**УДК 343.85:004:347.96**
**DOI 10.31558/2786-5835.2026.1.2.18**

***Черевко Кирило Олександрович,***
*кандидат юридичних наук, доцент, професор кафедри*
*кримінального права і кримінології ННІ № 1*
*Харківського національного університету внутрішніх справ*
*ORCID: https://orcid.org/0000-0002-3384-8388*

# ЮРИДИЧНА КЛІНІКА ЯК СУБ'ЄКТ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

*У статті досліджено роль та місце юридичних клінік закладів вищої освіти зі специфічними умовами навчання в загальній системі суб'єктів запобігання кіберзлочинності. Проаналізовано віктимологічний аспект кібершахрайства в умовах воєнного стану та визначено потенціал клінічної юридичної освіти як інструменту спеціально-кримінологічного запобігання. Особливу увагу приділено інтеграції спеціалізованих знань майбутніх кіберполіцейських у правопросвітницьку діяльність юридичної клініки. Запропоновано інноваційні форми взаємодії клініцистів із вразливими верствами населення з метою зниження рівня їхньої цифрової віктимізації.*

***Ключові слова:*** *юридична клініка, кіберзлочинність, кримінологічне запобігання, віктимність, юридична освіта, ХНУВС, кібершахрайство.*

**Постановка проблеми.** Протягом останніх років стрімка цифровізація суспільних відносин визначила ключові напрями розвитку української держави, що призвело до трансформації структури надання державних послуг. Впровадження у життя концепції «Держава в смартфоні» [1] призвела до розвитку системи електронних сервісів, активного переходу банківського сектору до онлайн-формату та цифровізації документообігу, що не в останню чергу забезпечило підтримку функціонування держави, особливо в умовах відсічі повномасштабній збройній агресії Російської Федерації. Проте ця «міграція» соціально-економічних процесів у цифровий вимір оголила системні вразливості, пов'язані з недостатнім рівнем цифрової грамотності великої частини населення.

Серед іншого звертає на себе увагу та обставин, що, за даними Офісу Генерального прокурора, спостерігається тенденція до зростання кількості зареєстрованих кримінальних правопорушень, передбачених ст. 361 КК України, порівняно з попереднім періодом [2]. Так, у 2025 році підрозділами Національної поліції було офіційно зареєстровано 26,9 тис. кіберзлочинів. До Департаменту кіберполіції надійшло понад 63,4 тис. звернень громадян [3]. Величезна різниця між зверненнями (63 тис.) та реєстрацією справ (27 тис.) свідчить про високу латентність та необхідність правової допомоги імовірним потерпілим щодо кваліфікації злочину.

Загальні задокументовані збитки громадян і компаній щороку обчислюються сотнями мільйонів гривень [4]. Традиційні методи поліцейської превенції

та реагування демонструють обмеженість у протидії кіберзлочинності. Правоохоронна система, попри значний прогрес у розбудові підрозділів кіберполіції, стикається з колосальним навантаженням. Класичні механізми масової комунікації правоохоронних органів (публікації на офіційних сайтах, брифінги, стандартні застереження) часто не досягають своєї мети, оскільки не охоплюють найбільш вразливі групи: внутрішньо переміщених осіб (далі – ВПО), осіб похилого віку, мешканців прифронтових регіонів, осіб з низьким рівнем життя. Саме ці категорії найчастіше стають жертвами шахраїв.

У зв'язку з обмеженістю звичайних поліцейських заходів у боротьбі з кіберзлочинністю виникає потреба у впровадженні нових механізмів запобігання. Таким інструментом може виступати інститут юридичних клінік при закладах вищої освіти. Юридична клініка, яка вважається переважно місцем здобуття практичного досвіду здобувачами вищої освіти, сьогодні може бути ефективним інструментом «soft power» та профілактичної, кримінально-превентивної комунікації.

**Аналіз останніх досліджень та публікацій.** Проблематика детермінації та запобігання злочинності загалом і кіберзлочинності зокрема перебуває у центрі постійної уваги вітчизняних та зарубіжних науковців. Теоретико-методологічні основи закладені у фундаментальних працях О. М. Бандурки, В. С. Батиргареєвої, В. В. Голіни, О. М. Джужи, А. П. Закалюка, С. Ф. Денисова, Ю. В. Орлова, В. П. Поповича, В. О. Тулякова та інших вчених.

