УДК 343.4:[342.7:004]](477+100)
DOI: 10.21564/2414-990X.173.361287

Національний та іноземний досвід кримінально-правового захисту цифрових прав особи

Артем Ігорович Шеруда*
Національний юридичний університет імені Ярослава Мудрого, Харків, Україна
**e-mail: a.i.sheruda@nlu.edu.ua*

Анотація
Актуальність дослідження зумовлено стрімкими процесами глобалізації, цифровізацією суспільних відносин, розвитком штучного інтелекту та появою нового об'єкта кримінально-правового регулювання – цифрових прав особи. Метою статті є аналіз національного та іноземного досвіду кримінально-правового захисту цифрових прав особи та з'ясування особливостей їх охорони. Методологія дослідження включає формально-юридичний, порівняльно-правовий, аналітичний і системно-структурний методи. Встановлено, що цифрові права особи є об'єктом еволюції традиційного права на приватність, таємницю кореспонденції та захист персональних даних. Констатовано, що кримінальне законодавство України вже має положення, які спрямовані на охорону цифрових прав, однак ці норми захищають їх опосередковано і не визначають цифрові свободи як окремий об'єкт регулювання. З'ясовано, що Будапештська конвенція, акти права Європейського Союзу, практика Європейського суду з прав людини як джерело національного права, а також іноземні підходи до регулювання цифрових прав мають важливе значення для формування відповідної державної політики. Доведено, що європейська модель будується на ризикоорієнтованому підході, американська – на прагматичному, а українська модель має заборонно-регуляторний характер. Перспективи подальших досліджень полягають в уточненні переліку цифрових прав та їх визначенні як самостійний об'єкт кримінально-правової охорони поряд із модифікацією кримінального законодавства відповідно до викликів гібридної війни, розвитку штучного інтелекту, кіберзагроз і цифровізації.

Ключові слова: кримінальне право; кримінальна відповідальність; кіберзлочин; кримінальна політика; штучний інтелект.

National and Foreign Experience in the Criminal-Legal Protection of an Individual's Digital Rights

Artem I. Sheruda*
Yaroslav Mudryi National Law University,
Kharkiv, Ukraine
**e-mail: a.i.sheruda@nlu.edu.ua*

Abstract
The relevance of the study is determined by rapid globalization, the digitalization of social relations, the development of artificial intelligence, and the emergence of a new object of criminal law regulation, namely the digital rights of the individual. The purpose of the article is to define the concept of "digital rights of the individual" and the body of these freedoms as an object of criminal law protection, as well as to clarify the specific features of their protection in the national and international dimensions. The research methodology includes formal legal, comparative legal, analytical, and systemic-structural methods. It has been established that the digital rights of the individual have evolved from the traditional rights to privacy, secrecy of correspondence, and protection of personal data. It has been found that the criminal legislation of Ukraine already contains provisions aimed at protecting digital rights; however, these norms protect them only indirectly and do not define digital freedoms as a separate object of legal regulation. It has been clarified that the Budapest Convention, acts of European Union law, the case law of the European Court of Human Rights as a source of national law, as well as foreign approaches to the regulation of digital rights, are of considerable importance for the formation of policies concerning this object. It has been proved that the European model is based on a risk-oriented approach, the American model on a pragmatic approach, while the Ukrainian model has a prohibitive-regulatory character. Prospects for further research are connected with clarifying the list of digital rights, distinguishing them as a separate object of criminal law protection, and modifying criminal legislation in accordance with the challenges of hybrid warfare, the development of artificial intelligence, cyber threats, and digitalization.

Keywords: criminal law; criminal liability; cybercrime; criminal policy; artificial intelligence.

Вступ

Інтенсивний розвиток цифрових процесів та інформаційних технологій сьогодні свідчить про те, що диджиталізація є не лише технічним процесом, а й ключовим чинником модернізації національної правової системи. Розвиток електронних комунікацій, використання інформаційно-комунікаційних технологій на високому рівні, виникнення публічних та приватних застосунків і сервісів, прогрес у сфері штучного інтелекту й автоматизованих систем зумовлюють появу нового об'єкта правового регулювання – цифрових прав людини. Вони охоплюють класичні права і свободи, які закріплені на консти-

туційному рівні та у спеціальному законодавстві, й нові сформовані свободи, які пов'язані з доступом до інтернету, захистом цифрової активності особи, її ідентифікації, персональних даних, безпечного користування інтернетом і цифровим середовищем. Варто додати також свободу вираження поглядів у цифровому середовищі та захист від свавільного втручання державних органів влади у цифрову активність особи. Тому питання кримінально-правової охорони цифрових прав особи є особливо актуальним як для України, так і світової спільноти.

Україна активно впроваджує електронні послуги та електронне урядування в контексті гармонізації законодавства з правом Європейського Союзу, що, з одного боку, є позитивною тенденцією. З іншого боку, цифрове середовище, розвиток якого сягнув такого рівня, стає простором для нових кримінальних викликів: кібератак, несанкціонованого викриття інформації, втручання в роботу автоматизованих систем, брак конфіденційності і фішингу. Об'єктом аналізу також є цифрові права як елемент основоположних прав та свобод. Хоча вони й закріплені на конституційному рівні, їхнє правове регулювання досі є ситуативним і фрагментарним. Дослідник І. В. Захарчук зазначає, що кримінально-правова охорона цифрових прав особи, що вже охоплює інформаційну сферу і національну безпеку, потребує детального переосмислення в контексті цифрових свобод особи як окремого об'єкта кримінального права [1, с. 270].

Стан наукової розробленості цієї проблематики демонструє, що українські науковці вже здійснюють переосмислення інформаційної безпеки та адаптацію цього поняття до цифрових прав людини як окремого об'єкта кримінально-правової відповідальності. Інформаційна безпека є об'єктом Особливої частини Кримінального кодексу України (далі КК України), хоча законодавець і не виділив її в окремий блок норм, на що вказує О. О. Пащенко [2, с. 13]. Для системи цифрових прав особи такий підхід означає, що навіть за відсутності прямої вказівки на родовий об'єкт і зафіксованої категорії «цифрових прав» кримінальне законодавство вже реагує на правопорушення у цій сфері, хоча і фрагментарно.

