

УДК 343.97

DOI <https://doi.org/10.24144/2307-3322.2025.92.4.26>

КІБЕРБЕЗПЕКА ТА КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: СУЧАСНІ ТЕНДЕНЦІЇ

Піщенко Г.І.,

*кандидат юридичних наук, доцент,
професор кафедри кримінального права та кримінології
навчально-наукового інституту права та психології
Національної академії внутрішніх справ
ORCID: 0000-0003-3299-521X*

Шопіна Ю.О.,

*кандидат юридичних наук,
доцент кафедри кримінального права та кримінології
навчально-наукового інституту права та психології
Національної академії внутрішніх справ
ORCID: 0009-0004-7734-2102*

Піщенко Г.І., Шопіна Ю.О. Кібербезпека та кіберзлочинність в Україні: сучасні тенденції.

У даний час протидія кіберзлочинності є однією з найактуальніших проблем у всьому світі. Зростаюча кількість кіберзлочинців, постійне вдосконалення інформаційних технологій і, як наслідок, нові можливості вдосконалення цих кримінальних правопорушень створюють чергові загрози для глобальних інформаційних мереж і суспільства в цілому.

Метою дослідження є виокремлення сучасних тенденцій кібербезпеки та кіберзлочинності в Україні.

Досліджуючи кіберзлочинність в Україні автори дійшли наступних висновків: кіберзлочинність є самостійним різновидом злочинності, що існує поряд з насильницькою, корисливою, корупційною, екологічною, організованою, професійною та іншими видами; має високотехнологічний характер, що полягає у використанні ІТ-технологій, комп'ютерних пристроїв, інформаційно-телекомунікаційних мереж, які є способом вдосконалення інших кримінальних правопорушень (крадіжка, шахрайство, вимагання та інші); характеризується високим ступенем латентності; тісно пов'язана з організованою злочинністю; набула високоорганізованого й професійного характеру, так як особи, що вчиняють кіберзлочини мають злочинну спеціалізацію та кваліфікацію з певних видів злочинних діянь; набула транснаціонального характеру в силу своєї приналежності до комп'ютерного «андеграунду» з отриманням злочинних доходів на території двох і більше держав і набуття статусу міжнародних злочинних груп.

Змістом запобігання кіберзлочинності мають бути заходи віктимологічної профілактики (підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації). Проблема запобігання кіберзлочинності є багатогранною і полягає не тільки в змінах законодавчої сфери, але й в удосконаленні технічної та технологічної сфер.

Ключові слова: кібербезпека, кіберзлочинність, кіберзахист, безпека в кіберпросторі, конфіденційні дані, загроза інформаційним даним та системам, несанкціоновані дії з інформацією, фішинг, онлайн-шахрайство, шкідливе програмне забезпечення, високотехнологічна злочинність, захист інформаційно-телекомунікаційних мереж.

Pishchenko G.I., Shopina Y.O. Cybersecurity and cybercrime in Ukraine: current trends.

Currently, combating cybercrime is one of the most pressing problems in the world. The growing number of cybercriminals, the constant improvement of information technologies and, as a result, new opportunities for improving these criminal offenses create new threats to global information networks and society as a whole.

The purpose of the study is to identify current trends in cybersecurity and cybercrime in Ukraine.

Investigating cybercrime in Ukraine, the authors came to the following conclusions: cybercrime is an independent type of crime that exists alongside violent, mercenary, corrupt, environmental, organized, professional and other types; it has a high-tech nature, which consists in the use of IT technologies, computer devices, information and telecommunication networks, which are a way to improve other criminal offenses (theft, fraud, extortion and others); characterized by a high degree of latency; closely related to organized crime; has acquired a highly organized and professional nature, as individuals committing cybercrimes have criminal specialization and qualifications in certain types of criminal acts; has acquired a transnational nature due to its affiliation with the computer «underground» with the receipt of criminal proceeds in the territory of two or more states and the acquisition of the status of international criminal groups.