Аналіз останніх публікацій засвідчує, що вітчизняна наукова думка активно адаптується до нових викликів. Зокрема, дослідниками встановлена вкрай несприятлива тенденція до інтенсифікації кіберзлочинності протягом 2015–2024 років, яка набула ознак системної кризи з істотним приростом після початку повномасштабної російської збройної агресії [5, с. 51].

Паралельно з розвитком кримінології та наукових досліджень про кіберзлочини в Україні активно розвивається концепція юридичних клінік як одного з найважливіших елементів практичної підготовки майбутніх юристів, забезпечення доступу соціально незахищених верств населення до правової допомоги. Сучасні дослідження в цій сфері направлені на впровадженні нових методик правової просвіти, зокрема за програмою «Street Law», яка курується Асоціацією юридичних клінік України (далі – АЮКУ) у партнерстві з громадським сектором [6]. Дослідники наголошують на тому, що правові проблеми вразливих груп населення часто виникають через дискримінацію або специфічні життєві обставини, що вимагає формування єдиних, стандартизованих підходів у наданні безоплатної правової допомоги [6].

Комплексний аналіз наукових праць (О. Шевчук, І. Юркевич [7], Н. Міловська [8]) та звітів АЮКУ[9] дає змогу констатувати, що інститут юридичних клінік в Україні перебуває на етапі глибокої трансформації.

**Формулювання цілей статті.** Основна мета статті полягає у розробці концептуальних засад функціонування юридичних клінік як суб'єктів запобігання кіберзлочинності та розробці, на цій підставі, практичних рекомендацій щодо їх залучення до превентивної діяльності в умовах цифровізації суспільного життя. Для досягнення цієї мети визначено такі завдання:

1. Здійснити кримінологічну характеристику сучасних проявів кібершахрайства.

2. Розкрити зміст та специфіку реалізації консультаційної та просвітницької функцій юридичної клініки в контексті реагування на кіберзагрози.

3. Проаналізувати та запропонувати інноваційні форми роботи юридичної клініки на прикладі Харківського національного університету внутрішніх справ.

4. Запропонувати інноваційні форми правопросвітницької діяльності та розробити алгоритм взаємодії клініцистів із потерпілими від кібершахрайств.

**Виклад основного матеріалу.** Офіційна статистика, дані Департаменту кіберполіції Національної поліції України свідчать про велику волатильність кіберзлочинного середовища, яке характеризується швидкою адаптацією до дій правоохоронців. Аналіз кількісних показників демонструє складну динаміку. Так, у 2024 році в Україні було відкрито 64 978 кримінальних проваджень щодо шахрайства, що засвідчило зниження на 21 %, порівняно з 2023 роком, який відзначився абсолютним антирекордом у 82 609 відкритих справ [10]. Однак це тимчасове статистичне «просідання» не треба трактувати як стратегічну перемогу над кіберзлочинами. Вже у 2025 році зафіксовано суттєве зростання кількості кіберзлочинів [11].

Згідно з офіційними звітами Державної служби спеціального зв'язку та захисту інформації України, протягом 2023–2024 років фіксується ускладнення кіберзагроз, серед яких домінують DDoS-атаки, використання програм-вимагачів та цілеспрямована компрометація внутрішніх мереж установ) [12]. Зловмисники дедалі частіше використовують незаконний обіг персональних даних – бази даних громадян, отримані внаслідок зламів або інсайдерських витоків, реалізуються на тіньових форумах і в подальшому застосовуються для високоточних, таргетованих шахрайських кампаній або шантажу [13].

З метою впорядкування розуміння ризиків доцільно представити структуровану типологію найпоширеніших схем кіберзлочинів.

**Фішингові кампанії** – це створення сайтів, що візуально повністю копіюють офіційні ресурси (банки, служби доставки тощо). Найбільш поширена група потерпілих – ВПО, особи похилого віку, особи, які перебувають у пошуку державної чи іншої соціальної матеріальної допомоги тощо [14, с. 83].

**Соціальна інженерія** (в тому числі дзвінки з банківських установ або вішинг) – це практика здійснення цільових телефонних дзвінків із представленням

себе як співробітника служби безпеки фінансової організації. Використовуючи психологічні методи впливу, зловмисники отримують доступ до SMS-кодів і паролів клієнтів для несанкціонованого входу до систем онлайн-банкінгу. Відзначається високий рівень поширеності серед осіб старшого та похилого віку, а також громадян із *низьким рівнем базової цифрової фінансової грамотності* [15, с. 126].

