УДК: 343.14
DOI https://doi.org/10.24144/2307-3322.2025.92.4.19

ПРАВОВІ РЕЖИМИ ДОСТУПУ ПРАВООХОРОННИХ ОРГАНІВ ДО ДАНИХ ІГРОВИХ ПЛАТФОРМ ДЛЯ ПРОФІЛАКТИКИ НАСИЛЬНИЦЬКОЇ ЗЛОЧИННОСТІ В УКРАЇНІ ТА США

Костюченко А.В.,
магістр права,
аспірант кафедри кримінального права та процесу,
Хмельницький університет управління та права імені Леоніда Юзькова
ORCID: 0009-0002-2482-9377

Костюченко А.В. Правові режими доступу правоохоронних органів до даних ігрових платформ для профілактики насильницької злочинності в Україні та США.

Дослідження здійснене з акцентом на порівняльному вивченню правових механізмів отримання правоохоронними органами доступу до інформації ігрових платформ з метою запобігання насильницьким кримінальним правопорушенням в Україні та США. Автором здійснено аналіз проблематики використання онлайн-ігрових середовищ для планування терористичних актів і координації екстремістської діяльності, що зумовлює необхідність правового врегулювання слідчого доступу до цифрових комунікацій користувачів. Досліджується американський підхід, закріплений у федеральному законодавстві про електронні комунікації, який розмежовує процедурні вимоги залежно від характеру запитуваних даних та передбачає багаторівневу систему судових санкцій. Розглянуто положення Закону про захист електронних комунікацій 1986 року та Патріотичного акту 2001 року. Окрему увагу приділено вивченню української моделі, що ґрунтується на інститутах кримінального процесуального права і стикається з практичними труднощами через транснаціональний характер ігрових сервісів. Проаналізовано застосування статей 159-160, 263-264 Кримінального процесуального кодексу України щодо тимчасового доступу та негласних дій. У статті розглядаються особливості міжнародного співробітництва у сфері отримання електронних доказів та роль добровільної взаємодії між державними органами і приватними компаніями. Визначаються конституційні межі втручання в приватність користувачів та механізми їх забезпечення в обох правопорядках. Встановлено відмінності у рівні деталізації процедур, ефективності міжнародної співпраці та прозорості взаємодії з технологічними корпораціями. Обґрунтовується необхідність створення спеціальних правових інструментів для оперативного реагування на цифрові загрози при збереженні балансу між потребами національної безпеки та захистом основних прав людини. Висвітлено практику використання агентів під прикриттям в онлайн-ігрових середовищах як превентивного методу роботи. За результатами дослідження автором сформовано пропозиції щодо вдосконалення вітчизняного правового регулювання через створення чітко визначених процедур взаємодії з іноземними платформами, встановлення обов'язкових вимог локального представництва технологічних компаній, а також розробку комплексних стратегій превентивного моніторингу онлайн-середовищ і своєчасного реагування на виявлені правопорушення.

Ключові слова: правові режими доступу, ігрові платформи, профілактика злочинності, електронні докази, міжнародна правова допомога, кіберпростір, судовий контроль.

Kostyuchenko A.V. Legal regimes of access of law enforcement agencies to data of gaming platforms for prevention of violent crime in Ukraine and the USA.

The study was conducted with an emphasis on a comparative study of the legal mechanisms for obtaining law enforcement access to information from gaming platforms in order to prevent violent criminal offenses in Ukraine and the United States. The author analyzed the issue of using the online gaming environment for planning terrorist acts and coordinating extremist activities, which necessitates the legal regulation of investigative access to users' digital communications. The American approach,

enshrined in federal legislation on electronic communications, is studied, which distinguishes procedural requirements depending on the nature of the requested data and provides for a multi-level system of judicial sanctions. The provisions of the Electronic Communications Protection Act of 1986 and the Patriot Act of 2001 are considered. Special attention is paid to the study of the Ukrainian model, which is based on the institutions of criminal procedural law and faces practical difficulties due to the transnational nature of gaming services. The application of Articles 159-160, 263-264 of the Criminal Procedure Code of Ukraine regarding temporary access and covert actions is analyzed. The article considers the features of international cooperation in the field of obtaining electronic evidence and the role of voluntary interaction between state bodies and private companies. The constitutional limits of interference with user privacy and the mechanisms for ensuring them in both legal systems are determined. Differences in the level of detail of procedures, the effectiveness of international cooperation and the transparency of interaction with technological corporations are established. The need to create special legal instruments for an operational response to digital threats while maintaining a balance between the needs of national security and the protection of fundamental human rights is substantiated. The practice of using undercover agents in the online gaming environment as a preventive method of work is highlighted. According to the results of the study, the author has developed proposals for improving domestic legal regulation through the establishment of clearly defined procedures for interaction with foreign platforms, the introduction of mandatory local presence requirements for technology companies, and the development of comprehensive strategies for preventive monitoring of online environments and timely response to identified violations.

