та способу дій зловмисників, законодавство виділяє різні кваліфікаційні ознаки шахрайських дій.

Згідно з ч. 1 ст. 190 Кримінального кодексу України (далі – ККУ) шахрайство визначається, як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою³¹.

³⁰ Дослідження Держфінмоніторингу «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2025». URL: https://fiu.gov.ua/assets/userfiles/411/%D0%A2%D0%B8%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%20%D0%94%D0%A1%D0%A4%D0%9C%D0%A3/Typology%202025_UA.pdf

Водночас законодавство окремо виділяє специфічні форми економічних злочинів. Зокрема, у диспозиції ч. 1 ст. 222 ККУ законодавством роз'яснено термін «шахрайство з фінансовими ресурсами» як надання завідомо неправдивої інформації органам державної влади, органам влади Автономної Республіки Крим чи органам місцевого самоврядування, банкам або іншим кредиторам з метою одержання субсидій, субвенцій, дотацій, кредитів чи пільг щодо податків у разі відсутності ознак кримінального правопорушення проти власності³².

Проте найбільш широкого вжитку набув термін «фінансове шахрайство», під яким розуміється дія, яка націлена на збагачення за рахунок фізичних, юридичних осіб шляхом застосування прийомів обману. До головних ознак фінансового шахрайства відносять невиконання вимог, коли відбувається грошова операція; зловживання службовим становищем задля отримання прибутку; отримання приватної інформації для подальшого використання її та привласнення коштів особи³³.

На практиці виділяють такі основні форми та способи шахрайства:

– заволодіння чужою власністю, вчинене у формі обману, коли жертві навмисне повідомляють хибну інформацію або замовчують інформацію, фальсифікують предмет угоди (наприклад, підмінюють коштовність підробкою), використовують обманні схеми у фінансових розрахунках,

³¹ Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>

³² Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>

³³ Кримінальна відповідальність за шахрайство з фінансами. АО «Бачинський і партнери». URL: <https://legaid.ua/ua/kryminalna-vidpovidalnist-za-shahrajstvo-z-finansamy/>

пропонують здійснити передоплату за товари або послуги, публікують фейкові оголошення про збір грошей на лікування дитини, допомогу військовим та ін., створюють фейкові сайти, що схожі на офіційні сторінки благодійних фондів, застосовують різноманітні трюки в азартних іграх та інші способи з метою введення жертви в оману;

– шахрайство у формі зловживання довірою. У цьому випадку шахраї використовують довіру жертви до нього, яка може виникати на тлі гарних або близьких стосунків із жертвою – спільні родичі, добрі знайомі. Також лиходій може користуватись певним службовим становищем (наприклад, представник податкової або видає себе за нього). Таким зловживанням буде і прийняття на себе зобов'язань, які не будуть виконуватись (типовий приклад: банкрут бере кредит або гроші в борг у знайомих)³⁴.

Щодо питання законодавчого регулювання питання шахрайства в Україні, то воно регламентується такими основними джерелами права:

– ст. 190, розд. VI «злочини проти власності» Кримінального кодексу України;

– Постанова Верховного Суду України, де проаналізовано та узагальнено практику розгляду судами справ по шахрайству (№ 10 від 06.12.2009), ККУ про адміністративні правопорушення;

– загальні питання, а передусім дотримання прав та свобод людини, ефективність слідства, справедливий суд регламентує практика Європейського суду з прав людини (ЄСПЛ).

Внаслідок швидкого розвитку інформаційних технологій у наш час стали більш поширені випадки шахрайства з використанням цифрових технологій. Тому для врегулювання цього питання у 2024 р. за основу був прийнятий Верховною Радою України законопроект щодо встановлення відповідальності за електронно-комунікаційне шахрайство, який доповнює

ККУ та спрямований на посилення боротьби із шахрайськими кол-центрами, які професійно займаються обманом громадян України³⁵.

Також у 2025 р. У Верховній Раді України зареєстровано законопроект № 14161 щодо створення та ведення реєстру осіб, платіжні операції яких потребують посиленого контролю³⁶. У народі їх називають «дропами», це особи, що стають нижчою ланкою в ієрархії кіберзлочинності, продаючи доступ до своїх банківських даних для обігу нелегальних грошей.