The content of cybercrime prevention should be victimological prevention measures (increasing the level of digital literacy of the population and promoting individual means of protecting personal information). The problem of preventing cybercrime is multifaceted and consists not only in changes in the legislative sphere, but also in improving the technical and technological spheres.

Key words: cybersecurity, cybercrime, cyberdefense, security in cyberspace, confidential data, threat to information data and systems, unauthorized actions with information, phishing, online fraud, malware, high-tech crime, protection of information and telecommunications networks.

Постановка проблеми. Запобігання кіберзлочинності є однією з найбільш актуальних і складних кримінологічних проблем, що існують в суспільстві. Висока латентність, винайдення та швидке поширення нових способів вчинення кіберзлочинів, вимагає від суспільства кардинально нових підходів у їх запобіганні.

Кібербезпека – це комплексна діяльність, що використовує технології, процеси та методи для захисту комп'ютерних систем, мереж, програм і даних від кібератак, несанкціонованого доступу, пошкодження та витоку інформації. Вона включає широкий спектр заходів від керування пароллями та захисту персональних пристроїв, до забезпечення безпеки корпоративних мереж та державних систем. Головною її метою є збереження конфіденційності, цілісності та доступності комп'ютерної інформації.

Кібербезпека захищає конфіденційні бізнес-дані, інтелектуальну власність та репутацію компаній від збитків і перебоїв в роботі. Поряд з цим, вона забезпечує сталий розвиток суспільства та цифрових комунікацій шляхом своєчасного виявлення та нейтралізації загроз.

У свою чергу, кіберзлочинність є злочинною діяльністю, що здійснюється за допомогою комп'ютерних систем, мереж та інформаційних технологій, яка несе безпосередню загрозу інформаційним даним та системам, державній інфраструктурі.

Метою здійсненого дослідження є виокремлення сучасних тенденцій кібербезпеки та кіберзлочинності в Україні.

Стан опрацювання проблематики. Аналіз наукового дослідження сучасного стану та тенденцій кібербезпеки та кіберзлочинності в Україні здійснювали у своїх публікаціях С. Бабанін [1]; О. Будунова [2]; В. Бутузов [3]; В. Голубєв [4]; О. Довгань та І. Доронін [5]; М. Карчевський [6; 7]; Ю. Когут [8]; М. Кравцова [9; 10]; Ю. Онищенко [11]; Ю. Піцик [12]; С. Шапочка [13] та інші науковці. Однак, сучасний стрімкий розвиток інформаційних технологій у світі, їх поширення в Україні, зумовлюють необхідність осучаснення наукових кримінологічних досліджень тенденцій у кібербезпеці та в поширенні кіберзлочинності.

Виклад основного матеріалу. На сьогодні, під час стрімкого зростання кіберзлочинів не сформовано єдиного загальноновизнаного поняття «кіберзлочинності». У своїх рекомендаціях експерти ООН, вважають, що термін «кіберзлочинність» охоплює будь-який злочин, який може вчинятися за допомогою комп'ютерної системи чи мережі, в межах комп'ютерної системи чи мережі, проти комп'ютерної системи чи мережі. По іншому, до кіберзлочинів належать такі суспільно небезпечні діяння, які вчиняються у кіберпросторі з допомогою чи в самих комп'ютерних системах чи комп'ютерних мережах, і навіть з використанням інших засобів доступу до кіберпростору, у межах комп'ютерних систем чи мереж проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

У Конвенції про Кіберзлочинність (м. Будапешт, 23.11.2001 р.) виокремлено п'ять видів комп'ютерних злочинів:

- незаконний доступ (протиправний навмисний доступ до комп'ютерної системи або її частини);
- незаконне перехоплення (протиправне навмисне перехоплення непризначених для загально-го користування комп'ютерних даних, що передаються в комп'ютерну систему, з неї або всередині такої системи, включаючи електромагнітні випромінювання комп'ютерної системи, що містять такі комп'ютерні дані);
- втручання в дані (протиправне пошкодження, знищення, погіршення, зміна або приховування комп'ютерних даних);
- втручання в систему (серйозне протиправне перешкоджання функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни чи приховування комп'ютерних даних);
- незаконне використання пристроїв (виробництво, продаж, придбання для використання, імпорту, оптовий продаж або інші форми надання в користування: пристроїв, включаючи комп'ютерні програми, розроблених або адаптованих для вчинення кримінальних правопорушень; комп'ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому або будь-якої її частини, з метою використовувати їх для вчинення кримінальних правопорушень; а також володіння одним із предметів зазначених вище, з наміром використовувати його з метою вчинення кримінальних правопорушень) [14].

