КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.9
DOI https://doi.org/10.32782/TNU-2707-0581/2026.4/27

Громко В. Я.
https://orcid.org/0000-0002-7185-317X
ЗВО «Університет Короля Данила»

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ТА ЗАПОБІГАННЯ КІБЕРШАХРАЙСТВУ В УКРАЇНІ: СУЧАСНІ ТРЕНДИ ТА ВІКТИМОЛОГІЧНИЙ АСПЕКТ

У статті досліджено особливості та ключові тенденції трансформації сучасної кіберзлочинності в Україні в специфічних умовах правового режиму воєнного стану. Констатовано, що стрімка цифровізація всіх сфер суспільних відносин, вимушений перехід бізнесу та державних інституцій у дистанційний формат, а також масова міграція населення зумовили системне зростання, безпрецедентну гнучкість та технологічну еволюцію кібершахрайства. У статті запропоновано визначення новітніх детермінантів кіберзлочинності в умовах війни та розробка активних заходів протидії. У процесі дослідження використано методи системно-структурного аналізу, порівняльно-правовий та кримінологічний методи.

Проаналізовано психологічні механізми впливу зловмисників на жертву. Доведено, що сучасні кримінальні стратегії базуються на психоемоційній уразливості громадян, їхньому перманентному стресі, почутті страху, але водночас і на патріотизмі, бажанні допомогти Збройним Силам України та гострosоціальних проблемах сьогодення (виплати матеріальної допомоги, пошук зниклих безвісти, евакуація, тощо). Окрему увагу приділено фактору технологічного ускладнення злочинних схем через інтеграцію інструментів штучного інтелекту, зокрема генерації дипфейків (аудіо та відеоімітації), передових технологій спуфінгу (підміни номерів та адрес) та високоточного таргетованого фішингу. Наголошено, що автоматизація кібератак суттєво підвищує рівень цифрової віктимізації населення, роблячи традиційні методи розпізнавання шахрайства неефективними.

У результаті дослідження обґрунтовано, що виключно каральний підхід та посилення кримінальної відповідальності демонструють обмежену ефективність, оскільки кіберзлочинність є транскордонною та високоанонімною. Доведено гостру потребу у розробці нових гнучких механізмів кримінологічної превенції. Вони мають базуватися на комплексному вивченні причин кібершахрайства, підвищенні рівня цифрової та медіаграмотності громадян, а також на синергетичній взаємодії між державними, правоохоронними органами, приватним ІТ та банківським секторами і міжнародними інституціями. Запропоновано концептуальну модель створення цілісної, динамічної та адаптивної системи захисту громадян у кіберпросторі, здатної реагувати на загрози у режимі реального часу.

Ключові слова: *кібершахрайство, спуфінг, кримінальний процес, кримінальне право, фішинг, цифровізація, кримінологія.*

Постановка проблеми. Стрімка цифровізація суспільних відносин в Україні та вимушена «міграція» соціально-економічних процесів у віртуальний простір в умовах воєнного стану призвели до системного зростання, гнучкості та технологічної трансформації кіберзлочинності. Сучасне кібершахрайство дедалі частіше застосовує у своїй діяльності психологічний вплив на

жертву, використовуючи її психоемоційний стан та сприйняття реальності з метою незаконної наживи. Зловмисники філігранно використовують психологічний стан громадян у період війни, їх страх, патріотизм, а також загострене відчуття справедливості.

Додатково ситуація ускладнюється стрімким розвитком технологій штучного інтелекту, які кіберзлочинці оперативно інтегрують у свої схеми (використання дипфейків, технологій спуфінгу та високоточний таргетований фішингу). Це максимально підвищує рівень цифрової віктимізації населення, особливо серед найбільш вразливих категорій громадян.

Водночас традиційні підходи та виключно внутрішньодержавні поліцейські заходи превенції демонструють обмежену ефективність через специфічні ознаки кіберзлочинності.