За словами народного депутата України від партії «Голос» Я. Железняка, який є одним з ініціаторів законопроекту, через систему «дропів» зараз проходить до 200 млрд грн, а втрати для бюджету становлять десятки мільярдів. Він зазначив, що дроп-схеми стали основним каналом оплати нелегального алкоголю, тютюну, азартних ігор та дедалі частіше використовуються кримінальними угрупованнями – від кол-центрів до наркоторгівців. За словами депутата, впровадження системи дозволить перейти від загальних обмежень на Р2Р-перекази до більш адресного контролю, який торкнеться лише ризикових клієнтів. Це має підвищити ефективність боротьби з тіньовими фінансовими потоками без створення додаткового тиску на добросовісних користувачів³⁷.

³⁵ Верховна Рада України прийняла за основу законопроект щодо встановлення відповідальності за електронно-комунікаційне шахрайство. Офіційний вебпортал Верховної Ради України. URL: <https://www.rada.gov.ua/news/razom/249836.html>

³⁶ Проект Закону про внесення змін до деяких законів України щодо створення та ведення реєстру осіб, платіжні операції яких потребують посиленого контролю. Урядовий портал. URL: <https://www.kmu.gov.ua/bills/proekt-zakonu-pro-vnesennia-zmin-do-deiakykh-zakoniv-ukrayiny-shchodo-stvorennia-ta-vedennia-reyestru-osib-platizni-operatsiyi-iakykh-potrebuiut-posylenoho-kontroliu>

³⁷ У Верховній Раді зареєстрували законопроект про реєстр «дропів». Fintech Insider. URL: <https://fintechinsider.com.ua/u-verhovnij-radi-zareyestruvaly-zakonoprojekt-pro-reyestr-dropiv/>

³⁴ Стаття 190 ККУ про шахрайство: від теорії до практики. Офіційний вебсайт Адвокатського об'єднання «Актум». URL: <https://www.actum.com.ua/blog-3-1/stattia-190-kk-pro-shakhraistvo-vid-teorii-do-praktyky>

Ключове значення, окрім способу вчинення злочину, для кваліфікації дій правопорушника як фінансове шахрайство має розмір завданих збитків. Саме фінансовий аспект визначає межу між адміністративним проступком та кримінальним злочином.

У 2026 р. кримінальна відповідальність за шахрайство починається із суми збитку від 6800 грн. Це пов'язано з критерієм «значної шкоди», який в Україні прив'язаний до прожиткового мінімуму для працездатних осіб. Отже, від цієї суми вже може бути порушено кримінальну справу за фактом шахрайства. Якщо сума менше, дії можуть розглядатися як адміністративне правопорушення, а не кримінальне. При «значній шкоді» (від 6800 грн до 170 000 грн) правопорушення карається штрафом, виправними роботами або обмеженням волі. За «шахрайство у великому розмірі» (понад 170 000 грн) можливий арешт або позбавлення волі до 5 років. Якщо шахрайство вчинено організованою групою або в особливо великому розмірі (понад 425 000 грн), покарання посилюється – позбавлення волі на строк до 12 років з конфіскацією майна. У таких випадках кримінальна справа за фактом шахрайства порушується автоматично за наявності заяви та доказів³⁸.

На сьогодні високі ризики кримінальної відповідальності та розвиток цифрових технологій змушують шахраїв відмовлятися від примітивних методів на користь багаторівневих схем. У наші дні зловмисники намагаються максимально дистанціюватися від жертви та правоохоронців, використовуючи посередників для маскуванню фінансових потоків.