В українському законодавстві такі діяння є злочинними і регулюються відповідними статтями Розділу XVI Кримінального кодексу України (далі – КК України) (злочини у сфері використання електроннообчислювальних машин), зокрема, статтями 361 (несанкціоноване втручання в роботу комп'ютерних систем), 361-1 (створення та розповсюдження вірусів); 361-2 (несанкціоновані дії з інформацією), 362 (несанкціоновані дії з інформацією, яка обробляється в ЄОМ).

Особливістю кіберзлочину вважають те, що він поєднується із використанням саме «кібернетичних технологій» у межах однієї комп'ютерної мережі або декількох таких мереж, як складової інформаційної (автоматизованої), інформаційно-комунікаційної чи електронної комунікаційної систем.

Комп'ютерний злочин є діянням, що, передусім, вчиняється з використанням будь-якої комп'ютерної техніки. Формами кримінально протиправного використання кібернетичних технологій у межах комп'ютерних мереж визначають, приміром, несанкціоноване отримання прав керування комп'ютерною мережею та її нерегламентоване використання (для прикладу, із метою спричинення аварії на виробництві шляхом дезорганізації управлінської діяльності підприємства), а також створення та використання із злочинною метою однієї комп'ютерної мережі (або поєднання декількох) проти інших таких мереж (для наприкладу, створення мережі заражених комп'ютерів для здійснення атак на веб-сайти тощо).

Таким чином, вважається, що поняття кіберзлочину є багатограним. При застосуванні норм закону про кримінальну відповідальність кіберзлочин не слід зводити до поняття «комп'ютерного кримінального правопорушення» (розділ XVI Особливої частини КК України), а враховувати, що таке діяння (кіберзлочин) вчиняється у кіберпросторі та / або з його використанням, що зазвичай супроводжується посяганнями на інші об'єкти кримінально-правової охорони [15, с. 117].

Науковцями зміст категорії «інформаційна безпека» пов'язується із безпечним функціонуванням автоматизованих (комп'ютерних) систем у всіх галузях суспільної діяльності. Антисоціальні прояви щодо недотримання правил роботи цих систем можуть призвести до значних порушень функціонування суспільства. Організовані злочинні угруповання, розуміють це і намагаються використати досягнення науково-технічного прогресу для своєї мети. У зв'язку з цим існує нагальна потреба визначення та визнання на науковому рівні організованої комп'ютерної злочинності як соціального явища і відпрацювання практичних, обґрунтованих заходів протидії їй [16, с. 118].

До найбільш характерних ознак організованої кіберзлочинності відносять:

- сукупність протиправних діянь (кіберзлочинів), учинених шляхом використання кібернетичних комп'ютерних систем управління та оброблення інформації (кіберзлочинність);
- вчинення злочинів даного виду в зв'язку зі створенням та діяльністю організованих злочинних кіберугруповань кримінально орієнтованих співтовариств користувачів кіберпростору;
- середовищем вчинення кіберзлочинів та діяльності організованих кіберугруповань є кіберпростір (штучне електронне середовище існування інформаційних об'єктів у цифровій формі, створене як наслідок функціонування кібернетичних комп'ютерних систем).

Тому, організовану кіберзлочинність визначають як сукупність кіберзлочинів, що вчиняються у зв'язку зі створенням та діяльністю у кіберпросторі організованих злочинних співтовариств його користувачів (кіберугруповань). Для досягнення злочинної мети члени кіберугруповань використовують кібернетичні комп'ютерні системи управління та оброблення інформації [17, с. 320-321].