Українські дослідники спрямовують свої пошуки на охорону цифрових прав при здійсненні правосуддя. Так, цифровізація правосуддя є предметом розгляду в контексті процесу автоматизації судочинства, ключових систем, що здійснюють правосуддя, використання відеоконференцій та інших електронних інструментів в судочинстві. Це провокує питання порушення цифрових прав особи і, окрім розширення доступу до правосуддя, породжують нові виклики для нього. Дослідник М. В. Шепітько акцентує на іншому вимірі

цифрових прав особи: не лише як право на захист даних, конфіденційність чи цифрову ідентифікацію онлайн-активності, а й як право на безпечне користування цифровими інструментами, що забезпечують правосуддя, і право на якісне правосуддя в умовах цифровізації [3, с. 70–72].

Водночас дослідження Н. В. Глинської та Д. І. Клепки [4, с. 34–42] свідчить про те, що цифрові права особи розвиваються невідривно від ключових стандартів кримінального провадження. Автори наголошують на тому, що верховенство права, правова визначеність, ризикоорієнтований підхід та роль людського фактора як гарантії справедливого і адекватного провадження мають зберігатися попри те, що до них додаються цифрові свободи особи.

Саме тому метою цього дослідження є визначення цифрових прав свободи як об'єкта кримінально-правової охорони і з'ясування його особливостей у порівняльно-правовому аналізі. Для досягнення зазначеної мети було поставлено такі завдання: з'ясувати історико-правові засади кримінально-правового захисту цифрових прав особи і підстави для формування кримінально-правової політики у цій сфері; дослідити міжнародно-правові засади кримінального захисту цифрових прав особи; проаналізувати кримінально-правовий захист цих прав у практиці Європейського суду з прав людини та порівняти іноземний досвід кримінально-правового захисту цифрових прав особи.

Огляд літератури

Аналіз використаної в дослідженні літератури свідчить про те, що національний та іноземний досвід кримінально-правового захисту цифрових прав особи розглянуто в контексті інформаційного права, інформаційної безпеки і міжнародних стандартів їх охорони. Науковці виходять із того, що цифрові права не є новелою кримінального законодавства і опосередковано зафіксовані в ньому як результат трансформації класичних прав із доданням цифрового чинника. В українському підході нормативними засадами формування цифрових прав особи є Конституція України [5], закони України «Про захист персональних даних» [6], «Про інформацію» [7], «Про електронну ідентифікацію та електронні довірчі послуги» [8], а також норми КК України про кримінальні правопорушення у сфері електронно-обчислювальних приладів і мереж [9]. Можна констатувати, що система національного законодавства в контексті охорони цифрових прав особи є комплексною, адже охоплює конституційні засади, акти кодифікованого та спеціального регулювання.

Окремі наукові праці заслуговують на висвітлення їх ключових аспектів. Зокрема, у монографічному дослідженні «Міжнародні стандарти та націо-

нальна кримінально-правова політика у сфері охорони інформаційної безпеки» за редакцією В. І. Борисова, М. В. Карчевського, М. В. Шепітька представлено якісно новий вимір дослідження. Автори комплексно досліджують міжнародні стандарти та зарубіжний досвід протидії кримінальним правопорушенням у сфері охорони цифрових прав особи, окремо зупиняючись на прагматичному американському підході в контексті CAN SPAM Act [10, с. 72–80].

Водночас у науковій літературі, зокрема в матеріалах круглого столу «Інформаційна агресія в сучасному світі: правовий аналіз та протидія», цифровізацію розглянуто як чинник, що розширює можливості розвитку суспільства, водночас створює виклики для категорії кримінального права й породжує нові інструменти ведення гібридних воєн. Також було введене нове поняття «інфоагресія», яке стосується охорони цифрових прав особи [11, с. 42–44].

Серед міжнародних актів, які були використані в дослідженні, на особливу увагу заслуговує практика Європейського суду з прав людини і два ключових рішення у справах K.U. v. Finland [12] і Benedik v. Slovenia [13]. Обидва рішення стосуються суміжного предмета позову, однак є дзеркальними і підкреслюють потребу пошуку балансу між завданнями кримінального переслідування і правом особи на цифрову безпеку і конфіденційність. Ці рішення були відібрані з метою демонстрації того, як те саме цифрове право особи – право на конфіденційність електронних даних – може порушуватися державою з метою встановлення істини у кримінальному провадженні й паралельно може захищатися державою з метою досягнення справедливості в межах кримінального провадження.

Проаналізовані джерела демонструють конституційну, кримінальну та міжнародну природу проблематики питання і свідчать про актуальність подальших системних пошуків та осмислення цифрових прав особи як окремого об'єкта кримінально-правової охорони на міжнародному і національному рівнях.

Матеріали та методи

Методологія дослідження базується на поєднанні загальнонаукових і спеціально-юридичних методів, оскільки завдання роботи потребували розкриття змісту цифрових прав, з'ясування їх особливостей, проведення порівняльного аналізу й аналізу нормативного закріплення їх на національному і міжнародному рівні. Саме тому методологічна база зумовлена міжгалузевим характером предмета дослідження, а вихідним матеріалом дослідження є нормативні положення Конституції України, КК України,

спеціального законодавства у сфері цифрових прав особи, міжнародного законодавства, регіонального законодавства та окремих його положень, а також практики Європейського суду з прав людини. Ці засади доповнюється науковими працями у сфері інформаційної безпеки, цифровізації та інфоагресії.

Ключовим у дослідженні є формально-юридичний метод. Його було використано для аналізу нормативно-правових актів національного та міжнародного характеру і визначення на їх основі засад охорони цифрових прав особи. Формально-юридичний метод сприяв дослідженню положень Конституції України та спеціальних законів із метою встановлення, які права та свободи вважаються цифровими, чи набули вони нормативного закріплення і як функціонують у нормативному середовищі. Застосування формально-юридичного методу дало змогу констатувати, що цифрові права особи поки окремо не закріплені в кодифікованому законодавстві України і потребують такої модифікації.

