

ДЕМЕДЮК С. В.,

кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України
(Національна академія
Служби безпеки України)
Стаття поширюється на умовах
ліцензії CC BY 4.0

УДК 343.9

DOI <https://doi.org/10.32842/2078-3736/2025.4.2.28>

СУЧАСНІ ТЕНДЕНЦІЇ ON-LINE ШАХРАЙСТВА В УКРАЇНІ

Онлайн-шахрайство є складною та динамічною загрозою в сучасному цифровому світі, що охоплює різні форми обману, включаючи фішинг, вішинг, смішинг, шахрайство через підроблені інтернет-магазини та схеми з криптовалютою. Ця стаття містить детальний аналіз основних аспектів онлайн-шахрайства, підкреслюючи його поширеність як в Україні, так і в усьому світі. Основна увага приділяється використанню соціальної інженерії, автоматизації шахрайських схем, бот-мереж та штучного інтелекту для створення злочинів із використанням дипфейків. Ці технології роблять шахрайство все більш складним для виявлення та боротьби з ним.

В Україні онлайн-шахрайство є одним з найпоширеніших кіберзлочинів, на яке припадає 36% усіх злочинів у цій сфері. Поширеними видами є підроблені веб-сайти, шахрайські продажі, дзвінки від нібито представників банків або державних установ, а також використання соціальних мереж та месенджерів для поширення підроблених інвестиційних пропозицій. У статті підкреслюється вплив війни в Україні, яка призвела до зростання кількості схем, що маніпулюють емоціями громадян через теми волонтерства та гуманітарної допомоги.

Автор вказує, що основною мотивацією злочинців є фінансова вигода, хоча деякі кіберзлочини пов'язані з гібридною війною та співпрацею з агресором. У статті підкреслюється важливість інтеграції міжнародного досвіду в боротьбі з шахрайством та адаптації правової бази для вирішення викликів цифрової ери.

Рекомендації зосереджені на впровадженні багаторівневих технологій захисту, моніторингу транзакцій, використанні штучного інтелекту для перевірки особи та боротьбі з підробками. Автор наголошує на необхідності глобальної координації та розробки інноваційних підходів до аналізу кіберзагроз для ефективного протистояння викликам сучасного кіберпростору.

Ключові слова: кіберзлочинність, онлайн-шахрайство, фішинг, вішинг, криптовалюта, електронні гроші.

Demediuk S. V. Current trends in online fraud in Ukraine

Online fraud is a complex and dynamic threat in the modern digital world, encompassing various forms of deception, including phishing, vishing, smishing, fraud via fake online stores, and cryptocurrency schemes. This article provides a detailed analysis of the main aspects of online fraud, emphasizing its prevalence both in Ukraine and globally. The focus is on the use of social engineering, automation of fraudulent schemes, bot networks, and artificial intelligence for creating deepfake crimes. These technologies make fraud increasingly difficult to detect and combat.



In Ukraine, online fraud is one of the most widespread cybercrimes, accounting for 36% of all crimes in this sector. Common types include fake websites, fraudulent sales, impersonation calls from alleged representatives of banks or government institutions, and the use of social media and messengers to spread fake investment proposals. The article highlights the impact of the war in Ukraine, which has led to a rise in schemes manipulating citizens' emotions through themes of volunteering and humanitarian aid.

The authors indicate that the primary motivation of criminals is financial gain, although some cybercrimes are linked to hybrid warfare and collaboration with aggressors. The article underscores the importance of integrating international experience in combating fraud and adapting the legal framework to address the challenges of the digital era.

Recommendations are centered on the implementation of multi-layered protection technologies, transaction monitoring, the use of artificial intelligence for identity verification, and combating forgeries. The authors emphasize the necessity of global coordination and the development of innovative approaches to analyzing cyber threats to effectively counter the challenges of the modern cyber landscape.