Посилення лише кримінальної відповідальності є недостатнім, що зумовлює гостру потребу в розробці нових, гнучких механізмів кримінологічної превенції. Також потребує детального вивчення питання співпраці між державними та правоохоронними органами, приватним банківським сектором та міжнародними інституціями.

Таким чином, постає об'єктивна необхідність в комплексному кримінологічному дослідженні соціальних, економічних та організаційних причин кібершахрайства для створення цілісної та динамічної системи захисту громадян у кіберпросторі.

Аналіз останніх досліджень і публікацій. Чимала кількість наукових статей присвячена дослідженню проблемних питань протидії кібершахрайству в Україні. Зокрема ці питання висвітлювалися в працях О.М. Бандурки, В.С. Батиргареєвої, В.В. Голіни, О.М. Джужи, О.М. Литвинова, А.П. Закалюка, С.Ф. Денисова, В.І. Трапезнікова, Ю.В. Орлова, В.П. Поповича, В.О. Тулякова, та інших вчених. Їх дослідження є цінними для продовження наукових пошуків, однак без належної уваги залишаються питання протидії кіберзлочинам в умовах воєнного стану, вивчення віктимної поведінки особи в розрізі протидії кіберзлочинам з використанням штучного інтелекту, та інші питання які заслуговують належного опрацювання серед наукової спільноти.

Постановка завдання. Мета дослідження окремих проблемних питань запобігання кібершахрайству в Україні, полягає у комплексному кримінологічному та віктимологічному аналізі суті структури та сучасних тенденцій розвитку кібершахрайства в Україні (зокрема в умовах воєнного стану та активного впровадження технологій штучного інтелекту), а також у розробці цілісної, багаторівневої системи протидії та запобігання цьому явищу через синергію нормативно-правового регулювання, інституційної взаємодії правоохоронних органів, технологічних інновацій приватного сектору та підвищення цифрової гігієни громадян.

Виклад основного матеріалу дослідження. На жаль, сучасне кібершахрайство в Україні набуло системного характеру, стало гнучким і дуже технологічним. Як можна прослідкувати по публікаціях в соцмережах та засобах масової інформації, зловмисники дедалі частіше використовують методи соціальної інженерії, граючи на емоціях, страху, патріотизмі, бажанні допомогти або жазі до легкої наживи. Поширеним є шахрайство на платформах оголошень та маркетплейсах. Цей вид злочину стабільно утримує перше місце за кількістю звернень до правоохоронців. Головний принцип зловмисників змусити жертву вийти за межі безпечного контуру торгового майданчика. За часту зловмисники знаходять оголошення на OLX чи іншому маркетплейсі й пишуть у сторонній месенджер (Viber, Telegram), повідомлення, що вже оформили покупку через вбудовану безпечну доставку, і надсилають посилання, яке візуально копіює офіційний інтерфейс платформи. Перейшовши за посиланням, жертва вводить дані своєї картки (включно з балансом та CVV-кодом) нібито для «зарахування коштів», але натомість їх втрачає. Ще одним поширеним видом шахрайства є фейкові інтернет-магазини. Створення професійно виглядаючих сторінок в Instagram або окремих сайтів-одноденок із дефіцитним товаром чи технікою за заниженими цінами. Шахраї вимагають повну або часткову передоплату, після чого блокують покупця.

Поширеним серед шахраїв способом заволодіння коштами також є так званий фішинг. Цей вид шахрайства еволюціонував від масових розсилок до точкових, психологічно вивірених атак. Зараз він тісно переплетений із актуальним контекстом життя в країні.

Ще один із поширених способів шахрайства є так званий вішинг та фейкові кол-центри.