Порівняльно-правовий метод застосовано в дослідженні для зіставлення європейського, англосаксонського та українського підходів до охорони цифрових прав і порівняння різних моделей та досвіду. Використання порівняльно-правового методу дозволило проаналізувати американські законодавчі документи, порівняти їх із українською нормативно-правовою базою, а також виокремити іноземні підходи до формування політики щодо цифрових прав особи і їх кримінальної правової охорони. Порівняльно-правовий метод був застосований для формулювання висновків і встановлення перспектив щодо подальшого розвитку національного законодавства в контексті охорони цифрових прав особи в кримінальному праві.

За допомогою аналітичного методу було опрацьовано наукові джерела та виокремлено дослідницькі позиції щодо питань, які були основою дослідження. За цим методом було виокремлено основні наукові підходи до розуміння цифрових прав, досліджено їх еволюцію від традиційних форм до сучасних, а також здійснено класифікацію кримінальних правопорушень у сфері інформаційної безпеки.

Системно-структурний метод дав змогу проаналізувати цифрові права особи в контексті взаємопов'язаних гарантій і механізмів їх охорони. За допомогою цієї техніки було встановлено місце цифрових прав особи в кримінальному законодавстві України і в міжнародному законодавстві. Застосування системно-структурного методу сприяло аналізу внутрішньої логіки законодавця при внесенні модифікацій у кодифіковане кримінальне законодавство і потенційні перспективи адаптації КК України.

Результати дослідження

Поняття цифрових прав особи та засади їх кримінально-правової охорони в національному законодавстві України

Питання цифрових прав особи та їх історичний розвиток становлять основу юридичного інтересу багатьох дослідників, адже ця сфера набуває особливої актуальності сьогодні з огляду на розвиток штучного інтелекту, процеси глобалізації, високу активність користування особами інтернетом, де потреба в захисті їхніх прав вже не може бути забезпеченою лише традиційними механізмами права. До цифрових прав належать права та свободи, що забезпечують вільний доступ до цифрових технологій, використання цифрових ресурсів та захист особи у цифровому середовищі. Це право на захист персональних даних, доступ до інтернету, право на цифрову ідентифікацію, право на доступ до відкритих даних, право на захист від цифрової дискримінації тощо [1, с. 269–270].

На окрему увагу заслуговує саме питання захисту цих свобод, оскільки цифрові права є об'єктом охорони кримінального законодавства, а отже, історична еволюція цього комплексу прав та їх генеза важливі для розуміння того, як розвивався сам кримінально-правовий захист цієї групи прав. Отже, кримінально-правовий захист цифрових прав особи в класичних правових системах розглянуто як конституційні гарантії із особливостями їх реалізації в громадянському суспільстві. Конституція України передбачає таємницю листування та кореспонденції, що охоплює електронні засоби комунікації (ст. 31); захист персональних даних, що стосується й даних у електронному форматі (ст. 32) та свободу думки й слова, а також право на поширення та збирання інформації, що стосується використання при цьому електронно-обчислювальної техніки (ст. 34) [5].

Окрім конституційного закріплення, гарантії цифрових прав містяться у спеціальних актах – законах України: «Про захист персональних даних» [6], «Про інформацію» [7], «Про електронну ідентифікацію та електронні довірчі послуги» [8]. Спеціальне законодавство фіксує регулювання конкретних сфер цифрових прав та демонструє, що їх еволюція відбувається поступово: хоча в Конституції України поняття «цифрові права» не закріплене, ця дефініція на практиці відбивається в окремому законодавстві, зокрема – у кодифікованому нормативно-правовому акті, КК України [9].

Особлива частина КК України містить норми щодо охорони інформаційної безпеки, хоча окремого розділу, що стосується виключно цього родового об'єкта, в акті не вказано. Значення інформаційної безпеки, за національним законодавцем, є неоднаковим у різних положеннях КК України: ч. 2 ст. 109

(публічні заклики щодо насильницької зміни чи повалення влади); ст. 114 (шпигунство); статті 111–111[1] (державна зрада та колабораційна діяльність) демонструють, що в інформаційній сфері основним об'єктом виступає національна безпека України (безальтернативний об'єкт) або ж існують й інші об'єкти, такі як цифрові права, де шкода національній безпеці заподіюється паралельно із цим об'єктом (альтернативний об'єкт) [2, с. 13].

Загальну еволюцію кримінально-правового захисту цифрових прав особи і разом із ним – підстави відповідальності – доцільно визначити за поділом кримінальних правопорушень у сфері цифрових прав та інформаційної безпеки на окремі категорії.

До першої групи належать ті правопорушення, що стосуються електронно-обчислювальних машин – комп'ютерів. Це значно розширює перелік цифрових прав, які потребують захисту, оскільки дає підставу додати до таких правопорушень ті, що перелічені в розд. XVI КК України; тож аналітичний аналіз дає змогу виокремити право на приватність та захист цифрових даних (ст. 361 КК України), право на безпечне використання сервісів та мереж (ст. 361[1] КК України), право на інформацію (ст. 363 КК України).

Друга група охоплює категорію цифрових прав, порушення яких посягає на засади національної та державної безпеки, обороноздатність країни та її устрій, – це розголошення державної таємниці, передача та збирання відомостей, що містять службову інформацію, розголошення відомостей військового характеру тощо. Потрібно зауважити, що ця група охоплює норми, які стосуються конституційного устрою держави і не спрямовані безпосередньо на охорону цифрових прав особи. Однак опосередковано діяння, передбачені цими положеннями, можуть зачіпати і сферу цифрових прав, оскільки розголошення військових таємниць, незаконний обіг інформації чи передача чутливої інформації створюють загрози для інформаційної безпеки особи вже безпосередньо та перешкоджають повній і безпечній реалізації цифрових свобод.

КК України подає третю групу кримінальних правопорушень проти інформаційної безпеки та цифрових прав, які стосуються посягання на інформаційний простір держави: про насильницьку зміну влади (ст. 109), про посягання на територіальну цілісність тощо (ст. 110), а також публічні заклики чи заперечення ведення агресивної політики проти держави і поширення такої інформації. Критичне застереження до цієї групи правопорушень аналогічне: вони не стосуються безпосередньо цифрових прав особи, однак охорона інформаційної безпеки держави впливає на здатність особи реалізувати цифрові права; що ефективнішою буде охорона інформаційної безпеки, то дієвішим стане і захист цифрових прав особи.