Key words: *cybercrime, online fraud, phishing, vishing, cryptocurrency, electronic money.*

Постановка проблеми. On-line шахрайство є однією з найпоширеніших загроз у сучасному цифровому середовищі. Воно охоплює різноманітні способи обману користувачів з метою заволодіння їхніми фінансами, конфіденційною інформацією або іншими активами. Основними типами шахрайства є фішинг, що передбачає використання підроблених веб-сайтів чи електронних листів для крадіжки даних, та вішинг, коли шахраї телефонують, видаючи себе за представників банків чи інших установ. Схожі методи, такі як смішинг (шахрайство через SMS), також набирають популярності.

Широко застосовується соціальна інженерія, що ґрунтується на маніпуляції емоціями або поведінкою жертви, а також підробка інтернет-магазинів, що спонукає користувачів робити покупки на шахрайських платформах. Особливого поширення набувають криптовалютні шахрайства, які використовують складність розуміння нових фінансових інструментів.

Сучасні тенденції свідчать про посилення автоматизації шахрайських схем, що забезпечує швидке поширення обману через бот-мережі. Зростає роль «даркнету», який виступає платформою для обміну шахрайськими інструментами та даними. У світовому контексті спостерігається підвищення масштабів шахрайства з використанням штучного інтелекту, зокрема для підробки голосу та відео.

Ця проблема вимагає інтегрованого підходу до аналізу, врахування міжнародного досвіду та постійного моніторингу нових шахрайських тактик.

На глобальному рівні on-line шахрайство демонструє динаміку зростання. Міжнародні дослідження свідчать, що ключовими факторами успішності шахрайських схем є швидке використання технологічних проривів, таких як штучний інтелект, та людська довірливість. Наприклад, у світі зростає кількість випадків deepfake-шахрайства, коли за допомогою синтетичного відео і голосу створюються правдоподібні повідомлення для виманювання грошей чи інформації.

У багатьох країнах кількість скарг на кіберзлочини зростає щороку. Наприклад, у США Федеральна торгова комісія звітує про мільйони звернень, пов'язаних із шахрайством, серед яких домінують фішинг та підроблені on-line продажі. Водночас Європейський Союз значну увагу приділяє гармонізації законодавства, спрямованого на захист споживачів у цифровій економіці.

В Україні проблема on-line шахрайства також актуальна, особливо в умовах широкого впровадження цифрових послуг та електронного урядування. Найпоширенішими видами шахрайства залишаються фішинг та псевдопродажі, а також шахрайські дзвінки,



що імітують представників банків чи державних органів. Особливо активно шахраї використовують соціальні мережі та месенджери для поширення фейкових пропозицій чи закликів до «інвестицій».

Крім того, війна в Україні створила нові виклики у сфері кіберзлочинності. Зокрема, спостерігається зростання шахрайських схем, які експлуатують волонтерську діяльність або гуманітарну допомогу. Ці схеми часто спрямовані на маніпуляцію емоціями громадян і спонукають до спонтанних фінансових переказів на рахунки шахраїв.

Загалом, проблеми протидії кіберзлочинності не одне десятиріччя є предметом наукових досліджень. Значну увагу цим питанням приділяли у своїх роботах відомі науковці та фахівці: Азаров Д. [3], Беяков К. [2], Бутузов В. [4; 5], Гавловський В. [6; 7; 17; 19], Гавриленко І. [8], Гриненко І. [9], Гуцалюк М. [10; 11], Золотар О. [2], Кудінов В. [12], Рижков Е. [15], Сліпченко Т. [16], Тітуніна К. [5, 7], Хахановський В. [1; 18; 19], Шеломенцев В. [13; 20; 21], зокрема і в зарубіжних виданнях [22-25].

Водночас, враховуючи стрімкий технологічний розвиток інформаційного простору та цифрового контенту, окремі напрями кіберзлочинів набувають особливого розвитку та поширення і є загрозою не лише сучасного світу, а й майбутніх процесів та суспільних відносин, зокрема це стосується і on-line шахрайства.