Зокрема, наведемо найбільш поширені схеми:

- використання «дропів» або грошових мулів
- людей, які за винагороду передають доступ до своїх банківських карток, онлайн-банкінгу чи криптогаманців третім особам. Такі платіжні

засоби використовують у шахрайських схемах, відмиванні коштів, наркотрафіку та інших злочинах (За свідченнями Департаменту кіберполіції України близько 70 % усіх зафіксованих кібершахрайств здійснюються саме з використанням платіжних реквізитів «дропів», залучаючи при цьому молодь, студентів, безробітних, ВПО та представників соціально вразливих категорій населення. Вербування відбувається через оголошення про «швидкий» або «легкий заробіток» передусім у месенджерах і телеграм-каналах)³⁹;

- поширення повідомлень про неіснуючі соціальні виплати з метою отримання доступу до банківських даних і викрадення коштів (Шахраї створюють фейкові повідомлення про «державну» або «міжнародну» допомогу з додаванням посилань на фішингові сайти, що імітують офіційні ресурси просячи ввести персональні дані чи реквізити банківських карток, які в подальшому використовують для викрадення коштів)⁴⁰;

- вимагання коштів від імені МВС України через підроблений вебсайт-дублікат (після переходу по шкідливому посиланню комп'ютер користувача блокують і змушують оплатити фейковий штраф, погрожуючи кримінальною відповідальністю)⁴¹;

- інвестиційне шахрайство через фіктивних брокерів (створення фіктивних платформ,

³⁹ Близько 70 % кібершахрайств пов'язані з використанням платіжних реквізитів «дропів». Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/blizko-70-kibersaxraistv-poviazani-same-z-vikoristanniam-platiznix-rekvizitiv-dropiv>

⁴⁰ До уваги! Шахраї поширюють повідомлення про неіснуючі соціальні виплати. Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/do-uvagi-saxrayi-posiriuiut-povidomlennia-pro-neisnuiuci-socialni-viplati>

⁴¹ Увага! Кіберполіція виявила випадки вимагання коштів від імені МВС України через підроблений вебсайт-дублікат. Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/uvaga-kiberpoliciia-viiavila-vipadki-vimagannia-kostiv-vid-imeni-mvs-ukrayini-cerez-pidroblenii-vebsait-dublikat>

³⁸ З якої суми настає кримінальна відповідальність за шахрайство. Офіційний вебсайт адвокатського об'єднання «Камінська та партнери». URL: <https://kaminska.com.ua/blog/z-yakoyi-sumy-nastaye-kryminalna-vidpovidalnist-za-shahrajstvo>

що імітують реальні торги акціями чи криптоактивами). Жертва бачить фальшивий прибуток у кабінеті й вносить нові суми, а при спробі виводу коштів шахраї вимагають додаткові «комісії» за верифікацію, після чого припиняють зв'язок);

- шахрайство за допомогою ШІ-інструментів (голосові та deepfake-атаки, де клонується голос близької людини чи, наприклад, відеодзвінки з «маскою» знайомого (рідного) обличчя. До того ж автоматизовані чат-боти говорять «мовою клієнта» з високим ступенем персоналізації. Найбільшу небезпеку становлять короткі голосові повідомлення в месенджерах з проханням про позику «до вечора»);

- шахрайські кол-центри (масштабні організації зі своїми професійними стандартами роботи, HR-структурами, навчальними програмами та KPI. Десятки операторів працюють за чіткими скриптами, наприклад, представляючись «службою безпеки» того чи іншого банку до «інвестиційних консультантів». Такі кол-центри перетворюють злочин на професійну індустрію психологічного насильства⁴²;

- шахрайство, вчинене шляхом створення фіктивних оголошень про продаж товарів в інтернет-магазинах, соціальних мережах (OLX, Prom, Instagram тощо);

- скімінг – спосіб крадіжки банківських даних. Шахраї встановлюють на банкомати або платіжні термінали спеціальні пристрої (скімери), які зчитують інформацію з магнітної стрічки картки. Додатково можуть використовувати приховані камери або фальшиві клавіатури для підглядання PIN-коду. Існує безконтактний скімінг. Технологія, яка дозволяє викрадати дані карток із функцією NFC, просто наблизившись до них з потужним зчитувальним пристроєм. Також Інтернет-скімінг, коли зловмисники зламують сайти інтернет-магазинів та вбудовують шкідливий код у платіжну форму. Коли жертва

вводить свої карткові дані, вони автоматично передаються шахраям⁴³;