**Компрометація акаунтів** – це викрадення доступу до месенджерів (Telegram, Viber тощо) шляхом розсилки підроблених повідомлень від фейкових «адміністраторів» онлайн-майданчиків. Згодом від імені зламаного профілю жертви розсилаються масові прохання терміново позичити кошти [16].

**Інвестиційне та криптовалютне шахрайство** – це залучення осіб до фіктивних інвестиційних платформ або псевдотрейдингових сервісів. Основна віктимна група – це молодь, підприємці та особи, які втратили основне джерело доходу внаслідок воєнних дій і шукають швидкі способи фінансового збагачення [17].

**Фейкові маркетплейси та збори коштів** – це експлуатація тематики воєнного часу, публікація фейкових зборів на потреби Збройних Сил України, евакуацію, лікування поранених, а також продаж неіснуючих дефіцитних товарів (наприклад, генераторів під час блекаутів) з вимогою повної передоплати [18, с. 149].

Як слушно випливає з досліджень проблематики соціальної інженерії (В. А. Світличний), сучасне кібершахрайство спирається не стільки на складний криптографічний злом систем (хоча технологічний аспект, пов'язаний зі статтями 361, 362 КК України, залишається домінуючим), скільки на злом людської свідомості – *соціальну інженерію* [19, с. 59].

По-перше, як засвідчують аналітичні дані Департаменту кіберполіції НПУ та дослідження вітчизняних науковців-кримінологів (В. С. Батиргареєва, О. М. Литвинов), зловмисники паразитують на гостросоціальних проблемах та кризових явищах. Люди шукають матеріальну допомогу або намагаються вирішити проблеми, спричинені енергетичною чи безпековою ситуацією в країні, і натрапляють на таргетовану рекламу шахраїв [20, с. 112]. Внутрішньо переміщені особи чи ті, хто втратив житло, часто діють у режимі «виживання». Під час отримання інформації щодо виплат від міжнародних організацій (зокрема ООН або Червоного Хреста) через соціальні мережі у таких осіб спостерігається явище звуження когнітивного фокусу. Внаслідок цього жертва може не звернути увагу на додатковий символ у доменному імені шахрайського сайта через його схожість з офіційним [21, с. 219].

По-друге, шахраї майстерно використовують тактику створення штучного дефіциту часу та індукування паніки. Під час телефонних дзвінків від фіктивних «співробітників служби безпеки банку» потерпілому повідомляють про нібито несанкціоноване списання коштів, яке відбувається просто зараз. Людина опи-

няється в ситуації ухвалення екстреного рішення. Про це вказали в своїй статті Френк Стояно та Пол Вілсон, які вказали на тиск часу, щоб зробити важливий вибір, шахраї змушують нас повірити, що ми повинні діяти швидко або втратити можливість [22, с. 77].

Вікова цифрова нерівність є самостійним фактором з високим рівнем віктимогенності. Люди похилого віку, які виросли в парадигмі абсолютної довіри до державних інституцій, друкованого слова та банківських службовців, механічно переносять цей рівень довіри на цифровий інтерфейс [23]. Низький рівень цифрової гігієни пенсіонерів робить їх беззахисними перед таргетованими кібератаками, а традиційні поліцейські превентивні дії зазвичай не здатні змінити сталі патерни їхньої поведінки.

Враховуючи зазначену вище кримінологічну та віктимологічну характеристику, юридична клініка закладу вищої освіти стає незамінним інструментом у системі превенції. У сфері протидії високотехнологічним загрозам функціональні можливості юридичної клініки значно розширюються, охоплюючи два основні напрями: консультаційний та правопросвітницький [24].

Консультації для постраждалих від кіберзлочину в юридичній клініці можуть бути схожі на екстрену допомогу. Головне завдання – стабілізувати емоційний стан клієнта і швидко обмежити збитки. Протокол реагування може включати допомогу в негайному блокуванні рахунків, карток, звернення до банку для зупинки транзакцій. Повернення контролю над зламаними обліковими записами, зміна паролів, двофакторна автентифікація. Навчання збереженню цифрових доказів, а саме скриншоти, збереження чеків, даних криптогаманців тощо. Юридична клініка може надавати правоохоронцям структурований пакет документів із первинною доказовою базою, що спрощує роботу кіберполіції [25, с. 10].