В електронному виданні «2024 Future of Fraud Forecast» від Experian окреслено сучасні виклики та інноваційні підходи до боротьби з цим явищем [26].

Підкреслено, що шахраї дедалі частіше використовують генеративний штучний інтелект для створення підроблених документів, профілів у соцмережах та фейкових відео. Це робить шахрайство доступнішим і складнішим для виявлення. У публікації пропонується використовувати багатогарбові технології захисту, щоб ефективно протидіяти цим загрозам. Також особливу увагу приділено проблемам фальсифікації особистостей (synthetic identity fraud), яка може призвести до втрат до 5 мільярдів доларів у 2024 році.

У статті «From Phishing to Friendly Fraud: Anticipating 2024's Fraud Dynamics» аналізується так зване «friendly fraud» - ситуація, коли клієнти навмисно або через непорозуміння запитують повернення коштів за товари чи послуги [27]. У 2023 році кількість таких випадків зросла на 19%. Як один із підходів до боротьби, рекомендується впроваджувати цифрові інструменти для підтвердження доставки товарів та полегшення процесів повернення, щоб зменшити мотивацію до зловживань.

У вказаних публікаціях також пропонується компаніям оцінювати свої ризики та впроваджувати новітні інструменти на базі штучного інтелекту для моніторингу транзакцій, перевірки особистостей і боротьби з фальсифікацією. Крім того, акцентується на зростанні шахрайства з чеками, яке стає актуальним через масові крадіжки пошти.

Метою цієї статті є дослідження проблематики on-line шахрайства та сучасна специфіка його прояву в Україні, враховуючи окремі характеристики та ознаки.

Виклад основного матеріалу. Зазначений сегмент кіберзлочинності є сучасним різновидом шахрайства (ст. 190 ККУ) і у переважній більшості є безпосереднім об'єктом протидії підрозділами кіберполіції НПУ (ч. 4 ст. 190 ККУ – шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки) [28]. Виділення цього виду кримінального правопорушення обґрунтовується значним зростанням використання телекомунікаційних технологій при їх вчиненні, що і визначає специфіку об'єктивної сторони цього злочину.

On-line шахрайства є найбільш поширеним видом кіберзлочину і в Україні (рис. 1). Питома вага його у загальній сукупності кримінальних правопорушень, при вчиненні яких використовуються сучасні інформаційні та телекомунікаційні технології, складає 36%. Несанкціоноване втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж складає 26%, а незаконні дії з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення – 22%, у загальній сукупності злочинів, протидія яким є пріоритетом кіберполіції.



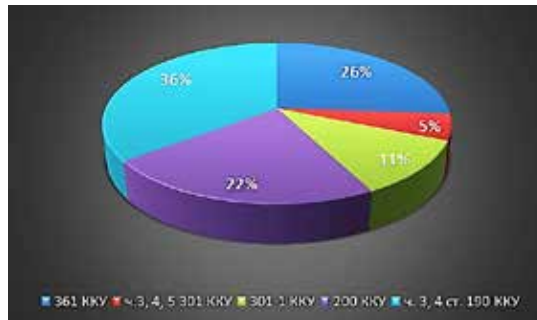


Рис. 1. Питома вага кіберзлочинів

Враховуючи латентність шахрайства, а також те що цей вид злочину загалом є об'єктом протидії не лише кіберполіції (за об'єктивною стороною складу злочину), важливим є зазначити на характері джерела за експертним опитуванням (рис. 2.). Лише у 59,8% це матеріали кримінальних проваджень. Близько 30% експертів були зорієнтовані на основі аналітичних матеріалів, що суттєво доповнює загальну характеристику поширення on-line шахрайства в Україні.