Проведені науковцями дослідження вказують на те, що найбільш характерними рисами, які притаманні комп'ютерним злочинам, учиненим із використанням мережі Інтернет (у відсотковому відношенні) є: транскордонність (57 %); висока технічна озброєність злочинців (53,6 %); використання в якості знарядь злочину інформаційних та телекомунікаційних технологій (53,5 %); високий рівень латентності (42,1 %); електронне середовище, як місце вчинення злочину (36,97 %); організований характер (27,13 %); корупційні зв'язки у правоохоронних органах (8,57 %) [18, с. 309].

Серед основних форм проявів транснаціональної організованої злочинності в Україні виокремлюють: фальшивомонетництво; забезпечення функціонування кримінальних ринків, пов'язаних із незаконним переміщенням товарів; незаконний обіг предметів культури і давнини; комп'ютерні злочини; транснаціональна незаконна торгівля видами флори і фауни, що охороняються законом; незаконний обіг небезпечних відходів; злочинність у сфері обігу радіоактивних матеріалів; злочини, пов'язані з порушенням авторських і суміжних прав («інтелектуальне піратство»); легалізація злочинних доходів; транснаціональні корупційні діяння [19, с. 178-179].

Транснаціональну організовану злочинність визначають як негативне соціальне явище, пов'язане зі створенням та діяльністю організованих злочинних угруповань (груп, організацій, банд, інших формувань) з метою вчинення тяжких та особливо тяжких злочинів проти власності; у сфері господарської (фінансової) діяльності; пов'язаних з тероризмом, піратством та різними формами екстремізму; наркобізнесом, сексуальною експлуатацією і торгівлею людьми; незаконним обігом зброї, лікарських препаратів, творів мистецтва, вибухових та інших небезпечних (радіоактивних, хімічних) речовин; утручанням у роботу комп'ютерних мереж і автоматизованих систем державного та військового управління, об'єктів критичної інфраструктури, що мають транснаціональний (транскордонний, міжнародний) характер [20, с. 465-466].

Науковці вважають, що на сучасному етапі розвитку суспільства транснаціональна організована злочинність являє собою один із вищих рівнів кримінальної еволюції, якісно нову форму розвитку організації злочинності. Її антисоціальна, протиправна діяльність виходить за межі території і юрисдикції однієї держави, а суб'єктами є стійкі злочинні організації, діяльність і сфера впливу яких, поширюється не на одну, а на декілька країн, суміжні держави, регіони тощо.

Транснаціональні організовані угруповання діють у різних регіонах світу, мають певну спеціалізацію, використовують різноманітні методи, прийоми (шантаж, залякування, корупційні схеми), а об'єднує їх спільна мета – отримання надвисокого (максимального) прибутку з одночасним забезпеченням мінімального ризику [21, с. 84-85].

Отже, кіберзлочинність – це будь-які дії навмисного характеру, що пов'язані з використанням комп'ютерів, комп'ютерних мереж або інших цифрових пристроїв для скоєння дій, що кваліфікуються КК України як злочини.

До кіберзлочинності можна віднести:

- а) фішинг – викрадення особистих даних через підроблені веб-сайти або електронні листи;
- б) онлайн-шахрайство з використанням фальшивих інтернет-магазинів, аукціонів або телекомунікаційних засобів;
- в) встановлення шкідливого (вірусного) програмного забезпечення;
- г) соціальна інженерія (соціологічний термін), що проявляється у маніпулюванні людьми (групою людей) з метою отримання вільного доступу до їхніх особистих даних;
- д) піратство (викрадення) – незаконне розповсюдження інтелектуальної власності;
- ж) кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, так звані «тройни», «боти»);
- з) протиправний контент – пропаганда екстремізму, тероризму, наркоманії, порнографії, культу жорстокості та насильства;
- і) рефайлінг – незаконна підміна телефонного трафіку;
- к) мальваре – створення та послідовне розповсюдження вірусів і шкідливого програмного забезпечення;

л) кард-шерінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення. Враховуючи вище перелічені діяння, об'єктом кіберзлочинів може стати будь-який користувач Інтернету.