Юридична клініка через правопросвітницьку діяльність може формулювати культуру цифрової безпеки за допомогою алгоритмів цифрової гігієни. Здобувачі вищої освіти можуть адаптувати юридичну та технічну термінологію для широкої аудиторії, доводячи, що кібербезпека стосується кожного, а не лише ІТ-фахівців.

Ефективність діяльності юридичної клініки має властивість до специфікації, якщо вона розгорнута на базі закладу вищої освіти зі специфічними умовами навчання в системі МВС, як, наприклад, у Харківському національному університеті внутрішніх справ (далі – ХНУВС). Специфіка діяльності ХНУВС полягає в тому, що він здійснює підготовку фахівців різних профілів: від цивільних юристів, психологів, які мають спеціальні звання поліції. Інтеграція цих напрямів у межах єдиної платформи юридичної клініки генерує унікальні інноваційні форми правозахисної та превентивної роботи.

Так, зокрема науково-педагогічний склад та здобувачі освіти навчально-наукового інституту № 4 (підготовки фахівців з інформаційно-аналітичного за-

безпечення та кібербезпеки Національної поліції України) ХНУВС володіють передовими технічними та правничими компетенціями, опановують інноваційні інструменти, зокрема хмарну платформу інтерактивного навчання з кібербезпеки RangeForce, що дає їм змогу тренувати навички реагування на кіберінциденти у реальному часі та отримувати відповідні сертифікати, які підтверджують їхній високий фаховий рівень [26]. До того ж створено та забезпечено щодобове функціонування кіберцентру, до функціонування якого безпосередньо залучені курсанти. Кіберцентр здійснює моніторинг цифрового середовища на предмет виявлення, нейтралізації або забезпечення вчасного реагування на кіберзагрози для національної безпеки та/або ризиків вчинення ординарних кіберзлочинів. Використання курсантами цього досвіду під час роботи у юридичній клініці дає змогу підвищити кримінально-превентивний функціонал останньої за напрямом запобігання кіберзлочинам.

Окремим, соціально відповідальним напрямом інноваційної роботи є подолання бар'єрів цифрової інклюзії серед осіб похилого віку. Пенсіонери часто відчувають страх перед сучасними смартфонами, що робить їх повністю залежними від сторонньої допомоги або легкою здобиччю для соціальної інженерії. Це прямо виходить з офіційних державних ініціатив та соціологічних звітів, які фіксують проблему «цифрового розриву» серед людей похилого віку [27].

Тому юридичні клініки можуть вийти за межі суто «соціального» проєкту і стали повноцінним інструментом практико-орієнтованого навчання і кримінально-превентивної діяльності. Сучасний юрист повинен володіти не лише знаннями законів, а й цифровими навичками (робота з реєстрами, системами електронного документообігу, онлайн-консультування). Впровадження цифрових технологій у діяльність юридичних клінік трансформує їх з традиційних осередків правової допомоги у високотехнологічні майданчики, де студенти здобувають компетентності, критично необхідні для роботи в умовах сучасного ринку юридичних послуг [7].

**Висновки.** Узагальнюючи результати дослідження, можна стверджувати, що зростання кіберзлочинності в Україні демонструє обмежену ефективність традиційної моделі поліцейської превенції під час її самостійного застосування. Зловмисники використовують психологічні вразливості населення, критичний стан суспільства, а також тематику державних виплат, волонтерських зборів і інвестиційних проєктів для шахрайства. Це обумовлює необхідність впровадження нових гнучких механізмів попередження кіберзлочинів.

Юридична клініка сучасного закладу вищої освіти повинна трансформуватися з вузькоспеціалізованого майданчика для відпрацювання практичних навичок здобувачів вищої освіти на потужний суб'єкт спеціальної кримінологічної превенції. Клініка може стати ідеальним каналом комунікації між державою та

найбільш вразливими групами населення, забезпечуючи їх оперативною консультаційною підтримкою у кризових ситуаціях та реалізуючи стратегію «Prevention through Education» [28; 29].

Поширення досвіду інноваційних форм роботи на базі закладів вищої освіти зі специфічними умовами навчання, як-от Харківський національний університет внутрішніх справ, здатне підвищити ефективність діяльності юридичних клінік за напрямом запобігання кіберзлочинам. Інтеграція спеціальних технічних знань курсантів, які використовують передові платформи кібернавчання (зокрема RangeForce) [30, с. 12] із правозахисним та педагогічним потенціалом студентів-клініцистів дає змогу створити унікальну гібридну модель захисту прав людини в цифровому вимірі. Юридична клініка може бути оптимальним суб'єктом спеціальної кримінологічної превенції кіберзлочинів, оскільки її діяльність спрямована на підвищення правосвідомості та критичного мислення громадян, що є єдиним дієвим запобіжником проти різних кіберзагроз.