З огляду на високий рівень диджиталізації та потребу в кримінально-правовому захисті й охороні цифрових прав, підстави їх порушення зводяться дослідниками до поняття інфоагресії. Проявом інфоагресії, особливо в контексті ведення гібридної війни, є атаки на інформаційний простір, який за своєю природою досить специфічний. Отже, науково-технічний прогрес та розвиток інформаційно-комунікаційних технологій уможливив генерацію інфоагресії на якісно новому рівні: ворожа пропаганда, мова ворожнечі, фейкові новини, публічні заклики до ведення агресивних війн та політики [11, с. 42–44]. Емпіричні дослідження українських науковців у цьому контексті підтверджують якісну трансформацію кіберзлочинності в умовах воєнного стану: зокрема, зафіксовано зростання цільового фішингу на 40 % у 2022 р., понад 300 випадків шахрайських криптообмінних операцій та 25-відсоткове збільшення фіктивних інвестиційних схем, що засвідчує неготовність чинного КК України до належної кваліфікації подібних посягань на цифрові права з огляду на відсутність визнання віртуальних активів як окремого об'єкта кримінально-правової охорони [14, с. 924–928]. Як свідчить аналіз кримінального законодавства, частина цих підстав для формування кримінально-правової відповідальності у сфері захисту цифрових прав осіб вже закріплена, однак для ефективної боротьби з ІПСО (інформаційно-психологічні операції) потрібен складний комплекс дій, який продовжує розроблятися; насамперед такі механізми мають бути розроблені в системі здійснення правосуддя. У контексті цифрових прав це питання стосується захисту права доступу до суду, безпеки цифрових судових реєстрів та систем, конфіденційності даних і недопущення свавільного втручання в процедуру здійснення правосуддя. Науково-технічний прогрес, а також судова реформа і активна диджиталізація державних інституцій створюють новий об'єкт кримінально-правової охорони, що потребує автоматизації правосуддя, більшого використання відеозв'язку та інформаційних систем при його здійсненні, нову цифрову інфраструктуру. Поряд із цим загострюються питання, що стосуються прав захисту підозрюваних: межі використання автоматизованих інструментів, зокрема системи штучного інтелекту, правоохоронними та судовими органами, принцип конфіденційності [3, с. 72].

Оскільки КК України поки комплексно не регулює ані питання цифрових прав особи, ані використання автоматизованих систем при здійсненні правосуддя, то доцільно посилатися на його найбільш релевантну норму, ст. 376[1], яка фактично забезпечує захист інформації під час здійснення правосуддя, хоча потребує певного уточнення. Положення охоплює умисне втручання в роботу автоматизованих систем у системі правосуддя, забезпечує кримінально-правову охорону інформації під час здійснення правосуддя, криміналізує

внесення неправдивих відомостей, несвоєчасне внесення інформації або несанкціоновані дії з інформацією.

Бланкетний характер норми ускладнює визначення об'єкта кримінально-правової охорони і потребує уточнення в контексті відсилання до підзаконних нормативно-правових актів регулювання Єдиної судової інформаційно-телекомунікаційної системи [3, с. 70]. Отже, охорона зазначених цифрових прав особи у сфері правосуддя паралельно захищає право на справедливий суд у цифровому середовищі, безпечне використання електронних судових сервісів, зокрема Єдиної судової інформаційно-телекомунікаційної системи, і цілісність цифрових даних, які циркулюють в інформаційних системах під час здійснення правосуддя. Уточнення зазначеної норми КК України має винятково важливе значення для охорони цифрових прав, оскільки регулювання потребує чіткого законодавчого визначення того, які саме цифрові системи, процеси та інформація перебувають під кримінально-правовою охороною.

Щодо цього особливої уваги набувають принципи визначення розумних меж цифровізації під час охорони цифрових прав людини. Стандартами цифровізації кримінального провадження насамперед є: 1) верховенство права як класичний принцип; 2) правова визначеність, що полягає у чіткому врегулюванні меж цифровізації; 3) пріоритетність цифрового формату провадження як базового вектора розвитку системи правосуддя; 4) гнучкості процесу цифровізації, оскільки цифровим процедурам мають бути передбачені альтернативи у вигляді традиційних процедур правосуддя; 5) ризикоорієнтований підхід, який має включати всі потенційні виклики цифровізації під час охорони та захисту цифрових прав людини; 6) збереження провідної ролі людського фактора, оскільки використання суто автоматизованих систем при здійсненні правосуддя може призвести до порушення цифрових прав людини; 7) прозорість використання цифрових технологій при здійсненні кримінального провадження, уникнення ефекту «чорної скриньки» [4, с. 34–41].

Загалом ці засади регламентують межі допустимого втручання цифрових технологій у систему правосуддя, рівень їх застосування, модель, на основі якої це застосування відбувається (ризикоорієнтований підхід) і гарантії для цифрових прав людини, які мають забезпечуватися при застосуванні автоматизованих систем. Тож підстави формування кримінально-правової політики у сфері захисту й охорони цифрових прав особи, безпосередньо залежать від розвитку інформаційного суспільства та новітніх технологій.

Активна інформатизація суспільства змінює традиційний формат правових галузей, зокрема кримінально-правової. Структура суспільних відносин

трансформується через збільшення кола кримінальних посягань у цифровій сфері, які потребують відповідної реакції. Змінюються способи та форма вчинення правопорушень у сфері цифрових прав, і це означає, що кримінальна правова політика формується з огляду на те, охорона яких прав сьогодні є принциповою і пріоритетною, і з урахуванням того, що права людини дедалі глибше інкорпоруються в цифрове середовище та набувають нового виміру [15, с. 107].