Слід відзначити, що ефективної системи профілактики даному виду злочинності у світі не існує через те, що шахраї – злочинці постійно вигадують все нові способи вчинення кіберзлочинів.

Кримінологами вже узагальнені поради які сприяють підвищенню безпеки, зокрема й собою, та допоможуть уникнути ролі «жертви» кіберзлочинів. Серед таких заходів можна виділити:

- використання захищених мереж;
- створення надійних паролей з періодичною їх зміною;
- використання інструментів конфіденційності та безпеки Google чи інших браузерів;
- постійна перевірка своїх облікових записів;
- встановлення та періодичне оновлення антивірусних програм для захисту пристроїв;
- бути в курсі та володіти інформацією про поширені способи, які використовують злочинці для того щоб розпізнавати їх.

Враховуючи сучасні виклики та необхідність покращення стану боротьби з кіберзлочинністю Уряд України в березні 2016 року прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки.

У тому ж 2016 році (червень) спочатку Президент України підписав Указ про створення Національного координаційного центру кібербезпеки, першочерговим завданням якого є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки в Україні. А у вересні того ж року, Верховна Рада України у першому читанні прийняла закон «Про основні заходи забезпечення кібербезпеки України» [22].

05 жовтня 2017 року Верховною Радою України цей закон був ухвалений в цілому. В ньому визначено основні засади функціонування національної системи кібербезпеки, а також закріплені права та обов'язки суб'єктів (держспецз'язок, міністерства, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти господарювання, якими є підприємства, установи та організації, що належать до критичної інфраструктури або надають послуги в інформаційній сфері та мають забезпечувати захист своїх інформаційних систем), що забезпечують кіберзахист. Також визначено й об'єкти кібербезпеки [23]. Цей Закон спрямований на захист суверенітету, територіальної цілісності України та забезпечення безпеки у кіберпросторі.

Кабінетом Міністрів України 07 березня 2025 року видано Розпорядження про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України [24].

Протидія кіберзлочинності вимагає від держави рішучих кроків і є одним із пріоритетних напрямів внутрішньої політики.

Необхідною є взаємодія з міжнародною спільнотою у боротьбі з цим відносно новим видом злочинності, який є міжнародною проблемою і не обмежується кордонами окремої країни. І це проблема не тільки правоохоронних органів, а й суспільства загалом.

Висновки. Дослідження тенденцій кіберзлочинності в Україні дало можливість дійти наступних висновків:

- кіберзлочинність є самостійним різновидом злочинності, що існує поряд з насильницькою, корисливою, корупційною, екологічною, організованою, професійною та іншими видами;
- вона має високотехнологічний характер, що полягає у використанні ІТ-технологій, комп'ютерних пристроїв, інформаційно-телекомунікаційних мереж, які виступають способом вдосконалення інших кримінальних правопорушень (крадіжка, шахрайство, вимагання та інші);
- кіберзлочинам притаманний високий ступінь латентності (до декількох тисяч відсотків, що обумовлено різними обставинами);
- кіберзлочинність тісно пов'язана з організованою злочинністю;
- кіберзлочинності притаманний високоорганізований і професійний характер, так як особи, що вчиняють кіберзлочини мають злочинну спеціалізацію та кваліфікацію з певних видів злочинних діянь;
- кіберзлочинність є транснаціональною в силу своєї приналежності до комп'ютерного «андеграунду» з отриманням злочинних доходів на території двох і більше держав і набуття статусу міжнародних злочинних груп.

Запобігання кіберзлочинності включає в себе заходи віктимологічної профілактики (підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації).