**Список використаних джерел**


1. Зеленський В. О. Виступ Президента України на форумі інтернет-діячів iForum-2019 (м. Київ, 23 травня 2019 р.). *Офіційне інтернет-представництво Президента України*. URL: https://www.president.gov.ua/news/vystup-prezydenta-ukrayiny-volodymyra-zelenskoho-na-forumi-55561
2. Про стан злочинності в Україні за січень–грудень 2025 року: статистична інформація. *Офіс Генерального прокурора*. URL: https://gp.gov.ua/ua/posts/statistika
3. Аналітичний огляд кіберзагроз в Україні за 2025 рік. *CERT-UA: Державний центр кіберзахисту*. URL: https://cert.gov.ua/reports
4. Щорічний звіт про результати діяльності Департаменту кіберполіції Національної поліції України за 2025 рік. *Департамент кіберполіції Національної поліції України*. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/
5. Галушко П. П. Кримінологічна характеристика та протидія кіберзлочинності в Україні в умовах війни: дис. … д-ра філос.: 12.00.08. Харків, 2025. 236 с.
6. Street Law як простір навчання та дії: АЮКУ представила свій досвід на Всесвітній конференції GAJE. *Асоціація юридичних клінік України*. URL: https://legalclinics.in.ua/street-law-yak-prostir-navchannya-ta-diyi-ayuku-predstavyla-cvij-dosvid-na-vsesvitnij-konferentsiyi-gaje/
7. Шевчук О., Юркевич І. Юридичні клініки в механізмі дуальної освіти: аналіз результатів педагогічного експерименту. *Актуальні проблеми правознавства.* 2021. Вип. 2. С. 69–76.
8. Міловська Н. В. Юридичні клініки у системі практичної підготовки фахівців у галузі права. *Нове українське право*. 2021. № 4. С. 144–150.
9. Форум юридичних клінік 2025: про виклики, розвиток і майбутні кроки спільноти. *Асоціація юридичних клінік України*. 2025. URL: https://legalclinics.in.ua/forum-yurydychnyh-klinik-2025-pro-vyklyky-rozvytok-i-majbutni-kroky-spilnoty/
10. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування у 2023 році: стат. звіт. *Офіс Генерального прокурора*. URL: https://www.gp.gov.ua/ua/posts/2013-2024-roki-pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-do-sudovogo-rozsliduvannya
11. Про стан злочинності в Україні за січень–грудень 2025 року: статистична інформація. *Офіс Генерального прокурора*. URL: https://gp.gov.ua/ua/posts/statistika

