

Демедюк С.В.

*кандидат юридичних наук,
заступник секретаря Ради національної
безпеки і оборони України
Національна академія Служби безпеки України*

ТЕМНА СТОРОНА КОМП'ЮТЕРНИХ МЕРЕЖ: ЗЛОЧИНИ ТА НЕЗАКОННА ДІЯЛЬНІСТЬ ОНЛАЙН

Постановка проблеми. Використання комп'ютерних систем та мереж злочинцями є однією з ключових загроз сучасного суспільства, яка має глобальний характер і постійно еволюціонує. Основною проблемою є те, що інформаційні технології, які створювалися для спрощення життя та підвищення ефективності в різних сферах, стали зручним інструментом для реалізації злочинних намірів. Кіберзлочинці використовують ці технології для крадіжок даних, шахрайства, вимагання, атак на критичну інфраструктуру, а також для дезінформації та маніпуляції громадською думкою.

Глобальні тенденції свідчать про зростання кількості та складності кібератак. Однією з ключових загроз є поширення програм-вимагачів, які шифрують дані користувачів із метою вимагання викупу. Активно розвивається також діяльність хакерських угруповань, які часто діють у складі організованих злочинних мереж або за підтримки державних структур. Злочинці постійно удосконалюють свої методи, використовуючи штучний інтелект, технології анонімізації та криптовалюти для ускладнення їхнього відстеження.

В Україні, з огляду на тривалу війну, кіберзлочинність набуває ще більшого значення. Атаки на державні установи, енергетичну інфраструктуру, банки та медіа-системи стали елементом гібридної війни, яку веде Російська Федерація. Кіберзлочинці також використовують війну для фінансових

шахрайств, спрямованих на пересічних громадян, зокрема через фейкові збори коштів або фішингові атаки. В умовах війни особливу небезпеку становлять дезінформаційні кампанії, що мають на меті підірвати довіру до уряду та суспільної єдності.

Таким чином, сучасна кіберзлочинність є не лише технологічним викликом, а й соціальним і політичним феноменом. Україна, як країна, що перебуває у стані війни, стикається з підвищеними ризиками в цій сфері. Це вимагає посилення кіберзахисту, розвитку міжнародного співробітництва та адаптації національних стратегій до умов глобальної кіберзагрози.

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], Беляков 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, у низці публікацій надається глибокий аналіз проблематики кіберзлочинності в сучасних умовах та пропонуються шляхи протидії цим загрозам. Так, дослідження [26] присвячене питанням кіберзлочинності в Україні під час воєнного стану. Автор аналізує активність кіберзлочинців, спрямовану на

злам урядових серверів та інших критичних об'єктів, та обговорює заходи протидії таким діям. У статті [27] досліджуються сучасні тенденції кіберзлочинності, зокрема організовані її форми. Автор пропонує заходи щодо посилення протидії кіберзлочинності та підвищення ефективності боротьби з нею. Поряд з тим, такі публікації базуються на зовнішніх джерелах, сторонніх дослідженнях і емпірична база є певним чином застаріла. Але, 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.

Метою цієї статті є дослідження проблематики щодо використання злочинцями комп'ютерних систем та мереж, враховуючи окремі характеристики та ознаки.

Виклад основного матеріалу. Кримінальні правопорушення у сфері використання комп'ютерів, систем та комп'ютерних мереж є найбільш поширеними і безпосереднім віддзеркаленням змісту та рівня кіберзлочинності. До цього переліку відносяться кримінальні правопорушення передбачені такими статтями ККУ:

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Стаття 361¹. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Стаття 361². Несанкціоновані збут або розповсюдження інформації з обмеженим

доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Стаття 363¹. Перешкодження роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Найбільш поширеними, за даними опитування [28], у зазначеному переліку є к/п, передбачені статтею 361 ККУ (53,02%) (табл. 1). Така тенденція корелюється і з даними ЄРДР (червона зона). Водночас, на відміну від опитування (6,67% – жовта зона), за даними ЄРДР значною поширеністю додатково характеризується і злочин передбачений ст. 362 ККУ (червона зона 35–48% за відповідними роками), що пояснюється врахуванням діяльності і інших правоохоронних органів.