Нині в суспільстві гостро відчуваються посягання на цифрові права особи через телебачення, інтернет, телекомунікаційні мережі тощо. Ці делікти суттєво відрізняються від традиційних, оскільки до посягання на кодифіковані права та свободи додається цифровий вимір, що становить більшу небезпеку через нові й вишукані шляхи його здійснення. Тож ще однією підставою є підвищений суспільний ризик нових інформаційних правопорушень [15, с. 114].

Серед ознак правопорушення в інформаційній сфері особлива увага приділяється об'єкту правопорушення – цифровим правам особи та інформаційним відносинам, предмету – інформаційній інфраструктурі, а також інформаційним правам і свободам людини, і знаряддям його вчинення – інформаційно-телекомунікаційним технологіям [15, с. 187]. Зазначене свідчить про зв'язок інформаційних правопорушень із правами людини та цифровою інфраструктурою, адже кримінально-правова політика формується задля охорони прав особи, які реалізуються через використання зазначених систем або порушуються через порушення при такому використанні.

Історико-правові засади кримінально-правового захисту цифрових прав особи демонструють поступову еволюцію від охорони традиційних моделей – таємниці комунікації, приватності, конфіденційності персональних даних – до визнання потреби їх окремого захисту у цифровому середовищі, що означає утворення нової сфери цифрових прав особи. У контексті кодифікованого кримінального законодавства це знайшло вияв у розширенні кола кримінальних правопорушень щодо посягань на інформаційні системи, цифрові дані й модифікацію системи правосуддя у зв'язку з цифровізацією.

Міжнародно-правові стандарти охорони цифрових прав особи в кримінально-правовому вимірі

Окрім національного законодавства, чинними для України є міжнародні договори та угоди, ратифіковані Верховною Радою України у встановленому законом порядку. Вони становлять частину національного законодавства держави. Міжнародна правова база налічує стандарти іменних правових організацій та право ЄС, що стосується охорони прав у цифровому просторі.

Так, 23.11.2001 р. Радою Європи була прийнята Конвенція про кіберзлочинність, або Будапештська конвенція, яка була ратифікована Україною 07.09.2005 р. (далі – Конвенція). Нею визначені основні групи прав, які потребують охорони в контексті правопорушень: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані зі змістом; 4) правопорушення, пов'язані із порушенням авторських і суміжних прав [10, с. 20–21]. Варто зазначити, що КК України досить широко включає положення зазначеної Конвенції. Більшість діянь, передбачених у ній, визнаються в українському законодавстві. Серед них – нелегальне перехоплення, навмисний доступ, втручання в дані чи підробка, що пов'язане з комп'ютерами (статті 163, 361, 362, 358 КК України відповідно).

Аналізуючи зміст Конвенції, доречно зазначити цифрові права особи, які підлягають кримінальній охороні: право на конфіденційність (статті 2, 3); право на цілісність цифрових даних (ст. 4); право на безпечне функціонування цифрових систем (ст. 5); право на захист від підробки в контексті цифрової інформації (ст. 6); право на достовірність інформації (ст. 7); право на захист цифрових майнових інтересів, що пов'язане із шахрайством (ст. 8); новела законодавства – цифрові права дитини, які пов'язані із захистом її від сексуальної експлуатації (ст. 9); права інтелектуальної власності – авторські та суміжні права, що набувають особливих механізмів охорони в контексті кримінальних правопорушень у цифровому просторі (кіберпіратство, майнові та немайнові особисті права автора тощо) за ст. 10 [16]. Окрім того, преамбула Конвенції пов'язує кримінально-правову охорону зазначених прав із традиційними засадами права на приватне життя, свободу вираження поглядів і захисту особистої недоторканності та інформації особи.

Подальший розвиток європейського підходу до кримінально-правової охорони цифрових прав особи відображено в так званому E-evidence Package ЄС – Регламенті (ЄС) 2023/1543 і Директиві (ЄС) 2023/1544, які формують наднаціональний механізм транскордонного отримання електронних доказів у кримінальному провадженні та доповнюють Будапештську конвенцію разом з її Другим додатковим протоколом. Як зазначається в науковій літературі, цей пакет залишає невирішеними питання балансу між ефективністю переслідування кіберзлочинів і захистом цифрових прав фігурантів кримінального провадження [17, с. 237–260], що становить актуальний виклик для держав – членів ЄС і для України як держави – кандидата на членство в ЄС у контексті гармонізації національного законодавства.

Нагальним питанням сьогодні в контексті охорони цифрових прав особи в ЄС є Акт про штучний інтелект (Artificial Intelligence Act, AI Act) [18].

Акт про штучний інтелект застосовує підхід, що ґрунтується на оцінюванні ризиків, класифікуючи системи штучного інтелекту на кілька категорій ризику, до яких застосовуються різні ступені вимог та зобов'язань. Тобто європейська модель відображає цілком ризикоорієнтований підхід.

Окрім цього, Акт про штучний інтелект ЄС забороняє використання прихованих технологій, що застосовуються в системах ІІІ, для маніпуляції або зловживання, невибіркове застосування біометричної ідентифікації, а також запровадження систем соціального скорингу на основі автоматизованого оцінювання громадян [4, с. 41–42]. Оскільки Акт про штучний інтелект ЄС є актом гармонізації для національного законодавства України, то це означає, що законодавець має внести в кримінально-правову сферу положення про захист цифрового права на приватність і захист персональних даних, що пов'язані із використанням штучного інтелекту особами; також право на недискримінацію і право не зазнавати упередженого оцінювання, здійсненого штучним інтелектом. Це підтверджує, як традиційне право на приватність і захист персональних даних модифікується в контексті додання до нього цифрового чинника.

Директива Європейського парламенту і ради ЄС 2016/1148 від 06.07.2016 р. [19] встановлює важливі засади охорони цифрових прав особи в кримінально-правовому вимірі. Акт встановлює обов'язки для держав-членів ухвалити національну стратегію щодо підтримання безпеки інформаційних систем, базові мінімальні вимоги щодо безпеки таких систем для операторів послуг і надавачів цифрових послуг і встановлює обов'язок держав-членів створити національні органи, які будуть слідкувати за дотриманням цифрових прав особи в контексті високого спільного рівня безпеки мережевих чи інформаційних систем у межах Союзу.