12. Російські кібероперації: аналітика за І півріччя 2024 року: аналітичний звіт. *Державна служба спеціального зв'язку та захисту інформації України*. 2024. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=68769
13. ENISA Threat Landscape 2023. *European Union Agency for Cybersecurity*. 2023. 153 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
14. Черевко К. О., Пашнєв Д. В. Кібератаки на об'єкти критичноїінфраструктури в умовах ведення війни: ключові поняття. *Вісник Кримінологічної асоціації України.* 2024. № 1(31). С. 72–91. DOI: DOI: https://doi.org/10.32631/vca.2024.1.15
15. Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України.* 2023. № 1(28). С. 124–133. DOI: https://doi.org/10.32631/vca.2023.1.10
16. Черевко К. О. Загальна характеристика кримінальних правопорушень, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем (кіберзлочинів): текст лекції з навчальної дисципліни «Кваліфікація кіберзлочинів» / Харківський національний університет внутрішніх справ. Харків, 2023. 15 с. URL: https://nm2.univd.edu.ua/download/96737
17. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні. *Кримінально-правові та кримінологічні засоби протидії злочинам протигромадської безпеки та публічного порядку:* зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків). Харків: ХНУВС, 2019. С. 137–138. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf
18. Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика: монографія. Одеса: Видавництво «Юридика», 2024. 242 с.
19. Світличний В. А. Деякі особливості атак хакерів із використанням соціальної інженерії. *Застосування інформаційних технологій у правоохоронній діяльності:* матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків: ХНУВС, 2023. С. 53–60.
20. Батиргареєва В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право.* 2020. № 1. С. 110–119. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_1_13
21. Кришевич О. В. Кримінальна відповідальність за шахрайство: доктрина, законодавство, практика: дис. … д-ра юрид. наук: 12.00.08. Хмельницький, 2025. С. 457. URL: https://nadpsu.edu.ua/wp-content/uploads/2025/08/dis_kryshevych.pdf
22. Stajano F., Wilson P. Understanding scam victims: seven principles for systems security. *Communications of the ACM*. 2011. Vol. 54, № 3. P. 70–75.
23. Манжай О. В., Кожем'якіна О. В. Соціальна інженерія як спосіб вчинення кіберзлочинів: кримінологічний та психологічний аспекти. *Право і безпека*. 2021. № 2. С. 88–95.
24. Типове положення про юридичну клініку закладу вищої освіти України: Наказ Міністерства освіти і науки України від 03.08.2006 № 592. URL: https://zakon.rada.gov.ua/laws/show/z0956-06#Text
25. Швець Д. В. Стратегічні напрямки використання новітніх технологій цифрового світу в попередженні злочинів. *Застосування інформаційних технологій у діяльності правоохоронних органів*: зб. матеріалів круглого столу (09 грудня 2020 р., м. Харків) / МВС України, Харк. нац. ун-т внутр. справ. Харків: ХНУВС, 2020. С. 8–10. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/fd754668-dd09-4989-9b83-63a4deb5748e/content
26. Курсанти факультету № 4 опановують хмарну платформу інтерактивного навчання з кібербезпеки RangeForce. *Харківський національний університет внутрішніх справ.* URL: https://univd.edu.ua/uk/news/17141
27. Платформа Дія.Освіта. *Міністерство цифрової трансформації України.* URL: https://osvita.diia.gov.ua/

28. Ciorbaru A. N. Crime Prevention Through Education. *SEA: Practical Application of Science*. 2018. Vol. VI, iss. 16. P. 115–119.
29. Lochner L., Moretti E. The Effect of Education on Crime: Evidence from Prison Inmates, Arrests, and Self-Reports. *American Economic Review*. 2004. Vol. 94, № 1. P. 155–189.
30. Ворона М. С. Створення системи інтерактивного навчання з кібербезпеки з використанням симуляційних середовищ: робота на здобуття кваліфікаційного ступеня магістра: спец. 125 – кібербезпека та захист інформації / наук. кер. М. В. Деркач. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2024. 85 с.

***Kyrylo Cherevko. Legal Clinic as a Cybercrime Prevention Entity***

*The rapid digitalization of society, significantly accelerated by the conditions of the ongoing martial law in Ukraine, has led to a proportional increase in the scale and complexity of cybercrime. Under these unprecedented circumstances, the state must utilize all available institutional mechanisms to protect citizens in cyberspace. This article thoroughly examines the role and place of legal clinics operating within higher education institutions with specific learning conditions–particularly the Kharkiv National University of Internal Affairs (KhNUIA) – within the comprehensive system of cybercrime prevention entities. The author provides a detailed analysis of the victimological aspect of cyber fraud committed during martial law. It is emphasized that the population's vulnerability has drastically increased due to psychological stress, internal displacement, and a general lack of digital literacy, making citizens highly susceptible to phishing attacks, fake volunteer fundraisers, and financial scams.*

*Consequently, the study highlights the immense potential of clinical legal education as an effective, community-oriented tool for special criminological prevention. Particular attention is focused on the practical integration of the specialized knowledge of future cyberpolice officers into the legal awareness and advisory activities of the legal clinic. Engaging specialized cadets in direct consultations fulfills a vital dual function: providing accessible legal assistance to victims of cyber offenses while simultaneously reinforcing the practical competencies of future law enforcement personnel. Furthermore, the article proposes a series of innovative forms of interaction between clinicians and the most vulnerable segments of the population. These initiatives include targeted digital hygiene workshops, step-by-step algorithms for identifying cyber threats, and interactive legal education campaigns. The systematic application of these measures aims to significantly reduce the level of digital victimization, foster public trust in the police, and enhance national cybersecurity resilience.*

***Keywords:*** *legal clinic, cybercrime, criminological prevention, victimhood, legal education, KhNUIA, digital hygiene.*

*Дата першого надходження статті до видання: 19.04.2026 р.*
*Дата прийняття статті до друку після рецензування: 29.04.2026 р.*