Попри те, що кіберполіція спільно з банками та мобільними операторами суттєво знизила ефективність класичного «дзвінка зі служби безпеки банку», цей інструмент залишається небезпечним через використання штучного інтелекту та дипфейків. Шахраї вже рідше використовують банальне словосполучення «вашу картку забло-

ковано». Тепер вони можуть представлятися представниками Національного банку, податкової або навіть поліції, заявляючи, що «з вашого рахунку зафіксовано фінансування заборонених організацій». Для так званого порятунку коштів чи закриття справи, жертву змушують переказати гроші на нібито безпечний або транзитний рахунок. Часто шахраї використовують технологію спуфінгу (підміни номера телефону), коли на екрані смартфона жертви дійсно відображається офіційний номер банку чи державної установи, що присипляє пильність.

З 2018 року при Службі безпеки України працює ситуаційний центр забезпечення кібербезпеки. Ця структура створювалася за допомогою Північноатлантичного альянсу, технічне обладнання та програмне забезпечення для роботи центру було надано в рамках виконання першого етапу угоди про реалізацію Трастового фонду Україна НАТО з питань кібербезпеки. На базі ситуаційного центру функціонує система управління подіями інформаційної безпеки, яка моніторить події у режимі реального часу і дозволяє аналізувати стан інформаційної безпеки. І це дає змогу оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі. В середньому, за статистикою Держслужби спеціального зв'язку та захисту інформації (Держспецзв'язку), щонеділі в Україні блокувалось до 50 тисяч кібератак на державні інформаційні ресурси [3].

Слід сказати, що з розвитком технологій а саме, появи штучного інтелекту, виявляти такі явища правоохоронним органам стало значно простіше, однак так само як правоохоронні органи використовують штучний інтелект в цілях захисту та безпеки, шахраї використовують його в цілях незаконного збагачення та наживи. Доречі, термін штучний інтелект широко використовується як в науці так і в повсякденному житті, однак єдиного визначення поняття що ж слід розуміти під штучним інтелектом так і немає. Спроби впорядкувати дану ситуацію можна прослідкувати в науковій праці доктора юридичних наук проф. О.А. Баранова, який дає визначення поняття штучного інтелекту зокрема зазначає: Штучний інтелект – це інтелект, що має штучне походження та імітує (моделює) певну сукупність когнітивних функцій еквівалентних відповідним когнітивним функціям людини, або штучний інтелект це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини [2, с. 45–46].

Передбачається, що з розвитком науки та технологій може з'явитись декілька відмінних фундаментальних підходів до побудови штучного інтелекту, які будуть базуватись на різних принципах створення його матеріальної основи, моделювання метакогнітивних функцій, реалізації алгоритмів імітування окремих когнітивних функцій тощо. Вже сьогодні відомі такі фундаментальні підходи щодо побудови штучного інтелекту:

– комп'ютерний, програмні засоби, швидко обчислювальні алгоритми, математичні методи опису складних динамічних систем та обробки великих даних, обчислювальні ресурси комп'ютерів та суперкомп'ютерів, хмарні технології тощо;

– хімічний із врахуванням математичної подібності між мережами хімічних шляхів і штучними нейронними мережами розроблена загальна теорія щодо нової конструкції на основі низькотемпературної плазми для створення штучного інтелекту, що працює із речовиною,

– біологічний, виявлено можливість проведення універсальних обчислень з формою тривимірної клітинної культури із вираховуванням основних властивостей нейронних мереж у ній, що відкриває перспективи створення біологічного штучного інтелекту,

– біологічний (молекулярний), досягнення у молекулярному програмуванні, біологічних обчисленнях, стовбурових клітинах і органоїдах, редагуванні генів для конкретних розробок і побудові нейронних обчислювальних моделей сприятимуть на основі цих структур створенню біологічного штучного інтелекту [4, с. 143–154].

Як можна прослідкувати, з розвитком штучного інтелекту розвивається також інтелект шахраїв. Злочини у кіберпросторі починають вчинятися із ще більшою витонченістю, філігранністю, а правоохоронним органам кожного разу стає все важче і важче з цим боротися. Це зумовлено в першу чергу тим, що кіберзлочинці, на відміну від правоохоронних органів, необмежені у своїх діях правами нормами чи повноваженнями які визначені законом. На жаль, можемо констатувати що закони України є не настільки гнучким, як кіберзлочинці. Однак й не можемо сказати що держава реагує на ці виклики надто пізно.