- фейкове інвестування (шахрайство за принципом «фінансової піраміди», де для створення ілюзії надійності жертві на перших етапах виплачують невеликі дивіденди, стимулюючи її вкладати значно більші суми);

- шахрайства через месенджери, викрадення акаунту. Зловмисники зламують доступ до вашого профілю у соцмережах або месенджерах (Telegram, Viber тощо). Після цього роблять масову розсилку по вашій контактній книзі від вашого імені. Зазвичай це термінові прохання про фінансову допомогу. Головна пастка в тому, що повідомлення приходить із вашого справжнього акаунту, тому в людей не виникає сумнівів, і вони стають жертвами обману, намагаючись вам допомогти;

- телефонне шахрайство або схема «німі» дзвінки (абонент відповідає, але на іншому кінці тишина. Такі дзвінки допомагають шахраям підтвердити існування номера, записати голос або навіть списати гроші при спробі передзвонити. Також зустрічаються випадки, коли дзвінок одразу скидають. Якщо абонент намагається передзвонити, з його рахунку можуть списати гроші)⁴⁴.

З початку повномасштабного вторгнення стали поширюватися схеми фінансового шахрайства, пов'язані з викликами війни, а саме спроби нажитися на таких болючих темах як ВПО, волонтерство, потреби ЗСУ; пошук зниклих безвісті тощо.

У щорічному звіті Кіберполіції за 2025 р.⁴⁵ наведено характерні приклади розкритих злочинів, серед них:

⁴³ Що таке скімінг та як захиститись від шахрайства? Блоги. Unex Bank. URL: <https://unexbank.ua/blog/sho-take-skimming-ta-yak-zahistitis-vid-shahrajstva>

⁴⁴ Телефонне шахрайство 2026: чому не варто відповідати на «німий» дзвінок. СтопКор. URL: <https://www.stopcor.org/ukr/section-suspilstvo/news-telefonne-shahrajstvo-2026-chomu-ne-var-to-vidpovidati-na-nimij-dzvinok-14-02-2026.html>

⁴⁵ Щорічний звіт Департаменту кіберполіції за 2025 рік. Офіційний вебсайт Департаменту кіберполіції Національної поліції України. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/>

⁴² Традиційні системи безпеки безсилі: нові шахрайські схеми 2025 року, через які українці втратили 1,4-1,6 млрд грн. International Financial Club “BANKIR”. URL: <https://bankir.kiev.ua/tradytsijni-systemy-bezpeky-bezsyli-novi-shakhrajski-skhemy-2025-roku-cherez-iaki-ukraintsi-vtratyli-1-4-1-6-mlrd-hrn/>

– розповсюдження фішингових посилок за допомогою інтернету (соціальні мережі, месенджери) щодо виплат грошової допомоги від Президента України, ООН, UNICEF та інших видів допомоги, що в подальшому давало змогу отримати доступ до електронного кабінету онлайн-банкінгу потерпілих;

– заволодіння коштами громадян України, Польської, Чеської Республік та інших країн Європейського Союзу, під приводом здійснення платежів за купівлю або продаж побутових товарів, надання послуг за допомогою Телеграм-боту разом із системою, яка підробляє платформи онлайн-оголошень щодо продажу товарів та вводу банківських карток;

– створення та координування роботи мережі кол-центрів, орієнтованих на громадян держав Європи, зокрема Латвійської Республіки з метою введення потерпілих в оману під приводом залучення інвестицій у криптовалюту через псевдоброкерські платформи;

– заволодіння коштами громадян України, під приводом пригону транспортних засобів, зокрема для потреб ЗСУ.

Також за допомогою функціонування пілотного проєкту Antifraud (з 01.05.2025) у системі зареєстровано 4539 подій онлайн-шахрайств з використанням платіжних реквізитів, за яким сформовано 4915 запитів до банківських установ.

Отримані відповіді за типом фінансових транзакцій:

- Р2Р-перекази – 50 % (за допомогою IBAN – 5 %);
- POS-термінали – 20 %;
- оплата послуг в мережі «Інтернет» – 15 %;
- зняття готівки в банкоматах – 5 %, розрахунки – 5 %.