Таким чином, за даними експертного опитування найбільшими збитками матеріального та нематеріального характеру характеризується також к/п передбачене ст. 361 ККУ (табл. 2). І хоча питома вага збитків до 5 млн. грн. у кож-

Таблиця 1

Співвідношення кількості злочинів за даними опитування та ЄРДР

Стаття ККУ	361	361-1	361-2	362	363	363-1
За даними опитування, %	53,02	6,35	4,76	6,67	2,86	1,11
ЄРДР 2021, %	50,73	1,06	4,26	43,50	0,36	0,09
ЄРДР 2022, %	41,08	8,20	1,76	48,73	0,09	0,15
ЄРДР 2023, %	59,18	0,91	4,30	35,28	0,29	0,05

Таблиця 2

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	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	Нематеріал ьні збитки
361									
361-1									
361-2									
362									
363									

ному конкретному випадку є переважаючою, лише ці к/п вказують і на великі збитки, що значно перевищують зазначену суму, а в окремих випадках більше 1 млрд. грн.

Водночас, інші к/п цієї групи характеризуються як у сукупному врахуванні, так і у кожному конкретному випадку, меншими сумами матеріальних збитків, переважно до 5 млн. грн. Хоча за ст. 362 ККУ наслідки вчинення к/п в окремих випадках характеризуються збитками і до 1 млрд. грн.

Крім того, за даними експертного опитування, при розгляді наслідків вчинення к/п цієї групи, із врахуванням суб'єкта посягання (табл. 3), найбільшими збитками характеризується також протиправна діяльність, передбачена статтями ККУ 361 та 362, а серед суб'єктів переважно їх зазнають фізичні особи та держава.

При вчиненні цієї групи злочинів, злочинці використовують різноманітні специфічні інструменти (послуги).

Серед операційних систем найчастіше використовується злочинцями Kali

Linux – 33%, що значно частіше у порівнянні з BlackArch Linux (11%), BackBox Linux (10%) та Parrot Security OS (9%) (табл. 4, рис. 1).

Водночас, з метою несанкціонованого втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж, значно зростає питома вага використання злочинцями операційної системи Kali Linux – 41% (рис. 2)

Серед спеціального програмного забезпечення експерти виділяють DoS-атаки (22%), спамінг (21%), брутфорс (24%) та пентестинг (9%) (табл. 5, рис. 3).

Водночас, з метою несанкціонованого втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж, значно зростає питома вага використання злочинцями спеціального програмного забезпечення Брутфорс та DoS-атак, а спамінг є більш характерним для розповсюдження шкідливих програмних чи технічних засобів та несанкціонованих дій з інформацією (табл. 5).

Таблиця 3

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

	361	361-1	361-2	362	363
Державі					
Державному органу					
Державному підприємству (установі)					
Комерційному підприємству					
Фізичній особі					

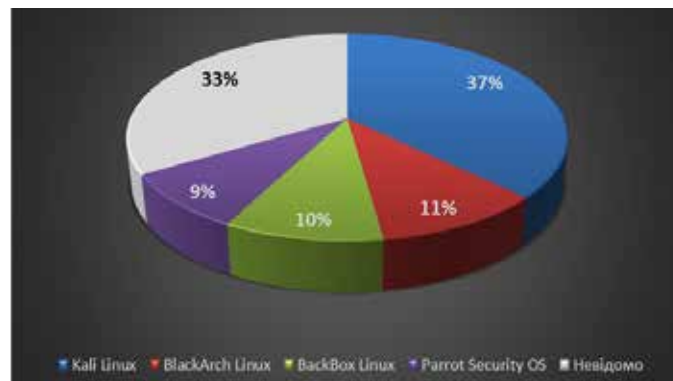


Рис. 1. Питома вага видів операційних систем, що використовуються злочинцями

Таблиця 4

Види операційних систем, що використовуються злочинцями

Операційні системи	361 ККУ	361-1 ККУ	362 ККУ
Kali Linux			
BlackArch Linux			
BackBox Linux			
Parrot Security OS			
Невідомо			