Так, з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» ситуація з протидією кіберзлочинам значно покращилася.

Даний Закон не просто визначає технічні параметри захисту інформації, а формує правове підґрунтя для запобігання, виявлення та протидії кіберзлочинності. З погляду сучасної кримінології та правозастосування, ключове значення цього Закону розкривається через кілька ключових аспектів, зокрема з урахуванням останніх масштабних оновлень, Закон безпосередньо впливає на формування стратегії запобігання кіберзлочинності, так званої кримінологічної превенції. У тексті чітко розмежовано поняття, які є базовими для кваліфікації злочинів у кіберсфері. Фокусується увагу правоохоронних органів в першу чергу на виявленні загроз, що в кримінології вважається найбільш ефективним методом нейтралізації злочинності на стадії замаху, або підготовки злочину. Також чітко визначається координаційна архітектура, де кожен суб'єкт виконує свою роль у системі кримінальної юстиції та попередження злочинів. Зокрема встановлюється що:

1. Національна поліція України здійснює безпосередню протидію кіберзлочинності, виявлення та розслідування кіберзлочинів, підвищення обізнаності громадян.

2. Служба безпеки України забезпечує контррозвідувальний захист інтересів держави у кіберсфері, боротьбу з кібертероризмом та кібершпигунством.

3. Міністерство оборони України та Генеральний штаб Збройних Сил України здійснює відсіч кіберагресії у військовій сфері.

4. Держспецзв'язок відповідає за формування та реалізацію державної політики в сфері координації кіберзахисту об'єктів критичної інфраструктури, управління правилами реагування.

5. Національний координаційний центр кібербезпеки (НКЦК) при РНБО забезпечує аналітичну складову, акумулює дані про кіберзагрози, що дозволяє кримінологам прогнозувати тенденції розвитку кіберзлочинності в Україні [6].

Слід сказати, що після початку повномасштабної війни росії проти Українського народу, система кібербезпеки зазнала значної трансформації, що суттєво вплинуло на фіксацію кіберінцидентів як потенційних правопорушень. Зокрема у держорганах та на об'єктах критичної інформаційної інфраструктури запроваджено посилені вимоги до призначення керівників підрозділів кіберзахисту, кандидатури яких погоджуються з установою Держспецзв'язку після перевірки СБУ. Запроваджено посилену відповідальність за неповідомлення або несвоєчасне повідомлення про кіберінциденти. Це мінімізує «латентність» технічних збоїв, які насправді могли бути результатом кримінального втручання.

Для належної роботи правоохоронних органів, критично важливою є норма Закону про взаємодію з приватним сектором, операторами електронних комунікацій та волонтерськими організаціями. Вона створює легальні рамки зокрема для своєчасного отримання цифрових доказів (з урахуванням норм КПК України), блокування джерел кібератак на ранніх етапах, спільного розслідування транскордонних кіберзлочинів.

Важливо відмітити те, що даний Закон діє в синергії з Кримінальним та Кримінально-процесуальним кодексами України що створює організаційно-технічне поле, без якого належним чином кваліфікувати кіберзлочини та кібершахрайства була б значно складніше [6].

Як слушно зазначає А.В. Микитчик, у статті «Заходи запобігання кіберзлочинності в Україні», традиційні підходи та виключно внутрішньодержавні правові заходи не здатні забезпечити ефективну протидію злочинам у віртуальному просторі через специфічні ознаки самої кіберзлочинності (такі як транскордонність, транснаціональність, висока латентність та швидкий динамічний розвиток).

У межах правового підходу, автор пропонує вдосконалення національного законодавства через реалізацію комплексної програми, яка складатиметься з чотирьох взаємопов'язаних рівнів:

1. Гармонізація кримінального законодавства про кіберзлочини. Національні кримінально-правові норми України мають бути уніфіковані та узгоджені з міжнародними стандартами (наприклад, положеннями Будапештської конвенції про кіберзлочинність). Це необхідно для того, щоб правопорушення в інформаційній сфері трактувалися і кваліфікувалися однаково в різних юрисдикціях, що унеможливить ситуації, коли діяння є злочином в одній країні, але залишається безкарним в іншій.