Проблема запобігання кіберзлочинності є багатогранною і полягає не тільки в змінах у законодавчій сфері, а й в технічній та технологічній сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бабанін С.В. Запобігання комп'ютерним кримінальним правопорушенням: наук.-практ. посіб. Дніпро: Дніпропетр. держ. ун-т внутр. справ, 2022. 91 с.
2. Будунова О. Теоретико-прикладні основи запобігання злочинності у сфері інформаційних технологій: монографія. Луцьк: Вежа-Друк, 2023. 343 с.
3. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 408 с.
4. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: навч. посіб. / В.О. Голубєв та ін.; заг. ред. Р.А. Калюжний. Запоріжжя: ГУ «ЗІМДУ», 2002. 292 с.
5. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: АртЕк, 2018. 106 с.
6. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: дис. ... д-ра юрид. наук: 12.00.08; Нац. акад. внутр. справ. Київ, 2012. 536 арк.
7. Протидія злочинам у сфері використання інформаційних технологій: інтегр. навч.-практ. посіб. / М.В. Карчевський та ін.; за ред. М.В. Карчевського. Харків: Право, 2019. 186 с.
8. Когут Ю.І. Протидія кібертероризму як загрози інформаційній безпеці України: автореф. дис. ... канд. юрид. наук: 21.07.01; ПрАТ «ВНЗ «Міжрегіон. акад. упр. персоналом». Київ, 2021. 20 с.
9. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08; Харків. нац. ун-т внутр. справ. Харків, 2016. 16 с.
10. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні: монографія. Харків: видав. Панов А.М., 2016. 210 с.
11. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації: автореф. дис. ... канд. наук з держ. упр.: 25.00.02; Нац. акад. держ. упр. при Президенті України, Харків. регіон. ін-т держ. упр. Харків, 2015. 20 с.
12. Піщик Ю.М. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика: автореф. дис. ... канд. юрид. наук: 12.00.08; ПрАТ «ВНЗ «Міжрегіон. акад. упр. персоналом». Київ, 2019. 20 с.
13. Шапочка С.В. Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж: автореф. дис. ... канд. юрид. наук: 12.00.08; Донец. юрид. ін-т МВС України. Кривий Ріг, 2018. 20 с.
14. Конвенція про кіберзлочинність (м. Будапешт, 23.11.2001 р.) (ратифікована із застереженнями і заявами Законом України № 2824-IV (2824-15) від 07.09.2005). Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 04.11.2025).
15. Федюк В.В. Поняття кіберзлочину та його застосування в нормах закону про кримінальну відповідальність. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали III Всеукр. наук.-практ. конф. (м. Київ, 23 листоп. 2023 р.). Київ, 2023. С. 115-118.
16. Гавловський В.Д. Організована комп'ютерна злочинність – загроза інформаційній безпеці держави. *Боротьба з організованою злочинністю та корупцією*: матеріали наук.-практ. конф. (м. Київ, 4-5 квітн. 2000 р.). Київ: РВВ МВС України, 2001. С. 116-118.
17. Шеломенцев В.П. Організована кіберзлочинність: до визначення поняття. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*: науково-практичний журнал. 2009. № 21. С. 314-321.
18. Тітуніна К.В. Характеристика комп'ютерних злочинів, учинених із використанням мережі Інтернет (аналіз матеріалів анкетування). *Боротьба з організованою злочинністю і корупцією (теорія і практика)*: науково-практичний журнал. 2009. № 21. С. 307-313.
19. Буркаль В.С. Протидія транснаціональній організованій злочинності у сфері економіки: дис. ... канд. юрид. наук: 12.00.08; Університет державної фіскальної служби України. Ірпінь, 2019. 234 арк.

20. Жаровська Г.П. Теорія та практика протидії транснаціональній організованій злочинності в Україні: дис. ... канд. юрид. наук: 12.00.08; Національна академія внутрішніх справ. Київ, 2019. 593 арк.
21. Ткачова О.В. Транснаціональна організована злочинність як сучасне явище: визначення й основні риси. *Теорія і практика правознавства*. 2021. Вип. 1 (19). С. 78-87; DOI: 10.21564/2225-6555.2021.19.235600 (дата звернення: 04.11.2025).
22. Указ Президента України Про Національний координаційний центр кібербезпеки від 07.06.2016 № 242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#Text> (дата звернення 04.11.2025).
23. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 04.11.2025).
24. Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України» від 7 березня 2025 р. № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text> (дата звернення 04.11.2025).