Key words: legal access regimes, gaming platforms, crime prevention, electronic evidence, international legal assistance, cyberspace, judicial control.

Постановка проблеми. У сучасному цифровому середовищі ігрові онлайн-платформи (Steam, Xbox Live, PlayStation Network, MMORPG-світи тощо) слугують потенційним полем для протиправної діяльності або її планування. Відомі випадки, коли зловмисники використовували чати відеоігор для координації дій або поширення екстремістських ідей (організація «Unite the Right» у приватних серверах Discord у 2017 р. [19]; планування стрілянини в Баффало з детальними нотатками в закритих чатах Discord у 2022 р [10]; мережі неонацистської та про-ІДІЛ пропаганди у спільнотах Steam [14]). Послідовно, перед правоохоронними органами постала проблема, яким чином отримати доступ до даних таких платформ (інформації про користувачів, їхніх повідомлень, поведінки в грі) з метою запобігання насильницьким кримінальним правопорушенням (терактам, масовим розстрілам, підготовці нападів). Слід зауважити, що зазначена проблема також породжує певну дилему, оскільки перед правоохоронними органами стоїть завдання забезпечити безпеку громадян, виявляти ранні ознаки планування кримінальних правопорушень, однак дані часто є приватними, захищеними правом на таємницю кореспонденції, персональними даними. Як наслідок, виникає конфлікт між вимогами безпеки і правом на приватність. Проблема ускладнюється транскордонним характером платформ, сервери відеогри можуть бути за межами країни, компанії підпорядковуються іноземним юрисдикціям. Таким чином, актуальним стає питання про правові режими, тобто сукупність норм і процедур, які регулюють доступ правоохоронних органів до інформації. У нашому дослідженні ми порівнюємо підходи України та США, двох країн, що мають різні правові системи, однак спільний виклик щодо протидії насильницькій злочинності в кіберпросторі.

Мета статті: проаналізувати та порівняти правові режими доступу правоохоронних органів до даних ігрових платформ у США та Україні для профілактики насильницьких кримінальних правопорушень. Дослідження спрямоване на з'ясування правових інструментів отримання інформації від ігрових сервісів, визначення видів доступних даних та умов їх отримання, оцінку балансу між потребами слідства та правами користувачів на приватність, а також окреслення прогалин і напрямків удосконалення законодавства для забезпечення ефективної профілактики кримінальних правопорушень при дотриманні конституційних прав громадян.

Аналіз останніх досліджень і публікацій. Основні підходи до доступу правоохоронців до онлайн-комунікацій у США системно викладені в роботах з електронного нагляду і цифрової приватності (Керр О.С. [12]; Томпсон II Р.М.; Коул Дж.П. [20]), які доволі справедливо розмежовують судовий ордер на вміст повідомлень і менш вимогливі процедури для облікових і технічних відомостей (IP-адреси, часи входів), а також окреслюють конституційні запобіжні механізми та роль федеральних актів ECPA/SCA.

В емпіричному вимірі практику видачі даних описують аналітичні огляди про те, що саме компанії реально надають слідству, й як це залежить від виду даних та підстав запиту (Пфефферкорн Р. [16], Кімпану К. [6]), а також публічні регламенти та звіти прозорості великих гральних і суміжних сервісів, які фіксують порядок взаємодії з поліцією (Discord [9]; Microsoft [13]). Дослідження ризиків безпеки у геймерських середовищах вказують на використання ігрових та «ігрово-суміжних» просторів для поширення екстремістських наративів і комунікації (Дейві Дж. [7], Робінсон Н., Віттекер Дж. [17]), що підсилює потребу у врегулюванні співпраці держави та платформ.