2. Розробка та імплементація процесуальних стандартів розслідування. Оскільки докази в кіберпросторі (цифрові або електронні докази) є специфічними, легко знищуваними та віртуальними, автор наголошує на необхідності імплементації в національне кримінально-процесуальне законодавство міжнародних стандартів. Це стосується процедур збору, фіксації, збереження та перевірки цифрових даних, щоб вони мали належну юридичну силу під час розслідування злочинів у глобальних мережах.

3. Міжнародне співробітництво на оперативному рівні. Законодавство має чітко врегулювати та спростити механізми взаємодії правоохоронних органів різних держав у режимі реального часу. Оскільки кіберзлочинець може перебувати в одній точці планети, а його жертва чи сервери із доказовою базою в іншій, оперативний обмін інформацією між спецпідрозділами є критичним для блокування кібератак та затримання зловмисників.

4. Дієвий механізм вирішення юрисдикційних питань у кіберпросторі. Однією з найбільших правових проблем є визначення того, який саме суд і законодавство якої саме країни мають право розглядати справу, якщо злочин вчинено у віртуальному просторі, що існує поза державними кордонами. Автор пропонує законодавчо закріпити чіткі правові інструменти для врегулювання цих юрисдикційних конфліктів на міжнародному та національному рівнях [7, с. 137–138].

Також, піднімають проблемні питання трансформації кібершахрайства та зростання кіберзлочинності в Україні в умовах воєнного стану співавтори у статті «Кіберзлочинність та кібершахрайство в умовах воєнного стану» Н.В. Сметаніна, Д.О. Пісенко, Т.А. Діброва. Зокрема автори виділяють три напрями боротьби з кіберзлочинністю:

1. Законодавчий (оптимізація відповідальності): Верховна Рада України ухвалила зміни до кримінального кодексу та кримінально процесуального кодексу України, посиливши кримінальну відповідальність за кіберзлочини в умовах воєнного стану.

2. Інформаційний (профілактика): Запуск Національним Банком України та Кіберполіцією масштабних просвітницьких проєктів, створення сервісів для перевірки сайтів на їх справжність.

3. Банківський сектор: Перехід на більш захищені картки (що знижує ризик класичного скімінгу в банкоматах) та впровадження внутрішніх систем запобігання зловживанням.

Автори зазначають, що посилення лише кримінальної відповідальності та санкцій недостатньо. Закликають до масштабного і глибокого кримінологічного дослідження соціальних, економічних та організаційних причин кібершахрайства. Вони наголошують на критичній необхідності постійно підвищувати рівень кібергігієни та інформувати населення про нові витончені методи шахраїв, щоб запобігати злочинам ще на етапі їхнього зародження [8, с. 544–547].

Як можна прослідкувати, єдиного рецепту протидії кіберзлочинності немає, тільки комплексні заходи реалізовані громадськістю та правоохоронними органами можуть здійснити реальний вплив на поширення та протидію такому явищу як кіберзлочинність. Важливу роль у протидії цій групі злочинів відіграє і активна поведінка самої жертви злочину. Так, К.О. Черевко, зазначає, чому громадяни стають жертвами кіберзлочинців, виділяючи кілька ключових факторів уразливості (віктимності), особливо в умовах воєнного стану, це:

1. Вплив воєнного стану та соціально-економічних умов: Зловмисники активно паразитують на гострососціальних проблемах, безпековій та енергетичній ситуаціях. Люди, які перебувають у так званому режимі виживання (зокрема ВПО або ті, хто втратив житло), шукають матеріальну допомогу й стають легкою здобиччю для таргетованої реклами шахраїв. При отриманні інформації про виплати у жертв виникає так зване явище звуження когнітивного фокусу, через що вони не помічають фейкових ресурсів.