Кримінально-правовий захист цифрових прав особи у практиці Європейського суду з прав людини

Кримінально-правовий захист цифрових прав особи в практиці Європейського суду з прав людини демонструє водночас важливість коректної охорони цифрових прав особи, проведення правосуддя в умовах цифровізації та вплив цих чинників на особливий об'єкт кримінального регулювання – цифрові свободи. Показовою є справа ЄСПЛ K.U. v. Finland (2008) [12], суть якої полягала в публікації недопустимого контенту за участю неповнолітньої особи. Остання стала жертвою розміщення на сайті знайомств оголошення сексуального характеру від його імені. Після отримання електронного листа від невідомого чоловіка про пропозицію зустрічі, батько заявника звернувся до поліції з проханням встановити особу, однак провайдер відмовився роз-

кривати дані про користувача, посилаючись на таємницю телекомунікацій. Поліція звернулася до суду з клопотанням зобов'язати провайдера надати ці дані, проте судова установа відмовилась із посиланням на право на таємницю листування (пп. 6–14).

Результатом розгляду справи стало встановлення ЄСПЛ порушення ст. 8 *Будапештської конвенції* та права на повагу до приватного життя. ЄСПЛ постановив, що держава не забезпечила ефективного захисту для заявника від втручання в його приватне життя, оскільки законодавство не встановило особу, яка розмістила оголошення (п. 1 фінального рішення). Практика ЄСПЛ демонструє позитивний обов'язок держави у кримінально-правовому вимірі охороняти цифрові права особи на приватність та безпеку і гарантувати дієвий правовий захист цих прав.

Дзеркальною справою є кейс Benedik v. Slovenia (2018) [13], що також стосується чутливого контенту. Швейцарська поліція повідомила словацьку поліцію, що конкретна IP-адреса використовується в мережі для обміну файлами, які містять заборонений контент. Після цього словацька поліція без отримання судового ордера на обшук звернулася до провайдера та отримала дані абонента, якому належить зазначена IP-адреса. На цих підставах було проведено кримінально-пошукові дії, вилучено комп'ютер, і згодом особа була визнана винною в поширенні порнографічних матеріалів (пункт 6-8).

Заявник, якого було затримано, звернувся до ЄСПЛ зі скаргою на те, що доступ до даних, що дали змогу його ідентифікувати, був отриманий поліцією неправомірним шляхом, без достатньої правової підстави, що порушувало його цифрові права та гарантії на захист приватного життя. Результатом справи стало встановлення ЄСПЛ порушення ст. 8 Конвенції, оскільки заявник мав обґрунтовані очікування щодо своїх цифрових прав, зокрема – право на приватність своєї інтернет-активності й захист від свавільного втручання в таку активність. Суд встановив важливий елемент охорони цифрових прав: навіть у межах кримінального провадження держава не може отримувати дані без належної правової підстави для їх пошуку (пп. 130–133).

Практика ЄСПЛ демонструє, що кримінально-правова охорона цифрових прав особи в європейському досвіді має дуальну природу: з одного боку, держава має забезпечити механізми для переслідування осіб, які порушують цифрові права інших; а з іншого боку, держава має утримуватися від порушення цифрових прав осіб при здійсненні кримінального розслідування. Таким чином, практика ЄСПЛ демонструє основне завдання кримінально-правової сфери в контексті цифрових прав особи – пошук балансу між охороною та розумним порушенням цифрових прав.

Прагматична модель США та порівняльний аналіз із національним підходом

Іноземний досвід кримінально-правового захисту цифрових прав особи для повного аналізу потребує звернення до інших підходів, що охоплюють відмінну від європейської правову систему та підхід до кримінально-правової охорони цифрових прав особи. Як приклад прагматичної моделі на противагу ризикоорієнтованій європейській можна навести CAN SPAM Act – Федеральний акт США для протидії розповсюдження фішингових листів та спаму. Це правопорушення має незначний матеріальний складник для особи, адже воно пов'язане із додатковими витратами на надання інтернет-послуг, що пов'язані із отриманням зайвої кореспонденції. Більшу небезпеку спам становить для провайдерів та організацій, що надають подібні послуги, оскільки неконтрольоване поширення фішингових листів створює додаткове навантаження на інформаційні системи. Це може призвести до їх збоїв і, як наслідок, до витоку інформації чи інших порушень цифрових прав.

CAN SPAM Act передбачає, що кримінальними правопорушеннями, які посягають на цифрові права особи, є: 1) несанкціонований доступ до захищеного комп'ютера й ініціювання передачі повідомлень; 2) використання захищеного комп'ютера для передавання повідомлень; 3) істотне викривлення інформації, що міститься у спам-листах; 4) реєстрацію з використанням такої інформації стосовно ідентифікації особи; 5) представлення себе шляхом обману особою або законним представником особи, на яку зареєстровано декілька IP-адрес [10, с. 72-73; 20]. Положення, передбачені пунктами 18 U.S.C. § 1037(a)(1)–(5) Акта, демонструють порушення наступних цифрових прав: право на безпечне користування цифровими системами, право на контроль над власною цифровою інформацією, право на достовірну інформацію про електронні повідомлення, право на цифрову ідентичність (що дуже важливо в контексті фальсифікації ідентифікаційних даних як підстава для нового виду кримінально-правової відповідальності), право на приватність і право на безпечне цифрове середовище.

Система охорони від спаму на кримінально-правовому рівні в США побудована у форматі тріади. На першому рівні – обов'язкові правила для комерційної розсилки, тобто гарантії і стандарти, які роблять її законною: механізми відмови «opt-out» і заборона оманливих повідомлень і маніпуляцій. Другий рівень – це обтяження для практик спаму: автоматизоване створення численних акаунтів для розсилки повідомлень і використання чужого комп'ютера з цією метою заборонені. Третій рівень – безпосередня кримінальна відповідальність за 18 U.S.C. § 1037, оскільки цей Акт доповнюється

нормою, що криміналізує спам-діяльність і її основні форми: спам, поєднаний з обманом, підробкою і з технічними зловживаннями [10, с. 78–80].