Рис. 2. Характер джерела інформації про злочини

Таким чином, 84% шахрайств вчиняються саме у формі діяльності передбаченої частинами 3 та 4 ст.190 ККУ (рис. 3), що ще раз підкреслює надзвичайну поширеність on-line шахрайства в Україні.

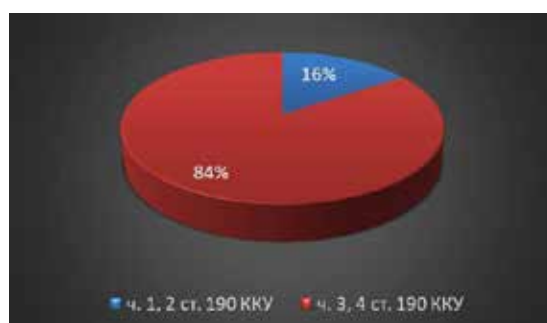


Рис. 3. Питома вага злочинів, передбачених ч. 3, 4 ст.190 ККУ



Водночас, за даними експертного опитування, діяння передбачені частинами 3 та 4 ст. 190 ККУ, також характеризуються найбільшими збитками (табл. 1). І хоча питома вага збитків до 5 млн. грн. у кожному конкретному випадку є переважальною, все ж мають місце значні збитки, що значно перевищують зазначену суму, а в окремих випадках більше 1 млрд. грн.

Таблиця 1

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	ч. 1, 2 ст. 190 ККУ	ч. 3, 4 ст. 190 ККУ
Менше 100 тис		
100 тис - 500 тис		
500 тис - 1 млн		
1 млн - 5 млн		
5 млн - 50 млн		
50 млн - 500 млн		
500 млн - 1 млрд		
більше 1 млрд		

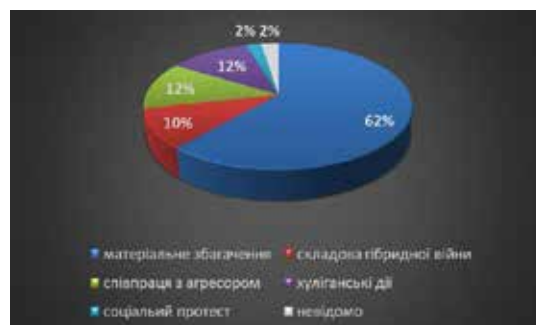
Крім того, при розгляді наслідків вчинення к/п цієї групи, серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас, значні збитки несуть також і державні та комерційні підприємства від протиправної діяльності, передбаченої саме частинами 3 та 4 ст. 190 ККУ (табл. 2).

Таблиця 2

Співвідношення злочинів за наслідками їх вчинення та за суб'єктом посягання

	ч. 1, 2 ст. 190 ККУ	ч. 3, 4 ст. 190 ККУ
Державі		
Державному органу		
Державному підприємству (установі)		
Комерційному підприємству		
Фізичній особі		

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, що характеризується вибіркою 62% в межах генеральної сукупності (рис.4). Водночас, вибіркою в межах 10% ця група злочинів характеризується як складова гібридної війни проти України. Має місце і співпраця з російським агресором у вчиненні цієї групи злочинів, яка оцінюється на рівні 12%.

**Рис. 4. Мотивація злочинців, що вчиняють злочини передбачені ч. 3, 4 ст. 190 ККУ**

За методологією Європол ІОСТА, із врахуванням значної різноманітності способів та засобів, що використовуються при здійсненні платежів, розрізняється два види шахрайства з платежами: з використанням картки та без такої.

Експертною групою було ідентифіковано 17 загроз поширення шахрайства з платежами без використання банківської картки (табл.3). За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами, пов'язані з: роздрібною торгівлею фізичними (51,4%) та віртуальними товарами (40,6%); конвертацією валют (криптовалют та електронних грошей) (46,6%); а також позиною (46,6%).