За результатами вжитих заходів банківськими установами заблоковано кошти у сумі 145 млн грн, які належали потерпілим від онлайн-шахрайств⁴⁶.

⁴⁶ Щорічний звіт Департаменту кіберполіції за 2025 рік. Офіційний вебсайт Департаменту кіберполіції Національної поліції України. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/>

Така кількість нових шахрайських схем змусила державу реагувати швидше, то на сьогодні фінансовим шахрайством в Україні посилено займаються такі правоохоронні органи, як: Національна поліція (зокрема, Департамент кіберполіції при інтернет-злочинах), Бюро економічної безпеки (БЕБ) – у сфері економіки, а також Служба безпеки України (СБУ) у випадках загрози державній безпеці. Захист прав споживачів фінансових послуг забезпечує Національний банк України.

Саме завдяки злагодженій роботі цих відомств та впровадженню нових методів моніторингу, ситуація з реєстрацією злочинів почала змінюватися. Про ефективність такого контролю свідчать офіційні цифри за останній рік.

Зокрема, за даними Опендатабот, у 2025 р. в Україні було зафіксовано 48 871 кримінальне провадження за статтею 190 ККУ «Шахрайство», що на чверть менше, ніж у 2024 р., коли правоохоронці зареєстрували майже 65 тис. справ. Як зазначається, наразі показники фактично повернулися до рівня 2016 р. Підозру було вручено в кожній п'ятій справі – 10 456 проваджень. До суду дійшло 18 % справ, а саме 8758 кримінальних проваджень. У 2024 р. цей показник був на рівні 24 %. Лідером за кількістю справ щодо шахрайства залишається Київ – 6825. Далі йдуть Дніпропетровщина із 4844 справами та Харківщина – з 3677 провадженнями. Також в Опендатабот повідомили, що майже по всій країні кількість нових проваджень зменшилася. Єдиний регіон, де зафіксовано зростання, Хмельниччина (+2,7 % за рік). Найбільш відчутне покращення ситуації спостерігається на Миколаївщині, де кількість нових справ скоротилася майже вдвічі, а також у Чернівецькій області: – 39 %⁴⁷.

Аналіз статистичних даних та звітів профільних відомств демонструє, що попри

⁴⁷ У 2025 році в Україні зафіксували понад 48 тисяч кримінальних проваджень щодо шахрайства. Юридична газета. URL: <https://yur-gazeta.com/golovna/u-2025-roci-v-ukrayini-zafiksuvali-ponad-48-tisyach-kriminalnih-provadzhen-shchodo-shahraystva-.html>

значні успіхи в блокуванні викрадених коштів, «людський фактор» залишається найбільш вразливою ланкою. Розуміючи, що суто технічних заходів захисту недостатньо, державна система фокусується на формуванні колективної стійкості через масове навчання та розвиток цифрових навичок населення.

Для запобігання злочинам державні структури активно впроваджують просвітницькі заходи. Наприклад, на сайті МВС регулярно публікуються статті у розділах «Кібербезпека», щодо заходів безпеки для громадян, де подано інформацію та основні правила безпеки щодо запобігання шахрайству в інтернеті. Національний банк України разом з Департаментом кіберполіції Національної поліції України та Державною службою спеціального зв'язку та захисту інформації України з 13 травня 2025 р. розпочав чергову хвилю Всеукраїнської інформаційної кампанії з платіжної безпеки – #ШахрайГудбай⁴⁸.

У межах Міжнародного дня безпечного інтернету (Safer Internet Day), ініційованого Європейським Союзом і підтримуваного в понад 160 країнах світу, Міністерство внутрішніх справ України інформує про освітню ініціативу Міністерства цифрової трансформації України. На платформі Дія.Освіта та в застосунку Дія розміщено відповідні матеріали й інструкції з кібергігієни. За результатами дослідження цифрової та ІІІ-грамотності 2025 р., 78 % українських підлітків і понад дві третини дорослих уже стикалися з інцидентами, пов'язаними з безпекою даних⁴⁹.

Окрім регулярних інструкцій щодо блокування шахрайських чатів, соцмереж та сайтів, кіберполіція запустила потужний

практичний інструмент – проєкт «Кібер Брами». Це онлайн-платформи, метою якої є надання користувачам інтернету інструментів та знань, необхідних для безпечного перебування в цифровому просторі.