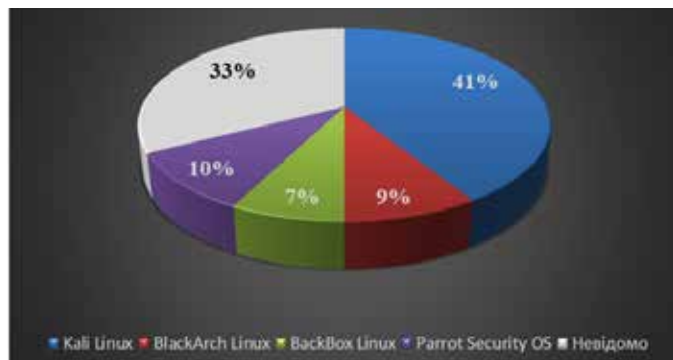


Рис. 2. Питома вага видів операційних систем, що використовуються при вчинення к/п, передбаченого ст. 361 ККУ

Таблиця 5

Використання злочинцями спеціального програмного забезпечення

Використання спеціального програмного забезпечення	361 ККУ	361-1 ККУ	362 ККУ
DoS-атака			
Спамінг			
Брутфорс			
Пентестинг			
Невідомо			



Рис. 3. Питома вага видів операційних систем, що використовуються злочинцями

Такого роду спеціальне програмне забезпечення злочинці можуть рівнозначно отримувати, використовуючи ресурси соціальних мереж, форумів та Darknet (табл. 6).

Досліджуючи зазначену групу злочинів, важливо також з'ясувати основні способи їх вчинення.

Експертною групою кіберполіції було виділено чотири ключові групи, що об'єднували основні способи вчинення таких злочинів (табл. 7).

За способом отримання доступу до телекомунікаційних каналів та комп'ютерних мереж найчастіше злочинці використовують перехоплення інформації при її передачі, а також відкритий доступ до ПК. Значно рідше використовується проникнення до приміщень. При цьому, перехоплення трафіку переважно здійснюється за допомогою шкідливого ПЗ, яке отримує авторизаційні дані з браузера (Stiller). Хоча значною питомою вагою серед способів перехоплення трафіку залишається фактор «людина посередині», а також «паралельна сесія» та «отруйний DNS».

За способом віддаленого отримання доступу, рівнозначним є використання злочинцями реальних паролів користувачів, як отриманих в мережі, так і шляхом перебору за допомогою спеціальних програм.

Шкідливе програмне забезпечення злочинці розповсюджують, використовуючи широкий перелік засобів: месенджери, соціальні мережі, електронну пошту, sms-повідомлення та різноманітні сайти.

Водночас месенджери та соціальні мережі є найбільш поширеним засобом отримання потерпілими посилання на шкідливе програмне забезпечення.

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, на що вказує більше 60% експертів за матеріалами проваджень (табл. 8). Поряд з цим, важливим є зазначити, що в межах 10% оцінюється можливість вчинення цієї групи злочинів як складової гібридної війни проти України. Водночас, трохи більший відсоток злочинів (до 13%) характеризується співпрацею з російським агресором.