Слід зауважити, що в Україні питання доступу до даних вирішуються ухвалою слідчого судді про тимчасовий доступ до речей і документів та негласними слідчими діями щодо інформаційних систем (ст.ст. 159–160, 263–264 КПК України), що підтверджується і процесуальною практикою [28]. Аналіз вітчизняних наукових праць дає підстави автору стверджувати про наявність суттєвих прогалин у взаємодії з іноземними сервісами, зокрема, й щодо строків зберігання даних і міжнародної допомоги (Ахтирська Н.М. [3; 24], Костюченко О.Ю. [25]). На транскордонному рівні рамкові механізми доступу і обміну даними ґрунтуються на Будапештській конвенції про кіберзлочинність та двосторонніх угодах про правову допомогу, які задають процедурні стандарти для запитів до іноземних провайдерів [26]. З аналізу джерел вбачається, що США розробили деталізовану систему градації даних і процесуальних стандартів їх отримання, тоді як Україна має базові правові механізми, однак потребує спеціалізованих норм для оперативної взаємодії з транснаціональними ігровими платформами, що створює необхідність дослідження американського досвіду для удосконалення вітчизняного правового регулювання.

Виклад основного матеріалу. Сполучені Штати Америки мають розвинену правову базу щодо доступу держави до електронних даних, сформовану насамперед Законом про захист електронних комунікацій 1986 року та Патріотичним актом 2001 року з подальшими змінами [11; 22]. Справедливим буде зауважити, що згадані законодавчі акти не створювалися спеціально для ігрових платформ, однак вони поширюються на них, оскільки ігрові сервіси забезпечують електронні комунікації та дистанційні комп'ютерні послуги. Американська правова система встановлює різний режим доступу залежно від типу запитуваної інформації, що створює збалансовану систему захисту приватності та забезпечення потреб охорони прав громадян.

Відповідно до положень Закону США «Про збережені комунікації» (Stored Communications Act), контент спілкування гравців (тексти чатів та голосові розмови), користується найвищим рівнем правового захисту, як приватне листування [15]. Для отримання такої інформації правоохоронні органи зобов'язані отримати судовий ордер, санкціонований суддею на підставі вірогідної причини вважати, що зміст містить докази кримінального правопорушення відповідно до вимог Четвертої поправки про захист від необґрунтованих обшуків і вилучень. Процедура передбачає подання до суду клопотання з конкретизацією акаунтів або часових рамок, які підлягають дослідженню, після чого ордер пред'являється постачальнику послуг. Компанія-провайдер несе правовий обов'язок надати запитаний контент за умови відповідності ордера законним вимогам [8]. Втім Бретен Б. звертає увагу на те, що технічним винятком слугують ситуації з наскрізним шифруванням, коли компанія фізично не має доступу до відкритого тексту повідомлень, однак більшість ігрових чатів не використовують таке шифрування і зберігають комунікації у вигляді доступних логів [5].

Метадані та дані облікових записів користувачів регулюються менш суворими стандартами доказування. До категорії належать персональна інформація користувачів, IP-адреси підключень, історія входів, списки контактів, дані про покупки, а також технічні логи активності без змісту повідомлень. Відповідно до Закону «Про збережені комунікації», правоохоронці можуть отримати таку інформацію через судовий наказ або адміністративну повістку, які мають нижчий поріг обґрунтування порівняно з ордером. Достатньо продемонструвати зв'язок запитуваних даних з розслідуванням [1]. Щоправда тут слід підкреслити, що національні органи безпеки у справах контртероризму отримали додаткові повноваження через Патріотичний акт, зокрема можливість використання листів національної безпеки, які дозволяють отримувати певні дані про користувачів без судового рішення та часто супроводжуються забороною розголошення факту запиту [2].

Найбільш втручальною формою доступу є прослуховування або моніторинг у реальному часі, що підпадає під дію Закону «Про прослуховування» і вимагає отримання спеціального ордера третього типу. Такий ордер видається лише після доведення вичерпання всіх інших методів роз-

слідування і демонстрації, що тільки прослуховування може забезпечити необхідні докази. Подібні ордери в практиці застосовуються рідко і переважно у справах про тероризм або організовану злочинність [23]. Практичні прецеденти прослуховування ігрових комунікацій у реальному часі невідомі, що може пояснюватися технічними складнощами та використанням альтернативних методів, включаючи діяльність агентів під прикриттям у віртуальному середовищі.