На національному рівні правопорушення в контексті фішингових розсилок регулюється підзаконним нормативно-правовим актом – постановою Кабінету Міністрів України «Про затвердження правил надання та отримання електронних комунікаційних послуг» [21]. Цією постановою визначено порядок надання інтернет-послуг, встановлено порядок регулювання електронних, текстових чи інших листів та повідомлень, що отримані без попередньої згоди абонента (спам), і заборона їх використання, замовлення і пропозиції розсилання таких фішингових матеріалів. Окрім того, заборонено використовувати ідентифікатори інших осіб, тобто комп'ютери чи інші технічні засоби, і фальсифікувати мережеві ідентифікатори.

Отже, порівняльний аналіз демонструє, що в загальних засадах український законодавець установив аналогічні норми до розглянутого американського акта. Проте на рівні матеріальних положень українське законодавство демонструє більш жорсткі умови, оскільки американський акт у певних випадках дозволяє фішингові листи, тоді як національне законодавство повністю їх забороняє.

Досвід кримінально-правового захисту цифрових прав особи свідчить про існування декількох моделей такої охорони і захисту. В ЄС переважає ризикоорієнтований підхід, підхід США демонструє більший прагматизм, а український підхід поєднує в собі заборонні й регуляторні компоненти. Порівняння іноземних моделей свідчить про те, що національна система вже набула подібних механізмів кримінально-правової охорони цифрових прав, однак потребує ще більш чіткого, системного і спеціального закріплення їх в окремих сферах.

Висновки

У результаті дослідження цифрових прав особи як об'єкта кримінально-правової охорони і здійснення порівняльно-правового аналізу цього об'єкта в різних правових системах та відповідно до різного законодавства встановлено, що цифрові права особи формувалися поступово і виокремилися в самостійний об'єкт національної та іноземної кримінально-правової охорони через еволюцію традиційних гарантій приватності, таємниці комунікації та захисту персональних даних, яка стала можливою із розвитком науково-технічного прогресу.

Констатовано, що чинне кримінальне законодавство України вже фіксує перелік норм, які забезпечують охорону цифрових прав, хоча як родовий

об'єкт вони в КК України не визначені. Насамперед ці права зафіксовані в сфері посягань на комп'ютерні системи, інформаційну безпеку, цифрові дані – суміжні поняття, які формують усю структуру цифрових свобод. Поки така охорона залишається ситуативною і не завжди відображає цифрові права в комплексі, що є недоліком національної системи, особливо в контексті гібридної війни.

Доведено, що міжнародно-правові стандарти, право ЄС, практика ЄСПЛ та міжнародні підходи до регулювання систем штучного інтелекту вже закладають подальшу основу для формування нових політик у сфері цифрових прав особи та їх кримінально-правової охорони. Практика ЄСПЛ підтверджує дуальну природу захисту і охорони цих прав: держава не тільки має надавати гарантії охорони, а й не порушувати засади цифрових прав особи; а чітке нормативне регламентування комплексу цифрових свобод у кримінальному праві сприятиме більш ефективному застосуванню механізмів їх охорони державою.

Порівняльно-правовий аналіз досвіду іноземних держав свідчить про те, що європейський підхід базується на ризикоорієнтованій моделі, американська модель тяжіє до прагматичної криміналізації найбільш суттєвих правопорушень у сфері цифрових прав особи, а український підхід поєднує заборонні та регуляторні чинники, потребує подальшого уточнення цифрових прав і їх охорони в окремому законодавчому комплексі. Перспективним вектором є законодавче встановлення переліку цифрових прав як окремого об'єкта кримінально-правової охорони і модифікація кодифікованого кримінального законодавства відповідно до викликів диджиталізації, гібридної війни, штучного інтелекту і появи окремого об'єкта охорони – цифрових свобод особи.

Список використаних джерел

[1] Захарчук І. В. Цифрові права громадян України: конституційно-правове закріплення та механізми реалізації. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 1, № 90. С. 268–273. https://doi.org/10.24144/2307-3322.2025.90.1.34.

[2] Пащенко О. О. Кримінально-правова охорона інформаційної безпеки нормами розділу І Особливої частини КК України. *Питання боротьби зі злочинністю*. 2024. Вип. 47. С. 11–17. https://doi.org/10.31359/2079-6242-2024-47-11.

[3] Шепітько М. В. Кримінально-правова охорона інформаційної безпеки під час здійснення правосуддя. *Питання боротьби зі злочинністю*. 2022. Вип. 44. С. 69–75. https://doi.org/10.31359/2079-6242-2022-44-69.

[4] Глинська Н. В., Клепка Д. І. Принципи визначення розумних меж цифровізації кримінального провадження України. *Питання боротьби зі злочинністю*. 2024. Вип. 47. С. 30–49. https://doi.org/10.31359/2079-6242-2024-47-30.

[5] Конституція України : офіц. текст від 28.06.1996 р. № 54к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#n4262 (дата звернення: 12.02.2026).

[6] Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.02.2026).
[7] Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/card/2657-12 (дата звернення: 12.02.2026).
[8] Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 12.02.2026).
[9] Кримінальний кодекс України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n721 (дата звернення: 12.02.2026).
[10] Борисов В. І., Карчевський М. В., Шепітько М. В. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки : монографія. Харків : Право, 2023. 152 с.
[11] Батиргареєва В. С. До проблеми «діджиталізації» інфоагресії. *Інформаційна агресія в сучасному світі: правовий аналіз та протидія* : матеріали міжнар. наук.-практ. круглого столу (м. Харків, 21 черв. 2024 р.) / редкол.: В. С. Батиргареєва та ін. Харків : Майдан, 2024. С. 42–44.
[12] Judgment of the European Court of Human Rights No. 2872/02 K.U. v. Finland. (December 2, 2008). URL: https://hudoc.echr.coe.int/fre?i=001-89964 (дата звернення: 12.02.2026).
[13] Judgment of the European Court of Human Rights No. 62357/14 Benedik v. Slovenia. (April 24, 2018). URL: https://hudoc.echr.coe.int/fre?i=001-182455 (last accessed: 12.02.2026).
[14] Dumchikov M., Maletova O., Yanishevska K. Virtual assets in cybercrime: a focus on Ukrainian realities. *Journal of Financial Crime*. 2025. Vol. 32, No. 4. P. 919–933. https://doi.org/10.1108/JFC-02-2024-0057.
[15] Арістова І. В., Баранов О. А., Дзьобань О. П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія. Київ : КВІЦ, 2019. 344 с.
[16] Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 12.02.2026).
[17] Tosza S. Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems. *Studia Iuridica Lublinensia*. 2024. Vol. 33, No. 5. P. 237–260. https://doi.org/10.17951/sil.2024.33.5.237-260.
[18] Artificial Intelligence Act : Legislative Act no. P9_TA(2024)0138. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (last accessed: 20.04.2026).
[19] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union : Directive of 19.07.2016 no. 2016/1148. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng (last accessed: 12.02.2026).
[20] Controlling the Assault of Non-Solicited Por last accessed: nography and Marketing Act of 2003 (CAN-SPAM Act). Public Law 108–187. U. S. Government Publishing Office: of. website. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf (last accessed: 20.04.2026).
[21] Про затвердження Правил надання та отримання електронних комунікаційних послуг : Постанова Кабінету Міністрів України від 25.06.2025 р. № 761. URL: https://zakon.rada.gov.ua/laws/show/761-2025-п#n788 (дата звернення: 12.02.2026).