Головними завданнями проєкту є:

- знищення російських осередків в інтернеті;
- зменшення рівня онлайн-булінгу, протидія шахрайствам та розповсюдженню наркотичних речовин;
- надання легкого доступу до інформації з кібергігієни та методик попередження кіберзагроз;
- забезпечення користувачів інтернету практичними рекомендаціями та інструментами для захисту їхньої особистої та робочої інформації в мережі;
- популяризація цифрової гігієни серед різних категорій користувачів, включаючи студентів, освітян та підприємців.

Завдяки проєкту громадяни зможуть отримувати корисну інформацію та з легкістю освоїти нюанси безпечного користування онлайн-платформами, зокрема, соцмережами⁵⁰.

Паралельно з освітніми ініціативами, працівниками Департаменту кіберполіції приділяється суттєве значення впровадженню інновацій та цифровізації процесу боротьби з кіберзлочинністю, зокрема за допомогою впровадження інноваційної системи автоматизованого обміну інформацією Antifraud, яка упроваджена у тісній співпраці з фінансовим сектором держави та правоохоронними органами. Зазначений пілотний проєкт суттєво ускладнив протиправну діяльність шахраїв і підвищив рівень захищеності фінансових операцій. Інноваційний проєкт Antifraud, який є унікальною розробкою Національної поліції України, реалізовано у тісній співпраці з банківськими установами, зокрема з Національним банком України та Українською

⁴⁸ Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/startuje-vseukrayinska-informaciina-kampaniia-z-platiznoyi-bezpeki-saxraigudbai>

⁴⁹ День безпечного інтернету: фокус на кібергігієні та цифровій стійкості. Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/den-bezpecnogo-internetu-mvs-zaklikaje-formuvati-kulturu-kibergigijeni-ta-dolucatisia-do-iniciativi-safer-internet-day>

⁵⁰ Про схеми онлайн-шахраїв та що є фейками в інтернеті – новий проєкт кіберполіції «Кібер Брами». Офіційний вебсайт Міністерства внутрішніх справ України. URL: <https://mvs.gov.ua/news/pro-sxemi-onlain-saxrayiv-ta-shho-je-feikami-v-interneti-novii-projekt-kiberpoliciyi-kiber-brama>

міжбанківською асоціацією членів платіжних систем «ЄМА» Проект Antifraud втілює сучасний підхід до запобігання фінансовим правопорушенням, забезпечуючи оперативне виявлення та блокування підозрілих транзакцій, мінімізацію ризиків для громадян і бізнесу, а також високий рівень міжвідомчої взаємодії на національному рівні⁵¹.

Важливо відзначити, що у щорічному звіті кіберполіції наголошується, що головним пріоритетом на 2026 р. залишається підвищення рівня цифрової культури суспільства. Планується розширення просвітницьких програм для різних цільових аудиторій – школярів, студентів, представників бізнесу та державних службовців, зазначаючи, що формування навичок безпечної поведінки в мережі є важливою складовою національної системи кібербезпеки та запорукою зменшення кількості кіберзлочинів.

Отже, фінансове шахрайство в Україні під час війни трансформувалося у складну технологічну загрозу, де основним інструментом зловмисників залишається психологічний тиск на людей. Держава демонструє активну позицію у цій боротьбі: від ухвалення профільних законів до реалізації масштабних національних кампаній з кібергігієни. Ці ініціативи спрямовані на те, щоб перетворити кожного користувача на свідому ланку системи безпеки. Проте зростання сум збитків свідчить, що боротьба ще триває, і успіх у ній залежить від синергії державних зусиль та готовності самих українців засвоювати навички цифрового захисту. Лише через постійну просвітницьку діяльність та колективну пильність ми зможемо ефективно протистояти фінансовому шахрайству та зміцнити економічну стійкість українського суспільства.

⁵¹ Щорічний звіт Департаменту кіберполіції за 2025 рік. Офіційний вебсайт Департаменту кіберполіції Національної поліції України. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/>