Таблиця 6

Джерела отримання злочинцями спеціального програмного забезпечення

Джерело отримання програмного забезпечення злочинцями	361 ККУ	361-1 ККУ	362 ККУ
Даркнет			
Форуми			
Соціальні мережі			
Невідомо			

Таблиця 7

Способи вчинення злочинів

	361 ККУ	361-1 ККУ	362 ККУ
За способом отримання доступу:			
Шляхом перехоплення інформ при її передачі телекомунікацій каналами і комп'ютерними мережами			
Шляхом проникнення до приміщення, в якому знаходиться ПК			
Шляхом відкритого доступу до ПК			
Невідомо			
За способом віддаленого отримання доступу:			
Використання зловмисниками реальних паролів користувачів, отриман в мережі			
Отримання паролів, ключів шляхом перебору за допомогою спеціальних програм			
Невідомо			
За способом отримання потерпілими посилання на шкідливе програмне забезпечення			
Месенджери			
Соціальні мережі			
Електронна пошта			
Sms-повідомлення			
Сайт			
Невідомо			
За способом перехоплення трафіку			
Людина посередині (man in the middle)			
Отруйний DNS (poison DNS)			
Паралельна сесія			
За допомогою шкідливого ПЗ, яке отримує авторизаційні дані з браузера (Stiller)			
Невідомо			

Таблиця 8

Мотивація злочинців

Мотивація злочинців	361 ККУ %	361-1 ККУ %	362 ККУ %
матеріальне збагачення	61	67	66
складова гібридної війни	10	11	9
співпраця з агресором	13	5	9
хуліганські дії	10	17	9
соціальний протест	2	0	5
невідомо	4	0	2

Експертним середовищем акцентовано увагу на вчиненні певної частини злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж організованими злочинними угрупованнями (далі – ОЗУ) (табл. 9). За наявними ознаками кваліфікації злочинів, передбачених ст. 361 ККУ більше 50 від-

Таблиця 9

Питома вага вчинених злочинів ОЗУ

Стаття ККУ	361 ККУ	361-1 ККУ	362 ККУ
ОЗУ, %	51,20	35,00	73,81
ОЗУ укр, %	14,70	17,50	35,70

сотків вчиняється у складі ОЗУ і майже три чверті – за ст. 362 ККУ. Водночас, експерти зазначають щодо загрози діяльності ОЗУ безпосередньо на території України: за ст. 361 ККУ – 14,7%; за ст. 361¹ ККУ – 17,5%; за ст. 362 ККУ – 35,7%.

Висновки. Дослідження кіберзлочинності висвітлює загрози, пов'язані з використанням комп'ютерних систем у злочинних цілях, особливо в умовах сучасних гібридних конфліктів. Встановлено, що найбільш поширеними злочинами є несанкціоноване втручання в роботу інформаційних систем, розповсюдження шкідливих програм та незаконне використання інформації. Значну частину правопорушень здійснюють організовані угруповання, часто використовуючи

спеціалізовані операційні системи та програмне забезпечення. Особливу загрозу становлять атаки, спрямовані на критичну інфраструктуру, державні установи та фінансові структури.

Важливим аспектом дослідження є мотивація злочинців, яка переважно зводиться до фінансової вигоди, хоча частина атак має політичний підтекст. Аналіз також свідчить про необхідність посилення міжнародного співробітництва у сфері кіберзахисту, удосконалення механізмів моніторингу та розробки ефективних методів протидії кіберзлочинності. Робота підкреслює критичну важливість адаптації законодавства до нових викликів у сфері інформаційної безпеки та розширення заходів превентивного характеру.

Анотація

Кіберзлочинність у сучасному цифровому світі стала однією з ключових загроз для державних установ, бізнесу та приватних осіб. Дослідження висвітлює основні аспекти нелегальної діяльності в комп'ютерних мережах, аналізуючи її соціальні, економічні та технологічні чинники. Основними видами злочинів є несанкціоноване втручання в роботу інформаційних систем, незаконне використання даних та розповсюдження шкідливого програмного забезпечення. Показано співвідношення поширення цієї групи злочинів за рівнем ризику на основі експертної думки та статистичними даними ЄРДР. Зазначено про певну кореляцію між обома підходами щодо незаконного втручання (ст. 361 ККУ) та розбіжність щодо несанкціонованих дій з інформацією (ст. 362 ККУ). Значна частина правопорушень має організований характер, а злочинці використовують сучасні інструменти, зокрема спеціалізовані операційні системи та методи анонімізації.