Таблиця 3

Загрози шахрайства з платежами, без використання банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ БЕЗ ВИКОРИСТАННЯ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
2.1. пов'язане з транспортом – авіаквитки		23,3				33,91
2.2. пов'язане з транспортом – квитки на поїзд або автобус		30				34,00
2.3. пов'язане з транспортом – оренда автомобілів		22,6				31,83
2.4. пов'язане з позиною (послугою, орендою приміщення тощо)		46,6				37,43
2.5. пов'язане з веб-сайтами азартних ігор		37,1				33,67
2.6. пов'язане з роздрібною торгівлею – фізичні товари		51,4				39,52
2.7. пов'язане з роздр торг– віртуальні товари		40,6				36,66
2.8. пов'язане з конвертацією валют (криптовалют та електр грошей)		46,6				38,95
2.9. з використанням паливних карток		37,4				34,62
2.10. з використанням карток у роздрібній торгівлі продуктам		28,3				32,53
2.11. з використанням клубних карток		16,3				28,33
2.12. з використанням подарункових карток		18,3				28,60
2.13. з використанням ігрових карток		19,7				29,01
2.14. на ринку мобільного зв'язку		30,6				32,23
2.15. в сфері комп'ютерних ігор (внутрішньоігрові перекази)		29,7				30,02
2.16. пов'язане з букмекерськими послугами		28,3				31,29
2.17. пов'язане з «move to»		21,1				29,89

Експертами зазначається про певне загальне зниження масштабів поширення цієї групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення, хоча окремі з них характеризуються меншим трендом до зниження масштабів, зокрема, пов'язані з: позиною, роздрібною торгівлею фізичними товарами, конвертацією валют (криптовалют та електронних грошей) та використанням паливних карток.

Зазначені види загроз шахрайства з платежами, без використання банківської картки, характеризуються і найвищим ризиком поширення у післявоєнний період, зокрема, пов'язані з: роздрібною торгівлею фізичними товарами (39,52%), конвертацією валют (криптовалют та електронних грошей) (38,95%), позиною (37,43%) та роздрібною торгівлею віртуальними товарами (36,66%).

Водночас, експертною групою було ідентифіковано 13 загроз, у якості різновиду поширення шахрайства з платежами, з використанням банківської картки (табл. 4). За сучасного стану, враховуючи і перші роки повномасштабного вторгнення, найбільшим поширенням серед таких загроз характеризуються: зняття готівки з банківських карт UA в межах UA (63,70%); шахрайство з платіжними картками (фішинг) (52,3%); зняття готівки з банківських карт UA за межами UA (46,0%); PoS-покупки з використанням скомпрометованої платіжної карти (45,1%), а також шахрайство з телефоном та інтернетом (вішинг) (44,9%).

Переважною частиною експертів зазначається про незмінність масштабів поширення зазначеної групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення. Водночас, окремі загрози, характеризувалися певним трендом підвищення масштабів поширення (рис. 5): шахрайство з платіжними картками (фішинг); зняття готівки з банківських карт UA в межах UA; зняття готівки з банківських карт UA за межами UA (рис. 5).



Таблиця 4

Загрози шахрайства з платежами, з використанням банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ З ВИКОРИСТАННЯМ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
3.1. Зняття готівки з банківських карт UA за межами UA		46,00				40,45
3.2. Зняття готівки з банківських карт UA в межах UA		63,70				42,23
3.3. Зняття готівки з іноземних банківських карток у межах UA		38,60				37,40
3.4. PoS-покупки з використанням скомпрометованої платіж карти		45,10				38,35
3.5. Шахрайство з платіжними картками: трешінг		30,90				33,40
3.6. Шахрайство з платіжними картками: фармінг		32,00				34,23
3.7. Шахрайство з платіжними картками: фішинг		52,30				42,80
3.8. Шахрайство з банкоматом: скімінг		37,40				35,67
3.9. Шахрайство з банкоматом: траппінг		29,10				33,04
3.10. Шахрайство з банкоматом: фантом		27,40				32,36
3.11. Шахрайство з банкоматом: jacking		26,90				32,17
3.12. Шахрайство з телефоном та інтернетом: вішинг		44,90				38,26
3.13. Шахрайство з телефоном та інтернетом: смішинг		38,60				36,06