Американська правова система забезпечує баланс між потребами слідства і приватністю через чітко визначені процедури судового контролю. Наявність ордера гарантує судовий нагляд і мінімізує ймовірні порушення приватності користувачів. У особливо чутливих випадках (запити даних щодо публічних осіб у ігровому контексті), компанії можуть залучати власних юристів для захисту конституційних прав, посилаючись на Першу поправку. Подібна практика вже склалася у відносинах з соціальними мережами. Корпорації регулярно відстоюють право не видавати дані без належного правового обґрунтування для збереження довіри користувачів [4].

Великі корпорації ігрової індустрії, зокрема Microsoft та Sony, публікують звіти прозорості про запити правоохоронних органів і декларують політику видачі даних виключно відповідно до законних вимог. Microsoft, для прикладу, у своїх звітах зазначає статистику ордерів і повісток по всіх сервісах, включаючи Xbox Live, що сприяє підзвітності та громадському контролю за процесом [13]. Окремим аспектом американської моделі виступає добровільна співпраця компаній з правоохоронними органами у профілактиці кримінальних правопорушень. Закон про захист електронних комунікацій дозволяє провайдерам повідомляти владу про виявлену в їхніх сервісах інформацію про кримінальні правопорушення, що готуються, хоча не покладає такого обов'язку. Ігрові компанії можуть самостійно звертатися до ФБР у випадках виявлення погроз масового насильства в чатах. Після трагічної стрілянини 2019 року американський уряд проводив консультації з представниками ігрової індустрії щодо можливостей моніторингу платформ для виявлення потенційних загроз [18]. Заслуговує уваги і той факт, що Рахункова палата США у 2024 році відзначила наявність механізмів обміну інформацією між ФБР, Департаментом внутрішньої безпеки та технологічними компаніями, однак констатувала відсутність цілісної стратегії такої взаємодії. Послідовно, за результатами аналізу Рахункова палата висловила рекомендації щодо розробки комплексного підходу до залучення ігрової індустрії у виявлення екстремістського контенту [21]. Компанії не мають правового обов'язку моніторити приватні чати, що могло б порушити приватність користувачів, але правила користування більшості платформ забороняють погрози насильством і тероризм. Модератори можуть добровільно передавати виявлені порушення правоохоронним органам, за винятком випадків наскрізного шифрування, коли технічно неможливо ознайомитися зі змістом повідомлень.

Отже, можна стверджувати, що американська модель сформувала багаторівневий режим доступу через ордери, судові накази або листи національної безпеки залежно від характеру даних, при якому компанії зазвичай виконують законні вимоги правоохоронців. Водночас функціонують механізми стримування через судовий контроль та можливість оскарження незаконно отриманих доказів, оскільки порушення процедур отримання даних може призвести до визнання доказів недопустимими згідно з Четвертою поправкою.

Розглядаючи ситуацію в Україні, слід зауважити, що наша держава стикається з більш складними викликами у доступі до даних ігрових платформ, враховуючи що більшість великих ігрових сервісів належать іноземним компаніям. Національне законодавство містить норми, які дозволяють отримувати електронні дані в рамках кримінального процесу, однак їх практичне застосування має суттєві обмеження. Основним нормативним актом є Кримінальний процесуальний кодекс України 2012 року з подальшими змінами, який передбачає кілька механізмів доступу до цифрових даних. Тимчасовий доступ до речей і документів регулюється положеннями ст. 160 КПК України і поширюється на електронні документи. Слідчий або прокурор може звернутися до слідчого судді з клопотанням про дозвіл тимчасового доступу, вказавши потрібні дані та їх зв'язок з кримінальним провадженням. За результатами розгляду клопотання, слідчий суддя виносить ухвалу, яка зобов'язує відповідну особу надати запитувані дані [28]. Однак наявний механізм має серйозне практичне обмеження, оскільки багато ігрових компаній не мають представництва або майна в Україні, що унеможливлює вручення судової ухвали. У таких випадках необхідно використовувати процедуру міжнародної правової допомоги на підставі двосторонніх договорів. Процедура передбачає направлення запиту через Міністерство юстиції або Генеральну прокуратуру, отримання рішення суду іноземної держави та передачу даних через відповідні правоохоронні органи. Колектив представників одеської наукової спільноти під керівництвом Зуєва В.В. спра-

ведливо зазначає, що на практиці процес може тривати місяці, що робить його непридатним для екстреної профілактики кримінальних правопорушень [29].