2. Психологічний тиск і соціальна інженерія: Сучасне кібершахрайство спирається переважно не на криптографічний злом технічних систем, а в першу чергу на злом людської свідомості. Шахраї використовують тактику штучного дефіциту часу (наприклад, фейкові дзвінки від імені банку про несанкціоноване списання коштів), змушуючи жертву діяти екстрено й необачно.

3. Вікова цифрова нерівність: Люди похилого віку мають високий рівень віктимності. Вони виросли в парадигмі абсолютної довіри до державних інституцій та банків, і автоматично переносять цю довіру на цифровий інтерфейс, маючи при цьому низький рівень цифрової гігієни.

4. Категорії найбільш вразливих груп населення: Внутрішньо переміщені особи (ВПО), пенсіонери, мешканці прифронтових регіонів, особи з низьким рівнем життя, а також молодь і підприємці, які шукають швидкі способи заробітку чи інвестицій через втрату доходу.

Автор також наводить типологію поширених шахрайських схем, кожна з яких орієнтована на певну віктимну групу, зокрема:

1. Фішингові кампанії (копіювання офіційних сайтів банків, служб доставки для отримання даних).

2. Соціальна інженерія (вішинг) телефонні дзвінки з банку для виманювання паролів та SMS кодів.

3. Компрометація аккаунтів, злам месенджерів та розсилка контактним особам прохань терміново позичити гроші.

4. Інвестиційне та криптовалютне шахрайство (псевдотрейдинг).

5. Фейкові маркетплейси та збори коштів. Псевдоволонтерські збори на ЗСУ, евакуацію, або продаж дефіцитних товарів, наприклад, генераторів під час блекаутів [9, с. 151–154].

Висновки. Сучасне кібершахрайство в Україні остаточно трансформувалося з суто технічної проблеми (зламу комп'ютерних систем) у складний психосоціальний феномен, побудований на соціальній інженерії та зломі людської свідомості. Умови воєнного стану, стрес, внутрішнє переміщення та виникнення нових гостросоціальних потреб значно підвищили рівень цифрової віктимності населення. Найбільш уразливими групами залишаються внутрішньо переміщені особи та люди похилого віку, які через низьку цифрову гігієну або звуження когнітивного фокусу в кризових ситуаціях стають жертвами витончених фішингових та вішингових атак, що подекуди вже підсилюються технологіями штучного інтелекту.

З іншого боку, державна система протидії продемонструвала значну еволюцію. Завдяки базовому законодавству сформовано чітку архітектуру кібербезпеки за участю Кіберполіції, СБУ, Держспецзв'язку та НКЦК при РНБО. Створення спеціалізованих ситуаційних центрів (зокрема за підтримки НАТО) та посилення вимог до захисту критичної інфраструктури дозволило ефективно стримувати масові технічні загрози. Проте класичні правоохоронні заходи виявляються обмеженими через транскордонний характер кіберзлочинів та надзвичайну гнучкість шахраїв, які не обмежені правовими нормами.

Ключ до ефективної протидії кіберзлочинам, як думається, лежить виключно в площині комплексної взаємодії:

1. На державному та міжнародному рівнях, необхідна подальша гармонізація українського законодавства з міжнародними стандартами (Будапештська конвенція), впровадження чітких процесуальних норм для електронних доказів та спрощення транскордонної взаємодії правоохоронців у режимі 24/7.

2. На технологічному рівні, продовження впровадження банками та мобільними операторами систем боротьби та виявлення кіберзлочинів.

3. На рівні громадянського суспільства та освіти, критично важливим є перехід від масового інформування до гнучких превентивних інструментів протидії кіберзлочинам. Унікальним прикладом цього є трансформація юридичних клінік при закладах вищої освіти, таких як Університет Короля Данила, що в Івано-Франківську.