Рис. 5. Сучасний тренд окремих загроз шахрайства з платежами

Оцінюючи ризики поширення групи загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період, такий же різновид шахрайства характеризується найвищим ризиком (рис.6): шахрайство з платіжними картками (фішинг) (42,8%); зняття готівки з банківських карт UA в межах UA (42,23%); та зняття готівки з банківських карт UA за межами UA (40,45%).

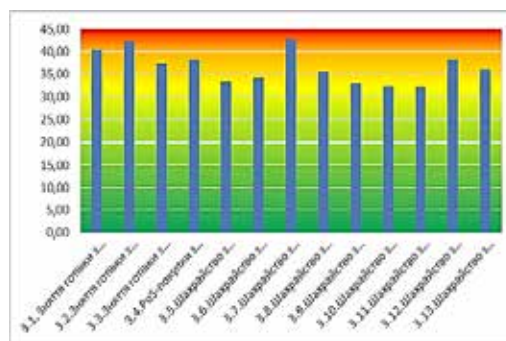


Рис. 6. Оцінка ризиків поширення загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період

Висновки. Онлайн-шахрайство стає все більш значущою загрозою у цифровій епосі, зокрема і в Україні. Цей вид злочинів характеризується фішингом, вішингом, смішингом та шахрайствами, пов'язаними із криптовалютами та соціальною інженерією. Стрімкий розвиток технологій, таких як штучний інтелект, сприяє появі нових методів шахрайства, наприклад, deepfake-злочинів, які використовують синтетичні відео та голос.

В Україні ключовими аспектами є використання цифрових технологій для обману та експлуатація емоцій, зокрема у сфері гуманітарної допомоги під час війни. Шахрайство через фальшиві сайти та псевдопродажі становить значну частку кіберзлочинів, а жертвами найчастіше стають фізичні особи, держава та комерційні організації.

Дослідження також свідчать про високий рівень ризику поширення загроз у післявоєнний період, таких як шахрайство з банківськими картками, зняття готівки за межами України, і шахрайство у роздрібній торгівлі.

Для ефективної протидії необхідно впроваджувати багатопланові технології захисту, інструменти штучного інтелекту для моніторингу транзакцій, підтвердження особистостей, і боротьби з фальсифікацією. Законодавчі ініціативи, координація на глобальному рівні та адаптація до швидко змінюваних умов кіберпростору є ключовими напрямками для стримування цих загроз.

Список використаних джерел:

1. Khakhanovskiy, V., & Hrebinkova, M. (2022). Identification, collection, and investigation of electronic imagery as sources of evidence. *Law Journal of the National Academy of Internal Affairs*, 12(4), 28–39. DOI: 10.56215/04221204.28
2. Zolotar, O. O., Zaitsev, M. M., Topolnitskiy, V. V., Bieliakov, K. I., & Koropatnik, I. M. (2021). Prospects and current status of defence information security in Ukraine. *Linguistics and Culture Review*, 5(S3), 513–524. DOI: 10.37028/Lingcure.V5ns3.1545
3. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. Київ : Атіка, 2007. 304 с.
4. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КИТ, 2010. 408 с.
5. Бутузов В.М., Тітуніна К.В. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією*. 2007. № 17. С. 316–324.
6. Гавловський В.Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право*. 2019. № 2(30). С. 105–110.
7. Гавловський В.Д., Тітуніна К.В. Деякі сучасні проблеми протидії комп'ютерній злочинності та комп'ютерному тероризму. *Науково-практичний журнал Міжвідомчого науково-дослідного центру з питань організованої злочинності та корупції*. 2008. № 19. С. 247–251.
8. Гавриленко І. Комп'ютерна злочинність. *Юридичний вісник України*. 1997. № 28. С. 3.
9. Гриненко І., Прокоф'єва-Янчиленко Д., Прокоф'єв М. Структура кримінальних відносин у кіберпросторі. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2013. Вип. 1. С. 27–33.
10. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1(28). С. 118–128.
11. Гуцалюк М.В., Хахановський В.Г. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2020. № 31(1), 13–19. <https://doi.org/10.37025/1992-4437/2019-31-1-13>.
12. Кудінов В.А., Орлов Ю.Ю. Підготовка фахівців з протидії кіберзлочинності. *Бюлетень з обміну досвідом роботи*. 2011. № 138. С. 23–34.
13. Погорецький М.А., Шеломенцев В.П. Комп'ютерна система як знаряддя вчинення злочину. *Вісник Харківського національного університету ім. В. М. Каразіна. Серія «Право»*. 2009. № 872. Вип. 6. С. 117–121.
14. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2 (2). С. 77–81.