Додаткові можливості у справах про тяжкі та особливо тяжкі кримінальні правопорушення надають негласні слідчі дії. Відповідно до ст.ст. 263-264 КПК передбачається можливість зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем [28]. Слід зауважити, що згадане зняття інформації з електронних систем може стосуватися онлайн-акаунтів і дозволяє правоохоронцям після ухвали слідчого судді отримати віддалений доступ до даних без логічного злому системи. Наприклад, за наявності збереженого логіну та паролю до акаунту Steam можливий огляд акаунту за ухвалою суду подібно до огляду мобільного телефону. Негласні дії згодом розсекречуються та можуть використовуватися як докази в суді. Огляд місця або речей застосовується у випадках, коли кримінальне правопорушення вже стався або існують невідкладні обставини. Слідчі можуть оглянути комп'ютер, ігрову консоль або телефон затриманого та отримати доступ до ігрових даних, включаючи переписку в додатках. Однак такий підхід є все ж реактивним, а не превентивним методом.

Окремої уваги заслуговує і те, що згідно з ч. 1 ст. 121 Закону України «Про електронні комунікації», оператори електронних комунікацій (інтернет-провайдерів) зобов'язані надавати доступ до інформації про споживача лише на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом [30]. Однак, ігрові компанії не є операторами електронних комунікацій, тому до них не застосовуються жодні спецнорми. У випадках, коли потрібний швидкий доступ до даних, правоохоронні органи змушені користуватися процедурою міжнародної правової допомоги, що на практиці є тривалою і малопридатною для екстрених ситуацій. У таких обставинах можливе використання неформальних каналів співпраці (пряма взаємодія з відділами безпеки компаній), однак в Україні така практика радше залишається винятком і не має належного правового регулювання

Варто також зауважити, що українське законодавство містить суттєві прогалини у регулюванні доступу до ігрових платформ. Відсутні спеціальні правила щодо зберігання логів ігрових чатів або обов'язку їх видачі, тому правоохоронні органи діють за загальними нормами, які не завжди пристосовані до специфіки ігрових сервісів. Відповідно до ст. 31 Конституції України, гарантується таємниця листування та інших комунікацій, що поширюється і на приватні чати в іграх [27]. Обмеження права допускається лише за рішенням суду у рамках закону, при цьому всі негласні дії мають санкціонуватися судом і стосуватися лише тяжких кримінальних правопорушень. Незаконний моніторинг ігрових чатів без судової ухвали може призвести до визнання доказів недопустимими.

На відміну від США, де компанії публікують статистику запитів правоохоронних органів, в Україні такої прозорості немає. Багато дій здійснюється негласно, що створює проблему довіри, хоча з міркувань безпеки повна відкритість процесу навряд чи можлива. Для профілактики кримінальних правопорушень українська кіберполіція активно працює в соціальних мережах і месенджерах, моніторячи публічні екстремістські групи. Ігрові середовища залишаються менш прозорими через закриті чати, тому застосовуються методи проникнення агентів під прикриттям у закриті спільноти. Чинне законодавство не забороняють представнику правоохоронних органів грати у онлайн-гру під вигаданим ім'ям, спілкуватися і таким способом збирати інформацію (за вчиненням кримінального правопорушення або інші розшукові заходи). Послідовно, превентивні методи запобігання насильницьким кримінальним правопорушенням в Україні можуть включати і такий «аналоговий» підхід як розвідку в онлайн-іграх.

Висновки. Підсумовуючи, США і Україна мають різні, однак концептуально схожі правові режими доступу до даних ігрових платформ, основані на судовому контролі та співпраці з провайдерами, проте відрізняються ефективністю та деталізацією процедур. Американська законодавча база детально визначає види даних та процедури їх отримання. Доступ до змісту повідомлень надається лише на підставі судового ордеру; можливість отримати метадані здійснюється за менш суворими інструментами; екстрений доступ забезпечується за згодою компанії або через листи уповноважених органів у сфері національної безпеки. Американські правоохоронні органи мають більший спектр можливостей, великі компанії переважно виконують законні вимоги та зберігають прозорість через звітність про кількість запитів.

В Україні нормативно-правова база все ж потребує вдосконалення. Положення КПК України передбачають інструменти тимчасового доступу та негласного зняття інформації, однак їх прак-

тична реалізація стикається з перешкодами, особливо коли дані фізично знаходяться за кордоном. Відсутність місцевого представництва міжнародних компаній та складність процедур міжнародної правової допомоги ускладнюють швидке отримання необхідної інформації. Попри обмеження, українські правоохоронці знаходять альтернативні шляхи (неформальна співпраця, використання агентів під прикриттям в онлайн-спільнотах).