Список літератури:

1. Безпека у кіберпросторі. Шлях України до НАТО. *Центр воєнної політики та правових досліджень*. URL: https://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1126-bezpeka-u-kiberprostori

2. Баранов О. А. Визначення терміну штучний інтелект. *Інформація і право*. 2023. № 1 (44). URL: https://orcid.org/0000-0003-3233-6687.

3. Lin L., Keidar M. Artificial Intelligence without Digital Computers: Programming Matter at a Molecular Scale. *Advanced Intelligent Systems*. 2022. Vol. 4, no. 12. DOI: https://doi.org/10.1002/aisy.202200124.

4. Bull L., Uroukov I. S. Towards Neuronal Computing: Simple Creation of Two Logic Functions in 3D Cell Cultures using Multi-Electrode Arrays. *International Journal of Unconventional Computing*. 2008. Vol. 4. P. 143–154.

5. Angeri H. Future of AI is Biological. *Towards Data Science*. 2019. URL: https://towardsdatascience.com/future-of-ai-is-biological-b512d6c40fe6 (дата звернення: 01.03.2023).

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

7. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні. *Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку* : зб. тез доповідей міжнар. наук.-практ. конф. до 25-річчя ХНУВС (м. Харків, 18 квітня 2019 р.). Харків : ХНУВС ; Кримінологічна асоціація України, 2019. С. 137–138.

8. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С. 544–547. DOI: https://doi.org/10.32782/2524-0374/2022-11/132.

9. Черевко К. О. Віктимологічний аспект діяльності юридичних клінік. *Журнал правових часописів Донецького національного університету імені Василя Стуса*. 2026. Т. 2, № 1. Ст. 18. DOI: https://doi.org/10.31558/2786-5835.2026.1.2.18.

Hromko V. Ya. CRIMINOLOGICAL CHARACTERISTICS AND PREVENTION OF CYBERFRAUD IN UKRAINE: CURRENT TRENDS AND VICTIMOLOGICAL ASPECT

The article examines the features and key trends of the transformation of modern cybercrime in Ukraine in the specific conditions of the legal regime of martial law. It is stated that the rapid digitalization of all spheres of social relations, the forced transition of business and state institutions to a remote format, as well as mass migration of the population have led to the systemic growth, unprecedented flexibility and technological evolution of cyberfraud. The article proposes the definition of the latest determinants of cybercrime in wartime and the development of active countermeasures. The research used methods of system-structural analysis, comparative law and criminological methods. The psychological mechanisms of influence of perpetrators on the victim are analyzed. It is proven that modern criminal strategies are based on the psycho-emotional vulnerability of citizens, their permanent stress, a sense of fear, but at the same time on patriotism, the desire to help the Armed Forces of Ukraine and acute social problems of today (payment of material assistance, search for missing persons, evacuation, etc.). Special attention is paid to the factor of technological complication of criminal schemes through the integration of artificial intelligence tools, in particular the generation of deepfakes (audio and video imitations), advanced spoofing technologies (number and address substitution) and highly targeted phishing. It is emphasized that the automation of cyberattacks significantly increases the level of digital victimization of the population, making traditional methods of fraud recognition ineffective. As a result of the study, it is substantiated that an exclusively punitive approach and increased criminal liability demonstrate limited effectiveness, since cybercrime is cross-border and highly anonymous. The urgent need for the development of new flexible mechanisms of criminological prevention is proven. They should be based on a comprehensive study of the causes of cyber fraud, increasing the level of digital and media literacy of citizens, as well as on synergistic interaction between state, law enforcement agencies, private IT and banking sectors and international institutions. A conceptual model for creating a holistic, dynamic and adaptive system for protecting citizens in cyberspace, capable of responding to threats in real time, is proposed.

Keywords: *cyber fraud, spoofing, criminal process, criminal law, phishing, digitalization, criminology.*

Дата першого надходження статті до видання: 17.07.2026
Дата прийняття статті до друку після рецензування: 31.07.2026
Дата публікації (оприлюднення) статті: 10.09.2026