15. Рижков Е.В., Хараберюш І.Ф. Правовий, кадровий та технічний аспект в боротьбі зі злочинністю у сфері інформаційних технологій. *Проблеми правознавства та правоохоронної діяльності*. 2002. № 1. С. 185–191.
16. Сліпченко Т. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства*. 2020. № 1 (21). С. 128–133.
17. Таран О.В., Гавловський В.Д. Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право*. 2021. № 4(39). С. 193–201.
18. Хахановський В.Г. Проблеми теорії і практики криміналістичної інформатики : монографія. Київ : Вид. Дім „Аванпост-Прим”, 2010. 382 с.
19. Хахановський В.Г., Гавловський В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. 2020. № 2(33). С. 99–110.
20. Шеломенцев В.П. Кібернетичний аспект комп'ютерних злочинів. *Правова інформатика*. 2009. № 4 (24). С. 62–66.
21. Шеломенцев В.П. Організована кіберзлочинність: до визначення поняття. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. Вип. 21. С. 314–322.
22. Halvin, S., Kenett, D.Y., Ben-Jacob, E., Bunde, A., Choen, R., Hermann, H., Kantelhardt, J.W., Kertesz, J., Kirkpatrick, S., Kurths, J., Portugali, J. & Solomon, S. (2012). Challenges in network science: applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics*, 214, 273–293.
23. Jansen, W. (2009). Directions in security metrics research. *The National Institute of Standards and Technology (NISTIR)*, 7564. Retrieved from http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf
24. Bartol, N., Bates, B., Goertzel, K. & Winograd, T. (2009). Measuring cyber security and information assurance: a state of the art report. Retrieved from <https://www.thecsiac.com/sites/default/files/cybersecurity.pdf>
25. Bodeau, D. & Graubart, R. (2011). Cyberresiliency engineering framework. MTR110237. Retrieved from http://www.mitre.org/sites/default/files/pdf/11_4436.pdf3
26. Future of Fraud Forecast. (2024) Experian. <https://www.experianplc.com/newsroom/press-releases/2024/experian-releases-2024-future-of-fraud-forecast-#:~:text=To%20thwart%20fraudulent%20activity%20in,mitigate%20risk%20and%20protect%20consumers>.
27. From Phishing to Friendly Fraud: Anticipating 2024's Fraud Dynamics. (2024) Merchant Fraud Journal. <https://www.merchantfraudjournal.com/from-phishing-to-friendly-fraud-anticipating-2024s-fraud-dynamics/>.
28. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ЮОСТА. *Південноукраїнський правничий часопис*. № 3. 2023. С. 44–46. DOI <https://doi.org/10.32850/sulj.2023.3.10>

Дата першого надходження рукопису до видання: 21.07.2025

Дата прийнятого до друку рукопису після рецензування: 22.08.2025

Дата публікації: 26.09.2025