References

[1] Zakharchuk, I.V. (2025). Digital rights citizens of Ukraine: constitutional and legal entrenchment and implementation mechanisms. *Scientific Bulletin of Uzhgorod National University. Series: Law*, *1*(90), 268-273. https://doi.org/10.24144/2307-3322.2025.90.1.34.

[2] Pashchenko, O.O. (2024). Criminal law protection of information security by the norms of Section I of the Special Part of the Criminal Code of Ukraine. *Issues of Crime Prevention, 47,* 11-17. https://doi.org/10.31359/2079-6242-2024-47-11.

[3] Shepitko, M.V. (2022). Criminal law protection of informative security during administration of justice. *Issues of Crime Prevention*, *44*, 69-75. https://doi.org/10.31359/2079-6242-2022-44-69.

[4] Hlynska, N.V., & Klepka, D.I. (2024). Principles of determining reasonable limits of the digitalization of criminal proceedings in Ukraine. *Issues of Combating Crime*, *47*, 30–49. https://doi.org/10.31359/2079-6242-2024-47-30.

[5] Constitution of Ukraine. (June 28, 1996). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#n4262.

[6] Law of Ukraine No. 2297-VI "On Personal Data Protection". (June 1, 2010). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[7] Law of Ukraine No. 2657-XII "On Information". (October 2, 1992). Retrieved from https://zakon.rada.gov.ua/laws/card/2657-12.

[8] Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services". (October 5, 2017). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[9] Criminal Code of Ukraine No. 2341-III. (April 5, 2001). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#n721.

[10] Borysov, V.I., Karchevskyi, M.V., & Shepitko, M.V. (2023). *International Standards and National Criminal-Legal Policy in the Field of Information Security Protection*. Kharkiv: Pravo.

[11] Batyrhareieva, V.S. (June 21, 2024). On the issue of "digitalization" of information aggression. In *Information Aggression in the Modern World: Legal Analysis and Counteraction: materials of the international scien. and pract. round table* (pp. 42-44). Kharkiv: Maidan.

[12] Judgment of the European Court of Human Rights No. 2872/02 K.U. v. Finland. (December 2, 2008). Retrieved from https://hudoc.echr.coe.int/fre?i=001-89964.

[13] Judgment of the European Court of Human Rights No. 62357/14 Benedik v. Slovenia. (April 24, 2018). Retrieved from https://hudoc.echr.coe.int/fre?i=001-182455.

[14] Dumchikov, M., Maletova, O., & Yanishevska, K. (2025). Virtual assets in cybercrime: a focus on Ukrainian realities. *Journal of Financial Crime*, *32*(4), 919-933. https://doi.org/10.1108/JFC-02-2024-0057.

[15] Aristova, I.V., Baranov, O.A., Dzioban, O.P., & et al. (2019). *Legal Liability for Offenses in the Information Sphere and the Foundations of Information Delictology*. Kyiv: KVITs.

[16] Convention on Cybercrime. (November 23, 2001). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text.

[17] Tosza, S. (2024). Electronic Evidence after E-evidence Package's adoption: Challenges for application and unresolved problems. *Studia Iuridica Lublinensia*, *33*(5), 237-260. https://doi.org/10.17951/sil.2024.33.5.237-260.

[18] Artificial Intelligence Act, Legislative Act No. P9_TA(2024)0138. Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.
[19] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng.
[20] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), Pub. L. No. 108-187. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf.
[21] Resolution of the Cabinet of Ministers of Ukraine No. 761 "On Approval of the Rules for the Provision and Receipt of Electronic Communications Services". (June 25, 2025). Retrieved from https://zakon.rada.gov.ua/laws/show/761-2025-п#n788.

Артем Ігорович Шеруда
аспірант кафедри кримінального права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, Харків, Україна
e-mail: a.i.sheruda@nlu.edu.ua
ORCID 0009-0001-0753-4094

Artem I. Sheruda
Ph.D. Student at the Department of Criminal Law
Yaroslav Mudryi National Law University
61024, 77 Hryhoriia Skovorody Str., Kharkiv, Ukraine
e-mail: a.i.sheruda@nlu.edu.ua
ORCID 0009-0001-0753-4094

Рекомендоване цитування: Шеруда А. І. Національний та іноземний досвід кримінально-правового захисту цифрових прав особи. *Проблеми законності*. 2026. Вип. 173. С. 331–350. https://doi.org/10.21564/2414-990X.173.361287.

Suggested Citation: Sheruda, A.I. (2026). National and Foreign Experience in the Criminal-Legal Protection of an Individual's Digital Rights. *Problems of Legality, 173*, 331-350. https://doi.org/10.21564/2414-990X.173.361287.

Статтю подано / Submitted: 06.04.2026
Доопрацьовано / Revised: 14.05.2026
Схвалено до друку / Accepted: 28.05.2026
Опубліковано / Published: 29.05.2026