Окрему увагу приділено проблемам кіберзлочинності в Україні, особливо в контексті гібридної війни та атак на критичну інфраструктуру. Аналіз показує, що значна частина кіберзлочинів спрямована на державні структури та фінансові установи, а мотивація злочинців часто має політичний чи військовий характер. У роботі представлено статистичний аналіз злочинних методів, використаного програмного забезпечення та каналів поширення незаконної діяльності, що дозволяє виокремити ключові тенденції.

Наукова стаття наголошує на необхідності адаптації законодавства до нових викликів, посилення міжнародної співпраці та вдосконалення механізмів моніторингу. Запропоновано шляхи підвищення ефективності боротьби з кіберзлочинністю, включаючи покращення кіберзахисту, розробку превентивних заходів та оптимізацію державних стратегій.

Ключові слова: кіберзлочинність, гібридна війна, критична інфраструктура, несанкціоноване втручання, шкідливе програмне забезпечення, організовані злочинні угруповання.

Demediuk S.V. The dark side of computer networks: crimes and illegal activities online

Summary

Cybercrime has become one of the most significant threats in the modern digital world, impacting government institutions, businesses, and individuals. This study examines the key aspects of illegal activities within computer networks, analyzing their social, economic, and technological dimensions. The most common types of cybercrime include unauthorized interference in information systems, illegal use of data, and the distribution of malicious software. The correlation between the prevalence of this group of crimes by risk level based on expert opinion and statistical data from the Unified Register of Pre-trial Investigations is shown. A certain correlation between the two approaches to illegal interference (Article 361 of the Criminal Code) and a discrepancy regarding unauthorized actions with information (Article 362 of the Criminal Code) are noted. A considerable portion of these offenses is carried out by organized criminal groups that employ specialized operating systems and anonymization techniques.

Special attention is given to cybercrime issues in Ukraine, particularly in the context of hybrid warfare and attacks on critical infrastructure. The analysis reveals that a significant number of cybercrimes target governmental and financial institutions, with perpetrators often driven by political or military motives. The study presents statistical analyses of criminal methods, software tools used, and channels for illegal activities, identifying key trends in the field.

This scientific article emphasizes the need to adapt legislation to emerging threats, strengthen international cooperation, and improve monitoring mechanisms. Proposed measures to enhance cybersecurity include developing preventive strategies, optimizing government responses, and refining methods to combat cybercrime effectively.

Key words: cybercrime, hybrid warfare, critical infrastructure, unauthorized interference, malicious software, organized criminal groups.

Список використаних джерел:

1. Khakhanovskiy, V., & Hrebenkova, M. Identification, collection, and investigation of electronic imagery as sources of evidence. *Law Journal of the National Academy of Internal Affairs*, 12(4), 28–39. 2022. 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'ютерні 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-Янчилєнко 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). С. 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. URL: <https://surl.li/ejzgwk>
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). Cyber resiliency engineering framework. MTR110237. URL: <https://surl.li/fixpgux>
26. Салманов, О. В. Кіберзлочинність і протидія їй в умовах воєнного стану в Україні. Злочинність і протидія їй в умовах війни та у повоєнній перспективі: міждисциплінарна панорама : зб. тез доп. Міжнар. наук.-практ. конф. (м. Вінниця, 19 квіт. 2024 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Вінниця : ХНУВС, 2024. С. 313–318.

27. Гуцалюк м.в. Сучасні тенденції організованої кіберзлочинності. Інформація і право. № 1(28)/2019. С. 118–128.
28. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. Південноукраїнський правничий часопис. № 3. 2023. С. 44–46. DOI: <https://doi.org/10.32850/sulj.2023.3.10>

Дата надходження статті: 11.08.2025

Дата прийняття статті: 21.08.2025

Опубліковано: 29.09.2025