Обидві країни намагаються збалансувати безпеку і приватність громадян. У США баланс забезпечується через розвинену систему судового нагляду, конституційні гарантії виключення незаконних доказів та суспільний контроль через публічні дискусії про межі державного втручання в приватні комунікації. В Україні баланс підтримується вимогою судової ухвали для більшості втручань і контролем слідчих суддів, однак громадський нагляд залишається менш розвиненим.

У контексті профілактики насильницьких кримінальних правопорушень доступ до даних ігрових платформ може відіграти критичну роль у своєчасному запобіганні терористичним актам або масовим вбивствам, якщо планування обговорюється в онлайн-іграх. США розробляють стратегії партнерства правоохоронних органів із технологічними компаніями. Україні варто перейняти такий досвід через укладання меморандумів з міжнародними компаніями про порядок екстрених запитів та розвиток спроможності кіберпідрозділів. Окремої уваги заслуговує і необхідність удосконалення законодавства, встановлення чіткого порядку взаємодії з іноземними сервісами та регламентування прямої співпраці у випадках загроз життю через спеціалізовані органи. Крім того, влучною на наш погляд, рекомендацією є запровадження вимог щодо локального представництва для сервісів, які масово працюють в Україні. Наявність контактної особи або офісу дозволила б оперативно направляти запити та отримувати дані.

Отже, правові режими доступу до даних ігрових платформ є важливим інструментом сучасної профілактики злочинності, але потребують обережного застосування з повагою до прав людини. США демонструють можливість поєднання потужних слідчих можливостей із запобіжниками від зловживань. Для України важливо адаптувати власний режим до міжнародних стандартів та реалій цифрового світу через чіткі процедури, міжнародну співпрацю та максимально можливу прозорість без шкоди для розслідувань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 18 U.S. Code § 2703 - Required disclosure of customer communications or records. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/ uscode/text/18/2703 (дата звернення: 24.11.2025).
2. 18 U.S. Code § 2709 - Counterintelligence access to telephone toll and transactional records. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/uscode/text/18/2709 (дата звернення: 24.11.2025).
3. Akhtyrska N. Legal regulation of electronic evidence and the practice of their use in the judiciary of Ukraine. *Uzhhorod National University Herald. Series: Law*. 2023. Vol. 2, no. 75. P. 141–150. URL: https://doi.org/10.24144/2307-3322.2022.75.2.23 (дата звернення: 24.11.2025).
4. Appellate Court. In re 381 Search Warrants Directed to Facebook, Inc. *Global Freedom of Expression*. URL: https://globalfreedomofexpression.columbia.edu/cases/re-381-search-warrants-directed-facebook-inc/ (дата звернення: 24.11.2025).
5. Brattain B. The Electronic Communications Privacy Act: Does the Act Let the Government Snoop Through Your Emails and Will It Continue?. *N.C. J.L. \& Tech. On.* 2016. Vol. 17. P. 185–218. URL: http://scholarship.law.unc.edu/ncjolt/vol17/iss5/6 (дата звернення: 24.11.2025).
6. Cimpanu C. FBI document shows what data can be obtained from encrypted messaging apps. *Cyber Security News | The Record from Recorded Future News*. URL: https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps (дата звернення: 24.11.2025).
7. Davey J. Extremism on Gaming (-Adjacent) Platforms. *Gaming and Extremism*. 2024. P. 95–109. URL: https://www.taylorfrancis.com/reader/download/fd222128-cd17-4977-bfcb-dda21bb13335/chapter/pdf?context=ubx (дата звернення: 24.11.2025).
8. Dennis S.J. Regulating Search Warrant Execution Procedure for Stored Electronic Communications. *Fordham Law Review*. 2018. Vol. 86. P. 2993–3032. URL: https://ir.lawnet.fordham.edu/flr/vol86/iss6/21 (дата звернення: 24.11.2025).

9. Discord. How Discord Works with Law Enforcement. *Discord - Group Chat*. URL: https://discord.com/safety/360044157931-working-with-law-enforcement (дата звернення: 24.11.2025).
10. Durbin Presses Social Media Platforms on their Roles in Promoting Extremist Content | United States Senate Committee on the Judiciary. *Home | United States Senate Committee on the Judiciary*. URL: https://www.judiciary.senate.gov/press/dem/releases/durbin-presses-social-media-platforms-on-their-roles-in-promoting-extremist-content (дата звернення: 24.11.2025).
11. Electronic Communications Privacy Act : An Act of 21.10.1986 no. 99-508. URL: https://www.congress.gov/bill/99th-congress/house-bill/4952/text (дата звернення: 24.11.2025).
12. Kerr O.S. Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't. *Northwestern University Law Review*. 2003. Vol. 97. P. 607–674. URL: https://doi.org/10.2139/ssrn.317501 (дата звернення: 24.11.2025).
13. Microsoft. Government Requests for Customer Data Report | Microsoft CSR. *Microsoft*. URL: https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data (дата звернення: 24.11.2025).
14. Newhouse A.B., Kowert R. Extremist identity creation through performative infighting on Steam. *Frontiers in Psychology*. 2025. Vol. 16. URL: https://doi.org/10.3389/fpsyg.2025.1586566 (дата звернення: 24.11.2025).
15. Overview of Governmental Action Under the Stored Communications Act (SCA). *Congress.gov*. URL: https://www.congress.gov/crs-product/LSB10801 (дата звернення: 24.11.2025).
16. Pfefferkorn R. We Now Know What Information the FBI Can Obtain from Encrypted Messaging Apps. *Just Security*. URL: https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/ (дата звернення: 24.11.2025).
17. Robinson N., Whittaker J. Playing for Hate? Extremism, Terrorism, and Videogames. *Studies in Conflict & Terrorism*. 2021. P. 1–36. URL: https://doi.org/10.1080/1057610x.2020.1866740 (дата звернення: 24.11.2025).
18. Romm T. White House questions tech giants on ways to predict shootings from social media. *The Washington Post*. URL: https://www.washingtonpost.com/technology/2019/08/09/white-house-questions-tech-giants-ways-predict-shootings-social-media/ (дата звернення: 24.11.2025).
19. Taddonio P. Tracing Violent White Supremacists & Online Radicalization from Charlottesville to Now. *Frontline*. URL: https://www.pbs.org/wgbh/frontline/article/white-supremacist-violence-online-extremism-charlottesville-terrorgram/ (дата звернення: 24.11.2025).
20. Thompson II R. M., Cole J. P. Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA). Congressional Research Service, 2015. 19 p. URL: https://sgp.fas.org/crs/misc/R44036.pdf (дата звернення: 24.11.2025).
21. U.S. Government Accountability Office (U.S. GAO). Countering Violent Extremism: FBI and DHS Need Strategies and Goals for Sharing Threat Information with Social Media and Gaming Companies. *U.S. Government Accountability Office (U.S. GAO)*. URL: https://www.gao.gov/products/gao-24-106262 (дата звернення: 24.11.2025).
22. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act): An Act of 26.10.2021 no. 107-56. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (дата звернення: 24.11.2025).
23. Wiretapping. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/wex/wiretapping (дата звернення: 24.11.2025).
24. Ахтирська Н.М. Міжнародне співробітництво під час кримінального провадження: теоретичні та практичні аспекти: монографія. Київ : Логос, 2019. 576 с. URL: https://nsj.gov.ua/files/1722510766Міжнародне%20співробітництво.pdf (дата звернення: 24.11.2025).
25. Ахтирська Н.М., Костюченко О.Ю. Міжнародне співробітництво під час кримінального провадження: навч. посіб. Київ: ВПЦ «Київ. ун-т», 2023. 335 с. URL: https://nsj.gov.ua/files/1722510970Ахтирська.pdf (дата звернення: 24.11.2025).
26. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001: станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 24.11.2025).
27. Конституція України: від 28.06.1996 № 254к/96-ВР: станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 24.11.2025).

28. Кримінальний процесуальний кодекс України: Кодекс України від 13.04.2012 № 4651-VI: станом на 1 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 24.11.2025).
29. Міжнародне співробітництво у кримінальному провадженні: навч. посіб. / В.В. Зуєв та ін.; ред. В.О. Туляков. Одеса: Нац. ун-т «Од. юрид. акад.», 2022. 221 с. URL: https://doi.org/10.32837/11300.26117 (дата звернення: 24.11.2025).
30. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 8 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 24.11.2025).